

# User Manual

# BASSET

This manual is intended for the users of the Watchdog Fraud client.

Watchdog  
Fraud 5

## Contents

---

Contents .....	2
Document information.....	5
<i>Document version</i> .....	5
Confidentiality notice.....	5
Chapter 1: Getting started .....	7
1.1 System Hardware .....	7
1.1.1 <i>Server setup (general)</i> .....	7
1.1.2 <i>Application Server</i> .....	8
1.1.3 <i>Alarms server</i> .....	9
1.1.4 <i>Database Server</i> .....	9
1.1.5 <i>Requirements for PC</i> .....	10
1.2 Client installation.....	10
1.3 Logging in for the first time .....	10
Chapter 2: Client Overview.....	12
2.1 Logging in .....	12
2.1.1 <i>SQL-login</i> .....	12
2.1.2 <i>Windows authentication</i> .....	12
2.2 Start screen .....	13
2.2.1 <i>Shortcuts, Pearl and Ribbon</i> .....	13
2.2.2 <i>Windows management</i> .....	15
2.2.3 <i>The data pane general functions</i> .....	15
2.3 Tabs.....	16
2.3.1 <i>Investigation</i> .....	16
2.3.2 <i>Administration</i> .....	16
2.3.3 <i>Settings</i> .....	16
2.4 Workflow .....	16
Chapter 3: Investigation Tab .....	19
3.1 Directly under the tab .....	19
3.1.1 <i>Start</i> .....	19
3.1.2 <i>Tools</i> .....	20
3.1.3 <i>Investigations</i> .....	25
3.1.4 <i>Action</i> .....	25
3.2 Workflow - Start .....	27
3.2.1 <i>Tasks</i> .....	27
3.2.2 <i>Alarms</i> .....	28
3.3 Workflow – Investigation.....	31
3.3.1 <i>Gallery</i> .....	31

3.3.2 Query tool .....	34
3.3.3 Find Similar .....	39
3.4 Workflow – Decision / Action .....	40
3.4.1 Send Notification .....	40
3.4.2 Closure .....	41
3.5 Cases.....	42
3.5.1 Cases Overview.....	43
3.5.2 Cases Properties .....	43
Chapter 4: Administration Tab.....	48
4.1 Directly under the tab .....	48
4.2 Overview (Dashboard).....	48
4.3 History (Event Log).....	48
4.3.1 Update .....	48
4.3.2 Users .....	48
4.3.3 Time Period .....	49
4.3.4 Events Log.....	49
4.5 Tools .....	49
4.5.1 Delete Alarms .....	49
4.5.2 Fraudster Profile (CHANGE THIS INFO) .....	50
Chapter 5: Settings Tab.....	53
5.1 Personal.....	53
5.2 General .....	53
5.3 Risk assessment.....	54
5.3.1 Alarm groups .....	54
5.3.2 Column settings.....	55
5.3.3 Weights.....	55
5.3.4 Subtracting columns .....	55
5.3.5 Subtracting values .....	56
5.4 Table Cleaning.....	56
5.5 User Manager .....	57
5.5.1 General tab: .....	58
5.5.2 Members tab.....	58
5.5.3 Access tab .....	58
5.5.4 Permission tab.....	59
5.5.5 Effective Permission tab .....	60
5.6 Internal Notifications .....	60
5.7 External Notifications.....	62
5.8 Matching in Fraud Profile Defaults .....	65
5.9 Investigation Resolution .....	65
5.10 Case Manager .....	66

5.11 Roaming partners .....	67
5.12 Subscriber Groups.....	72
5.13 Destination Groups .....	72
5.14 Cell Sites.....	74
5.15 Alarms.....	75
5.15.1 Alarms Pane .....	75
5.15.2 Specific alarms .....	76
5.15.3 Profiling.....	93
5.15.4 Generic Alarms .....	94
5.15.5 Subsets.....	98
5.15.6 List .....	99
5.15.7 Groups .....	100

## Document information

Document title: Watchdog Fraud 5 User Manual

Filename: Watchdog Fraud 5.1 User Manual 1.4

Version: 1.4

Revision: 14

Document created: 2010-03-10 09:35

Author: Jörgen Caceres

## Document version

- 1.0 Client manual released 2009-06-25. Authors: [Jörgen Caceres](#) and [Erick Ujiji](#).
- 1.1 Client manual reviewed. Some new pictures. 2009-06-25. Nicolaj Aarøe.
- 1.2 Client Manual reviewed. Several changes due to client change. 2010-02-03 JC: Build117
- Client manual reviewed. Changes due to re-branding. 2010-03-03.
- 1.3 Several changes in contents due to functional changes, by Jörgen Caceres on 2010-08-25 (Client build 139).
- 1.4 Several changes in contents due to functional changes, by Jörgen Caceres on 2010-09-09 (Client build 141) Rev. 14 further functional changes introduced in the manual.

## Confidentiality notice

No parts of this publication may be reproduced, transmitted, transcribed, stored in retrieval system, or translated into any language or computer language, in any forms or in any means, without the written permission of Basset AB, P.O. Box 1156, SE-172 23 Sundbyberg, SWEDEN.

This document is published without any warranty. Improvement and changes to this product description, necessitated by typographical errors, inaccuracies of current information, or improvements to the system, may be made by Basset, at any time and without notice.

All screenshots and examples are based on example data.



## Chapter 1: Getting started

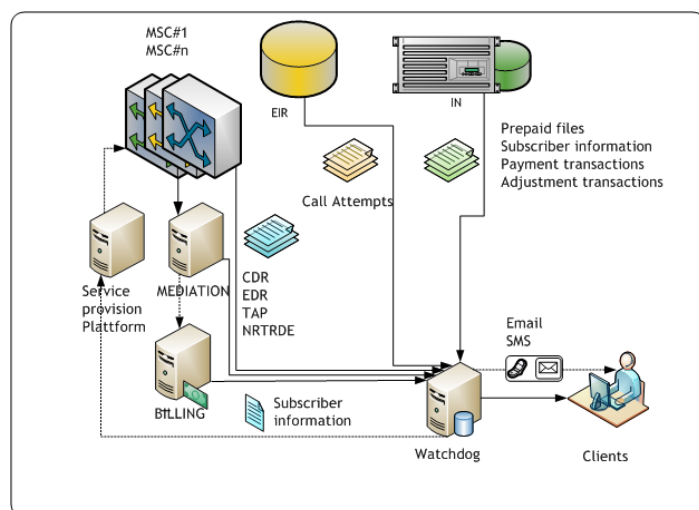
This chapter is dedicated to getting started with the Watchdog 5.0. The description requires that all back-end applications are installed correctly according to the operator's installation documents. Some parts may be different in the local installation, than described in this document, depending on configuration of the installation.

### 1.1 System Hardware

In this subsection, the file-flows and general set-up of the servers is presented. For a more detailed description of file-flows, please see the installation documents.

Please note, that the actual physical server set-up may differ from the flows presented below.

#### 1.1.1 Server setup (general)



The Watchdog system connects to several other subsystems in the operator's mobile or fixed telephone system.

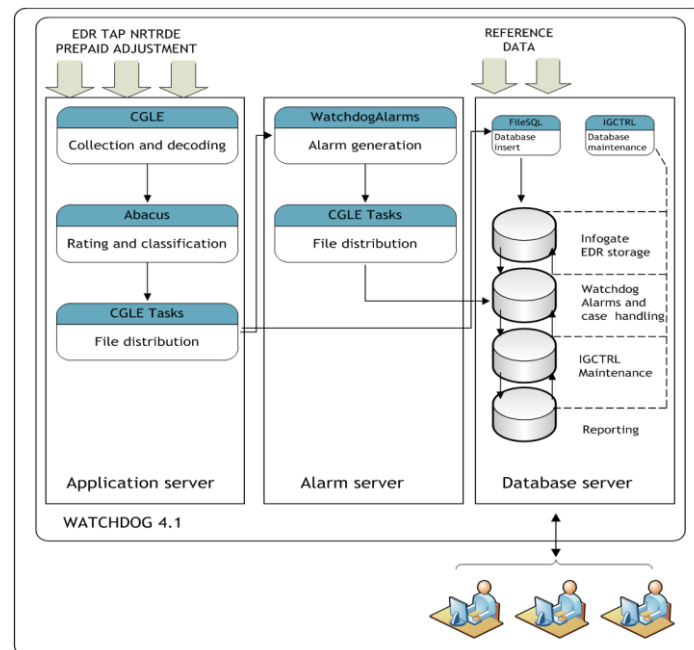
In order for the Watchdog to be able to detect anomalies, input is needed from various parts. This input is compared with

other incoming data from a different part of the network.

The picture above shows how Watchdog fits into any telephony system. Any kind of standardised file may be handled by the Watchdog system. Files may or may not be already formatted to Watchdog's internal file handling format. This depends on the type of mediation installed previously in the telephone system.

If the files are not pre-formatted to Watchdog standard, Watchdog will re-format the files according to the requirements of the billing system and the operator. The settings for the re-formatting are configured by Basset during the initial installation process. The settings may be re-configured by request of the operator. The re-configuration is handled as a change request (see Support chapter).

## 1.1.2 Application Server



The application server is the server that manages the incoming files, rates them and distributes them to the other servers.

### 1.1.2.1 CGLE

The CGLE application collects files from various sources, such as the mediation device, the switch, the roaming billing, the IN-platform etc.

The collected files are

created by different standards, and must therefore be changed to a Watchdog internal file standard. This is done by the CGLE. When files are decoded, they are picked up by the Abacus rating engine. Files collected by the CGLE are typically files that need to have a value attached to them.

### 1.1.2.2 Abacus

Abacus will rate the files according to the settings determined by the operator. Accurate rating is depending on the correct classification of file, which is done to determine what kind of file is handled at the moment. The classification is used to rate the file correctly.

If classification fails, the unhandled files are dropped in a specific repository folder for further manual management. (This needs to be checked every day).

If classification succeeds, the files are picked up and distributed to other servers.

### 1.1.2.3 CGLE Tasks

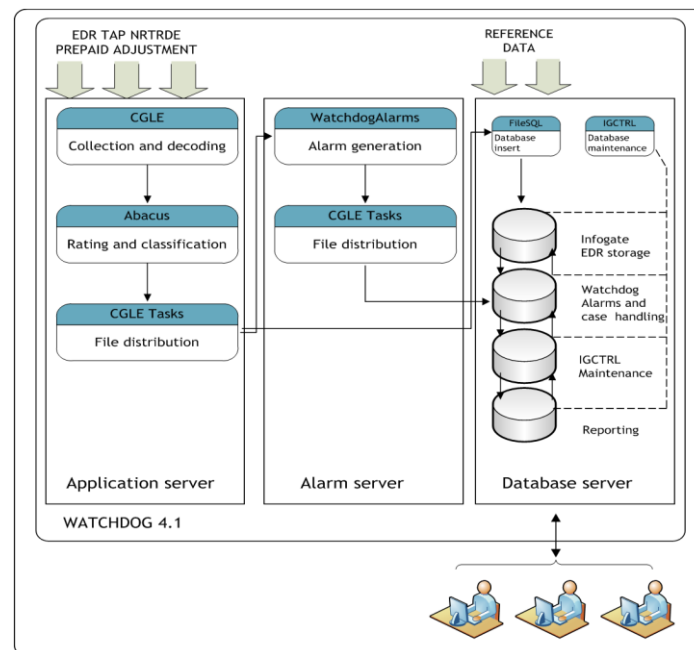
This application picks up and distributes the files to the two other types of servers:

- To the Alarms server, to generate alarms
- To the Database server to be stored.

Distribution is made with FTP.



### 1.1.3 Alarms server



The alarms server contains two main applications.

The Watchdog Alarms, which generates the alarms according to the settings configured by Basset or by the operator. The settings are also referred to as “thresholds”.

The CGLE tasks, which transfers the alarms to the data-

base server in order for the active alarm to be displayed in the Watchdog Client.

### 1.1.4 Database Server

The database server contains, other than the databases, two main applications. These applications are not used by the operators since they are performing automated jobs and database maintenance.

#### 1.1.4.1 Infogate Database

This database stores all CDRs that have been sent from the mediation/switch. After 30 days the CDRs are deleted in a regular cleaning job. If further storage is necessary, the Infogate database needs to be backed up on a daily basis.

#### 1.1.4.2 Alarms Database

The alarms database is used to show alarms in the client. All alarms are stored, regardless of status, until they are deleted. In conjunction with the alarms, a certain (limited) number of CDRs are transferred from the Infogate database to facilitate statistics and short time searches.

#### 1.1.4.3 IGCTRL Database

This database contains settings and configuration for the IGCTRL application, which is responsible for automated jobs and cleaning jobs.

#### 1.1.4.4 Reports Database

The reports database stores all reports settings and is used to create reports that are stored elsewhere in the system.

#### 1.1.5 Requirements for PC

In order to run the Watchdog client the user needs a regular PC (desk- or laptop) with at least Microsoft Windows XP service pack 2; there should be at least 1024 Mbit ram. To run reports, Microsoft Internet Explorer browser is needed. The client is adapted to a minimum screen resolution of 1280x1024.

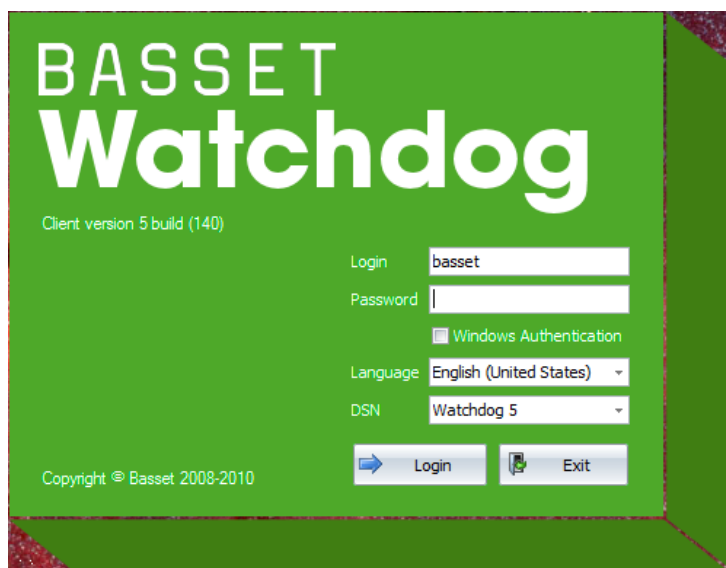
### 1.2 Client installation

The regular way to install the client on your PC is to use the wizard provided by Basset. If the user is more advanced as a PC user, the user may install Watchdog client manually.

Before installing the client, make sure the administrator of the system has given the user a user name, a password, and the corresponding permissions in the system.

### 1.3 Logging in for the first time

After completing the installation of the client, the user may log in for the first time.



More details about logging in are shown in [Chapter 2.1 Logging in](#).

If no DSN (Data-base System Name) is shown, either directly or through the drop-

down menu, the user may insert the name manually by activating the field and type the correct DSN name, according to the choice you made earlier, either in the wizard or in the ODBC connection.

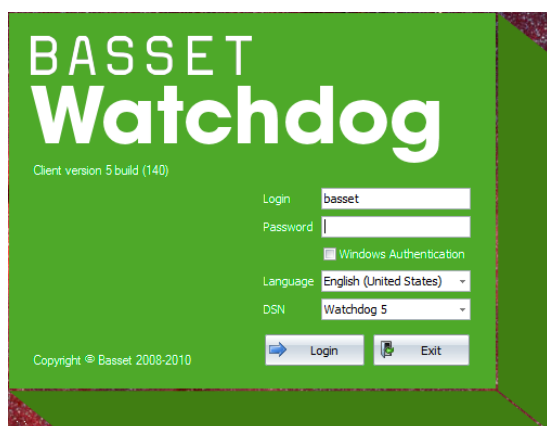


## Chapter 2: Client Overview

---

This chapter will give you the overview of the client. The details of the functions will follow in the subsequent chapters.

### 2.1 Logging in



The log-in may be done in two ways: either by a normal SQL-login through the log-in interface, or by using Windows authentication.

#### 2.1.1 SQL-login

The user types the assigned user name and the assigned password in the respective fields.

There is a choice of languages between (currently) English and Spanish.

Clicking “login” button will open the client; “exit”-button will cancel the login and close the splash-screen.

#### 2.1.2 Windows authentication

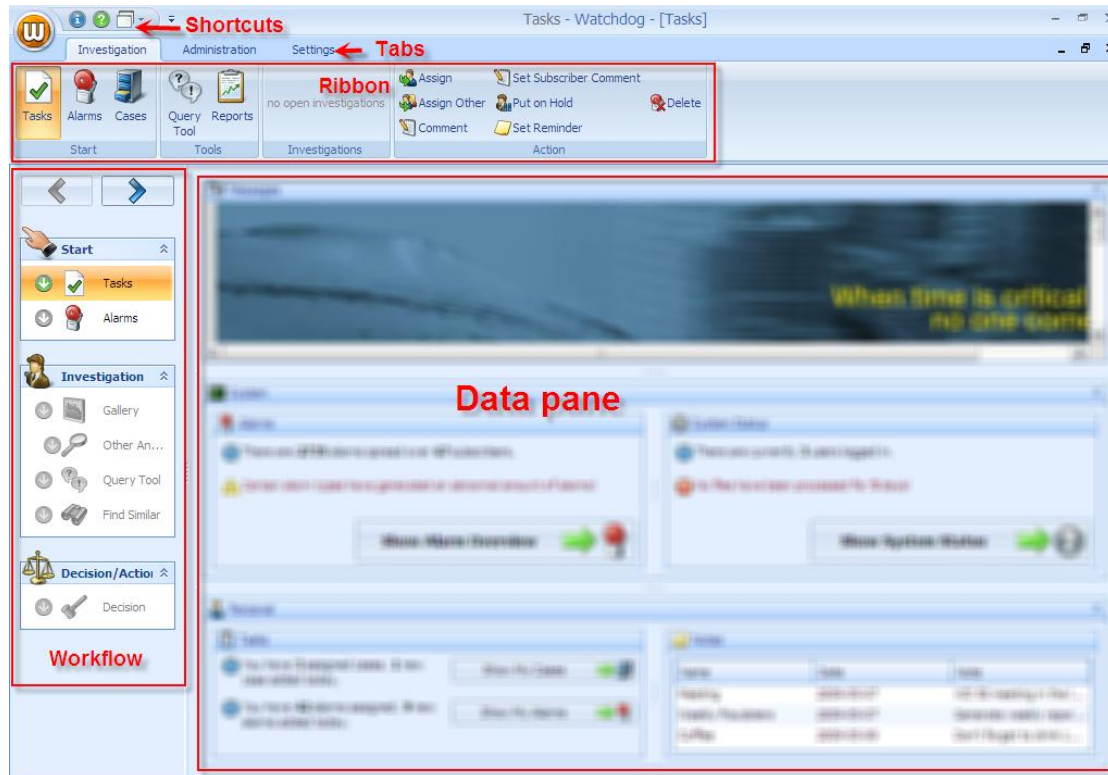
The first time this option is used: the user will start the application by clicking on the icon, and checking the windows authentication box. “Login” and “Password” fields will become grey, meaning they are not applicable for login. This is because the Watchdog Client will use the same log-in credentials as the system that the client is installed on, i.e. the user’s regular user name and password. Click the button “→ Login” to proceed.

In all subsequent logins, the user will not receive the splash-screen, but is immediately logged in to the client, when the icon is clicked.

**N.B. that the option of windows authentication has to be activated by the administrator when setting up the user.**

## 2.2 Start screen

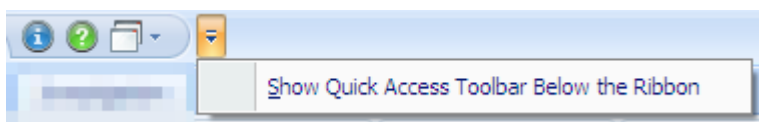
When Watchdog starts, the start screen will show. This screen contains personalised modules configured by the user. Watchdog's client is designed according to the standard lay-out of mainstream Microsoft applications.



The Watchdog application is managed with the parts shown. Settings, commands, workflows etc. are decided by the using the shortcuts, ribbon or workflow; the result or the feedback is shown in the data pane. In certain cases, the workflow and/or data pane are covered by a new window, depending on the settings.

### 2.2.1 Shortcuts, Pearl and Ribbon

The shortcuts are also called “**Quick Access Toolbar**”. It may be moved from the

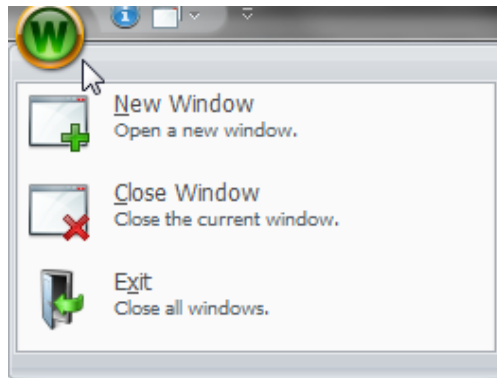


default position to below the ribbon by clicking on the menu

button on the right side of the shortcuts. Items (icons) may be moved from the ribbon to the shortcuts, to be personally configured by the user (see about the Ribbon, [further down](#)). The added items may be removed from the shortcuts.

In the default state, the shortcuts are (i), for information on the current Watchdog client; (?) to show the manual; and (☰) to show the window management menu.

The “pearl” is the green-on-green “W” (for Watchdog). When the user hovers on the pearl, the border changes colour from white to yellow, to reflect the selection.

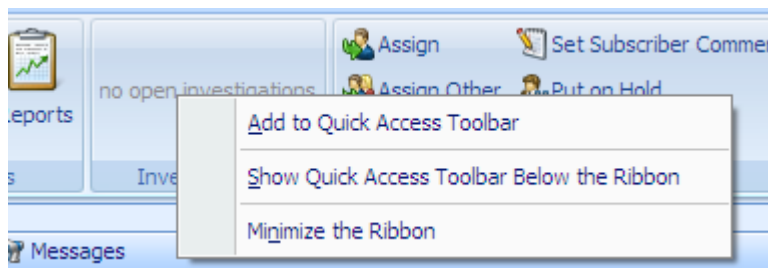


The commands available under the pearl are:

- **New Window:** this command will open an entirely new instance of the Watchdog client. Since the user is already logged in, it will open directly without any new log-in requirement.
- **Close Window:** closes the window that the user is currently using. All other instances remain open.
- **Exit:** This command will close

all instances of Watchdog. To return to Watchdog, a new log-in has to be performed.

The ribbon is the common name of the icons on top of the client. The ribbon varies in size and content, depending on the tab chosen. More information about the content is found under the respective tab description, chapters 3, 4 and 5.

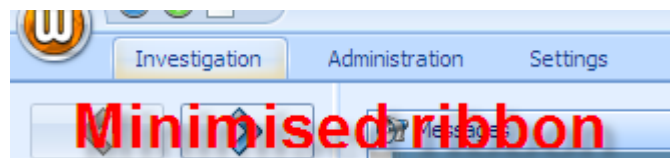


The Ribbon may be customised by right-clicking on any of the icons.

The menu will affect the respective icon on which the cursor was hovering.

The commands in the menu are:

- **Add to Quick Access Toolbar:** adds this item to the shortcuts above (or below) the ribbon.
- **Show Quick Access Toolbar Below the Ribbon:** moves the shortcuts to a position below the ribbon, but above the workflow/data pane modules.
- **Minimise the Ribbon:** The ribbon is minimised and will disappear as long as it is not needed. The tabs re-



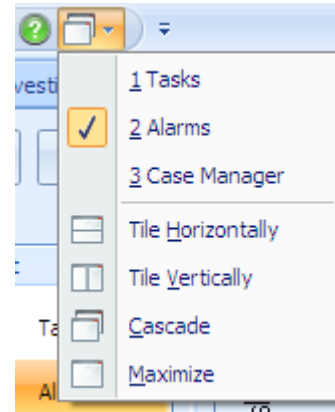
main on the top of the workflow/ window. Clicking on a tab will re-activate the ribbon on top of the current window.

In order to reset the minimised ribbon, right-click on any of the tabs and uncheck the checked “Minimize the Ribbon”-command which is high-lighted as active.

## 2.2.2 Windows management

All selections will be implemented by opening a new window on top of, but inside, the client. The user may handle multiple windows in different ways.

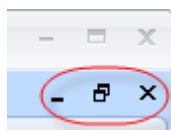
In the “Shortcuts” section (a.k.a. the Quick Access Toolbar), the (☰) button will give the following context-dependable menu.



At the top the user may see the currently opened windows. The active window is high-lighted by a (✓). In the picture on the right, the active window is the “Alarms” window.

Under the divider, there are four different options on how to manage the open windows:

- **Tile Horizontally:** the windows are stacked from top to bottom.
- **Tile Vertically:** the windows are stacked from left to right.
- **Cascade:** this is where the windows are stacked over one another.
- **Maximize:** this is the default setting, where the user only may see and work with one window at a time. The other windows are hidden beneath the currently opened window. It is then possible to choose which window to view by selecting it in the top part; if the user wishes to close an active window it is done by closing the internal window in the client. (See picture on the left).



## 2.2.3 The data pane general functions



The modules in the data pane show the various contents in the different tabs and functions. Many times

the modules contain a large amount of information, expanding beyond the frame of the module. In such cases a scrolling bar is shown left and bottom in the frame.

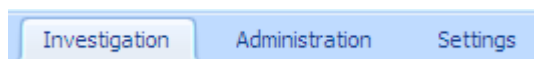
However it is also possible to collapse and expand each module, in order to increase visibility in the modules of interest.

Besides from the obvious visibility of an expanded module, it is also possible to determine which modules are expanded and collapsed by looking at the chevrons on the right side of the modules. Downwards pointed chevrons (▼) indicate a collapsed module, with a possibility to expand by clicking a single click on the chevrons. Upward pointed chevrons (▲) indicate an expanded module, with the possibility to collapse by a single click on the chevrons.

Expansion and collapse of the modules is also achieved by double-clicking on the module's top bar itself.

When a module is collapsed, the expanded modules will occupy the rest of the available space, making it possible to see more information if it is available.

## 2.3 Tabs



The access to the various parts of Watchdog is controlled by the tabs on the top. The three main tabs Investigation, Administration and Settings contain the work areas with their respective action icons.

### 2.3.1 Investigation

The investigation tab is used for the handling of alarms and cases. From this tab it is also possible to generate reports and to make queries towards the data bases. Detailed information is found in [Chapter 3](#).

### 2.3.2 Administration

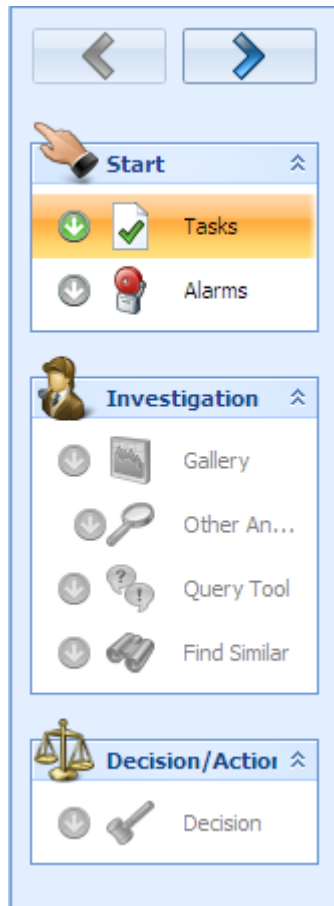
Administration means the handling of the Watchdog system, to maintain and to monitor the system so that it performs according to standards. [Chapter 4 describes](#) this tab in detail.

### 2.3.3 Settings

All the settings are configured in the Settings tab. This is described [closer in Chapter 5](#).

## 2.4 Workflow





quate icon in the ribbon.

In order to facilitate the work of finding fraud and to better detect and classify anomalies in the operators' networks, the design of the Watchdog client is tailored according to a specific workflow, which has been developed from "best practice" around the world.

The client automatically jumps to the next step when a step is fulfilled and the right-arrow button at the top is clicked. The correct correlating data is shown in the data pane in each step, with some exceptions that are described in [chapter 3.1](#). It is always possible to go back in the process, by clicking on the left-arrow button. From start, the left-arrow is not active, since there is no previous step.

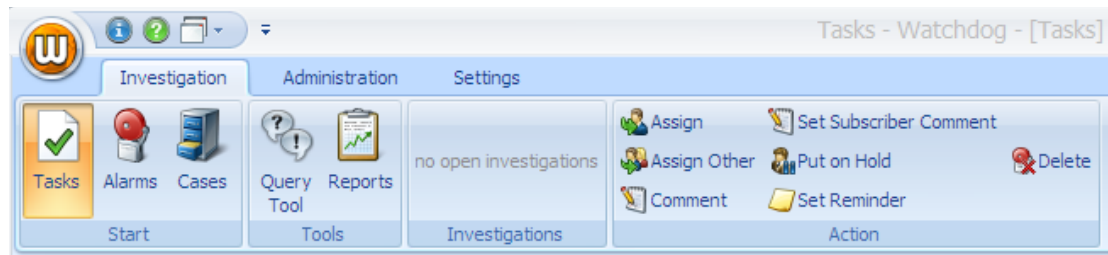
If the workflow is not wanted or needed, there is a possibility to skip steps in the workflow, or not to use the predefined workflow at all, by clicking on the ade-



## Chapter 3: Investigation Tab

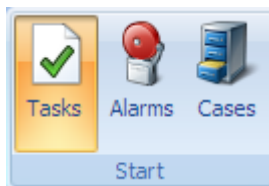
This is where the system automatically starts. In the data pane, the welcome screen is shown as described in [Chapter 2.2](#).

### 3.1 Directly under the tab



The four main areas in the Investigation tab are: Start, Tools, Investigations and Actions. The icons in the different areas give the possibility to proceed independently of the workflow.

#### 3.1.1 Start

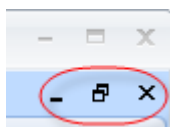


The Start area contains the three icons Tasks, Alarms and Cases. The client starts with the Tasks icon automatically, in order for the user to follow the predefined workflow.

When an icon is selected it is high-lighted.

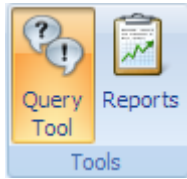
Clicking the Alarms icon will present the current alarms in the alarms database, see [Chapter 3.2.2](#).

Clicking the Cases icon will open the case manager, see [Chapter 3.5](#).



If the user wishes to return to the Tasks screen, it is done by closing the internal window in the client. (See picture on the left).

### 3.1.2 Tools



The Tools area gives the possibility of creating database queries and generating reports.

#### 3.1.2.1 Query tool – overview

The following chapters about the Query tool deal with the “ad-hoc” query tool available in the Tools area of the Investigation ribbon, i.e. not connected to any particular case. The investigation query tool in the workflow is exactly the same, described in [Chapter 3.3.2](#), with the difference that it is connected to the case the user is working with at the moment.

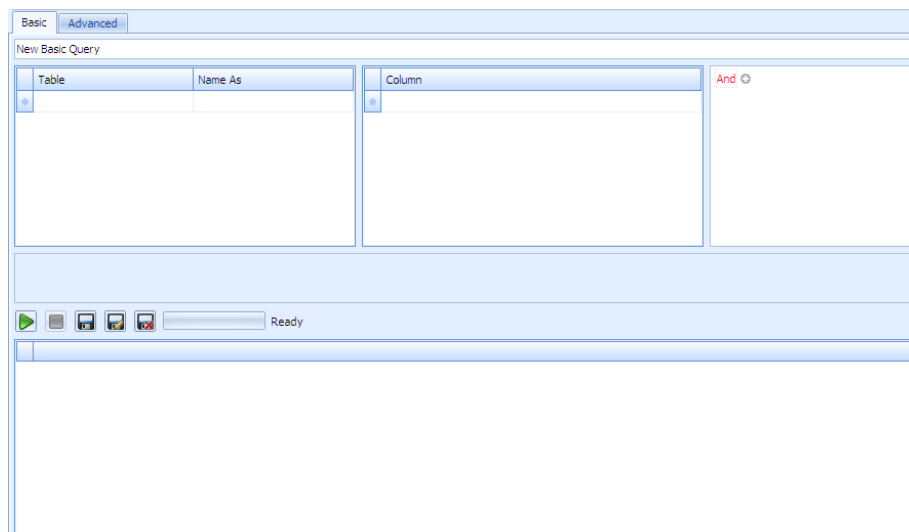
Although the Watchdog interface gives the user full ability to perform all tasks via the graphical interface, there are situations when it is necessary to search for data in other ways.

This possibility is given with the Query tool. It is NOT possible to change, erase or otherwise affect the data bases through the Query tool.

Since the databases are based in SQL, the language is used in the Query tool to search for data.

Queries are considered as either basic, or advanced. The basic query means that the user is selecting variables from pre-defined values with the help of the GUI – the query is formulated as the user makes the choices. The advanced query is for the user that is experienced and knowledgeable in the SQL and has the skills to formulate free-text questions.

There is an option to store queries in order to repeat them at a later stage.



The default screen when opening the query tool starts with the basic option. The tool is prepared to receive input for a new basic query.

There are four main areas in the query tool screen:

- **The table module:** This module is used to select which table should be searched and gives the possibility to name the variable independently.
- **The column module:** here the selection is done of which column should be used in the table that is high-lighted on the left.
- **The rules/relationship module:** this module applies the rules and sets the relationships between the variables previously chosen in the table and column module
- **The RUN and record module:** this part will execute a query and save it in the client to be used repeatedly.

The screenshot shows the query tool interface with three main sections: 'Table', 'Column', and 'And'. The 'Table' section has a header with 'Table' and 'Name As' and a list of tables below. The 'Column' section has a header with 'Column' and a list of columns below. The 'And' section has a header with 'And' and a list of rules/relationships below. At the bottom, there is a 'Ready' button and a status bar.

### 3.1.2.2 Query tool – new basic query

**Step 1:** In order to execute a basic query, the user needs to select where the data is to be retrieved.

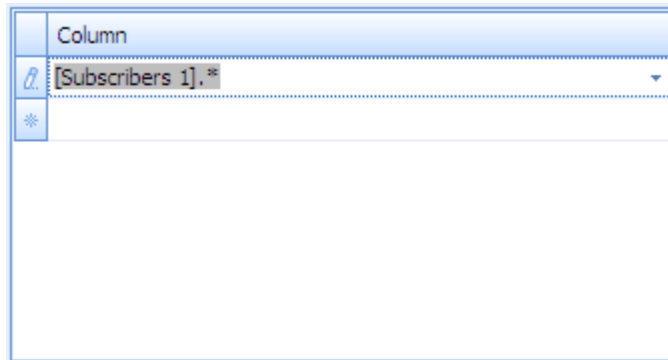
The screenshot shows the 'Table' module with a dropdown menu open, displaying a list of tables: 'CallsHistory', 'Subscribers', and 'InfoGate'. The 'Table' header is visible above the dropdown.

Clicking on the header cell will activate the input cells below. Click on the drop-down arrow and the system will give you which options there

are to choose.

“Name as” cells are text input cells where the user may choose a logical name for the selected table. If no name is entered, the system will set a name (e.g. “subscribers 1”). This name is used in later steps.

**Step 2:** In the columns module, the user selects from which set of data the query will retrieve the result.



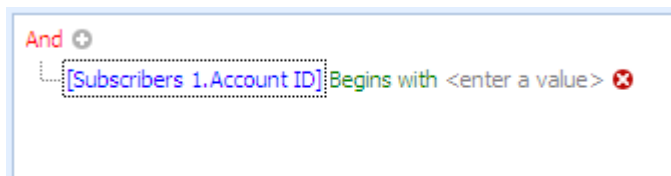
Note that the name within the brackets [Subscribers 1] is the logical name you have chosen in the previous step.

The drop-down menu gives all the available

options of values in the table. A star (\*) means that the query will retrieve the result from all data in the table. Another selection will limit the amount of data available for the query.

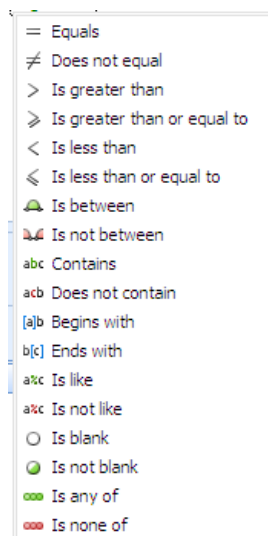
When the selection is made, the area below the two modules (table and column) is activated, and the query is shown in SQL text.

```
SELECT [Subscribers 1].*
FROM [Subscribers] AS [Subscribers 1]
```



**Step 3:** Determination and management of which data should be presented in the result.

There are a lot of options depending on which input has been done in the previous two steps.

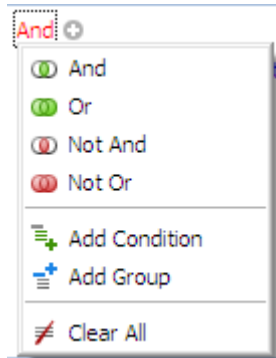


To access the values, click on the (+) icon next to the word "And". The available expressions will expand, and show their parts in different colours. Clicking on each variable will open the options for that variable.

E.g.: [Subscribers 1.Account ID] Begins with <enter a value> has three parts, each with its' own options.

- [Table.column] will give all the available columns in the table.

- The operator (“Begins with” by default) has the options shown on the picture on the left.
- Clicking on <enter a value> will show a field to insert the parameter to look for.
- The white X on red circle (✖) will delete the whole expression.



If the user wishes to add more conditions, or change expressions, it is done by clicking on the “And”.

It is also possible to clear all expressions at the bottom of the menu.

**Step 4:** the text area now contains the full expression:

```
SELECT [Subscribers 1].*
FROM [Subscribers] AS [Subscribers 1]
WHERE [Subscribers 1].[AccountID] = '146873'
```

To run the query, use the buttons below the text area:



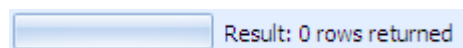
The green arrow runs the query.

The grey square turns red during the execution, will abort the query.

Diskette saves changed existing query.

Diskette with a pencil saves a new query.

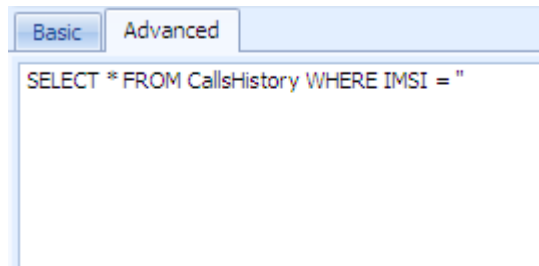
Diskette with a red X will delete the query from the storage.



Next to the buttons, there is a progress bar to show that the query is running. After execution, the result is displayed below the buttons and a summary of the result will show to the left of the progress bar.

### 3.1.2.3 Query tool – new advanced query

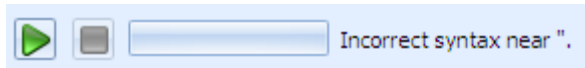
If the user is experienced in using SQL, it is possible to use “free-text” queries in the advanced tab.



When clicking the “Advanced” tab, a supporting text will show directly under the tab, to indicate where the insertion of the SQL query should be done.

The existing text may be erased or replaced.

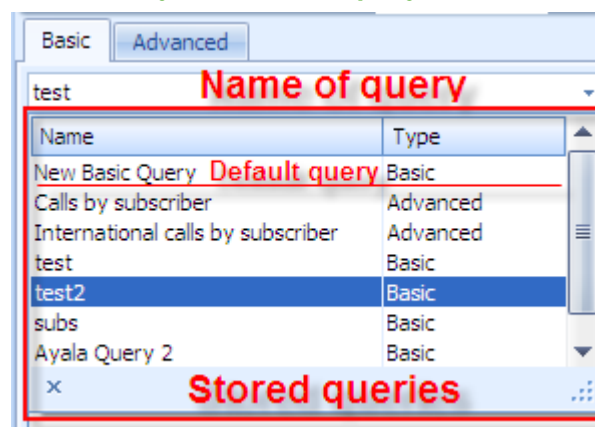
Directly below the query area, a button toolbar appears. This toolbar has a run



button, a stop/abort button and a progress bar.

When the query has run, the results are shown directly below the button toolbar. If anything is wrong with the query, the fault messages are shown on the right of the progress toolbar, see picture above.

### 3.1.2.4 Query tool – stored query



### 3.1.2.5 Reports tool



The Reports tool is connected to the SQL server’s reporting services (included in the server software). The reports are administered in the reporting services tool, not included in the client.

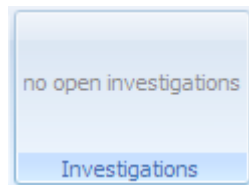
The user may order (and subscribe to) reports and set parameters to delimit the chosen data.

How to order a report:

How to subscribe to a report:



### 3.1.3 Investigations



The investigations area reflects which subscriber the user is currently working with.

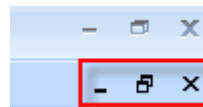
If no subscriber has been chosen, the area will show “no open investigations”.

The subscriber may be chose only when the workflow is in the “Alarms” step – where the alarms are shown.

If more than one subscriber is chosen, they will show side to side in the investigations area. The user may work with one subscriber at a time. That subscriber is always high-lighted to indicate which of the current subscribers the user is handling at the moment.



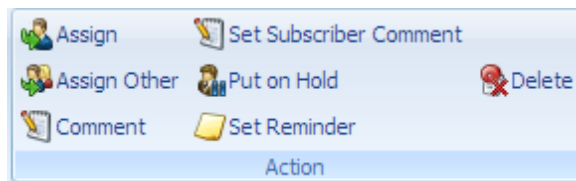
To remove any of the subscribers in click to high-light the subscriber, then *dow* by clicking on the (X) – see



the Investigations area, close the *internal win-* picture on the right. This

will close the current subscriber and it will disappear from the investigations area.

### 3.1.4 Action



The Action area is relevant to the handling of the alarms; however it is independent of the workflow. In a way, these are shortcuts to actions available in

the alarms window.

#### 3.1.4.1 Assign & Assign other

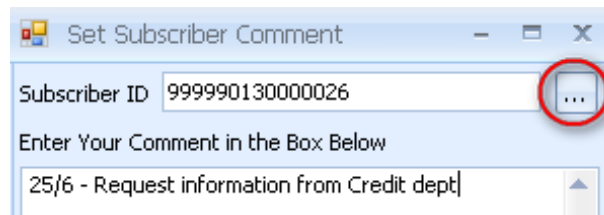
This function is used to assign an alarm to a system user in order to make the handling of alarms more efficient.

The user may assign an alarm to himself; this will be reflected in the alarm’s status, where the “assigned to”-column field will be filled with the user’s name.

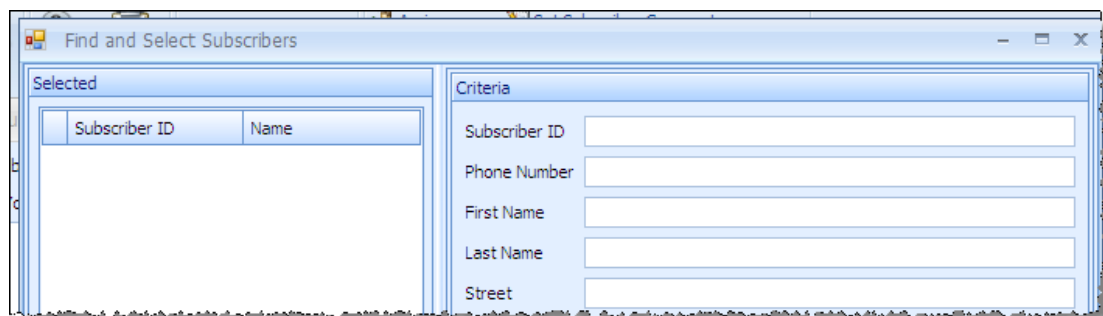
A user may, **depending on permissions**, assign and alarm to someone else. This may e.g. be used by a manager to delegate tasks to the co-workers.

#### 3.1.4.2 Comment

Clicking on the Comment button will introduce a comment to the current subscriber alarm, if any subscriber is chosen.



If no subscriber is chosen, and empty dialogue box will open, with the possibility to search for a subscriber.



#### 3.1.4.3 Set subscriber comment

This function is similar as the one described above. The only difference is that the comment is on the subscriber itself, rather than the alarm.

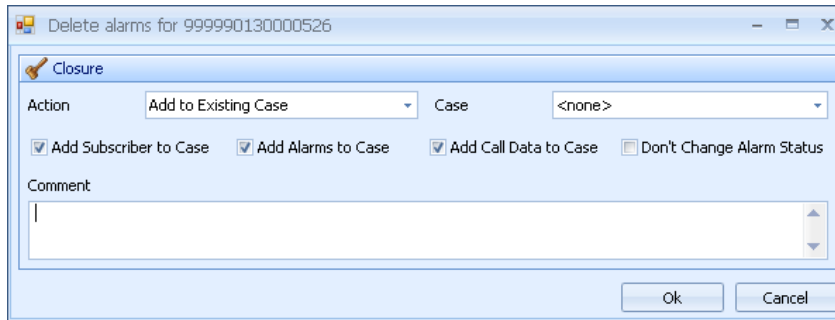
#### 3.1.4.2 Put on hold

The Hold command changes an alarm's status from Open/Assigned to Hold. This enables a temporary removal of the alarm from the Alarms list by using a filter. If a new alarm is generated for the same customer, the alarm status will however change back to Open/Assigned.

#### 3.1.4.3 Set reminder

The Reminder command changes an alarm's status from Open/Assigned to Reminder. This enables a temporary removal of the alarm from the Alarms list by using a filter. After a set number of days, the alarm status will however change to Open/Assigned again and it will reappear in the list.

### 3.1.4.4 Delete

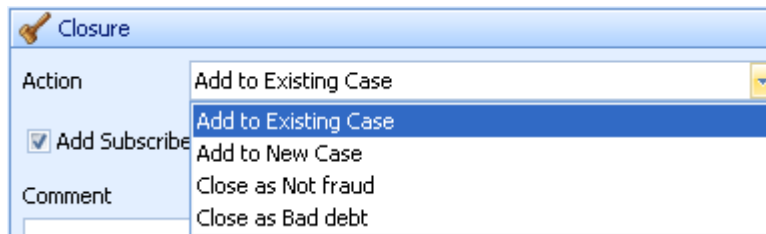


This command deletes the selected subscribers. The selection

may be one or several subscribers.

Clicking on the delete button will initiate the delete dialogue. The user is prompted to handle the deletion of the alarm. The user may also add a comment which will be stored for future reference.

The Action options are handling the delete reasons and other issues. Two options



are default options, always available:

- **Add to existing case:** the alarm is

deleted from the list, and added to any of the existing cases.

This means that a drop-down menu is available on the right of the handling options, containing the existing cases.

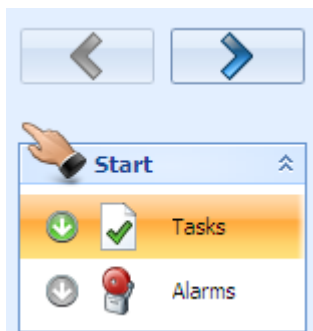
- **Add to new case:** the alarm is deleted from the list, and added to a new case which has not been yet created. A field will become visible where the name of the new case is to be entered.

The other options in the picture above are set by the user in the [Settings tab, Investigation resolution, Chapter 5.8](#).

## 3.2 Workflow - Start

The Workflow is developed to give the user the sense of direction during the investigation of possible fraud. Following the workflow, the user will cover each step necessary to determine whether an anomaly should be considered as fraud or not fraud.

### 3.2.1 Tasks

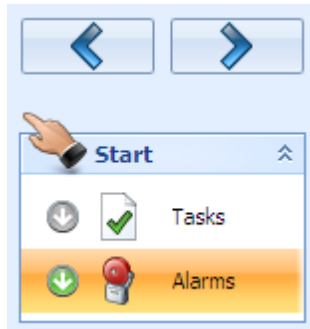


The starting point for the investigations is "Tasks". Here, the user gets an overview of the system. This part is fully configurable according to the users' set-

tings – the user gets a familiar view on his client each log-in.

### 3.2.2 Alarms

The client will jump to this position, after “Tasks”, if the user clicks on the right arrow



button at the top or if the user clicks on any other alarms view button.

#### 3.2.2.1 The data pane for Alarms

There are three main parts of the Alarms data pane: Chart, List and Subscriber. Furthermore, there is a toolbar at the top of the data pane, containing commands for filtering the information available, which is one way of customising the alarms view.

The main parts are flexible in appearance, meaning the user may adjust the size of each part of the data pane. These settings are kept for the duration of the session, but will revert to a default state when the user logs out.

#### 3.2.2.2 Alarm list toolbar



The main purpose of the alarm list toolbar is to manage the data shown in the alarms list.

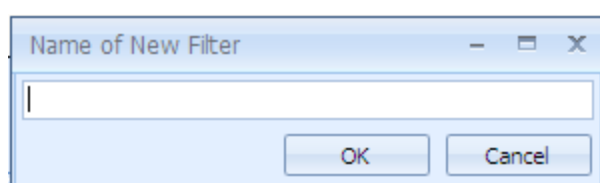
The three first icons  will show the list in three ways:

- By alarms: each alarm is shown individually for the IMSI number.
- By subscriber. If a subscriber has several alarms, they will be grouped under the same IMSI number. This is the default setting, and the list will always start with this setting.
- Show or hide hidden alarms.

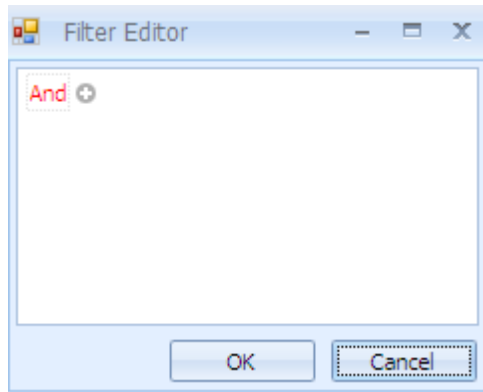
The Filter command will filter all the alarms according to the setting of the filter.

The user chooses the appropriate filter in the dropdown menu. The filtering is done automatically and directly.

The user may **create** a new filter; **edit** an existing filter, **delete**, **share**, **save** a filter.



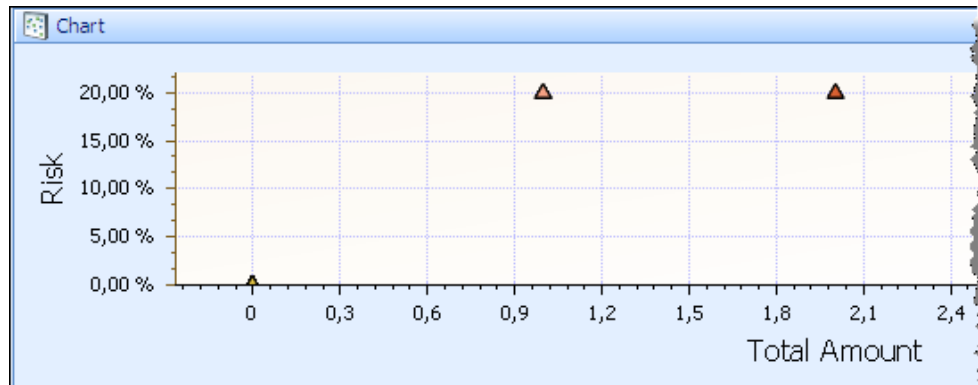
- Create a new filter: Clicking on the icon will produce a dialogue box; name the new filter accordingly.



- **Edit the newly created filter:** automatically, a new dialogue will open; start the editing by clicking on the “And” or the +. The logic for entering filtering settings is the same as for queries in the query tool, [see subsection 3.1.2.2 Step three](#).

- **Delete a filter:** clicking on the icon will delete the current filter.

### 3.2.2.3 Chart

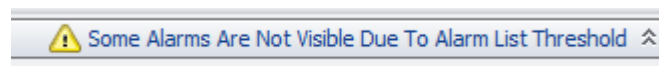


The Chart section shows the Alarms from the Risk and Amount point of view.

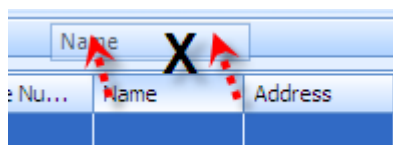
The Amount is always in the currency used by the system in the Alarms list. The Risk is according to the Risk Weight Ratio settings.

### 3.2.2.4 List

The alarms list will be populated when the Alarms step is initiated. The list is updated automatically and intermittently. It is not possible to manually update the list.



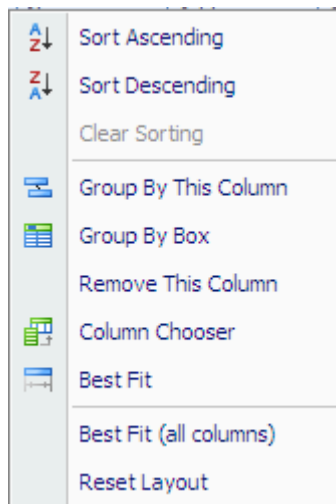
At the top of the list, the above warning message may appear. This means that the amount of alarms of a certain type has exceeded a set threshold in “Settings – General”. This threshold applies to alarms of the same type.



The alarms list shows data extracted from the CDR, and contains many of its' columns. Some columns may be regarded as redundant or un-

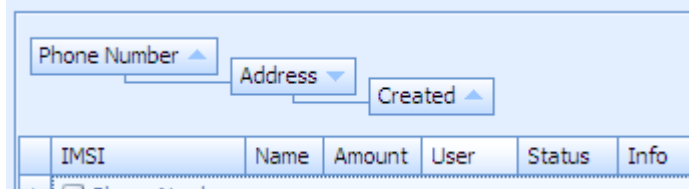
necessary by the user, and therefore it is possible to customise the view of alarms by grouping or removing the columns.

One simple way of doing this is to drag-and-drop the column header into the list header. A black “X” will show, indicating the removal of the column.



If the user right-clicks on any column header, the list menu will show.

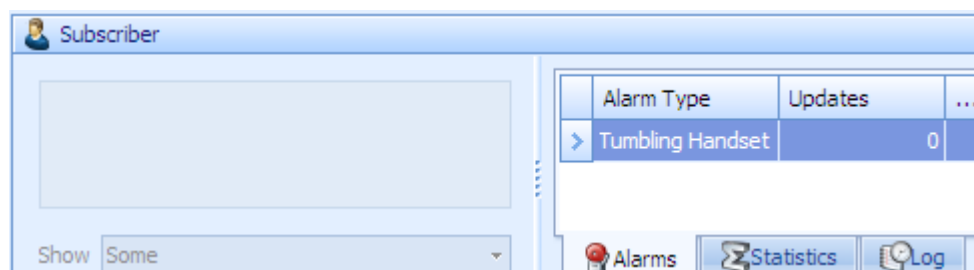
- The “Sort” command applies only to the current column, i.e. the column where the right-click was executed.
- A user may group the alarms list with any of the included columns.
- If a complex grouping is necessary, the user may create a grouping box, where the values may be entered by drag-and-drop of the column headers. The grouping headers may be sorted ascending or descending depending on the arrow on the right side.



- Remove this column will exclude the column from showing in the list.
- Column chooser opens a box, where column headers may be dropped for later management.
- “Best fit” will adjust the columns’ width according to its header or content.
- The user may adjust all columns at the same time.
- The user may reset the layout of the alarms list. It will then revert to the default state.

### 3.2.2.5 Subscriber

The subscriber section reflects the selection made in the list above. When an alarm is selected, the subscriber and alarm details show in the subscriber section. The subscriber section is also visible in the next step (Gallery).



On the left, information about the subscriber will show, according to the subscriber list in the subscriber database (external). The drop-down menu contains the option

“Show empty fields”. Checking this option will show all fields that have no value, as well as the normally populated fields.

The right side contains the alarms connected to the selected subscriber. It is possible to filter the list by clicking on the header in each column.

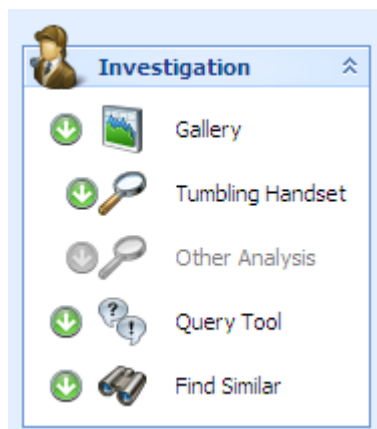
There are three main tabs in the subscriber section:

- Alarms: Shows the total number and types of alarms with this subscriber.
- Statistics: Shows statistics connected to the selected alarm.
- Log: This tab gives details on how this subscriber alarm has been handled.

### 3.2.2.6 The user's actions

To continue from this step (Alarms) the user may double-click on an alarm, or click on the right-arrow at the top of the workflow area.

The system will proceed with the high-lighted alarm. If several alarms are marked, the system will choose the top most alarm.



## 3.3 Workflow – Investigation

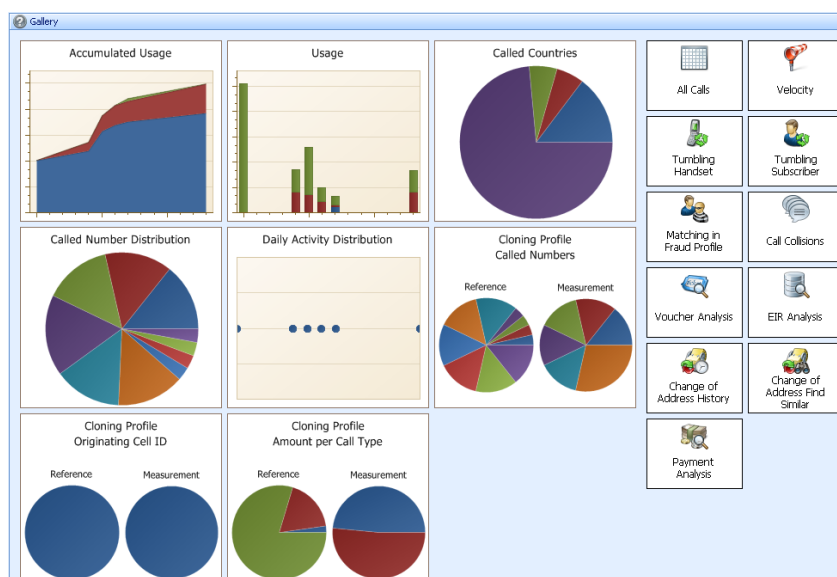
The investigation area directs the user into the analysis phase. The user has to determine whether the alarm raised is fraud or not fraud.

On entry, the two icons Gallery and Find Similar are high-lighted, to indicate that they are both always available.

Gallery contains one or two underlying steps, depending on the type of alarm.

Tumbling alarm will activate the “Tumbling handset” analysis automatically. If the alarm is of any other kind, then the only step available is “Other Analysis”.

### 3.3.1 Gallery



The Gallery is where all actions on an alarm are shown.

The main part has eight various types

of analysis readily available. Miniature graphs give a quick view of the subscriber's activity up to this day.

All graphs are clickable, in order for the user to look into the case in more detail. A new data pane will open on top of the gallery and the workflow will continue to the next step – “Other Analysis”.

The quick-glance graphs are relevant to all types of alarms. This gives the user the possibility to detect other things than what the system suggests.

On the right side, there are several more actions that may or may not be relevant, but are not feasible to show in a quick-glance graph.

Returning to the “Gallery” is done by clicking on the “Gallery” icon, or by clicking on the left-arrow button (back) on top of the workflow area.

### **3.3.1.1 Accumulated Usage**

The usage of the subscriber is shown as an area graph, including all call types.

### **3.3.1.2 Usage**

This graph shows the usage differentiated by call type.

### **3.3.1.4 Called Countries**

Here, a list of called countries in clear text shows where the subscriber has been calling. This list may be used to follow a typical behaviour of the subscriber.

### **3.3.1.5 Called Number Distribution**

The list shows the called numbers in clear text. This list helps to determine the subscribers' normal behaviour.

### **3.3.1.6 Daily Activity Distribution**

This graph shows the distribution of activities during the day, i.e. when the subscriber usually makes calls, etc. It determines the normal behaviour of the user and shows possible anomalies.

### **3.3.1.7 Cloning Profile – called numbers**

The pie-chart graph shows how the called numbers are typically distributed in a reference period compared to a measurement period. If the comparison shows anomalies, it may indicate possible fraud by cloning.

### **3.3.1.8 Cloning Profile – originating cell ID**

The pie-chart graph shows how the originating cell ID: s are typically distributed in a reference period compared to a measurement period. If the comparison shows anomalies, it may indicate possible fraud by cloning.



### **3.3.1.9 Cloning Profile – amount per call type**

The pie-chart graph shows how the amounts per call type are typically distributed in a reference period compared to a measurement period. If the comparison shows anomalies, it may indicate possible fraud by cloning.

### **3.3.1.10 All Calls**

The function of toggling all calls for a subscriber is used to establish a pattern for the subscriber. This function is connected to the workflow, meaning that it concerns only the subscriber currently being investigated.

To get a generic “all calls” report, use the ad-hoc query tool.

### **3.3.1.11 Velocity**

This analysis is used when calls are made consecutively from two different cells, if the cells are separated by a distance and time too far for a regular subscriber to cover; it determines whether the SIM-card has been cloned. It will display the IMSI numbers, where the numbers were at the time of the call (by identifying cell ID), and does a calculation of the velocity between the calls made.

In the case of international velocity, the analysis displays the countries involved.

### **3.3.1.12 Tumbling Handset**

The tumbling handset analysis shows how many handsets the SIM card has been switched between. The analysis also checks the durations and amounts for the calls made, as well as which numbers has been called, where the calls originated and terminated.

### **3.3.1.13 Tumbling Subscriber**

This analysis checks how many SIM-cards have been used in the same handset. It also shows the calls made by the subscriber with the various SIM-cards.

### **3.3.1.15 Call Collision**

This analysis helps determine how and when call collisions have occurred. A call collision is when two calls overlap each other in time. I.e. the second call starts before the first call ends.

Call collisions may be a sign of cloning.

### **3.3.1.16 Voucher Analysis**

To take a closer look at how the vouchers are managed, double-click voucher analysis. The data pane will show the used vouchers, their numbers, and how many times a voucher has been loaded.

### 3.3.1.17 EIR Analysis

The Equipment Identity Register is the database that lists all handsets in the country. It is possible to see where and how the handset was used, as well as who else than the current subscriber has been using the same handset. The unique identifier is the IMEI-number.

	Weak	0	1	2	3	4	5	Strong
First Name				<input checked="" type="checkbox"/>				
Last Name								
Street							<input checked="" type="checkbox"/>	
Street Nr								<input checked="" type="checkbox"/>
Floor								<input checked="" type="checkbox"/>
ZIP								<input checked="" type="checkbox"/>
City								<input checked="" type="checkbox"/>
Company								<input checked="" type="checkbox"/>
Phone Number								<input checked="" type="checkbox"/>
IMSI								<input checked="" type="checkbox"/>
Subscriber ID								<input checked="" type="checkbox"/>
Account ID								<input checked="" type="checkbox"/>
Sub Account ID								<input checked="" type="checkbox"/>
Services								<input checked="" type="checkbox"/>
Subscriber Type								<input checked="" type="checkbox"/>
Tariff Plan								<input checked="" type="checkbox"/>

Un-Checked = Don't use for matching

OK Cancel

### 3.3.1.18 Change of Address History

To follow the activities of the current subscriber, it is possible to check the account and subscriber history as two logs under this button.

### 3.3.1.19 Change of Address Find Similar

It is possible to compare the current subscriber with other subscribers who have the same address. This is useful if the potential fraudster for example changes the name, but keeps the address. The matching is done by the “fuzzy matching” settings dialogue, where it is possible to determine which variables to match and the accuracy of matched values.

### 3.3.1.20 Payment Analysis

In order to determine whether a subscriber is a good customer or not, it may be useful to check

the subscriber’s account and investigate the payment history of the customer.

With this information the operator may want to change settings for this subscriber to eliminate false alarms.

## 3.3.2 Query tool

### 3.3.2.1 Query tool – overview

The following chapters about the Query tool deal with the investigation query tool available in the investigation area in the workflow.

The “ad-hoc” query tool in the tools section is exactly the same in functions, described in [Chapter 3.1.2](#). The difference between the query tools available is that while the “ad-hoc” query tool is a generic tool used at any time for any subscriber, the investigation query tool is used in conjunction with a specific subscriber and/or alarm.

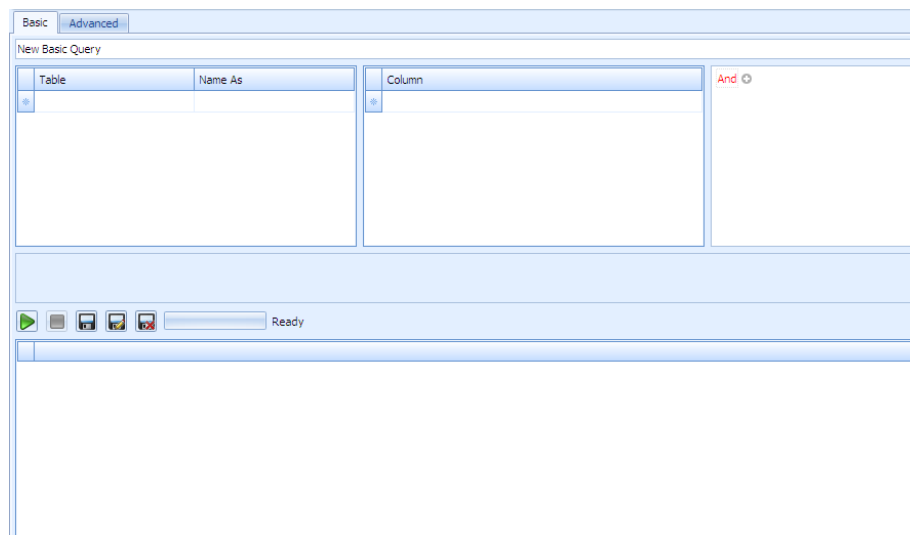
Although the Watchdog interface gives the user full ability to perform all tasks via the graphical interface, there are situations when it is necessary to search for data in other ways.

This possibility is given with the Query tool. It is NOT possible to change, erase or otherwise affect the data bases through the Query tool.

Since the databases are based in SQL, the language is used in the Query tool to search for data.

Queries are considered as either basic, or advanced. The basic query means that the user is selecting variables from pre-defined values with the help of the GUI – the query is formulated as the user makes the choices. The advanced query is for the user that is experienced and knowledgeable in the SQL and has the skills to formulate free-text questions.

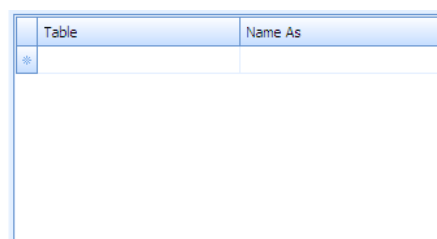
There is an option to store queries in order to repeat them at a later stage.



The default screen when opening the query tool starts with the basic option. The tool is prepared to receive input for a new basic query.

There are four main areas in the query tool screen:

- **The table module:** This module is used to select which table should be searched and gives the possibility to name the variable independently.



- **The column module:** here the selection is done of which column should be used in the table that is high-lighted on the left.
- The rules/relationship module: this module applies the rules and sets the relationships between the variables previously chosen in the table and column module
- The RUN and record module: this part will execute a query and save it in the client to be used repeatedly.

### 3.3.2.2 Query tool – new basic query

**Step 1:** In order to execute a basic query, the user needs to select where the data is to be retrieved.

Clicking on the header cell will activate the input cells below. Click on the drop-down arrow and the system will give you which options there

are to choose.

“Name as” cells are text input cells where the user may choose a logical name for the selected table. If no name is entered, the system will set a name (e.g. “subscribers 1”). This name is used in later steps.

**Step 2:** In the columns module, the user selects from which set of data the query will retrieve the result. Note that the name within the brackets [Subscribers 1] is the logical name you have chosen in the previous step.

The drop-down menu gives all the available options of values in the

table. A star (\*) means that the query will retrieve the result from all data in the table. Another selection will limit the amount of data available for the query.

When the selection is made, the area below the two modules (table and column) is activated, and the query is shown in SQL text.

```
SELECT [Subscribers 1].*
FROM [Subscribers] AS [Subscribers 1]
```

And (+)  
[Subscribers 1.Account ID] Begins with <enter a value> ✕

**Step 3:** Determination and management of which data should be presented in the result.

There are a lot of options depending on which input has been done in the previous two steps.

- = Equals
- ≠ Does not equal
- > Is greater than
- ≥ Is greater than or equal to
- < Is less than
- ≤ Is less than or equal to
- Is between
- Is not between
- abc Contains
- acb Does not contain
- [a]b Begins with
- b[c] Ends with
- asc Is like
- asc Is not like
- Is blank
- Is not blank
- ∞ Is any of
- ∞∞ Is none of

To access the values, click on the (+) icon next to the word “And”. The available expressions will expand, and show their parts in different colours. Clicking on each variable will open the options for that variable.

E.g.: [Subscribers 1.Account ID] Begins with <enter a value> has three parts, each with its' own options.

- [Table.column] will give all the available columns in the table.
- The operator (“Begins with” by default) has the options shown on the picture on the left.
- Clicking on <enter a value> will show a field to insert the parameter to look for.
- The white X on red circle (✕) will delete the whole expression.

And (+)  
 (1) And  
 (1) Or  
 (1) Not And  
 (1) Not Or  
 Add Condition  
 Add Group  
 Clear All

If the user wishes to add more conditions, or change expressions, it is done by clicking on the “And”.

It is also possible to clear all expressions at the bottom of the menu.

**Step 4:** the text area now contains the full expression:

```
SELECT [Subscribers 1].*
FROM [Subscribers] AS [Subscribers 1]
WHERE [Subscribers 1].[AccountID] = '146873'
```

To run the query, use the buttons below the text area:



The green arrow runs the query.

The grey square turns red during the execution, will abort the query.

Diskette saves changed existing query.

Diskette with a pencil saves a new query.

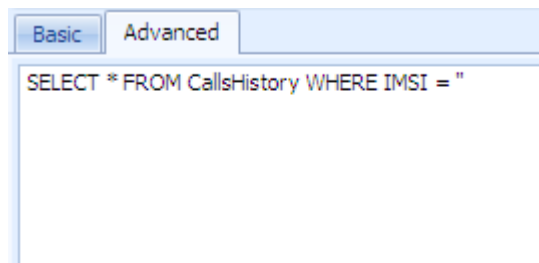
Diskette with a red X will delete the query from the storage.

Result: 0 rows returned

Next to the buttons, there is a progress bar to show that the query is running. After execution, the result is displayed below the buttons and a summary of the result will show to the left of the progress bar.

### 3.3.2.3 Query tool – new advanced query

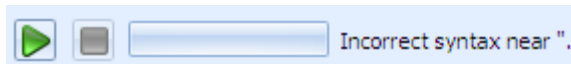
If the user is experienced in using SQL, it is possible to use “free-text” queries in the advanced tab.



When clicking the “Advanced” tab, a supporting text will show directly under the tab, to indicate where the insertion of the SQL query should be done.

The existing text may be erased or replaced.

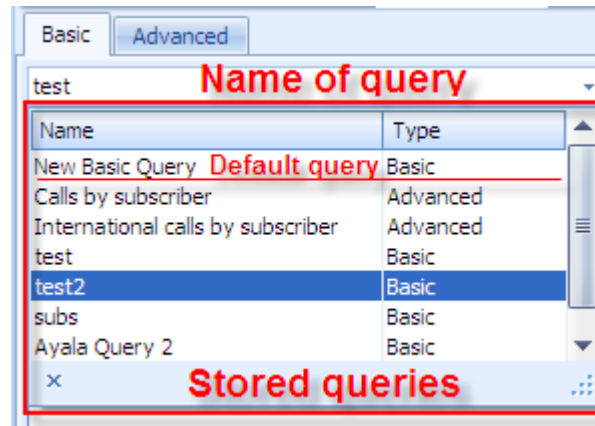
Directly below the query area, a button toolbar appears. This toolbar has a run



button, a stop/abort button and a progress bar.

When the query has run, the results are shown directly below the button toolbar. If anything is wrong with the query, the fault messages are shown on the right of the progress toolbar, see picture above.

### 3.1.2.4 Query tool – stored query

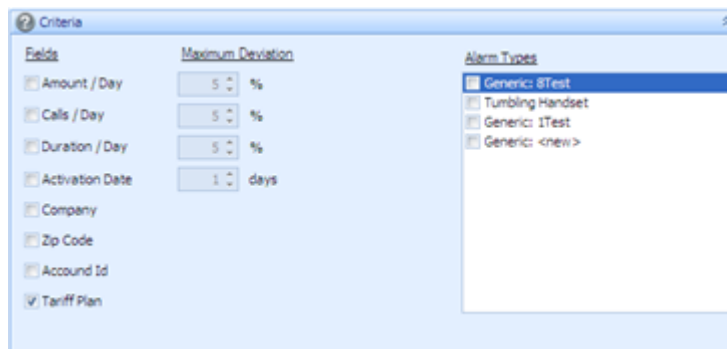


### 3.3.3 Find Similar

The function of “Find Similar” gives the user a possibility to look for other subscribers that have the similar type of profile regarding financial or technical issues. The user also has the possibility to investigate the matching subscribers separately, or insert them into an on-going investigation.

The function is optional and available at any moment in the Investigation Workflow.

#### 3.3.3.1 Criteria



The first step is to determine what kind of criteria the matching should consist of.

The Fields are enabled by checking the box on the

left. When the box is checked, the maximum deviation field is lit up, allowing the user to detail the deviation percentage where applicable, or the number of days when it comes to activation date.

It is also possible to match based on alarm types; the alarm types available in the right field are the alarms triggered by the current subscriber.

When the settings are configured, proceed by pressing the “Search” button. The Criteria area will minimise itself automatically, allowing for more space to the other areas in the data pane.

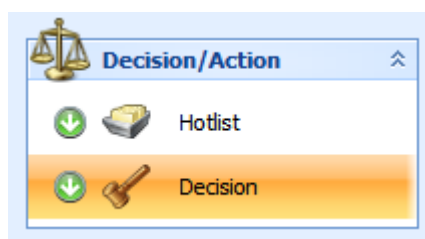
### 3.3.3.2 Matching subscribers and Selected Matching Subscriber

The result of the search made above, is projected as a list in the “Matching Subscribers” field.

The user may choose to...

- ...browse through the result, where the subscriber’s values are displayed below the list in the “Selected Matching Subscriber” field. The values include the selected subscriber’s alarms (if any), the statistics and the log. Furthermore, the selected subscriber’s information in the subscriber file is available on the left, in a similar fashion to the current subscriber (i.e. the subscriber being investigated). The current subscriber’s corresponding values are available at the bottom of the data pane (as in all other Investigation workflow data panes).
- ...investigate the matching subscribers, either separately or added to an existing investigation in the case manager.
- ... Ignore the result and continue to the next step in the workflow, in case of no more information being available from this function.

## 3.4 Workflow – Decision / Action



The “Hotlist” button will open the hotlists available, exactly as the hotlist button in the toolbar (see [5.14.4.6 Hotlist](#)).

The last step of the workflow is the decision – whether the investigated alarm is a possible fraud situation or if the alarm may be deleted with no further due.

When the “Close Investigation” button is pressed, the investigation closes automatically, and the workflow returns to the first step ([“Tasks”](#)) again.

### 3.4.1 Send Notification

At times it may be necessary to notify the subscriber that there are registered anomalies in the account. This could be the case in possible shutting down or suspension of the subscription, or if the system otherwise has affected the subscriber.

The message may be sent via e-mail or SMS.



### 3.4.1.1 Email

Select “Email” in Type drop-down menu. The recipient’s name should appear in the field automatically from the information in the Subscriber file.

Select appropriate template from the drop-down menu. In case new templates should be configured, click the “Configure” button. This will open the “[External notification](#)” screen (Chapter 5.6) in the “Settings” tab.

The email function will have a subject line and a message field, where the text will appear automatically depending on the selected template.

Click “Send” button to initiate sending the message to the subscriber.

### 3.4.1.2 SMS

Select “SMS” in the drop-down menu. The recipient’s telephone number (MSISDN) will be inserted automatically from the Subscriber file.

Select the template in the drop-down menu. If a configuration of a new template is needed, click “Configure” button. This will open the “[External notification](#)” screen (Chapter 5.6) in the “Settings” tab.

The SMS send notification only contains a “Message” field.

Click “Send” button to initiate the sending process.

## 3.4.2 Closure

The closure will define how the alarm is ultimately handled. If there is any possibility of fraud, a case should be created and the alarm added to the case. If there is a suitable existing case, the alarm may be added to the respective case.

- **Action:** Decides where to put the alarm. It is possible to configure the actions in the [Settings tab](#). There are however some default actions available:
  - **Add to existing case:** puts the alarm into an existing case, selected on the right of the “Action” field.
  - **Add to new case:** opens a field on the right where it is possible to create a new case. The alarm will be added to the created case.
  - **Close as Not Fraud:** deletes the alarm without saving any data in the system (normally – this may be configured in the Settings tab)
  - **Close as Bad Debt:** deletes the alarm without saving any data in the system (normally – this may be configured in the Settings tab)
- **Checkboxes:** Determines what kind of data will be included in the addition of alarms in cases. This data is copied from the regular file-flow to a case

database, and is therefore not affected by the normal cleaning routines of the databases.

- **Add subscriber to Case:** default checked. Will add the subscriber info from the info file to the case.
  - **Add alarms to case:** the alarms are deleted from the alarms list, but saved in the case.
  - **Add call data to Case:** useful when cases are longer than 6 months (the usual cleaning time for the all calls database). The calls are copied and saved in the case database and kept there until the case is closed.
- Comment: the user has the possibility to add comments containing additional information, e.g. what has been done on the case, who has been contacted, who received a report etc.

Click **“Close investigation”** button to end the workflow.

### 3.4.2.1 Hiding alarms

Choosing any other of reasons than “Add to Existing/New Case” will make a new row of options appear.

Hiding alarms will cause the chosen alarm type belonging to the subscriber under investigation to disappear from the list of alarms during a set period of time. When that time period expires, the alarm will re-appear in the alarm list.

Checking **“Hide Alarms”** will activate this function.

The drop-down box **“Alarm Types to Hide”** will show the alarm types available for this subscriber (i.e. it checks the subscriber’s alarms).

The date-picker on the right will show a default setting of dates and time according to [Settings – General](#) (Chapter 5.2). Only the set values are shown in the date picker.

## 3.5 Cases

The Case repository is where data is collected in certain cases. These cases may



be:

- When a decision is uncertain, i.e. the user is not certain that the alarm is not fraud.
- When data needs to be collected for a long time.




- When data needs to be gathered with other input types than normally available from Watchdog, such as scanned files or reports from other systems.

Data collected in the Cases repository will stay there until manually removed by the user.

Data collection is done in the Investigation workflow, in the [Decision step \(Chapter 3.4\)](#).

### 3.5.1 Cases Overview

The cases overview shows all cases in the Cases repository. There are three main icons available for cases:

-  Folders: All cases are stored in folders
-  Filters: The user may filter cases according to a set of variables, independent of which folder the cases are stored in.
-  Individual case: Each case is represented in the list and supplied with all list data in the screen.

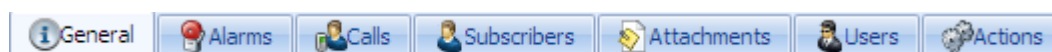
The “+” sign in front of filters and folders indicates the corresponding filter / folder contains cases.

Clicking on the “+” will open the respective filter / folder and change into a “-”.

Double-clicking a case will open the properties below the cases list.

### 3.5.2 Cases Properties

The selected case is displayed in full in the properties pane. If the user makes any changes, they will need to be saved with the “Save Case” button at the bottom right part.



#### 3.5.2.1 General

The General tab contains overview information about the case.

- Name: the name given to the case. It should be a logical and easily readable name. A good suggestion is to avoid names like “Case no.1” etc.
- Status: the status is selected from a drop-down list containing the following variables:
  - **New:** the case has now been assigned to anyone or there has been no action in the case.
  - **Open:** the case is under investigation.
  - **Pending:** the case is awaiting action or input from someone else.

- **Closed:** all actions are finished and the user has closed the case.
- Type: This field is used to determine which kind of fraud the case is connected to.
- Resolution: The user sets what kind of resolution the case has caused.
- Description: A text field to allow the user to further comment on the case.
- Summary: The summary shows five different variables with a value (number of instances of each variable) for a quick glance:
  - **Alarms**
  - **Users**
  - **Attachments**
  - **Calls**
  - **Subscribers**
- Log entries: Displays the history of the case. The latest event is topmost as default. This list is generated automatically.
- Pending actions: Displays a list of pending actions, created and edited in the “Actions” tab. This list is generated automatically.

### 3.5.2.2 Alarms

A list of included alarms is presented in order for the user to use as a base for the analysis.

Right-click the alarm to remove it from the list.

### 3.5.2.3 Calls

A list of included calls (provided the “Add call data to Case” box was checked in the [decision step of the workflow](#)).

### 3.5.2.4 Subscribers


Subscriber data is provided from the Subscriber file. This is only available if the “Add subscriber to case” box was checked in the decision step of the workflow. Right-click the subscriber row to remove a subscriber from the case.

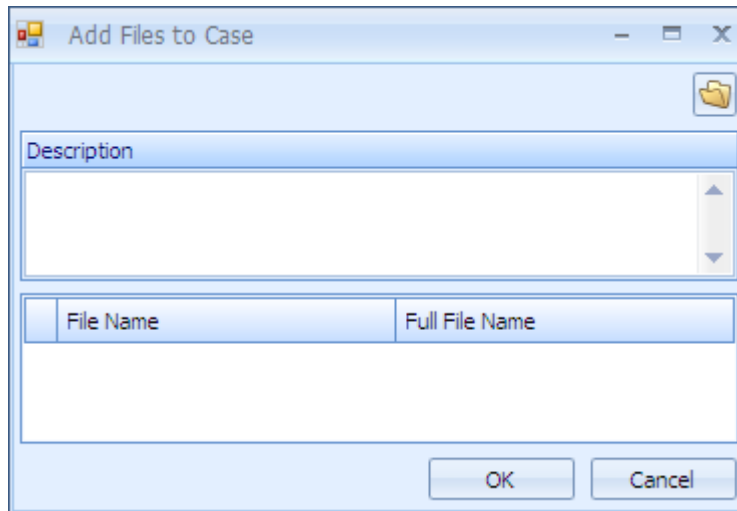
The subscribers may be part of an account; in this case they are collected under the accounts folder.

### 3.5.2.5 Attachments

Attachments of various sorts may be attached to the case. Example of files could be PDF-documents, Word-documents, reports, Excel-files, pictures, etc.

Right-clicking the root folder will enable you to add a folder or to add a file. A dialogue box will open to allow for addition of file.

Click on the browse button  to find the file in the local computer.



The user has a possibility to add a description of the added file. This description will show in the list.

There is a possibility to add several files at one time.

Double-clicking on a file in the list will

open the file.

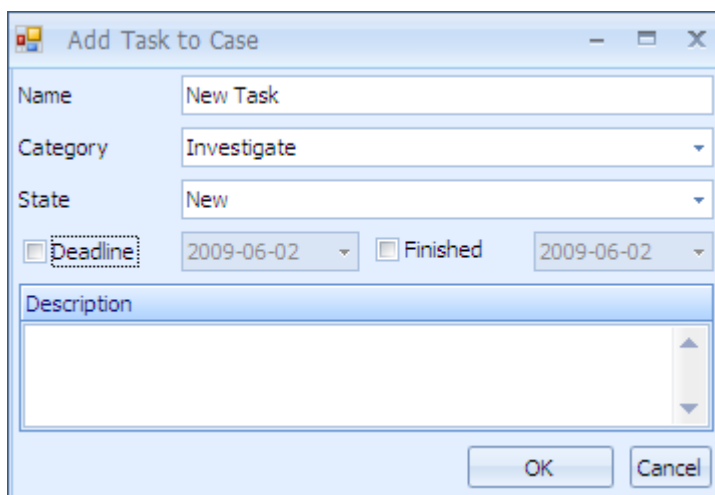
### 3.5.2.6 Users

To add a new user to the case: right-click in the data pane's white area. Select the user in the dialogue box.

The user will appear in the list. Edit the user's permissions by checking the boxes. Default state is no permissions.

To remove a user from the case, right-click the user's row.

### 3.5.2.7 Actions



This is a list to remind the case users of tasks in conjunction with the case. In order to add a new task, right-click on the list's empty space.

The dialogue box gives the user the following possibilities:

- Name the task according to a logical standard.
- Select the category of task from a drop-down menu containing Investigate, Send to CreditControl or Case FollowUp.
- Set the status to any of the following variables:
  - New
  - Pending
  - On hold

- Finished
  - Cancelled
  - Overdue
- If feasible, the user may add a dead-line by checking the box and setting a date.
- The user may indicate that a task is closed by checking the “finished” box and setting a date.
- A short description facilitates the understanding of the task.

The user may edit the task or delete the task by right-clicking the task row.

### **3.5.2.8 Exiting the Cases**

To exit the cases at any time click on the [X] on the top right.



## Chapter 4: Administration Tab

### 4.1 Directly under the tab



The three main areas in the Investigation tab are: Overview, History and Tools.

### 4.2 Overview (Dashboard)



### 4.3 History (Event Log)

When the History button / Event Log is selected, it is high-lighted and the below window is opened.

Events					Users	
Level	Date	User	Description	Source	Name	Last Log On
Information	2010-02-08 15:01:28	BassetLabs	Logged off	Client	BassetLabs	2010-02-08 15:01:28
Information	2010-02-08 15:01:03	BassetLabs	Logged on	Client		
Information	2010-02-08 14:59:25	Adam Chodorowski	Logged off	Client	Adam Chodorowski	2010-02-08 14:59:25
Information	2010-02-08 14:59:05	Adam Chodorowski	Logged on	Client	Ape Limecorn	2009-12-03 16:00:00
Information	2010-02-08 14:58:58	Adam Chodorowski	Logged off	Client	Daniel Salokas	
Information	2010-02-08 14:58:33	Adam Chodorowski	Logged on	Client	El Maco	2010-02-05 16:00:00
Information	2010-02-08 14:58:22	Adam Chodorowski	Logged off	Client	Hans Molin 2	
Information	2010-02-08 14:57:49	Adam Chodorowski	Logged on	Client	nico	

#### 4.3.1 Update

On top left of the events pane there is a button for setting the amount of time in **seconds** needed for **auto update** of the User Event Log is entered. Next to it there is the **Manual Update** button which is used for manually update.

#### 4.3.2 Users

On the right side, the names of those currently logged into Watchdog are shown. The logged in users are indicated with a small ball.



### 4.3.3 Time Period

On the right bottom are the settings for dates range, “Time Period”. The range allows the user to set and retrieve data on those who were logged in Watchdog during a particular period or day.

### 4.3.4 Events Log

The columns in the Event Log are **(a)** Level **(b)** Date **(c)** User **(d)** Description and **(e)** Source. Each of the columns is described below.

**(a) Level:** Here the users can filter the different warnings or information signs by clicking on *Level* and selecting different alternatives from the drop down list.

**(b) Date:** Displays date the user logged into Watchdog.

**(c) User:** Displays name of user/s

**(d) Description:** Displays record of what the user did.

**(e) Source:** Displays source of data used

## 4.5 Tools

### 4.5.1 Delete Alarms



Delete Alarms Alarm button is used when there is a need to delete an alarm/s. When the button is clicked on the following window appears.

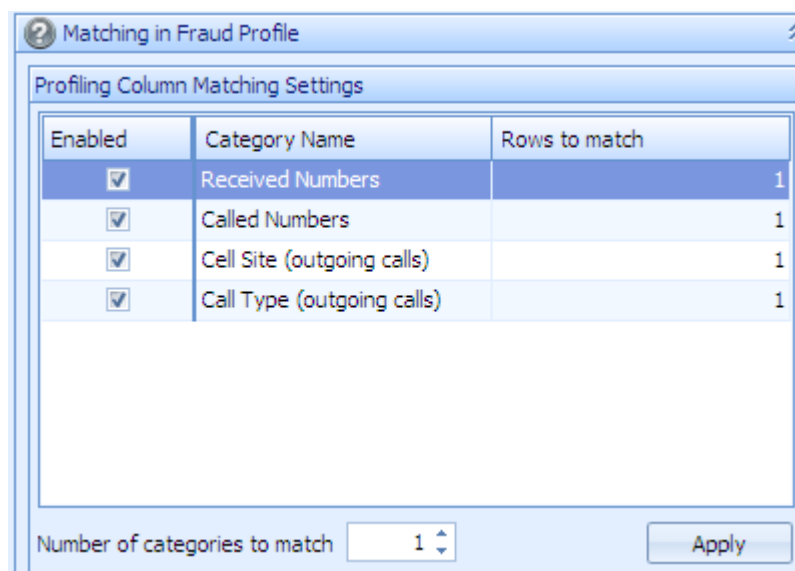
Older Than Date: 04/05/2009 Older Than Days: 30		Comment:
<b>Assigned User</b> <input type="checkbox"/> El Taco (perher) <input type="checkbox"/> Ako Ginipiggu (ako) <input type="checkbox"/> Bko Ginipiggu (bko) <input type="checkbox"/> Cko Ginipiggu (cko) <input type="checkbox"/> (Newbie) <input type="checkbox"/> wdadm (wdadm) <input type="checkbox"/> asd (smurf)	<b>Alarm Status</b> <input type="checkbox"/> Open <input type="checkbox"/> Assigned <input type="checkbox"/> On Hold <input type="checkbox"/> On Reminder	<b>Alarmtype</b> <input type="checkbox"/> Call Collision <input type="checkbox"/> Generic <input type="checkbox"/> EIR Blacklist <input type="checkbox"/> EIR Greylist <input type="checkbox"/> Tumbling Subscription <input type="checkbox"/> Tumbling Handset <input type="checkbox"/> Switch Audit

At the top to the left there is the “**Older Than Date**” and “**Older Than Day**” columns. These are used to filter alarms that are older than a given period of time or days. The dialogue screens “**comment**” is for writing reason/s for deleting an alarm. But any comment related to the alarm could be entered.

- **Assigned Users:** Delete alarms by assigned by or to a specific user.
- **Assigned Users:** Delete alarms by assigned by or to a specific user.
- **Alarm status:** Delete alarms of different statuses. E.g. alarms that are open, assigned, on hold or on reminder.
- **Alarm type:** Delete alarms of different types e.g. handset tumbling, call collision, velocity etc.

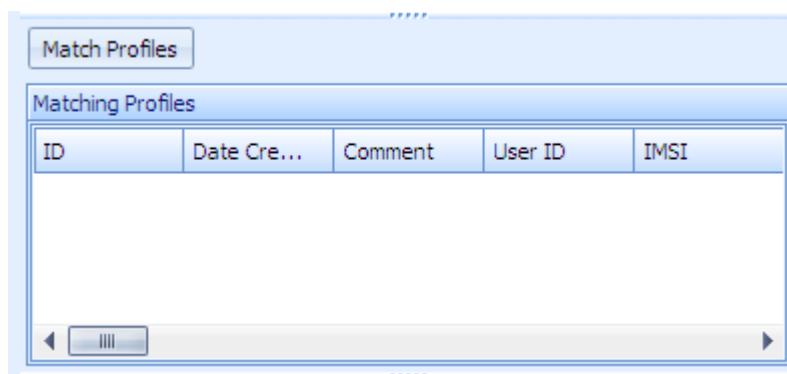
#### 4.5.2 Fraudster Profile (CHANGE THIS INFO)

Checking whether the possible fraudster has been caught by the system at an earlier time (provided that the data has been saved when deleting the alarms), is done by matching the currently investigated subscriber with the saved data. Before executing the match search, the settings for the search have to be configured.



The categories are fixed in the system. The user may enable or disable the category, by checking or unchecking the box on the left.

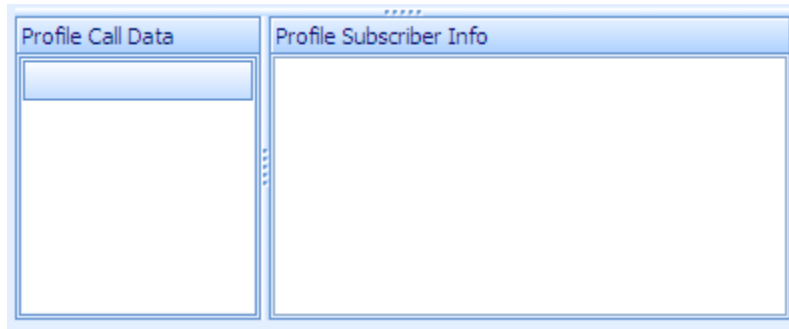
On the right, the user may determine how many rows have to match for the successful result. This is done by double-clicking the "Rows to match" field and changing the default value of 1.



Furthermore, the user may determine how many of the categories have to match for a successful result.

When the configuration is ready, clicking the “Apply” button will set the configuration.

To initiate the matching of the subscriber with the profiles available, the user will



click “Match profiles” button.

The result will contain the ID of the

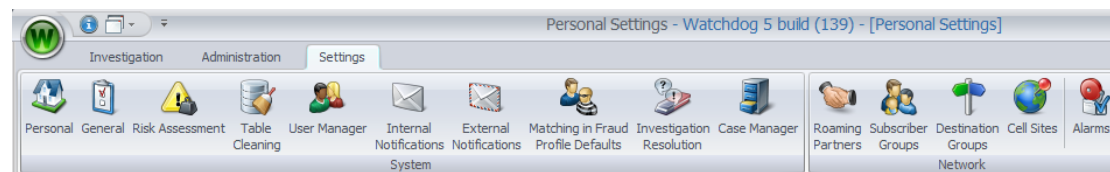
profiles in the data base, when the profile was created, any comments and by whom the comments were made, and finally the IMSI numbers used by the profile.

The profiles’ call data and the profile subscriber info for the high-lighted profile are shown at the lower part of the data pane.

At the data pane’s bottom the subscriber data for the investigated subscriber is available.



## Chapter 5: Settings Tab



### 5.1 Personal



Choosing this icon will enable the user to change the SQL Password. The password has to be secure, i.e.:

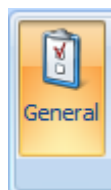
- minimum password length is 8 characters
- password must contain at least three different types, i.e.
  - lowercase alpha (a, b, c...z)
  - uppercase alpha (A, B, C...Z)
  - number (1, 2, 3...0)
  - special characters (!@#\$...)

Maximum password age is 90 days. A reminder warning will show 10 days before expiry. If password is not changed, the user is blocked. Contact Basset Helpdesk.

Account will lock after 6 failed attempts. For unlocking and re-activation of password, contact Basset Helpdesk.

A user cannot re-use passwords.

### 5.2 General



When this icon is selected it is high-lighted a window appears that is divided into two i.e. **Administration** and **System**.

Administration		System	
OperatorCode	SWEIQ	NTLoginOption	3
NameOfSystemOwner1	BassetLabs	SystemType	0
PhoneNumberOfSystemAdministrator	123456789	WatchDogServerName	BTSTEST05
WatchDogVersion	5.0	UnitDistance	2
RRContact	Nicolaj Aarøe	UnitTime	1
RRCompany	BassetLabs	UnitVelocityDistance	2
RRFaxNumber		UnitVelocityTime	3
RRPhoneNumber		UMNTGroupName	

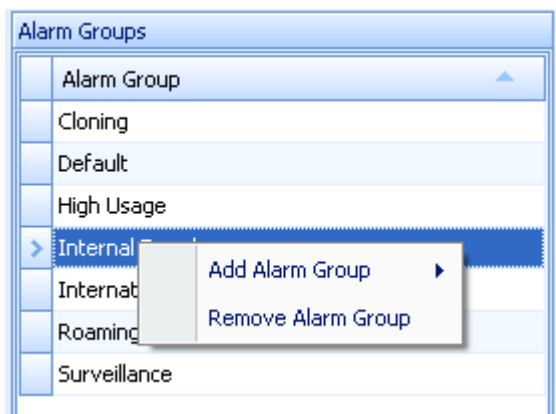
Both the **Administration** and the **System** windows provide information that is mostly used by system administrators: The users are not supposed to change any information in this window.

## 5.3 Risk assessment



When this icon is selected it is high-lighted; a new window below appears. Risk assessment is used for evaluating the total risk for a subscriber by combining values for different factors for example amount, severity etc. Risk assessment configuration is global, which means that if one user changes configuration it will be applicable for all users.

### 5.3.1 Alarm groups



**Alarm Group:** Names of the different alarm groups in Watchdog. To add or remove a group, left click and add or remove. The contents of the alarm groups are set in the Alarms settings, in the right column, "Groups".

Risk assessment configuration may be based on any of the fields available in the alarm list that include alarm and subscriber information. This information is provided for in the subscriber file.

### 5.3.2 Column settings

Columns			
Column Name	Overall Weight	Percent	Number of Weights
Amount	10	66.7%	4
Severity	5	33.3%	5

Add Column  
Remove Column

UniqueRecordID  
IMSI  
UserID  
Phone Number  
Name  
Address

- **Column name:** The variables (e.g. amount, severity etc) whose values are used to assess risk. Find the list of all available variables that can be configured by pointing the column name with the cursor right clicking.
- **Overall Weight:** Weight given to each variable. The size of the weight corresponds to the level of importance/ severity of the variable. A higher value indicates that the user has made a decision that the given variable has a higher risk.
- **Percent:** The percentage risk is divided proportionally based on the Overall Weight. The range is 0 % to 100% where 100% is the highest risk.
- **Number of Weights:** The number of weight per variable.

### 5.3.3 Weights

- **Integer:** Enter the proportion of the overall weight.

Weights				
Integer Value	Weight	Interval	Percent	
Click here to add a new row				
1	1	<input checked="" type="checkbox"/>	25%	
10	2	<input checked="" type="checkbox"/>	50%	
50	3	<input checked="" type="checkbox"/>	75%	
100	4	<input checked="" type="checkbox"/>	100%	

- **Weight:** Enter the weight (according to risk level).

- **Interval:** Check if the set value are an interval

- **Percent:** Proportion weight.

- **Add new row:** Click here to enter values.

### 5.3.4 Subtracting columns

Subtracting Columns	
Column Name	Number of Subtracting Values
Zip	1
	1

Add Column  
Remove Column

From the subtracting columns window the users can remove e.g. particular address, company, IMSI, country in order to reduce or remove the risk of an alarm being triggered for the columns subtracted.

**Column name:** Name of the column whose risk is to be reduced.

**Number of subtracting values:** The number the given value that has been subtracted.

### 5.3.5 Subtracting values

- **String value:** Subtracted value e.g. zip, if it's an address and name, if its company etc.
- **Percent subtract:** The percentage

risk to be subtracted.

**Note:** The user adds both the string value and the percent subtract.



## 5.4 Table Cleaning

When this icon is selected it is high-lighted a window below appears.

From the window the users can control the length of time Watchdog data should be stored before being deleted.

	Enabled	Name	Days to Keep	Modified by	Modified
>	<input checked="" type="checkbox"/>	AlarmComments	60	basset	24/08/2007 14:12:43
	<input checked="" type="checkbox"/>	AlarmsCurrent	15	basset	24/08/2007 14:12:43
	<input checked="" type="checkbox"/>	AlarmsDeleted	15	basset	24/08/2007 14:12:43
	<input checked="" type="checkbox"/>	CallCollisions	15	basset	24/08/2007 14:12:43
	<input checked="" type="checkbox"/>	FilesRead	15	basset	24/08/2007 14:12:43
	<input checked="" type="checkbox"/>	EventLog	2	basset	14/04/2009 11:46:34
	<input checked="" type="checkbox"/>	OME	30	basset	24/08/2007 14:12:43

The columns in the window are:

- **Enabled:** Displays where data that is to be deleted is enabled.
- **Name:** Displays type of data that is to be deleted
- **Days to keep:** Displays length of time data is set to be kept in Watchdog.
- **Modified by:** Displays identity (name) of the user who has done modification.
- **Modified:** Displays date modification was made.
- **Save/Cancel:** Save or cancel the modifications made.

Observe that settings can be made separately e.g. for call data and alarms.



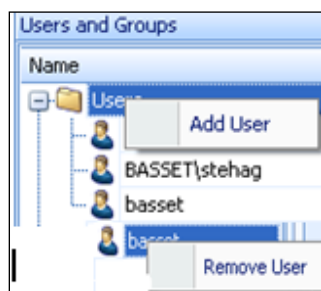
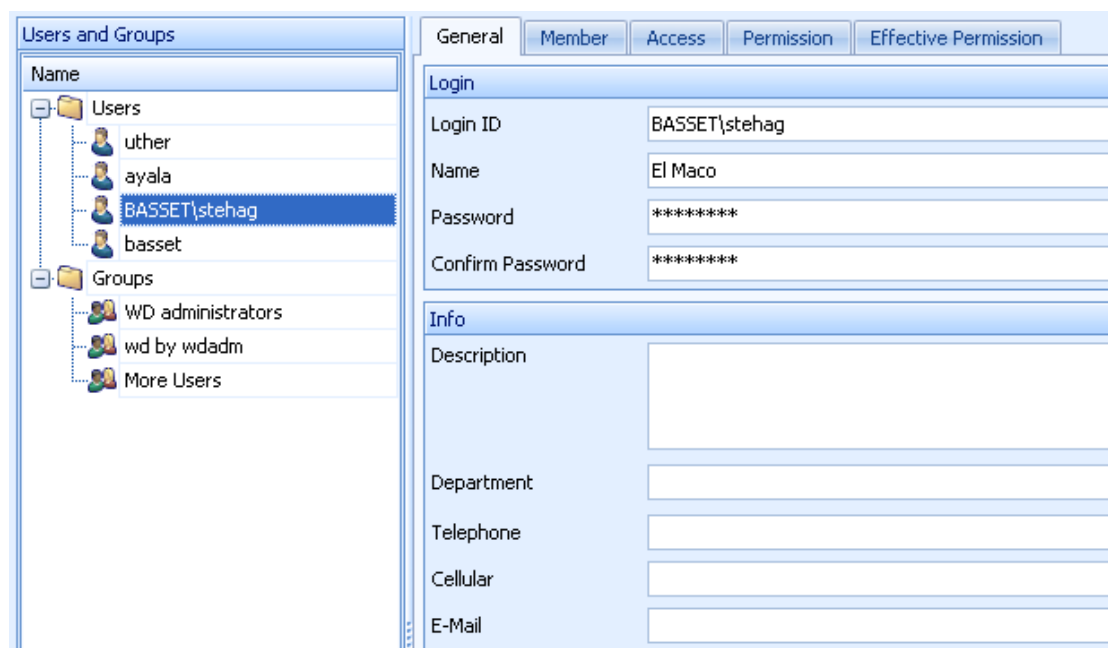
## 5.5 User Manager



When this icon is selected it is high-lighted a window below appears.

From the window Watchdog users/groups are defined and administered.

The User Manager allows access rights to different users to access different areas of the Watchdog system. User rights may be set at user and group levels. When the User Manager command is selected, a list of the current users and groups appears. The user manager window is divided into the following columns:

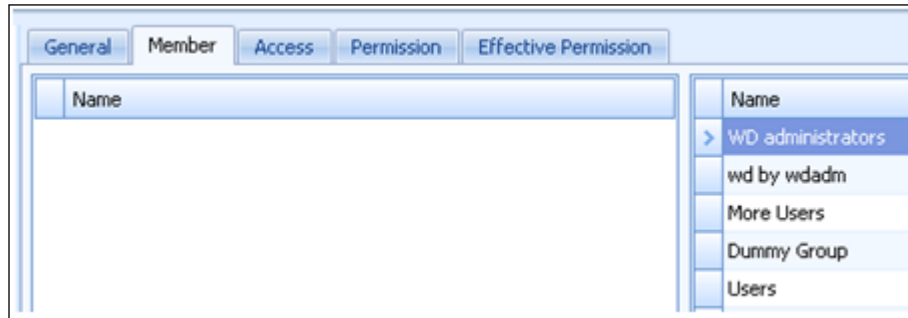


- **Users and Groups: Users** contains a list of contains names of individual users or the **groups** in which they are configured in the system.
- **Add** users or user Groups by pointing the cursor Users and right clicking on the mouse. To **remove** a particular user or Group point the cursor to the name of the user you want to **remove** before right clicking.

### 5.5.1 General tab:

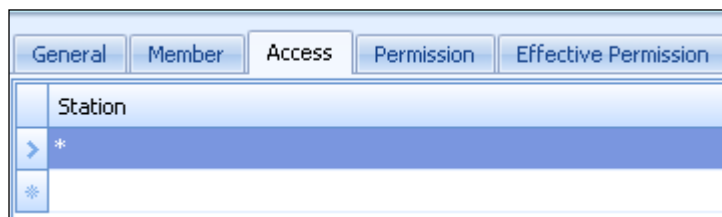
Mandatory parameters for login are entered in this tab under the login column e.g. login name, password and password confirmation. In the info columns description, department, telephone number and email are entered. At the right bottom of the window is a save and cancel button.

### 5.5.2 Members tab



The **member** tab of the user displays which groups the user belongs to. The user may be a member of one or several groups, and the “name” list shows which groups the user is currently a member of.

### 5.5.3 Access tab



The access tab allows the system administrator to configure the workstations users' login from. The user is provided access by adding the names of their workstations in access list. It is possible to configure one or several workstations in the list. An asterisk means that “All workstations” are configured. Only those that are configured in this list are allowed to login.

### 5.5.4 Permission tab

General Member Access Permission Effective Permission				
Name	View	Edit	Insert	Delete
Administration				
Dashboard				
Delete All Alarms				
Event Log				
Roaming Reports				
General				
Exclusion				
Hotlist				
System Access				
Write Global Filters				
Investigation				

The permission tab has settings in which different kinds of permission can be given where possible or necessary to specific users or User groups. The tab has the following columns:

- **Name:** Permission can be given or denied on the listed objects.
- **View:** Sets permission to view (function) objects in name column by marking the boxes.
- **Edit:** Sets permissions to edit data related to (function) objects in name column.
- **Insert:** Sets permission to add data related to (function) objects in name column.
- **Delete:** Sets permission to delete data related to (function) objects in name column.

The following permissions status can be granted by ticking the right box:



**Grant Permission**

This grants permission to the user and gives access to a function (object).



**Deny Permission**

This denies the user permission to access to a function/object.



**No Specific Permission**

It means that no explicit permission has been set for a user or user groups. This could be e.g. System access, delete alarms, views alarms etc.

### Base filter tab

Base Filter	{EditValue is null}
-------------	---------------------

The base filter is a tool to assign an alarm filter to a user. The alarm filter selected from the drop down list will function as default for the named user. The user will not

be permitted to view any other alarm than that set in the base filter. *Only* the alarm that has been permitted will be displayed to the user regardless of whether he creates a new filter and configures it for display, it won't be visible. This function is very useful when other department than the fraud department need access to alarms in the system, for example a roaming manager needs access to only roaming alarms.

### 5.5.5 Effective Permission tab

General Member Access Permission Effective Permission					
Name	View	Edit	Insert	Delete	
System Access	<input checked="" type="checkbox"/>				
Assign	<input checked="" type="checkbox"/>				
Assign Other	<input checked="" type="checkbox"/>				
Add Alarm Comment	<input checked="" type="checkbox"/>				
Put on Hold	<input checked="" type="checkbox"/>				
Set Reminder	<input checked="" type="checkbox"/>				
> Delete Alarm	<input checked="" type="checkbox"/>				

The Effective Permission displays a combination of the permissions set on the specific user and the groups the user is assigned to. The list displays the real permission that will be applicable for the user. The user is either given full or limited access.

For example, apart from the rights a user has he can also be given or denied the right to assign cases to other users at group level. Another example is that example users that have access to cases will see all cases in the system, for users that do not have a global case permission may be given special permissions on certain cases

**NOTE: All the above tabs are found in both Users and Group levels except for Effective Permission Tab which is not in Groups.**

## 5.6 Internal Notifications



When this icon is selected it is high-lighted and the window below appears.

Internal notifications settings are done from the window as shown.

Internal notification is used to automatically create and send e-mail messages from Watchdog to notify for example the fraud management on selected alarms. This notification is used when the users are interested on getting a notification on given alarms.

Name <input type="text"/>						Create	Delete
Enabled	Name	Created	Created by	Modified	Modified by		
<input type="checkbox"/>	New Automail	16/11/2007	basset	02/06/2009	basset		
<input type="checkbox"/>	Automail by w...	27/11/2007	<unknow...	11/01/2008	WD test		
<input checked="" type="checkbox"/>	Nicos mail	07/02/2008	nicolaj aarøe	22/08/2008	basset		
<input checked="" type="checkbox"/>	Automail Test	25/08/2008	basset	25/08/2008	basset		
<input checked="" type="checkbox"/>	aaa asd	23/03/2009	basset	23/03/2009	basset		

The following parameters are available;

- **Name:** Enter name for a user who a notification is to be sent.
- **Create:** Click to create.
- **Delete:** Delete a user
- **Enabled:** Enable as user. No notification will be sent without enabling first.
- **Name:** Name of users configured into system (mark the box) ready for notification upon enabling.
- **Created by:** Who made created.
- **Created:** Date of creation
- **Modified by** Who made the modification
- **Modified:** Date of modification.

Details	
Name	New Automail
Recipients	stephan.haglund@bassetlabs.com, ada@ada.com
SMS Recipients	
Date (from-to)	01/01/2007 - 17/11/2007
<input checked="" type="checkbox"/> Severity (from-to)	Lowest (1) - High (4)
<input type="checkbox"/> ActiveTime (hrs)	
<input type="checkbox"/> Amount	
<input type="checkbox"/> Mail per Subscriber	
<input type="checkbox"/> Only Include New Alarms	
<input type="checkbox"/> Send Mail Attachements With .xls Suffix	

• **Name:** An arbitrary name of the auto mail item. It's displayed in the Name column in the Edit Auto mail list.

• **Recipients** The e-mail address to which messages are sent. A list of addresses can be entered Use a semicolon (;) to separate the numbers.

• **SMS recipients:** The phone number

to which messages are sent. A list of addresses can be entered Use a semicolon (;) to separate the numbers.

- Names of those getting notification via SMS
- **Date:** Period in which the notifications are to be sent.

- **Severity:** Watchdog will generate a message only if the alarm has a severity level within the specified interval.
- **Active Time:** The user might not want a notification to be sent to him immediately an alarm is generated. He can set how long after an alarm generation he wants the notification to be sent. This is done in hours. The set hours are therefore the lag time between alarm generation and generation/sending of notification.
- **Amount:** Watchdog can be set to generate notification (e-mail messages, SMS) if specific monetary is exceeded on a given alarm/s. This only applies to alarms based on a monetary value.
- **Mail per subscriber:** Send notification regarding each subscriber who triggers an alarm.
- **Only include new alarms:** Send notification regarding newly generated alarms.
- **Send attachment with "xls" suffix:** Send the notification on an excel spreadsheet.

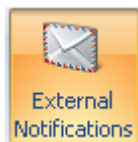
**Assigned user:**  
Watchdog will gener-

ate a notification message only if the alarm is assigned to the users selected in this list.

**Status:** Watchdog creates notification messages only for alarms with the status selected here.

**Alarm type:** Watchdog generates notification messages only for the types of alarms that have been selected here.

## 5.7 External Notifications



When this icon is selected it is high-lighted a window below appears.

External notifications settings are configured in done in the following windows.

<input type="text"/> <input type="button" value="Add"/>						<input type="button" value="Remove"/>
SMS	Name	Created by	Created	Modified by	Modified	
>	subscriber letter		23/02/2005	basset	13/09/2006	
	new letter by wdusr2	wdusr2	27/11/2007	wdusr2	27/11/2007	

- **Name:** Enter name for the subscriber who a notification is to be sent.
- **Create:** Click "Add" to add a new user.

- **Delete:** Delete a subscriber
- **Enabled:** Enable as subscriber. No notification will be sent without enabling first.
- **Name:** Name of subscriber configured into system (mark the box) ready for notification upon enabling.
- **Created by:** Who made created.
- **Created:** Date of creation
- **Modified by** Who made the modification
- **Modified:** Date of modification.

The screenshot shows the BASSET software interface. The 'Details' window on the left has fields for 'Name' (subscriber letter), 'Type' (Subscriber Letter), and a 'Comment' text area. Below these is an 'Autotext' section with a font dropdown (Arial), size (12), and bold, italic, and underline buttons. The autotext content reads: 'Dear <sub:Name>', 'Your account [Subscriber Data.Phone Number] has been subject to abuse and disconnected.', 'Sincerely', and 'GM'. On the right, the 'Tags' list includes 'Subscriber Data' and 'Call Data (slow)', each with a plus and minus icon. Below these are various system parameters, each preceded by a green plus icon: UniqueRecordID, FileNumber, Recordtype, IMSI, ANumber, AHandset, BNumber, BHandset, BNumberCountry, CNumber, CallType, StartOfCall, Length, Volume1, Volume2, Amount, and OrigPartyExchan.

#### Details

**Name:** The name of the letter.

**Type:** Type of letter to be sent to the subscriber.

**Comment:** Any comments that are necessary are entered here.

**Tags** If a system parameter is included in the text, Watchdog will insert the value of this parameter in the text. To include a tag, place the cursor where the tag should be included and then double-click the tag. This window contains a list of system parameters. These are information from the subscriber file and call information. If any of the system parameters are included in the text, Watchdog will insert the value of this parameter in the text. This enables the use of dynamic letters e.g. subscriber's address and current account balance (if available). Note that the tags may vary from operator to operator depending on what is their subscriber file. To include a tag, place the cursor where the tag should be included and then double-click the tag. The letter appears in the bottom window and can also be printed then sent to customer. Remember to always save whatever information is added or modified



## 5.8 Matching in Fraud Profile Defaults

Profiling Column Matching Settings			
Enabled	Category Name	Rows to match	
<input checked="" type="checkbox"/>	Received Numbers		2
<input checked="" type="checkbox"/>	Called Numbers		1
<input checked="" type="checkbox"/>	Cell Site (outgoing calls)		2
<input checked="" type="checkbox"/>	Call Type (outgoing calls)		4

## 5.9 Investigation Resolution



When this icon is selected it is high-lighted investigation resolution window appears. Settings for investigations resolution is done in the shown window.

The different resolutions that are taken or are supposed to be taken after making a decision on the way forward as far as fraud analysis is concerned are set in this window. An investigation can end with a resolution that it was e.g. bad debt, fraud, not fraud etc (see [3.3.1.14 Matching in fraud profile](#)).

Investigation Resolution						
	Enabled	Name	Modified By	Modified	Created By	Created
>	<input checked="" type="checkbox"/>	Not fraud 2	basset	23/04/2009	basset	20/08/2004
	<input checked="" type="checkbox"/>	Bad debt	basset	23/04/2009	basset	15/03/2005
	<input checked="" type="checkbox"/>	New Investigation Resolution	basset	23/04/2009	basset	23/04/2009



Save



Cancel

The Investigation Resolution window has the following parameters:

- **Enabled:** Check to enable the resolution.
- **Name:** The resolution reached by the user.
- **Modified:** The user who made the modification to the current item
- **Created by:** The user who created the current item.
- **Created:** when an investigation resolution was reached.

## 5.10 Case Manager

Case Type						
	Enabled	Name	Modified By	Modified	Create...	Created
	<input checked="" type="checkbox"/>	Fraud zadf sdgf	basset	23/04/2009	basset	20/08/2004
>	<input checked="" type="checkbox"/>	Case Status-Delete Reason by wdustr1	basset	23/04/2009	<unknown...	27/11/2007
	<input checked="" type="checkbox"/>	Case Status-New Case Status	basset	23/04/2009	wdkst	30/11/2007
	<input checked="" type="checkbox"/>	Case Status-GSM-Gateway	basset	23/04/2009	basset	10/07/2006
	<input checked="" type="checkbox"/>	Case Status-Not fraud either	basset	23/04/2009	basset	01/04/2009
	<input checked="" type="checkbox"/>	Case Status-This is not Fraud	basset	23/04/2009	basset	07/04/2009
	<input checked="" type="checkbox"/>	Case Type	basset	23/04/2009	basset	23/04/2009
Case Resolution						
	Enabled	Name	Modified By	Modified	Created By	Created
>	<input type="checkbox"/>	case resolution	basset	23/04/2009	basset	23/04/2009

Case Manager has two windows i.e. Case type and Case resolution.

- **Case Type:** The possible case types that can be investigated. Roaming, Gateway, High Usage, Internal fraud etc.
- **Case Resolution:** The decisions/conclusions that can be drawn about a case at the end of an investigation. For example the case could be closed as fraud. The case could then be set to be used in profiling (e.g. Fraud-create profile). Or it could be fraud but no profile is created.

The following parameters are available in both Case type and case resolution.

### Case Type

- **Enabled:** Check to activate the created case type.
- **Name:** Name of the case created.
- **Modified by:** Who last modified case.
- **Modified:** Date of last modification.
- **Created by:** Who created the case.
- **Created:** Date of creation.

### Case resolution:

- **Enabled:** Check to activate the created resolution.
- **Name:** Name of the resolution created.
- **Modified by:** Who last modified resolution.
- **Modified:** Date of last modification.
- **Created by:** Who created the case.
- **Created:** Date of creation.

## 5.11 Roaming partners



When this icon is selected it is high-lighted the menus below are revealed.

It is here that roaming partners are configured and reports created ready to different partners. These reports contain information about visiting roamers, i.e. foreign subscribers that have made calls in our own network. The settings include a list of the roaming partners with individual thresholds, and functionality to automatically send information about their subscribers' usage.

List	General Settings							
	Company	Operator Code	Netcode	Country Code ▲	Created by	Created on	Modified by	Modified on
	Cosmo Bulgaria Mobile EAD	BGRCM	28405	Bulgaria (359)	<unknown (28)>	28/11/2005	<unknown...	05/12/2005
	Telecel Faso	BFATL	61303	Burkina Faso (226)	<unknown (27)>	03/02/2006	basset	03/06/2009
	Telecel Burundi	BDITL	64282	Burundi (257)	<unknown (27)>	17/03/2006	basset	03/06/2009
	Entel Telefonía Movil S.A.	CHLMV	73001	Chile (56)	<unknown (28)>	28/11/2005	<unknown...	05/12/2005

### List

The list tab contains the below named columns:

**Company:** Names of partners

**Operator Code:** The name of the Public Land Mobile Network (PLMN).

**Netcode:** The network code is a numerical code, defined by the GSM Forum, which identifies a network. It is composed of the first five positions of the IMSI.

**Country Code:** International country codes

**Created by:** The user who created a partner in the list.

**Created on:** The date which a partner was entered in the list.

**Modified by:** The user who has made modifications in the list.

**Modified on:** The date modification was made.

## Adding/deleting roaming partners

The information that appears in the list is added/deleted in the details menu. The **details** that can be specified are: Company, Operator code, Netcode, Country, Contact person (name to a roaming partners contact), Phone (phone number to a roaming partners contact) and Email to the same contact.

**Report** menu shows

- **Auto mail:** This option is selected if the roaming high usage report is to automatically send to the roaming partner. The reports are sent to the address specified email address.
- **SMS interworking partners:** The partners who the auto mail is sent via SMS.
- **Auto print:** Select this option if the roaming high usage report is to be automatically printed. The reports will be printed on the Watchdog server's default printer.
- **Don't print unless fraud (mmhh):** The roaming high usage report is created only if there an alarm has been generated for a subscriber belonging to the current roaming partner.

**Start time:** The roaming high usage reports may be generated at different times for each roaming partner. This field is for specifying when the report schedule should start running. Note! Select "Enable extended scheduling" on the general roaming partner settings to enable start time.

**Interval (min):** This field is used to specify how often the reports should be generated. The unit of measurement in this parameter is minutes. Example: If Start time is set to 02:00, the first report will be created at this time. If Interval is set to 480, that means that a report will be created at *every eight hours* ( $8 * 60 = 480$ ), i.e.

02:00, 10:00, and 18:00. Note! Select “Enable extended scheduling” on the general roaming partner settings to enable interval.

**Thresholds** menu shows:

- **Time (min):** The maximum time a roaming subscriber, who belongs to the current roaming partner, is allowed to call in your network before an alarm is generated. The value applies to the time period defined in Time Period in the general settings for roaming partners.

**Amount (SDRs):** The maximum amount a roaming subscriber, who belongs to the current roaming partner, is allowed to spend in your network before an alarm is generated. This value is set in the general settings for roaming partners. This threshold is set in SDRs.

List		General Settings	
<b>General</b>			
Time Period (hrs)	25	<b>Default Values</b>	
Currency Name	SDRs	Allowed Time (min)	350
Exchange Rate	0.00674	Allowed Amount	55
Severity Level	Medium (3)	<b>Max Values</b>	
	<input type="checkbox"/> On	Allowed Time (min)	400
		Allowed Amount	5000
<b>Extended Scheduling</b>			
<input type="checkbox"/> Enable Extended VR Alarm		CDR Delay (min)	60

### General setting

The parameters set here are applicable to all roaming partner.

**General** menu displays:

**Time period:** Each roaming partner has a monetary threshold, which specifies how much its subscribers are allowed to spend. This amount is specified on the Roaming Partner List window. The Time Period parameter specifies how much time has to elapse before the spent amount is calculated.

**Currency name:** The applicable currency in the roaming high usage reports.

**Exchange rate:** A multiplier that is used to convert the call charges to the local currency of the selected currency.

**Severity level:** The degree of importance.

**On:** Enables the use of **severity** field.

**Default values menu** displays parameter values that will be used if no specific values are set for a roaming partner.

**Allowed Time (min):** The maximum time a subscriber is allowed to generate traffic in your network before an alarm is generated. The value referred to is set in the *Time Period*.

**Allowed Time (Amount):** The maximum amount a roaming subscriber is allowed to spend in another operators network before an alarm is generated. The value referred to is set in the *Time Period*.

### Max values

**Allowed Time (min):** See default values.

Allowed Time (Amount): see default values.

**Enable extended scheduling:** Used to activate the functionalities **start time** and **interval**.

**CDR Delay (min):** is used to create a lag and allow all roaming calls to be released from the network, produced by the switch, transferred via mediation device, converted into WatchDog format, Classified, Rated and finally used for alarm generation.

If a report is generated at 00:00 to include data from the last 24 hours it will only contain data that is available for the WatchDog system, if a roaming call is performed between 23:30 – 23:58 most likely the CDR will not be available.

When setting the **CDR Delay** setting what should be considered as the absolute maximum time from when a call is closed to it is available for WatchDog. For exam-

ple if the switch would release it calls every 15 minute the maximum time should be added with 15 minutes plus all other delays, the setting is customer specific.

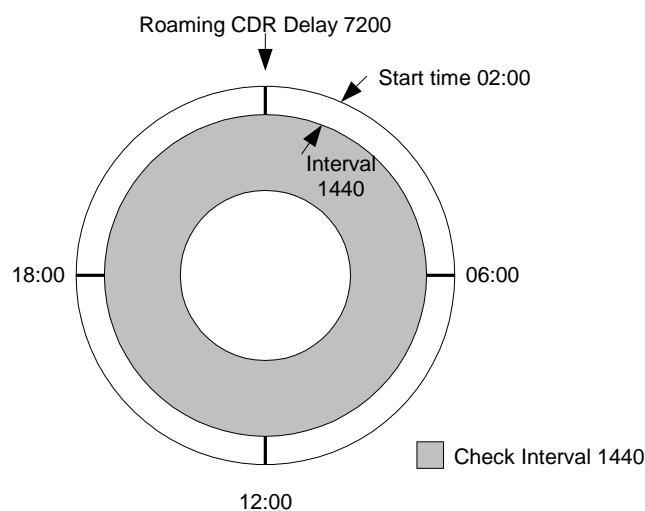
The **CDR Delay** is specified in seconds.

In the above screen shoot the **CDR Delay** is set to 7200 (60 seconds \* 60 minutes \* 2 hours = 7200 seconds) minutes for all roaming reports.

### Example

The general setting **CDR Delay** is 7200 seconds (2 hours) and a report is to be generated every 24 hours containing the last 24 hours of calls the roaming report settings should be specified as below. The data in the report should be from 00:00 to 00:00.

- Start Time 02:00 (Must take CDR Delay into consideration when specifying Start Time)
- Interval 1440 (The report generation will start 24 hours after Start Time)
- Check Interval 1440 (The report will contain the last 24 hours of calls)



## 5.12 Subscriber Groups



When this icon is selected it is high-lighted and window below are displayed

Name	Description	Modified By	Modified
BUSINESS	xxx	basset	23/04/2009
Pnork		basset	28/01/2008
test 2		basset	02/06/2009
Private	Privat kunder	WD test	21/01/2008

Identifier	BUSINESS
Name	BUSINESS
Description	xxx

**Name:** Name of subscriber group

**Description:** Description of subscriber group.

**Modified by:** The user who has made modifications in the list.

**Modified:** The date modification was made.

- **Identifier:** An identifier to the subscriber group in question
- **Name:** Name of the identified group
- **Description:** Description of the identified group.

## 5.13 Destination Groups



When this icon is selected it is high-lighted investigation Destination Groups is displayed. Settings for these groups are done as shown in the windows shown.

To detect if a subscriber is making calls to high number of national destinations, configuration has to be done to allow grouping of all national prefixes into national destinations groups. For this to work the threshold is set so that alarm is generated if a subscriber calls more than a given number of destinations within a given time



period. The configuration made here helps in generating multiple destinations alarm, which a generic alarms.

Destination Groups						
Name <input type="text"/>		<input type="button" value="Add"/>		<input type="button" value="Import"/>		<input type="button" value="Remove"/>
	Destinations	Name	Created by	Created	Modified by	Modified
>	837	<All>	basset	02/11/2007	basset	09/06/2009
	4	DestinationD	basset	09/06/2009	basset	09/06/2009
	4	DestinationC	basset	09/06/2009	basset	09/06/2009
	4	DestinationB	basset	09/06/2009	basset	09/06/2009
	4	DestinationA	basset	09/06/2009	basset	09/06/2009

The **Destination Groups** list contains groups that may contain one or more destinations. These fields are used to add destinations:

- **Name:** Add an arbitrary destination name.
- **Add:** Click to add a destination.
- **Import:** Used to import a destination or groups of destinations from Abacus which is the Basset's Rating Module. By clicking the import button the Abacus Global file opens and all available destinations are availed ready for importation.
- **Remove:** For deleting an already entered destination.

The information entered above are displayed in these fields

- **Destination:** Number of destinations in the group.
- **Name:** Name of the group

**Created by:** The user who created a partner in the list.

**Created on:** The date which a partner was entered in the list.

**Modified by:** The user who has made modifications in the list.

**Modified on:** The date modification was made.

By selecting a destination group all destinations that are configured in the selected destination group are displayed in the **Destinations** list.



Destinations						
Prefix: <input type="text"/>		Name: <input type="text"/>		<input type="button" value="Add"/>		<input type="button" value="Remove"/>
Enabled	Prefix	Name	Created by	Created	Modified by	Modified
<input checked="" type="checkbox"/>	07544*	07544 prefix	basset	12/09/2006	basset	12/09/2006
<input checked="" type="checkbox"/>	07732*	07732 prefix	basset	12/09/2006	basset	12/09/2006
<input checked="" type="checkbox"/>	07846*	07846 prefix	basset	12/09/2006	basset	12/09/2006

These fields are used to add prefixes:

**Prefix:** Enter prefix here.

- **Name:** Enter prefix name here.
- **Add:** Click to add both prefix and prefix name.
- **Remove:** Delete entered prefix.

The entered information is displayed in the following fields:

- **Enabled:** A tick  shows that a prefix is included in the selected group.  
A cross  shows that a prefix is included in another group than the selected while [ ] blank shows that a prefix is not included in any group.

- **Prefix:** Displays all added prefixes. Note that a prefix cannot be configured in more than one destination group.
- **Name:** Name of the prefix Group

**Created by:** The user who created a partner in the list.

**Created on:** The date which a partner was entered in the list.

**Modified by:** The user who has made modifications in the list.

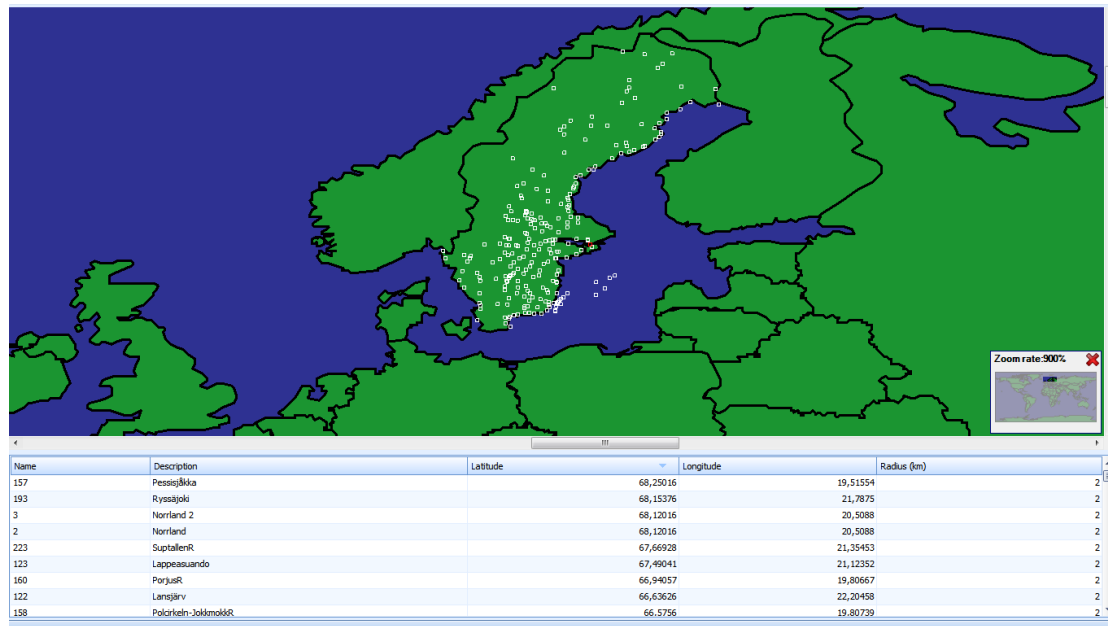
**Modified on:** The date modification was made.

## 5.14 Cell Sites



When this icon is selected it is high-lighted and the Cell Sites Window is displayed.

The window shows the world and the location of cell sites in the selected country. In the example below the map of Sweden and all the cell sites are displayed as dots.



The information below is uploaded from a file which the user prepares before hand.

**Name:** Name of the cell site.

**Description:** Description of the cell site.

**Latitude:** The latitude of the location of the cell site.

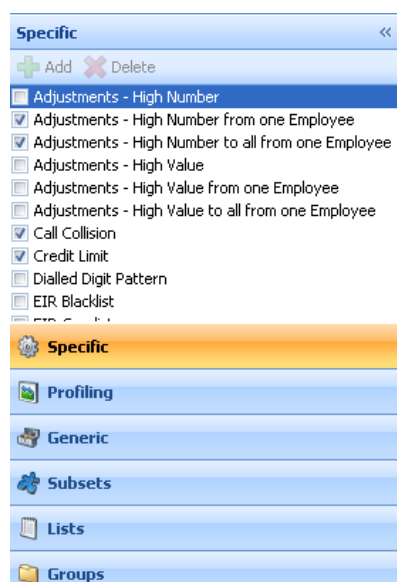
**Longitude:** The longitude of the location of the cell site.

**Radius:** The radius the cell site covers. A radius is not possible to specify if a default site radius is set.



## 5.15 Alarms

When this icon is selected it is high-lighted alarm setting menu is displayed and a list of alarms.



### 5.15.1 Alarms Pane

To set any of the alarms click on the either Specific, Generic or Profile depending on that type of alarms one intends to set.

To set Subset, Lists or alarm Groups click the right button on the menu.

Then tick the box besides the alarm that's to be set to open setting for that particular alarm.

### 5.15.2 Specific alarms

These are alarms that the user cannot create nor add new rules to, as opposed to Generic alarms where rules can be added and new alarms created.

#### 5.15.2.1 Adjustment alarm

There are six adjustment alarms in Watchdog i.e. *Adjustment High Number*, *High number from One Employee*, *High Number to all from one Employee*, *High Value*, *High value from one employee* and *High Value to all from one employee*.

#### 5.15.2.2 High Number of Adjustment alarm

The High Number of Adjustment alarm alerts if a subscriber receives a higher number of adjustments than allowed in a specified time period. These alarms are generated when Watchdog receives new adjustment files.

Specific		General	
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input checked="" type="checkbox"/> Adjustments - High Number <input checked="" type="checkbox"/> Adjustments - High Number from one <input checked="" type="checkbox"/> Adjustments - High Number to all from <input checked="" type="checkbox"/> Adjustments - High Value <input checked="" type="checkbox"/> Adjustments - High Value from one Er <input checked="" type="checkbox"/> Adjustments - High Value to all from c <input type="checkbox"/> Call Collision <input type="checkbox"/> Credit Limit	Name: Adjustments - High Numbe <input checked="" type="checkbox"/> Enabled	Severity: High (4)
		Number of Adjustments: 500	Time Period (hours): 1000
		<input type="text"/> Comment	

The below explanation applies to all Adjustment - high number alarms.

Select the alarm to set by ticking (checking) the box to the far left besides the selected alarm under the menu **Specific**. A number of parameters are displayed to the right under the **General** menu. The parameters available for setting are:

- **Name:** Name of the alarm
- **Severity:** The degree of importance for this alarm.
- **Number of adjustments:** Sets the number of allowed adjustments in a given time period. The time period is specified in the Time Period field.
- **Time period:** This displays the time period within which the count for the number of adjustments is made.

### 5.15.2.3 High Number Alarm definition

#### Adjustment – High Number

This alarm alerts when an employee exceeds the allowed number of adjustments than allowed in a specified time period.

#### Adjustment – High Number to all from one Employee

This alarm alerts when an employee exceeds the allowed number of adjustments to any subscriber.

#### Adjustment – High Number from one Employee

This alarm alerts when one employee is making adjustments higher than the number allowed or set in the threshold to a single subscriber.

### 5.15.2.4 High Value of Adjustment alarm

High Value alerts when an employee makes adjustments with a higher value than allowed to any subscriber.

Specific		General	
+ Add    ✕ Delete <input checked="" type="checkbox"/> Adjustments - High Number <input checked="" type="checkbox"/> Adjustments - High Number from one <input checked="" type="checkbox"/> Adjustments - High Number to all from <input checked="" type="checkbox"/> <b>Adjustments - High Value</b> <input checked="" type="checkbox"/> Adjustments - High Value from one Er <input checked="" type="checkbox"/> Adjustments - High Value to all from c <input checked="" type="checkbox"/> Call Collision <input checked="" type="checkbox"/> Credit Limit		Name: Adjustments - High Value <input checked="" type="checkbox"/> Enabled Severity: Medium (3) Value of Adjustments: 100 Time Period (hours): 1000 Comment:	

The below explanation applies to all Adjustment – high Value alarms.

Select the alarm to set by ticking (checking) the box to the far left besides the selected alarm under the menu **Specific**. A number of parameters are displayed to the right under the **General** menu. The parameters available for setting are:

- **Name:** The name of the alarm
- **Severity:** The degree of importance for this alarm.
- **Value:** Value of allowed adjustments during the time
- **Time period:** This displays the time period within which the count for the number of adjustments is made.

### 5.15.2.5 Adjustment – High Value Alarm definition

#### Adjustment – High Value

This alarm alerts when one subscriber receives adjustments with higher value than        allowed in a specified time period.

#### Adjustment – High Value to all from one Employee

This alarm alerts when an employee makes adjustments with a higher value than        allowed, to any subscriber. The alarm is generated when Watchdog receives new        adjustment files.

#### Adjustment – High Value from one Employee

This alarm alerts when one employee is making adjustments of higher value than        allowed or set in the threshold to a single subscriber.

### 5.15.2.6 Call collision

Call Collision alarm is generated when a Subscriber ID is making two calls at the same time, which could be an indication of cloning.

The screenshot displays the configuration window for the 'Call Collision' alarm. It is divided into two main sections: 'Specific' and 'General'.

**Specific Section:** Contains a list of alarm types with checkboxes. The 'Call Collision' option is selected and highlighted in blue. Other visible options include 'Adjustments - High Number', 'Adjustments - High Number from c', 'Adjustments - High Number to all t', 'Adjustments - High Value', 'Adjustments - High Value from one', 'Adjustments - High Value to all fro', 'Call Collision (Roaming)', 'Changed Account', 'Changed Subscription', 'Credit Limit', 'Dialled Digit Pattern', 'EIR Blacklist', 'EIR Greylist', and 'Failed Voucher Recharge'.

**General Section:** Contains configuration details for the selected 'Call Collision' alarm.
 

- Name:** Call Collision
- Severity:** High (4)
- Allowed Collision (sec):** 5
- Ignore same handset:** ☐
- Ignore same cell:** ☐
- Ignore calls classified as:** A list box containing 'Threeparty', 'CallWaiting', 'CallForwarding', 'Prepaid', 'Incoming', 'Outgoing', and 'Voicemail'. 'Threeparty' is currently selected.

Call collision has the following settings:

**Name:** Name of the alarm.

**Severity:** The degree of importance for this type of alarm.

**Allowed collision (sec):** This setting allows for overlapping time in a call collision, when the alarm could be caused by non-synchronized switches.

**Call flags to ignore:** Some call types always raise call collision alerts even if they are not call collision. These are false alarms that should not be generated. Examples of such false alarms occur when a call is put on hold while an ongoing call is being completed. These settings allow exclusion of such false alarms. Ignore such calls types by selecting and checking the box besides it.

#### 5.15.2.7 International Call Collision

**Observe:** International call collision has the exact same settings except that it for international calls is doing the comparison between roaming CDRs, sent to the operator by its' partners in TAP-files. This means the detection may be delayed by up to 48 hours. If the operator is using NRTRDE, the detection is quicker (down to 4 hours).

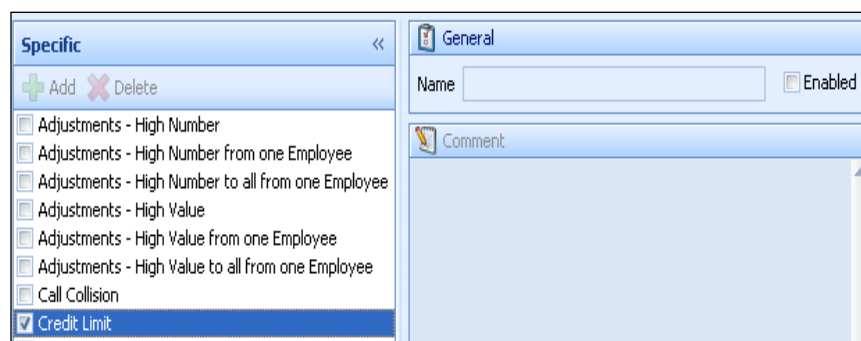
#### 5.15.2.8 Credit Limit

The credit limit alarm detects subscribers that exceed the credit limit set in the billing system. The alarm is based on call data, information that is sent from the billing system and alarm settings. The alarm is set to allow for detection before subscribers exceed the set credit limit.

For the alarm to work certain conditions must be fulfilled e.g. having information on each subscriber's credit limit and current account balance. Additional information that may be used in the analysis should be included in the credit limit calculation.




### Action

When Credit Limit alarm is selected windows displaying different settings are displayed.



Displayed in the **General** settings are:

- **Name:** Displays name of alarm.
- **Enabled:** Check to enable or activate the alarm.

<div>Status</div>							
<div> <div>Start</div> <div>Idle.</div> </div>							
<div>Bill Cycles</div>							
		Name	Description	Threshold ▲	From	To	Subscribers
>		a					190
		b					143
		c					141
<div>Tariff Plans</div>							
		Name	Description	Line Rent	Subscribers		
>		T3C10			1		
		T3C11			1		
		T3C12			1		

## Status settings:

- **Start:** Execution of the credit limit alarm
- **Idle:** No execution going on currently.

## Bill Cycles settings:

- **Name:** Name of the cycle.
- **Description:** A description of the cycle.
- **Threshold:**
- **From:** Time from which the credit limit is calculated.
- **To:** Time which the credit limits is calculation ends (otherwise if no field is selected watchdog will be set to calculate from the last invoice date according to the subscriber file and to today's date).
- **Subscribers:** The number of subscribers in the current bill cycle.

## Tariff Plans settings

- **Name:** Name of the tariff plan
- **Description:** A description of the tariff plan.
- **Line rent:** The line rent for the tariff plan.
- **Subscribers:** Number of subscribers using the current tariff plan.

## Alarm presentation

If alarms are generated they appear in the Alarms list as seen below.

Credit limit	126 GBP	Credit Limit Alarm(100+16.66)
Credit limit	230 GBP	Credit Limit Alarm(0+200+30)

The Info column contains details about each alarm.

Example: [Credit Limit Alarm: (100 + 16.6667 + 10)>100 % of 50 |

The following information is included:

(Unbilled + Line Rent + Balance) > Percentage of Credit limit of Actual Credit Limit.



### 5.15.2.9 Dialed digit pattern

The dialed digit pattern alarm detects if a subscriber is calling within a closed number range. This is an indication of hacking. The following settings are available this alarm.

**Severity:** The degree of importance.

**Time period:** The time within which the alarm us

**Threshold:** The number of calls that have to be made before the alarm is triggered.

**Number Serie:** This series is counted upwards or downward. See the example below,

Time for start of call	Called Bnumber	Lowest within span	Highest within span	Threshold
12:00:01	707107920	707107910	707107930	<b>Time Period:</b> 1 hour
12:00:02	707107921	707107911	707107931	<b>Threshold:</b> 10 calls
12:00:03	707107922	707107912	707107932	<b>Number serie</b> +10
12:00:04	707107923	707107913	707107933	
12:00:05	707107924	707107914	707107934	
12:00:06	707107925	707107915	707107935	
12:00:07	707107926	707107916	707107936	
12:00:08	707107927	707107917	707107937	
12:00:09	707107928	707107918	707107938	
12:00:10	707107929	707107919	707107939	
12:00:11	707107930	707107920	707107940	<b>Alarm</b>
12:00:12	707107931	707107921	707107941	

#### 5.15.2.10 EIR Blacklist

The screenshot shows a configuration window for 'EIR Greylist'. On the left, under the 'Specific' tab, there is a list of settings including 'Adjustments - High Number', 'Adjustments - High Number from one', 'Adjustments - High Number to all from', 'Adjustments - High Value', 'Adjustments - High Value from one Er', 'Adjustments - High Value to all from c', 'Call Collision', 'Credit Limit', 'Dialled Digit Pattern', 'EIR Blacklist', and 'EIR Greylist'. The 'EIR Greylist' option is selected. On the right, under the 'General' tab, the 'Name' field is set to 'EIR Greylist', the 'Enabled' checkbox is checked, and the 'Severity' dropdown is set to 'Medium (3)'. There is also a 'Comment' field.

The EIR alarm is specific for GSM networks.

An EIR, Equipment Identity Register, is used to prevent calls from stolen or unauthorized handsets. The switches will list call attempts from handsets that are not valid according to the EIR. Watchdog may collect these lists and display them for the user.

#### 5.15.2.11 Failed Voucher Recharge

The screenshot shows a configuration window for 'Failed Voucher Recharge'. On the left, under the 'Specific' tab, there is a list of settings including 'Adjustments - High Number', 'Adjustments - High Number from one Employee', 'Adjustments - High Number to all from one Empl', 'Adjustments - High Value', 'Adjustments - High Value from one Employee', 'Adjustments - High Value to all from one Employ', 'Call Collision', 'Credit Limit', 'Dialled Digit Pattern', 'EIR Blacklist', 'EIR Greylist', and 'Failed Voucher Recharge'. The 'Failed Voucher Recharge' option is selected. On the right, under the 'General' tab, the 'Name' field is empty, the 'Enabled' checkbox is checked, the 'Severity' dropdown is set to 'Medium (3)', the 'Time period (days)' spinner is set to 30, and the 'Number of failed recharges' spinner is set to 5. There is also a 'Comment' field.

This alarm is for detecting a subscriber who has tried to make a recharge but failed.

The setting for the alarm is:

**Severity:** The degree of importance of the alarm.

**Time period (days):** The time within the measurement is done.

**Number of failed recharges:** The number of recharges allowed before the alarm is triggered.

### 5.15.2.12 Velocity

The velocity alarm detects calls that are being made at the same time from the same handset and distance the between the locations that calls are being made are abnormally too far for a subscriber to have been at almost the same time. This is an indication of cloning. This alarm analyses roaming data to detect cloned phones that are used abroad.

The screenshot displays the configuration interface for the 'Velocity' alarm. It is divided into two main sections: 'Specific' and 'General'.

**Specific Section:** This section contains a list of various alarm types, each with a checkbox. The 'Velocity' alarm is currently selected and highlighted in blue. Other visible options include 'Adjustments - High Value from on...', 'Adjustments - High Value to all fro...', 'Call Collision', 'Call Collision (Roaming)', 'Changed Account', 'Changed Subscription', 'Credit Limit', 'Dialled Digit Pattern', 'EIR Blacklist', 'EIR Greylist', 'Failed Voucher Recharge', 'Prepaid Audit', 'Prepaid High Amount on Account', 'Prepaid High/Low Amount on Acco...', 'Prepaid Internal Fraud', 'Prepaid Multiple Refill of Account', 'Prepaid Voucher Reuse', 'Rating Validation', 'Roaming - First call ever is roamin...', 'Roaming - First roaming call', 'Routing Fraud', 'Service Fraud', 'Switch Audit', 'Transaction', 'Tumbling Handset', 'Tumbling Subscription', 'Velocity (Roaming)', and 'Zero Usage'.

**General Section:** This section contains configuration parameters for the selected 'Velocity' alarm.
 

- Name:** Velocity
- Severity:** High (4)
- Use common radius:** ☐
- Common radius (m):** 2 000
- Radius multiplier:** 2
- Use planar coordinates:** ☐
- Fudge missing last cell:** ☐
- Ignore same handset:** ☐
- Ignore calls classified as:** A list of call types with checkboxes. 'Threeparty' is selected. Other options include CallWaiting, CallForwarding, Prepaid, Incoming, Outgoing, Voicemail, NotRated, WAP, SMS, Roamer, MMS, VPN, TAP, UMTS, and Data.

The velocity analysis is a complement to the call collision alarm to detect cloning. This alarm detects cloning cases even if a call collision has not occurred. Watchdog analyses the moving patterns of the subscribers. If two calls have been made from two different locations, and the time between the calls indicates that it would be impossible to move between the locations the calls were made within the time span the calls occurred, an alarm is generated. The speed and distance settings are flexible and may be changed by the system administrator at any time.

- **Name:** Name of alarm
- **Enabled:** Select to activate the alarm.
- **Severity:** The degree of importance of the alarm.
- **Use common radius (m):** Select this option if the same cell site radius should be used for all cell sites.
- **Minimum distance (radius multiples):** The minimum distance a subscriber is allowed to travel with a speed up to what is specified in the Velocity column.
- **Use planar coordinates:** A coordinate system drawn on a flat surface, or plane. Planar coordinates are usually expressed as pairs of rectangular X,Y values.
- **Fudge missing last call:** to be defined.
- **Ignore same handset:** Select if to ignore same handset.
- **Ignore calls classifies:** Select to ignore call types.

#### 5.14.2.13 Velocity thresholds

Velocity Thresholds	
Minimum Distance	Threshold
Click here to add a new row	
0 m	83.33 m/s
250 m	700.00 m/s
700 m	1,500.00 m/s
210,000 m	138.89 m/s
400,000 m	277.78 m/s
1,000,000 m	333.61 m/s

The setting for distance and threshold is done in the velocity threshold window.

- **Minimum distance:** The minimum distance a subscriber is allowed to travel with a speed up to what is specified in the *threshold* column.
- **Threshold:** The speed a subscriber is allowed to travel with the distance set in the minimum distance column.
- **Click here to add:** Selected if the user wants to add minimum distance or threshold.

#### 5.15.2.14 Prepaid Audit

<b>Specific</b> << <div> <span>+</span> Add <span>×</span> Delete         </div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Adjustments - High Number</li> <li><input checked="" type="checkbox"/> Adjustments - High Number from one</li> <li><input checked="" type="checkbox"/> Adjustments - High Number to all from</li> <li><input checked="" type="checkbox"/> Adjustments - High Value</li> <li><input checked="" type="checkbox"/> Adjustments - High Value from one Er</li> <li><input checked="" type="checkbox"/> Adjustments - High Value to all from c</li> <li><input checked="" type="checkbox"/> Call Collision</li> <li><input type="checkbox"/> International Velocity</li> <li><input checked="" type="checkbox"/> Prepaid Audit</li> </ul>	<b>General</b> <div> Name <input type="text"/> <input type="checkbox"/> Enabled         </div> <div> Severity <input type="text" value="High (4)"/> </div> <div> Allowed lag (hours) <input type="text" value="53"/> </div> <div> Comment <input type="text"/> </div>
---	---

This alarm is generated if a prepaid customer, not activated in the prepaid platform, is making calls. The following parameters are available.

- **Name:** Name of alarm.
- **Enabled:** Select the On check box to activate the alarm.
- **Severity:** The grade of importance for this type of alarm.
- **Allowed lag:** A prepaid customer can fail to be in prepaid subscriber file delivered from the prepaid platform because they are new customers and that an updated file has not yet been delivered. To prevent Watchdog from generating alarm on such a customer, a lag time is set to allow for a specific period to elapse before an alarm is generated. The lag time is to allow a new file to arrive and hence not to create false alarms.

#### 5.15.2.15 Prepaid High Amount on Account

This alarm is generated if a prepaid customer's account balance, specified in the CDR, exceeds the alarm threshold. The following parameters are available.

- **Enabled:** Select the On check box to activate the alarm.
- **Severity:** The degree of importance of the alarm.
- **Max Amount:** If a subscriber's account balance reaches minimum of this amount, an alarm will be generated.

#### 5.15.2.16 Prepaid internal fraud

This alarm is generated if a prepaid customer makes calls that are not being registered in the prepaid platform. This is an indication of that the subscriber is activated

in the switch and not in the prepaid platform. The following parameters are available.

- **Enabled:** Select the alarm check box to activate the alarm
- **Severity:** The degree of importance for this type of alarm
- **Threshold:** Sets the threshold in percentage of the maximum difference in number of calls between the prepaid platform and the switch.
- **Min calls:** Sets the minimum number of calls before generating an alarm, this to avoid false alarms if only a number of calls has been made

## 5.15.2.17 Prepaid high/low amount on account

Settings by Prepaid Status					
Name	Comment	Minimum Amount	Maximum Amount	Severity	
Click here to add a new row					
Mansa Musa Okello	WDA test	1	500		
Kennedy Andersson	Manpower	909	3,999		
Jane Martha		200	1,000		
Bror Manza	En lurig liten rackare	20	100		
Ali Moses Johns	foobar	150	200		

This alarm allows Watchdog to process files from the prepaid platform that contains account balance and subscriber status. Thresholds may then be set for maximum or minimum amount per subscriber type.

- **Name:** A name for the subscriber.
- **Comment:** Comment on the account.
- **Max Amount:** The maximum account balance allowed.
- **Min Amount:** The minimum account balance allowed.
- **Severity:** The grade of importance for this type of alarm.

## 5.14.2.18 Prepaid multiple refill account

<b>Specific</b> << <div> <input checked="" type="checkbox"/> Add           <input checked="" type="checkbox"/> Delete         </div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Adjustments - High Number</li> <li><input checked="" type="checkbox"/> Adjustments - High Number from one</li> <li><input checked="" type="checkbox"/> Adjustments - High Number to all from</li> <li><input checked="" type="checkbox"/> Adjustments - High Value</li> <li><input checked="" type="checkbox"/> Adjustments - High Value from one Er</li> <li><input checked="" type="checkbox"/> Adjustments - High Value to all from c</li> <li><input checked="" type="checkbox"/> Call Collision</li> <li><input checked="" type="checkbox"/> Credit Limit</li> <li><input checked="" type="checkbox"/> Prepaid Multiple Refill of Account</li> </ul>	<b>General</b> <div> Name <input type="text"/> <input type="checkbox"/> Enabled         </div> <div> Severity <input type="text" value="Medium (3)"/> </div> <div> Time Period (hours) <input type="text" value="24"/> </div> <div> Max Recharges <input type="text" value="5"/> </div> <div> Comment <input type="text"/> </div>
---	---

This alarm is generated if a prepaid customer loads his account more times than the alarm threshold. The following parameters are available.

- **Enabled:** Select the alarm check box to activate the alarm.
- **Severity:** The degree of importance for this type of alarm
- **Time period:** The time period's sets during what time period the alarm should count the number of adjustments.
- **Max Recharges:** Sets the maximum number of recharges during the configured time period.

#### 5.15.2.19 Prepaid Voucher reuse

Load several accounts with same voucher. This alarm is generated if several prepaid accounts have been loaded using the same voucher (PIN code). The available settings are:

- **Enabled:** Select the alarm check box to activate the alarm.
- **Severity:** The grade of importance for this type of alarm.

#### 5.15.2.20 Rating Validation

Settings by Call Type					
Enabled	Call Type	Relative Difference	Absolute Difference	Severity	
<input checked="" type="checkbox"/>	Local	0 %	0		3
<input checked="" type="checkbox"/>	Long Distance	0 %	0		1
<input type="checkbox"/>	International	0 %	0		3
<input checked="" type="checkbox"/>	Premium Rate	120 %	20,000		3
<input checked="" type="checkbox"/>	Roaming	10 %	0		3
<input checked="" type="checkbox"/>	Data	5 %	0		3
<input type="checkbox"/>	Visiting Roamer	9 %	0		3
<input checked="" type="checkbox"/>	Mobile	0 %	0		3

The Rating Validation alarm allows for the comparison of the pricing done in the prepaid platform and Watchdog. If the pricing differs more than the threshold an alarm is generated. The thresholds may be set per call type. In other words the rating validation alarm allows comparing the pre-rated CDRs with the Basset rating module price.

The available settings are;

- **Enabled:** Select box to activate the alarm
- **Call type:** The type of call to be validated.
- **Relative difference:** If the pre-rated CDR and the Watchdog rating differs more than X percent an alarm is generated.
- **Absolute difference:** If the pre-rated CDR and the Watchdog rating differs more than X local money an alarm is generated
- **Severity:** The grade of importance for this type of alarm

#### 5.15.2.21 Roaming-first call ever roaming

This alarm is generated if the first call after activation is a roaming call.

The parameters available are;

**Enabled:** Select to activate the alarm.

**Severity:** The grade of importance for this type of alarm

#### 5.15.2.22 Roaming – first roaming call

This alarm is generated when the subscriber is making their first roaming call.

The parameters available are;

**Enabled:** Select to activate the alarm.

**Severity:** The grade of importance for this type of alarm

#### 5.15.2.23 Routing fraud

The routing fraud alarm is generated when traffic is sent via non-agreed trunks/routes. This information is read by Watchdog from an external file.

The parameters available are;

- **Enabled:** Select to activate the alarm.
- **Severity:** The grade of importance for this type of alarm.

#### 5.15.2.24 Service fraud

An alarm will be generated if a subscriber is using services that are not included in

The screenshot displays the Watchdog Fraud configuration window. It is divided into two main sections: 'Specific' and 'General'. In the 'Specific' section, a list of fraud types is shown with checkboxes, and 'Service Fraud' is currently selected. The 'General' section contains configuration options for the selected alarm, including a text field for 'Name', a dropdown for 'Severity' set to 'Medium (3)', and a list of 'Call flags to ignore' with checkboxes for 'Threeparty', 'Callwaiting', 'Callforwarding', 'Prepaid', 'Incoming', 'Outgoing', 'Voicemail', 'NRTRDE', and 'HUR'.

the subscription. If a subscription includes only national calls, an alarm will be generated if a subscriber makes e.g. international calls. The parameters available are;

**Enabled:** Select to activate the alarm.

**Severity:** The grade of importance for this type of alarm.



**Ignore flags:** Select the services that the used services alarm should ignore

#### 5.15.2.25 Switch Audit

This alarm detects subscribers that are activated in the switch but not in the billing system. Each subscriber identity, found in the call data, is matched to the customer database. If a match isn't found, it means that someone is making calls without being in the billing system. This may be an indication of fraud. The reason may also be as simple as that the customer database is not yet updated hence the need for the time lag to prevent false alarms. The parameters available are;

- **Enabled:** Select to activate the alarm.
- **Exclude roamers:** Visiting roamers are normally not included in the customer database. All their calls would hence generate this alarm. Select this option to exclude visiting roamers from the switch audit analysis
- **Allowed lag:** The maximum number of hours a subscriber is allowed to be active in the switch without being active in the customer database.
- **Severity:** The grade of importance for this type of alarm.

#### 5.15.2.26 System event

This alarm is triggered every time there is an error e.g. failed auto mail, report etc.

#### 5.15.2.27 Transaction

Transaction alarm is triggered whenever a subscriber is denied or prevented from carrying out any form of transaction.

### 5.15.2.28 Tumbling subscription

Specific		General	
<input type="checkbox"/> Add <input type="checkbox"/> Delete		Name	Tumbling Subscription <input checked="" type="checkbox"/> Enabled
<input checked="" type="checkbox"/> Adjustments - High Number <input checked="" type="checkbox"/> Adjustments - High Number from one <input checked="" type="checkbox"/> Adjustments - High Number to all from <input checked="" type="checkbox"/> Adjustments - High Value <input checked="" type="checkbox"/> Adjustments - High Value from one Er <input checked="" type="checkbox"/> Adjustments - High Value to all from c <input checked="" type="checkbox"/> Call Collision <input checked="" type="checkbox"/> Credit Limit <input checked="" type="checkbox"/> Dialed Digit Pattern <input checked="" type="checkbox"/> EIR Blacklist <input checked="" type="checkbox"/> EIR Greylist <input checked="" type="checkbox"/> Tumbling Subscription		Severity	Medium (3)
		Tumblings Allowed	4
		Entities Allowed	2
		Time Period (hours)	48
		Comment [Empty text area]	

The alarm **Tumbling subscriber** detects when one handset (ESN/IMEI) is being used by many different subscribers (MIN/IMSI). The following parameters are available for this alarm.

- **Name:** Name of alarm.
- **Severity:** The degree of importance of the alarm.
- **Tumblings allowed:** The number of tumblings that are allowed during the time span set in *Time Period*. For this alarm, the number of tumblings means the number of different subscribers (IMSI/MIN) that are allowed to use the same handset (IMEI/ESN).
- **Entities Allowed:** The number of subscribers allowed use of the same handset and not generate an alarm. If two subscribers repeatedly switch between the same handset, each switch is counted as a tumbling event.
- **Time period:** Calculation for the tumblings is done within the period given here. The period is usually 24 hours but any convenient amount of time can be given.

### 5.15.2.29 Excluded handset

Excluded Handsets		
Handset Id	Hexadecimal	Comment
Click here to add a new row		
355015324568451	<input type="checkbox"/>	Stolen SIM in this handset
35570802217*	<input type="checkbox"/>	Customer care series
355708022174*	<input checked="" type="checkbox"/>	Stolen shipment
355708022174941	<input checked="" type="checkbox"/>	Suspect dealers handset
355708022174942	<input type="checkbox"/>	Stolen shipment
355708022174943	<input checked="" type="checkbox"/>	Stolen shipment
355708022174945	<input checked="" type="checkbox"/>	Suspect dealers handset
355708022174946	<input type="checkbox"/>	Stolen shipment
355708022174949	<input checked="" type="checkbox"/>	Suspect dealers handset
355708022174989	<input type="checkbox"/>	Stolen SIM in this handset
355708022274*	<input checked="" type="checkbox"/>	Stolen shipment

IMEI numbers added to this list will not be included in the analysis for tumbling subscribers. This is useful e.g. if there are handsets that are used with different SIM cards for test purposes or for rented handsets.

- **Handset ID:** To add an IMEI number to this list on the first row in the window and enter the handset ID (IMEI).
  - **Hexadecimal:** Check the box if the value that has been entered is a hexadecimal.
  - **Comment:** A comment why the IMEI number has been added to the list
- NOTE: The list is shared by both subscription and handset tumbling.**

### 5.15.2.30 Tumbling handset

Specific	General
<div> <div> <div>+</div> Add <div>×</div> Delete </div> <div> <input checked="" type="checkbox"/> Adjustments - High Number <input checked="" type="checkbox"/> Adjustments - High Number from one <input checked="" type="checkbox"/> Adjustments - High Number to all from <input checked="" type="checkbox"/> Adjustments - High Value <input checked="" type="checkbox"/> Adjustments - High Value from one Er <input checked="" type="checkbox"/> Adjustments - High Value to all from c <input checked="" type="checkbox"/> Call Collision <input checked="" type="checkbox"/> Credit Limit <input checked="" type="checkbox"/> Dialled Digit Pattern <input checked="" type="checkbox"/> EIR Blacklist <input checked="" type="checkbox"/> EIR Greylist <input checked="" type="checkbox"/> Failed Voucher Recharge <input checked="" type="checkbox"/> Tumbling Handset </div> </div>	<div> <div> <div>Name</div> <div>Tumbling Handset</div> <div><input checked="" type="checkbox"/> Enabled</div> </div> <div> <div>Severity</div> <div>Low (2)</div> </div> <div> <div>Tumbings Allowed</div> <div>4</div> </div> <div> <div>Entities Allowed</div> <div>2</div> </div> <div> <div>Time Period (hours)</div> <div>48</div> </div> <div> <div>Comment</div> <div></div> </div> </div>

- **Name:** Name of alarm.
- **Severity:** The degree of importance of the alarm.
- **Tumbings allowed:** The number of tumbling's that are allowed during the time span set in *Time Period*. For this alarm, the number of tumbings means the number of different subscribers (IMSI/MIN) that are allowed to use the same handset (IMEI/ESN).
- **Entities Allowed:** The number of subscribers allowed use of the same handset and not generate an alarm. If two subscribers repeatedly switch between the same handset, each switch is counted as a tumbling event.
- **Time period:** Calculation for the tumbings is done within the period given here. The period is usually 24 hours but any convenient amount of time can be given.

### 5.15.2.31 Zero Usage

Specific	General
<div> <div> <div>+</div> Add <div>×</div> Delete </div> <div> <input checked="" type="checkbox"/> Adjustments - High Number <input checked="" type="checkbox"/> Adjustments - High Number from one <input checked="" type="checkbox"/> Adjustments - High Number to all from <input checked="" type="checkbox"/> Adjustments - High Value <input checked="" type="checkbox"/> Adjustments - High Value from one Er <input checked="" type="checkbox"/> Adjustments - High Value to all from c <input checked="" type="checkbox"/> Call Collision <input checked="" type="checkbox"/> Credit Limit <input checked="" type="checkbox"/> Dialled Digit Pattern <input checked="" type="checkbox"/> EIR Blacklist <input checked="" type="checkbox"/> EIR Greylist <input checked="" type="checkbox"/> Zero Usage </div> </div>	<div> <div> <div>Name</div> <div>Zero Usage</div> <div><input checked="" type="checkbox"/> Enabled</div> </div> <div> <div>Severity</div> <div>Medium (3)</div> </div> <div> <div>Time Period (days)</div> <div>20</div> </div> <div> <div>Days until next alarm</div> <div>1</div> </div> <div> <div>Comment</div> <div></div> </div> </div>

As opposed to the high usage alarm, Watchdog offers a zero usage alarm. If a subscription is not used for a specified period of time, an alarm will be generated.

- **Name:** Name of alarm.
- **Severity:** The degree of importance of the alarm.
- **Time period (days):** The Time Period specifies the time span during which a subscription should remain unused before an alarm is generated.
- **Days until Next Alarm:** If an alarm has been generated, a new alarm will be generated if the subscription is unused still when this number of days have passed

### 5.15.3 Profiling

The screenshot shows the 'Profiling' configuration window. On the left, under the 'Profiling' tab, there are 'Add' and 'Delete' buttons, and a list of items with checkboxes: 'Local Amount', 'Long Distance Amount', 'Long Distance nbr of calls', 'Local Duration', and 'Long Distance Duration' (which is selected). On the right, under the 'General' tab, the configuration for the 'Long Distance Duration' alarm is shown. It includes a 'Name' field with 'Long Distance Duration', an 'Enabled' checkbox, a 'Severity' dropdown set to 'Medium (3)', a 'Call Type' dropdown set to 'Long Distance', a 'Measurement' dropdown set to 'Duration', a 'Percentage' spinner set to '200 %', and an 'Absolute' spinner set to '3,600'. At the bottom, there is a 'Comment' field.

The profiling alarm generates alarms per each individual subscribers calling behaviour. If the calling behaviour changes (increases or decreases) around a certain threshold, an alarm is generated. The alarm calculates a daily average for the reference period and the check period, then compares it to the set threshold.

Profiling uses two periods for calculation:

**Check period:** Last 2 days call behaviour.

**Reference period:** Last 10 days call behaviour.

Watchdog calculates if there has been a change in call behaviour during the check period as compared to the reference period. The data is based on the Watchdog Alarms statistics. This means that the periods may be longer than the data stored in calls history. Please note that the number of days to store the statistic is changed in WatchdogAlarms.

**Note:** The reference period and check period cannot be changed by the user.

The following parameters should be specified.

- **Name:** The name of the alarm, the name will be visible in the alarm list.
- **Enabled:** Check to activate the alarm
- **Severity:** The degree of importance for this alarm.
- **Call type:** The call type specifies for which type of call type the alarm should be generated.
- **Measurement:** The item that is to be measured.
- **Percentage:** The allowed difference between the reference period and check period. The difference is written in percent and to write a threshold for an increasing behaviour write the threshold in a positive value, the opposite for a decreasing behaviour
- **Absolute:** The minimum amount, number of call or duration that must be reached by a subscriber during the reference or check period before Watchdog starts doing the *measurement*. This is to avoid false alarms.

#### 5.15.4 Generic Alarms

The generic alarms allow the Watchdog user to configure alarms with great flexibility. By adding rules in the alarm setting, the alarm can be tailored to detect a particular type of fraud in the network. The rules may be based on both CDR and subscriber data. This allows for a great flexibility from the operator side since the operator can choose the information to be included in the subscriber file.

#### Generic alarms pane

**Generic** <<

+ Add - Delete

- ☐ Blacklisted Handsets
- ☐ Blacklisted Number
- ☐ Call Record Validation
- ☒ Destinations - Multiple
- ☐ Extended Services
- ☐ Global Fraud
- ☒ High Risk Cell Sites
- ☒ High Risk Countries
- ☒ High Usage - Long - All
- ☐ High Usage - Long - International
- ☐ High Usage - Long - Local
- ☐ High Usage - Long - Long Distance
- ☐ High Usage - Long - Mobile
- ☐ High Usage - Long - Roaming
- ☐ High Usage - Medium - All
- ☐ High Usage - Medium - GPRS
- ☐ High Usage - Medium - International
- ☐ High Usage - Medium - Local
- ☐ High Usage - Medium - Long Distance
- ☐ High Usage - Medium - Mobile
- ☐ High Usage - Medium - Roaming
- ☐ High Usage - Short - All
- ☐ High Usage - Short - GPRS
- ☐ High Usage - Short - International
- ☐ High Usage - Short - Local
- ☐ High Usage - Short - Long Distance
- ☐ High Usage - Short - Mobile
- ☐ High Usage - Short - Roaming
- ☐ High Usage - Single Call - International
- ☐ High Usage - Single Call - Local
- ☐ High Usage - Single Call - Long Distance
- ☐ High Usage - Single Call - Mobile
- ☐ High Usage - Single Call - Roaming
- ☐ High Usage Alarm
- ☐ HotListed Handset

**General**

Name: High Usage - Long - All

Type: Generic Alarm

Severity: Medium (3)

**Limits**

Name	Value
<input checked="" type="checkbox"/> Time period (seconds)	1209600
<input checked="" type="checkbox"/> Amount	7000
<input type="checkbox"/> Number of events	0
<input checked="" type="checkbox"/> Duration (seconds)	10000
<input type="checkbox"/> Percentage of amount	0
<input type="checkbox"/> Volume downloaded (bytes)	0
<input type="checkbox"/> Volume uploaded (bytes)	0
<input type="checkbox"/> Volume total (bytes)	0
<input type="checkbox"/> Percentage of duration	0
<input type="checkbox"/> Volume downloaded higher than uploaded (percent)	0
<input type="checkbox"/> Volume uploaded higher than downloaded (percent)	0

☐ Match all

☐ Use multipliers

**Comment**

The generic alarms pane contains all the configured alarms, the limits that are allowed by the user. The following parameters are available:

**Generic:** The alarms list.

**Name:** A logical alarm name. The name will be visible in the alarms list and in the reports section

**Type:** The type identifies the kind of alarm. Currently there are five different types available.

**Generic alarms:** Allows the user to create an alarm that alerts if a subscriber is calling as per the set rules but exceeds the limits.

**Global fraud alarm:** Alerts if a subscriber is calling more international destinations than allowed or set in the threshold.

**Same called number alarm:** Alerts if a subscriber is calling the same B-number more times than allowed or set in the threshold.

**Destination fraud:** A generic destination fraud alerts if a subscribers calls more national destinations than the threshold.

**Single call:** Allows a user to create an alarm that alerts if a subscriber is that exceeds the limits.

**Severity:** Set the importance of the alarm. 1 being the lowest severity while 5 is the highest.

- **Limits:** The limits set the threshold for the alarm, when the threshold is exceeded an alarm is generated, as long as the rules are true for the call. Depending on type (of alarm) there are different limits settings. Some of the available watchdog limits are:
  - **Time period:** Sets the period in which the system should read the CDR's. The time period is calculated from the last CDR, in seconds.
  - **Amount:** Allows for the setting of threshold for the value of the calls. The pricing used is configured in Watchdogs rating module Abacus.
  - **Number of Events:** The Number of Events limit allows setting a threshold for the number of calls from a subscriber.
  - **Duration:** Allows for the setting of the threshold for the total duration of calls from a subscriber.
  - **Percentage of Amount:** This threshold is calculated on the total Amount of the subscriber's call within the time period. The set percentage applies to the rule, i.e. the amount produced by the calls set by the rule should not be above a certain percent of the total amount of all calls.

**Example:**

Time Period	= 86400
Calltype	= International
Percentage of Amount	= 10%
Amount	= 100
Match All	= Checked

If the above settings were used an alarm would trigger if at least 10% of **all calls** during the set time period for one subscriber come from CDRs where call type is *international* **and** the value of the *international* calls are greater than 100. "Match All" setting means that all the above conditions must be fulfilled for an alarm to generate. If it's not checked any one of the above conditions would trigger an alarm.

- **Volume Downloaded:** Alerts if the total downloaded volume exceeds the threshold for the configured time period.
- **Volume Uploaded:** Alerts if the total uploaded volume exceeds the threshold for the configured time period.
- **Volume Total:** Alerts if the total volume exceeds the threshold for the configured time period.
- **Volume Downloaded:** Alerts if the total downloaded volume exceed the threshold for the configured time period.
- **Uploaded:** If it is configured to 100 means that the downloaded volume must be 100% greater than the uploaded during the configured time period before the alarms should be generated.
- **Volume Uploaded higher than Downloaded:** The Volume Uploaded higher than Downloaded setting is written in percentage form. If it is configured to 100 means that the uploaded volume must be 100% greater than the downloaded during the configured time period before the alarms should be generated.
  - **Value:** Alarm name
  - **Name:** Threshold value

**Match all:** Check if all the limits (conditions) have to be met the alarm to triggered.

**Use multipliers:** Check to allow for multipliers to be used for this alarm.

**Note: There are different settings for different alarms.**

The alarms described below are configured as standard generic alarms; however other alarms may be added if and when the user wishes.



#### **5.15.4.1 Blacklist**

It is possible to blacklist telephone numbers (A numbers), telephone units, and cell sites. This means that Watchdog will generate alarms each time any of the listed items are being used. This alarm is for investigating the behaviour certain subscribers or to survey traffic from a given area.

#### **5.15.4.2 Global fraud**

This alarm is generated if a subscriber calls more than a specified (allowed) number of different countries within a specified (allowed) period of time.

#### **5.15.4.3 High-risk cell sites**

This alarm is a complement to the high usage alarm, enabling lower thresholds for calls from certain cell sites. The settings include a list of all cell sites that should be considered as high-risk cell sites, and thresholds for each item.

#### **5.15.4.4 High-risk countries**

This alarm is a complement to the high usage alarm, enabling lower thresholds for calls to certain countries. The settings include a list of all countries that should be considered as high-risk countries, and thresholds for each item. If calls are

#### **5.15.4.5 High usage**

The high usage alarms detect subscribers making calls representing high amounts of money. The number of time periods is flexible, as the duration of each period. The high usage alarm may be based on different quantitative units, such as monetary value, duration, number of calls, and percentage of total monetary value.

#### **5.15.4.6 Hotlist**

It is possible to hotlist telephone numbers (B numbers), telephone units, and cell sites.

This means that Watchdog will generate alarms each time a call is made to any of the listed items. This alarm may be used e.g. to investigate which subscribers that are using a certain service.

#### **5.15.4.7 Multiple destinations**

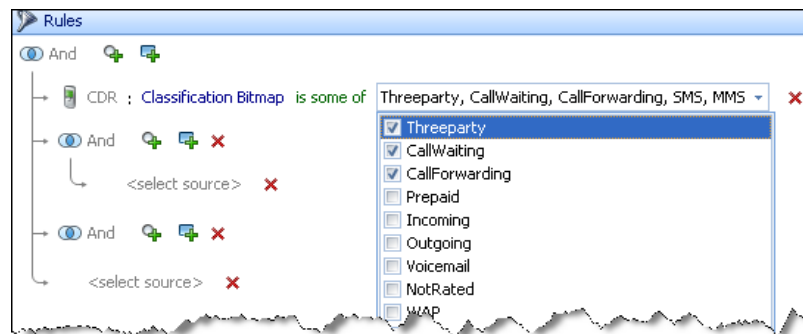
The multiple destinations alarm detects if a subscriber calls a high number of national destinations. The alarm configuration allows grouping of all national prefixes into national destinations groups; the threshold is set as calling above a number of destinations within a time period.

#### **5.15.4.8 Same called number**

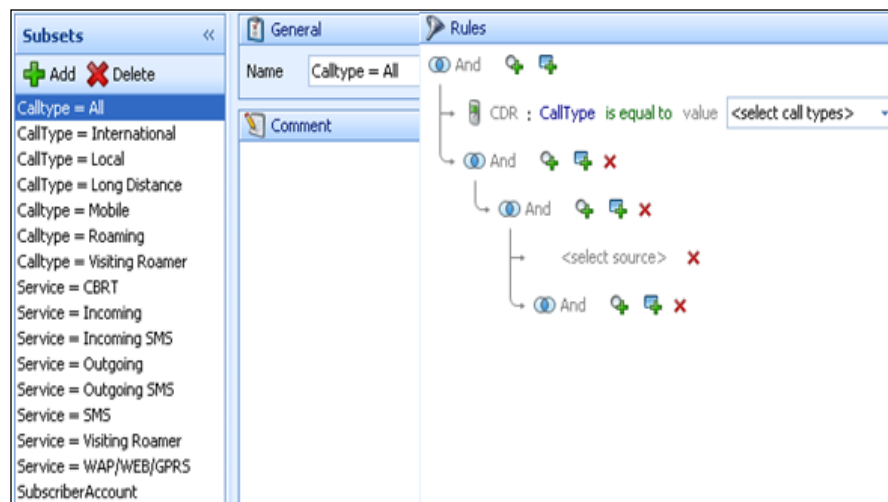
This alarm is generated if subscriber calls the same number more than a specified number of times and within a specified period of time.

#### 5.15.4.9 Short duration calls

If a subscriber exceeds a number of short duration calls, an alarm will be generated.



#### 5.15.5 Subsets



A subset is group of rules that are re-used in more than one alarm. The subset facilitates the administration and enhances the efficiency of the system. For example in a case where e.g. 4 different generic alarms that are using the same rules to generate alarms, but are all using different thresholds. The best practice would be to first create a subset with all the rules, which encompasses all the 4 different alarms. Then set the generic alarm to use the subset as a rule, but with different thresholds. The following are in the menu.

- **Subsets:** The created subsets.
  - **Add:** Click to add a new subset.
  - **Delete:** Delete an already created subset.
- **General:** Displays name of the current subset.
- **Rules:** Rules for the current alarm are set here.

### 5.15.6 List

A list is used in a generic alarm as a rule for alarm creation. The list is included in alarms like black-list, hot list, high-risk countries and exclusions.

A rule that is configured to look in a list is using the IN () function. Depending on the criteria of the matching against the list the values should either match or not match.

- **Name:** The name of the list, which describes what kind of information the list contains.
- **Type:** Specify for example country and site (location).
- **Comment:** Any necessary comments about the alarm.

#### List contents

Value	Comment	Expiration
0717374614		07/10/2006
0713123134	Abdul	07/10/2006
0713123335	Omal	07/10/2006
0713123306	Elpidy	07/10/2006
0713123551	Dotto	12/10/2006

The contents list has the parameters below:

**Value:** Value of the items in the list e.g. IMSI, IMEI etc.

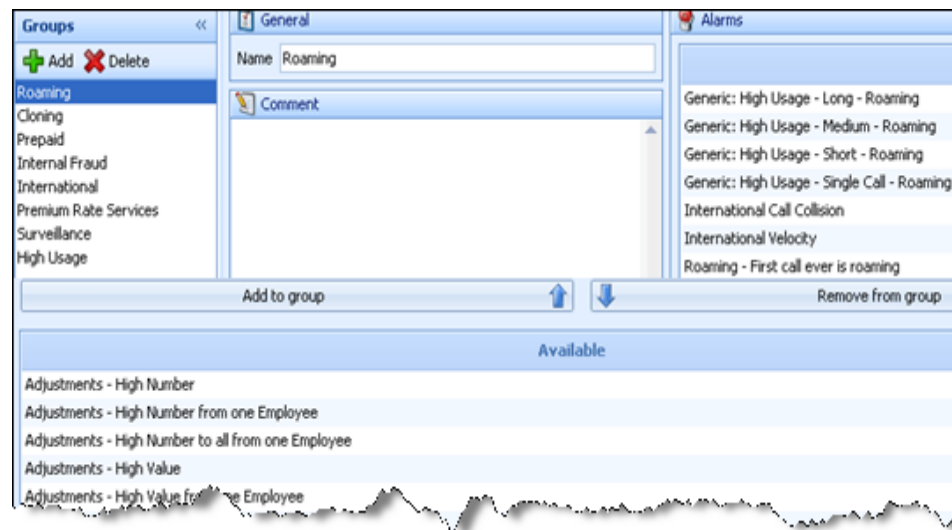
**Comment:** A comment for the value. The comment will be shown in the information field of the alarm.

**Add manually:** Add the values manually. The button is not activated until something is written in the field next to it.

**Add:** Select and add values from the contents list.

**Expiration:** The time until the value is automatically removed from the list by the system. The date time picker sets the value.

### 5.15.7 Groups



The alarms groups are used to group several alarms under one umbrella. This is used mainly in the Risk Assessment, in order to facilitate the risk assessment procedure.

For example under surveillance group, the following alarms can be assembled; blacklisted handsets, blacklisted number, hotlisted handset, hotlisted number etc. The groups are used in for risk assessment. See risk assessment- Alarm Groups- 5.2.1.

- Groups: Alarms groups.
  - **Add:** Used for adding a group alarm.
  - **Delete:** Used for deleting a group alarm.
- General:
  - **Name:** Name of the group alarm
  - **Comment:** Comment on the group alarm.
- Alarms: The alarms that are contained in the current group.
- Add group: Used for adding an alarm to the group alarm.
- Remove group: Used to remove an alarm from a group alarm.