
# 4TimeWeb Short Manual

# 4TimeWeb Short Manual



Printed: maj 2013 in (whereever you are located)

# Contents

# Chapter

# 1 Introduction

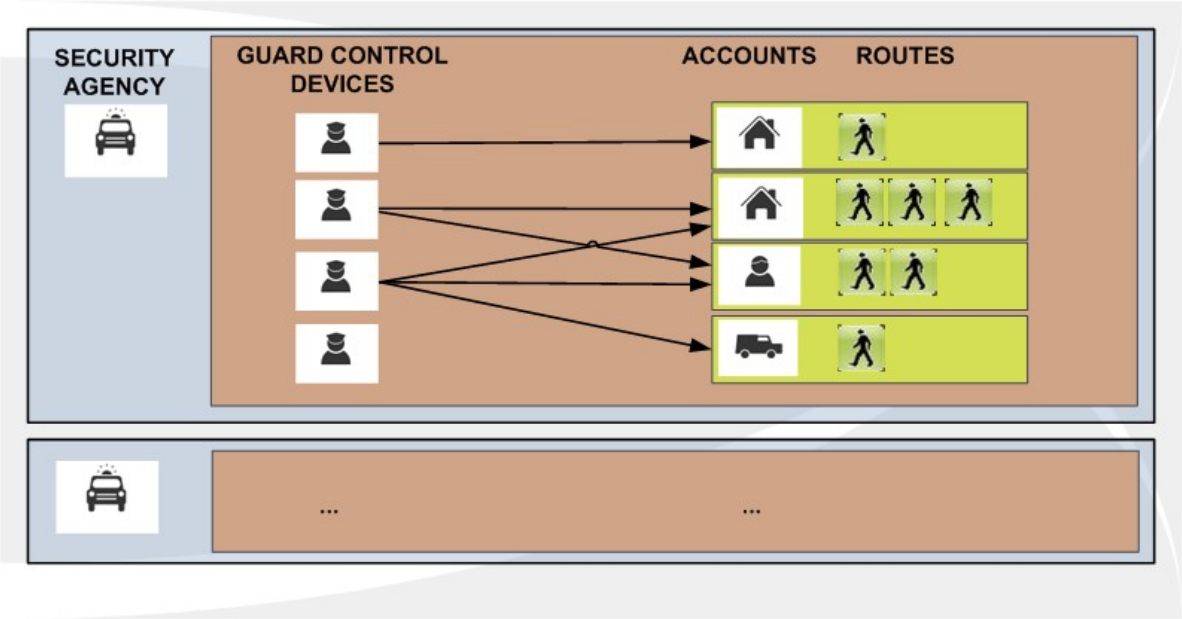
4TimeWEB is a system for monitoring active guard control devices, and is intended for operation in dispersed networks. The system is designed for security agencies, or for end customers, with access available via a web browser.

The 4TimeWEB system is currently available in beta version. This means that the functions described may be different in the final version. Client functionality will be added in future versions of the system.

## Basic terminology

### Terminology

- **Security Agency -** a company providing physical protection services, whose personnel are equipped with work control devices
- **Devices -** devices for monitoring the time, place and effectiveness of guards' work in real time
- **Account -** a client account (building, person or vehicle) equipped with a tag that can be read by the monitoring device
- **Route** - a round route defined using tags

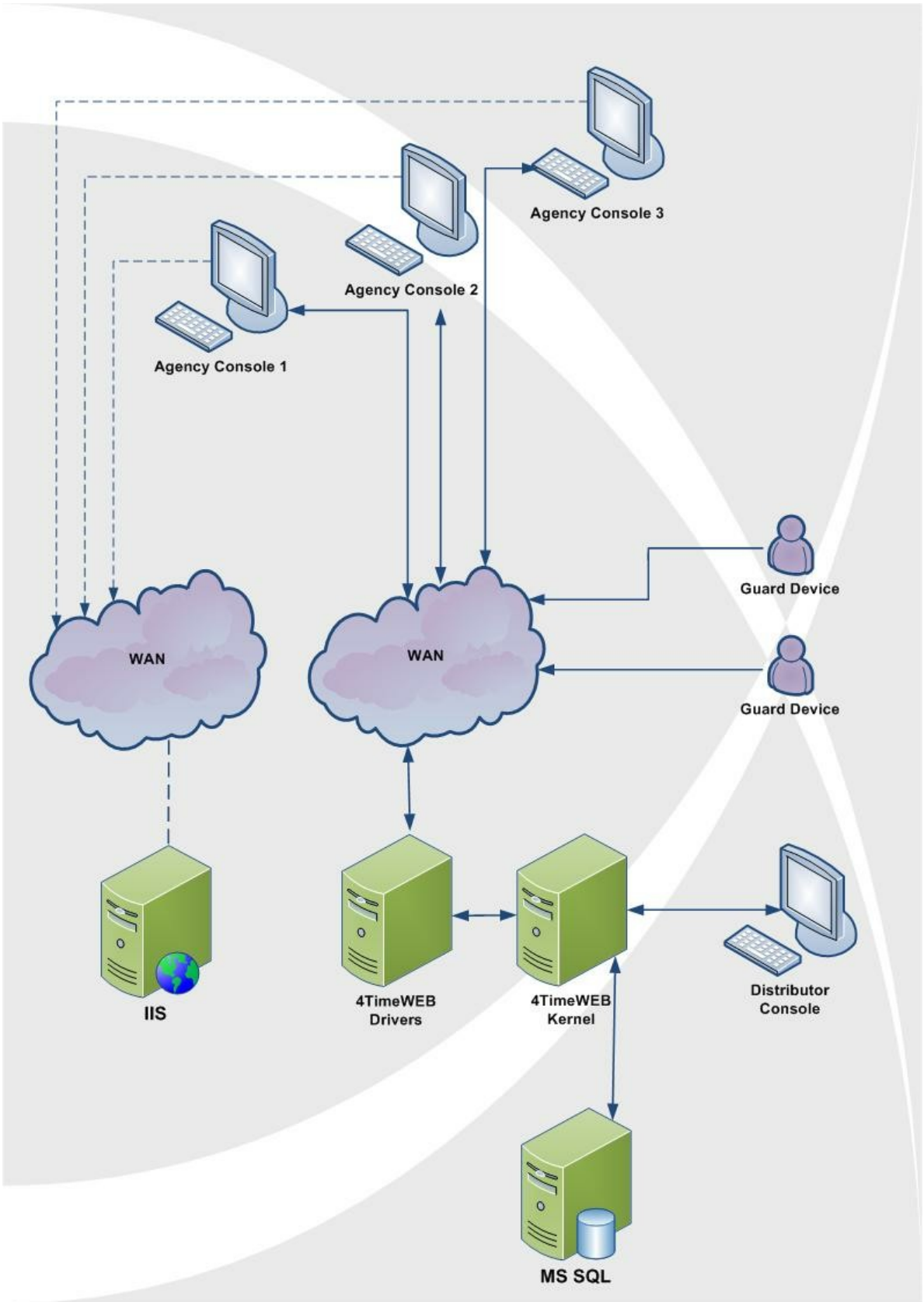



## General system structure

The 4TimeWEB system is a fully network-based solution designed using three-tier modular architecture.

The central module is a Kronos NET system Kernel, which is responsible for e.g. signal processing, providing data from the database, and monitoring the work of the other modules.

The diagram below shows an example structure. For simple installations, all the modules can be installed on one computer.



The Security Agency Consoles do not require installation - they are downloaded and run from a web browser once the link to the MS IIS server on which they are located is given.

## Hardware requirements

Chapter currently under construction

## Licence control

The program is protected from unauthorized use and copying by Alladin HASP keys. These keys are specially prepared for the manufacturer and can not be substituted with others. The key is required for the program to function correctly, and must be connected to the computer where Kernel is installed. A Remote HASP driver can also be used which will send license data to Kernel from a HASP key connected to another computer with a USB port.

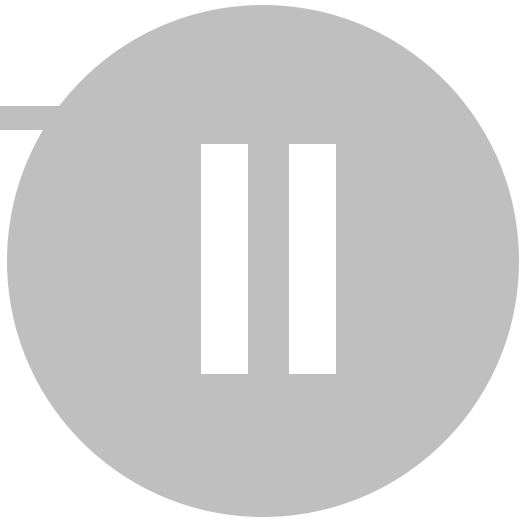
In the case of the subscription version, responsibility for updating the key rests with the system user.

Violation of restrictions on the number of accounts monitored and the product validity as contained in the key result in the system immediately ceasing operation and is considered by the manufacturer to be a violation of copyright and property law.

The programme works without a key for a maximum of 5 active devices. This option, however, is purely for testing purposes and cannot be used commercially.

The licensor and their distributors provide the software on an AS IS basis. The manufacturer accepts no responsibility for fulfilling expectations regarding system functionality, or for possible system faults and any losses incurred as a result of these errors.

# Chapter



# 2 Quick start - distributors

The following tutorial allows you to quickly familiarize yourself with the 4TimeWeb system for Distributors. The instructions in the following chapters are purposefully concise so that you can start using the program and its functions as soon as possible. The goal is not to learn every detail, but to familiarize yourself with the basic principles and operation of the system.

For more detailed information on the functions described in the tutorial, please refer to the chapters on specific functions and modules where you can find more useful information and a description of the advanced features of the 4TimeWeb system.

Distributor modules require installation and correct system configuration.

## 2.1 System installation

This chapter aims to guide you in the easiest way through the installation and configuration of the programme, and familiarise you with the types and system components.

### Terminology

- **Module -** any system console, Kernel, drivers or tools programmes that are components of the 4TimeWeb system.
- **Kernel -** the central system module responsible for signal processing, providing data from the database, and monitoring the work of the other modules.
- **Console -** a family of modules that allows the user to work with the system, e.g. monitoring, billing or data entry.
- **Driver** - a family of modules that enables communication between external devices and the 4TimeWeb system.
- **Tools programmes** - programmes for system and database management, configuration and diagnostics.
- **HASP key -** a device containing 4TimeWeb licence information.
- **MSSQL -** a high performance Microsoft database server, either the free or commercial version.

## Consoles

### Administration Console

This module is for entering Security Agency data, as well as the devices required to service monitored accounts. Monitoring parameters and Security Agency billing can be controlled from here.

### Security Agency Console

This module is accessible via a web browser and is used by Security Agencies to enter, edit and monitor their accounts and devices.

> Security Agency Console installation requires Microsoft IIS server components to be installed.

## Tools Programmes

### Tools

This module is used for the configuration and management of 4TimeWEB system components.

### Data Base Manager

This module is used to manage the system database.

# Drivers

## MailGate driver

This driver is used for sending automatic email notifications, as well as sending email entered manually at the console level.

## GSMGate driver

This driver is used for sending automatic SMS text message notifications, as well as sending messages entered manually at the console level.

## Device drivers

A family of drivers receiving signals from guard control devices, and relaying them to the Kernel for further analysis.

## Security Agency Console Driver

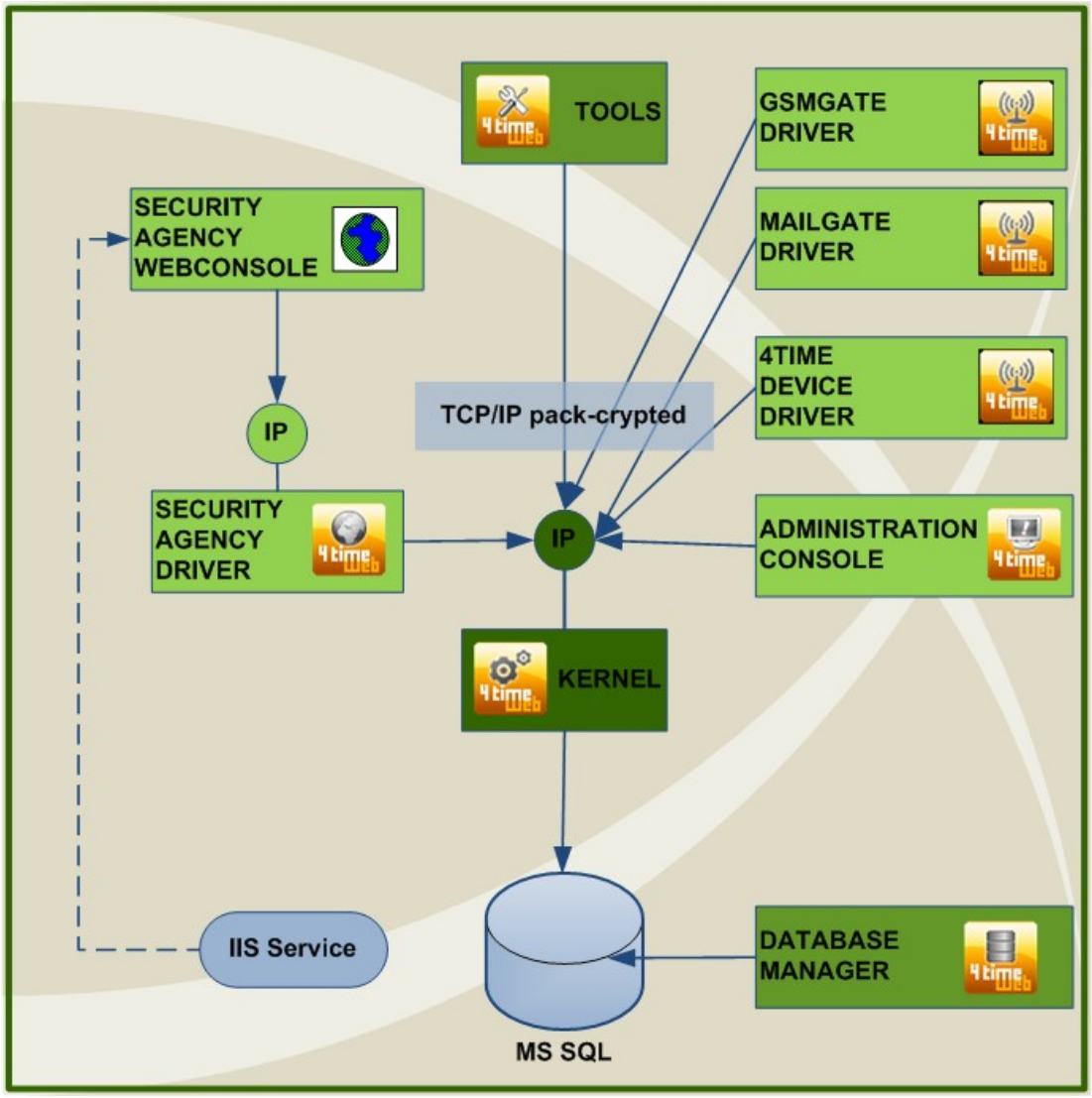
This driver is used for communicating and for transmitting data between the Security Agency Console and the 4TimeWEB system Kernel.

The driver opens the default port **TCP 4509**, which the Security Agency Consoles connect to.

## Policy File Driver

Policy access rules driver required for Microsoft Silverlight consoles.

The PolicyFile Driver opens the port **TCP 943**, which the Security Agency Consoles connect to before verification by the system.




## IIS server installation

- The server is a standard Windows component. The computer on which the IIS server will be installed must have the external port redirected to port 80:

- For **Windows Vista** and **Windows 7**:
  - Click on Control Panel -> Programmes and functions -> Enable or disable *Windows*. In the window that appears, find the *Internet information services* option on the components list and open it. Select the *IIS services management console* in the directory *Web management tools*. Next, click on the *WWW services* component, and then open it and select *Asp* and *ASP.NET* in the *Create application services* directory.
- For **Windows XP**:
  - Click on *Control Panel -> Add or Remove Programmes -> Add/Remove Windows Components.* In the window that appears, find the *Internet information services (IIS)* option on the components list, select it and click on details. In the next window select the following options from the list for installation: *World Wide Web Services* and *Internet information services Internet Information Services Snap-In*
- For **Windows 2003 Server**:
  - Click on *Control Panel -> Add or Remove Programmes -> Add/Remove Windows Components.* In the window that appears, find the *Application server* option on the list of components, select it and click on details. In the next window select the following options from the list for installation: *Internet information services (IIS), ASP.NET, and Application server console*.

If the page does not work properly despite correct installation (especially if there was no ASP.NET option or similar on the list of components to be installed), try entering the following command in the command console:
*C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet regiis.exe -i .*

Home editions of MS Windows do not have IIS servers.

After correct installation on disk *C*:, the following directory should appear: *C:\inetpub\wwwroot* .
When you enter the address http://localhost into the web browser, you should see the welcome page. If it does not appear you should first check your authorisation and the authentication methods used. This can be done using the *Internet Information Services Snap-In* available in:

- (for **Windows XP**) - *Control Panel -> Administration tools -> Internet information services*
- (for **Windows 2003 Server**) ; - *Control Panel -> Administration tools -> Internet information services (IIS) manager*
- (for **Windows Vista** and **Windows 7**).;- *Control Panel -> Administration tools -> Internet information services (IIS) manager*

To run the application you must also install Microsoft . NET Framework 3.5 SP1.

## Server installation and system launch

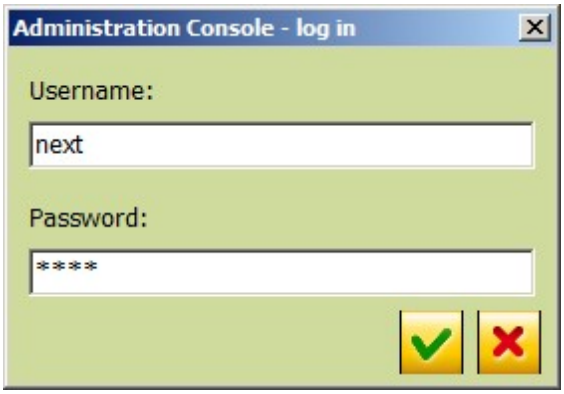
To install the 4TimeWEB system:

1. Run the installation programme using the Setup.exe file and follow the installation instructions.
2. Read and accept the licence agreement conditions and choose the default installation folder.
3. Select 'Server' installation, which will install:

- The Kernel
- The consoles (Administration console and Security Agency console)
- The drivers (MailGate, GSMGate, device drivers)
- The tools programmes (Tools, DBM)
- Components for using HASP keys
- The MS SQL 2005 Express database

To select different installation components, for example drivers, select non-standard installation.

4. Click *Next,* and then *Install* and wait until the installation is complete. After completing installation, the programme will ask you to restart the system, which is necessary to initialise the service.
5. Open the Administration Console from the start menu or from the shortcut on the desktop.
6. Log on to the system using: username *next* password *next.*




## Client installation

This chapter describes the installation of client modules and how to configure them to comuunicate with the main module, Kernel.

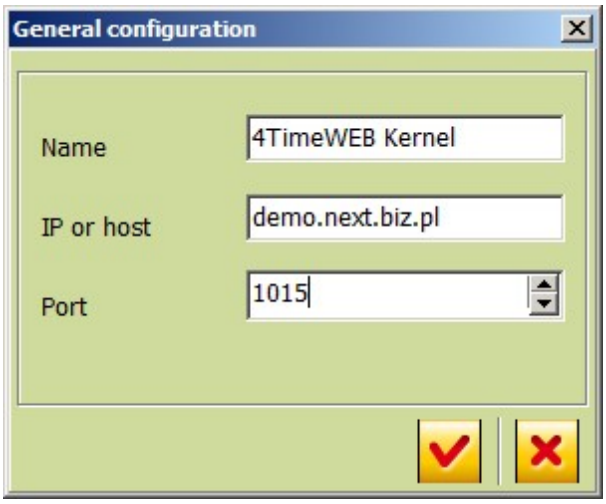
To install the 4TimeWEB system modules:

1. Run the installation programme using the Setup.exe file and follow the installation instructions.
2. Read and accept the licence agreement conditions and choose the default installation folder.
3. Select 'Client' installation, which will install:

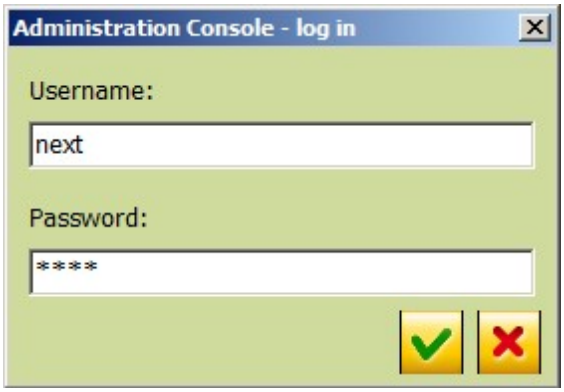
- The Administration Console
- The Tools programme

To select different installation components, for example drivers, select non-standard installation.

4. Click *Next* and then *Install* and wait until the installation is complete. After completing installation, the programme will ask you to restart the system, which is necessary to initialise the service.
5. Run the Tools programme, select general configuration, add the name to the list (any name) as well as the IP address and the 4TimeWEB system Kernel access port.




6. Run the Administration Console
7. Log on to the system using: username *next* password *next.*




The Security Agency Console does not require installation from the *.exe file. The Agency Console is run from a browser by entering the appropriate website address (details in Quick start - Security Agency)

## 2.2 Initial start-up

This chapter describes the basic steps related to creating definitions and templates after initial system start-up.

**Terminology**

- **Definitions -** lists, templates, dictionaries and example accounts

- **Alarm -** the account status displayed on the Agency Console on receipt of an alarm signal.
- **Signal -** information sent by the device and received by the 4TimeWEB system driver

The definitions, templates and dictionaries are created and added using the Administration Console. The module shortcut can be found on the desktop or in the start menu.
Access to the Console is only available to users with the appropriate authorisation. The user with this default authorisation is: username *next* password *next*.

## Default definitions and templates

Before adding a new agency you must first enter the necessary data using the **templates** tab on the Administration Console:

- **Locations** - languages and list of holidays for a given location.

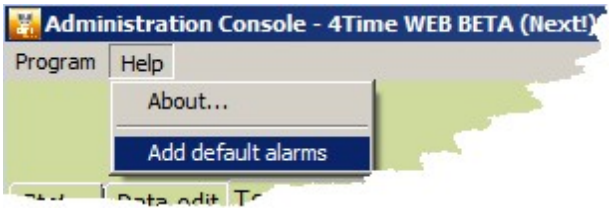
- **Alarms** - a list of alarms that can be generated by the system.

- **Device templates** - signal templates and device testing management.

If the device language is not defined, the default description from the signal template is used, as well as the default alarm name.

In the first steps, the system recommends adding the **default alarm values** proposed by NEXT!

Default data can be added from the Help menu:



Templates can be imported from/to an XML file using the import/export icons.

Export device template

Import device template

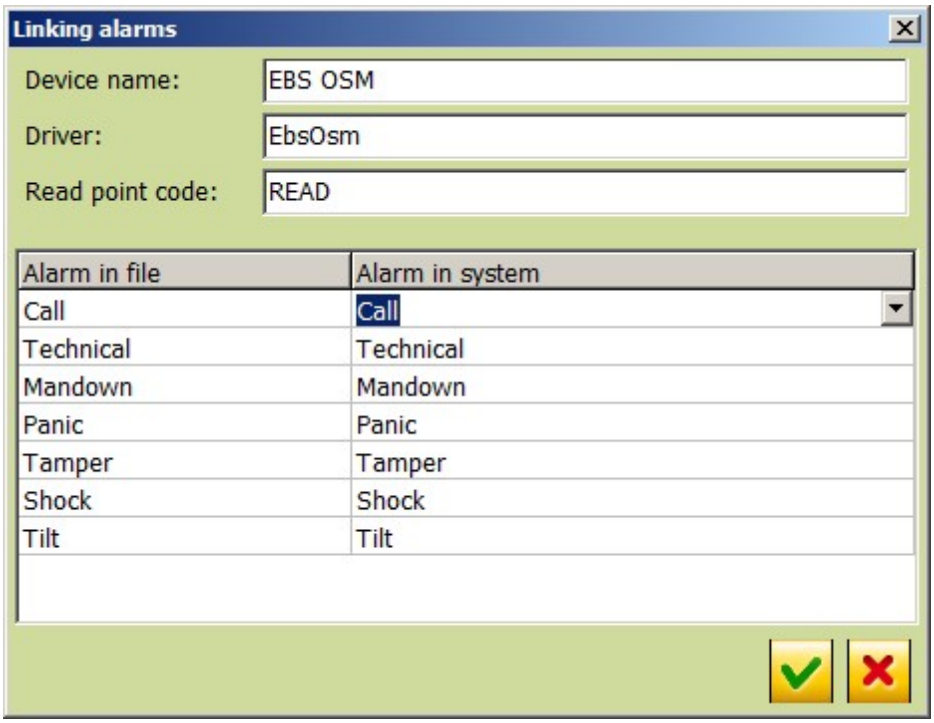
## Adding templates from a file and descriptions in a different language.

Example device templates are installed together with the system.

Import a template by clicking on the *import* icon.

Select the path and template file (the default path for the example template is: C:\4TimeWEB\EBS OSM eng.XML).

Click to confirm if all the information is correct, if not then correct the data.

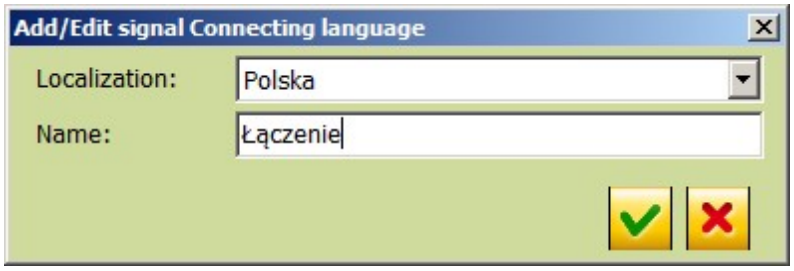



To add a description in a different language, first create the language name on the languages tab under templates.

Edit a signal from a device added by clicking on the edit icon.

Add a description in a different language by clicking on the plus icon.

Select the required language for the description and choose an appropriate name.




Confirm adding a description.

Confirm signal editing.

## 2.3 Assigning devices to accounts

This chapter describes the basic steps required to allow for monitoring of guard control devices by security agencies.

### Terminology

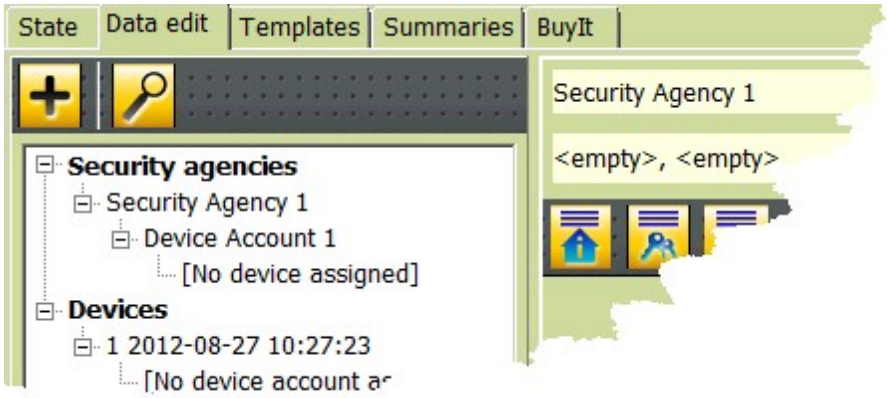
- **Security Agency -** a company using the system. One agency can contain several different accounts and the devices assigned to them.
- **Account -** a protected building, vehicle, person or vending machine defined in the system.
- **Device -** a representation of a physical round control device in the 4TimeWEB system.
- **Device number -** a device identification number

To monitor a device, it must be registered manually or automatically and must be assigned to one of the selected agency's accounts.

A device can be assigned to many accounts, but only those belonging to one agency.

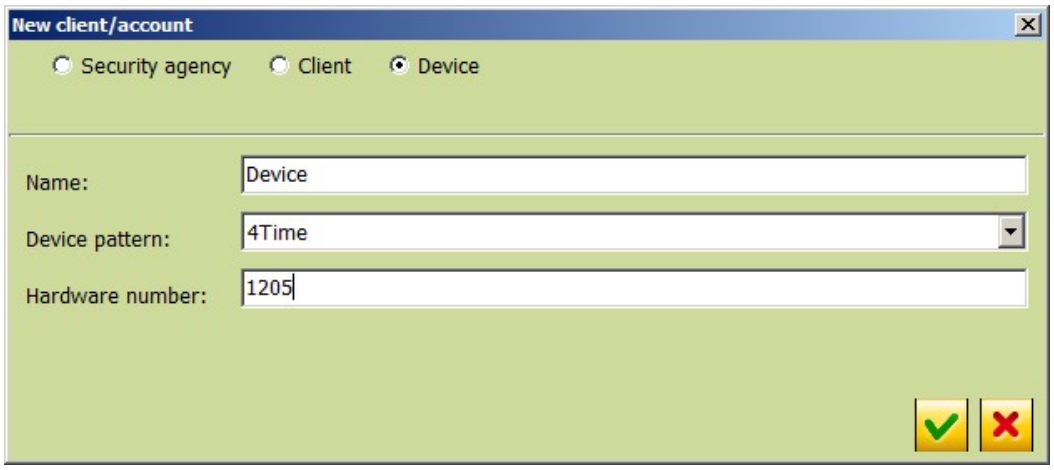
## Adding a new Device

Go to the *Data edit* tab.

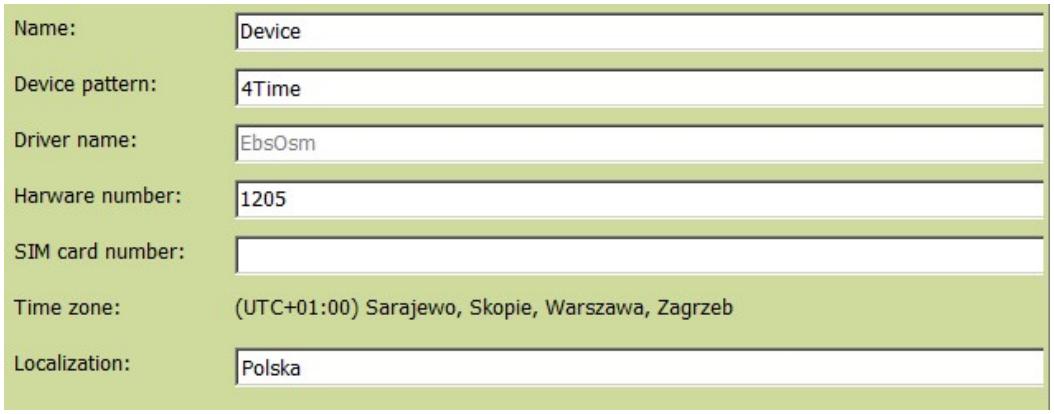



Manually add a new device by clicking on the *plus* icon.

Select *Devices* and give the device a name, choose a device template, and give it suitable a device number.




After adding the device give the location.




If the language is not defined, the default signal descriptions and alarm names will be used.

Confirm.

Devices are also automatically added to the system when a signal is received from a new device not previously registered in the system. In this situation it automatically appears on the device list with the time the first signal was received.

A newly-added device is not assigned to any agency. As a result it is not included in the system licence and signals and alarms from such a device are not analysed.

## Adding a new security agency

Add a new security agency by clicking on the *plus* icon.

Select security agency and enter the name.


 Confirm.

Enter the agency data:

General tab:
- Address: town, street, house number, district, region
- Correspondence address: town, street, house number, district, region.

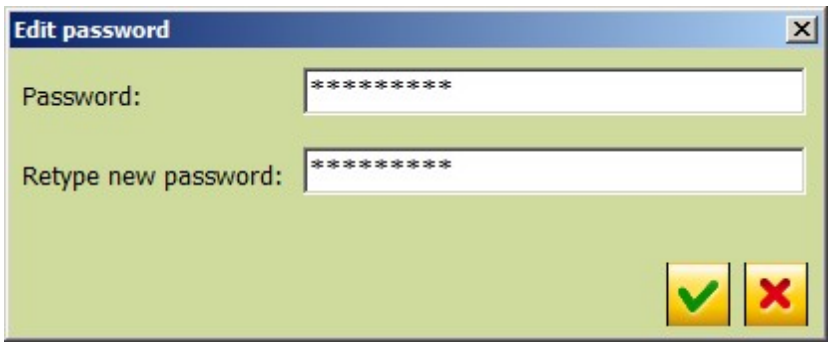
Login tab:

 Add a new user on the Security Agency by clicking on the *plus* icon.

Enter the name and login.


Click on the edit password icon and enter the password twice.

 Edit password icon.




Confirm

Give the user the appropriate access:
- viewing and managing alarms
- edit device and account data
- edit security agency data.

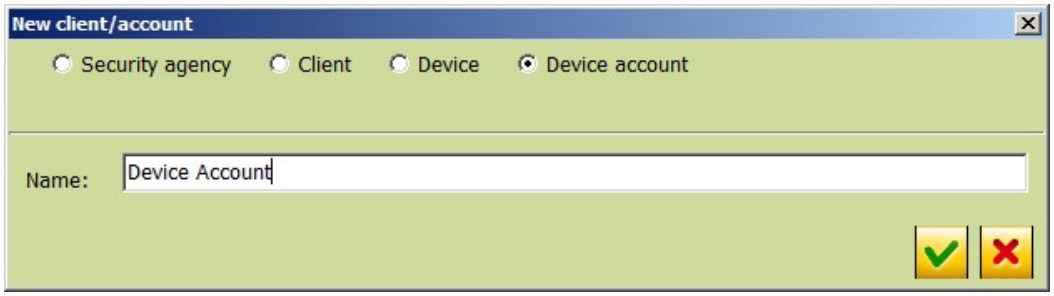
Confirm.

## Adding a new account and assigning devices

Accounts can also be created in the agency console by appropriately authorised users.

Add a new account by selecting a given security agency and clicking on the *plus* icon.

Select Device account and enter a name.



Confirm.

Enter the account data:

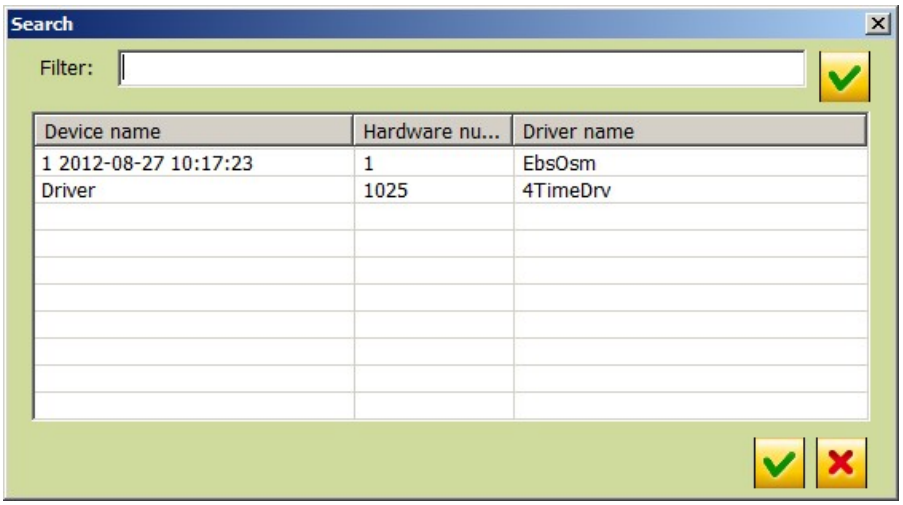
Account type:
- building
- vehicle
- person
- vending machine.

Description.

Address: street, house number, town, district, region.

Add a device to an account on the assigned devices tab by clicking on the *plus icon*.

Search for unassigned devices by clicking on the confirm icon next to the filter.




Select the device you are interested in.

Confirm your choice.

Using the Agency Console, unassigned devices can also be assigned to a selected account by appropriately authorised users (details in Adding Accounts and assigning devices).

## 2.4 Monitoring and reporting on system operation

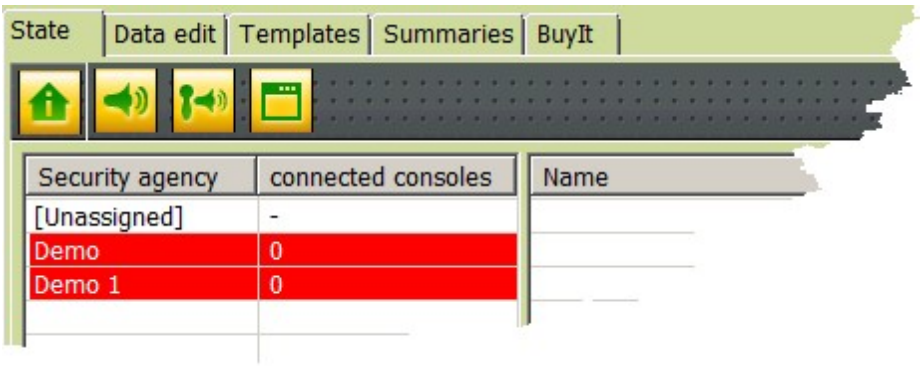
This chapter describes how to monitor system operating status and how to create and send reports.

### Terminology

- **System events -** information generated by the 4TimeWEB system relating to its operation.

### System status

System status can be monitored using the Administrator Console. This includes signals, account events, system events and agencies connected together with information about alarms.




To monitor system status select the status tab, which contains information about:

Security agencies:

- the number of connected Security Agency Consoles in the system for each agency.

If there are no Security Agency Consoles connected, the agency name is highlighted in red.

- alarms serviced by security agencies

The Administrator Console user can remove an alarm from service by right-clicking it with the mouse.

Signals - a list of the most recent signals received.

Account events - a list of the most recent account events.

System events - a list of the most recent system events.

You can view signal, event or account event details by double-clicking on the required item.

## Summaries

The Administrator Console can be used for creating and sending summaries.


The following reports are available under the *Summaries* tab:

Change history - changes to security agency data, devices or accounts in a given time period, including details of the changes made.

Summaries:
signals - signal history for a given period, with the option to filter, print, export or save to a csv file
events - event history for a given period, with the option to filter, print, export or save to a csv file
payments - payment history for a given period, with the option to filter, print, export or save to a csv file

Summary schedule - summaries selected by the user that are sent automatically by email.

## Summary schedule

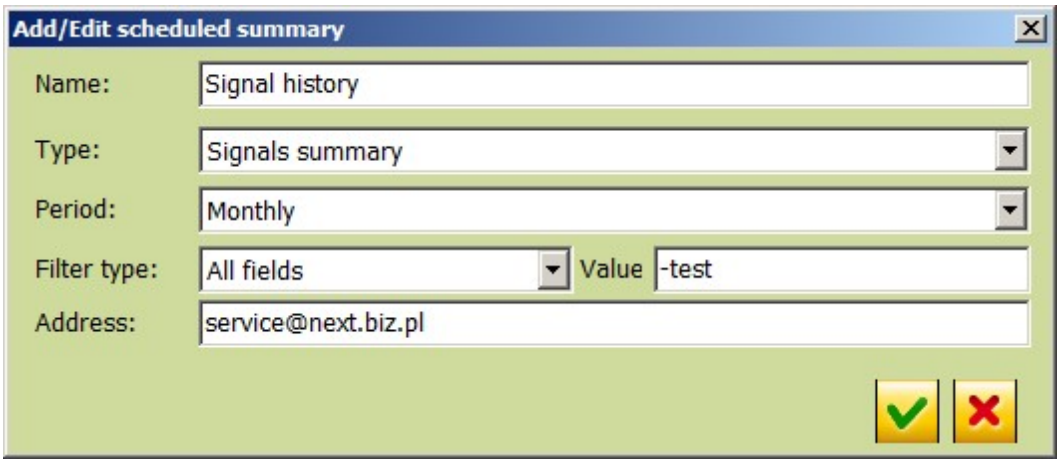
Summaries can be sent to a chosen email address according to a schedule. To do this:

Select summary schedule from the summaries tab.

Add a new summary to the schedule by clicking on the *plus* icon.

Enter:

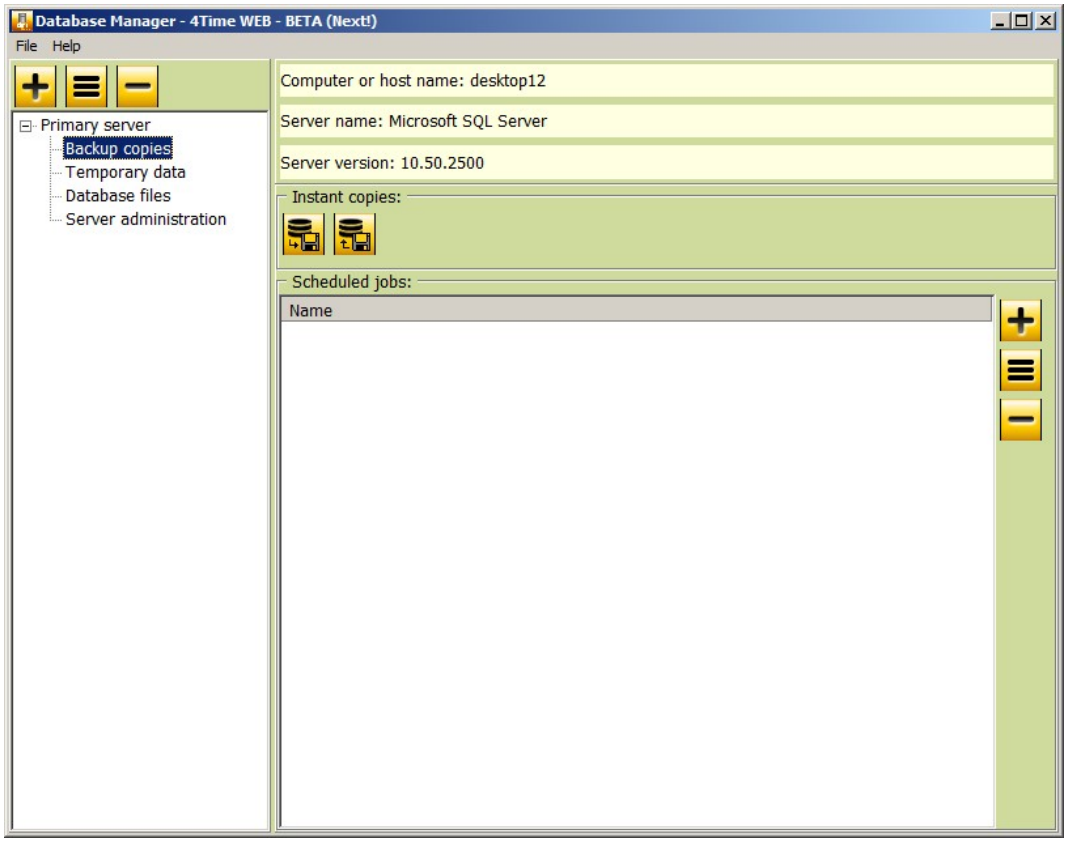
- the summary name
- the type of data contained in the summary
- the period for which the summary will be generated
- the filters used for the summary
- the email address to which the summary will be sent




Summaries are sent according to the schedule via the MailGate module, which must be running and configured to work with the 4TimeWEB system.

## Backup copies

Backup database copies must be created to secure the system against data loss. Backup copies can be created in a special Database Management (DBM) programme included in the system.




Copies can be created manually or set up to be created automatically.

Create a single copy by clicking on the backup up copy creation icon.

Select the chosen destination and give the copy a name.

Set up automatic backup by clicking on the plus icon.

Choose a name and select the chosen destination.

Choose the type of automatic backup:

- single: enter the date and time when you want the backup copy to be made
- permanent: enter the time and the frequency in days when the backup copy is to be created.

To restore the database from a copy made earlier:

Disable all 4TimeWEB services.

Select the backup copy tab in the Database Manager

(DBM).

Click on the restore database icon.

Select the destination in which the backup copy was made.

Wait for the copy to be restored.

Enable all previously disabled 4TimeWEB services.

# Chapter

# 3 Quick start - Security Agency

The manual below helps you to familiarize yourself with the 4TimeWeb system. It is purposefully concise in order for you to start working with the system as soon as possible.

Detailed information can be found in the relevant chapters.

The Security Agency Console is run directly in the web browser. It is not necessary to install or configure it.

In order to start a web browser with Microsoft Silverlight installation is necessary. An internet connection and link to the main module is also necessary.

## 3.1 Alarm handling

This chapter deals with alarm handling.

### Terminology

- **Alarm -** account status signaled in the Console after an alarm signal is received.
- **Signal -** information from a device received by System driver.
- **Event -** information generated by a user or System based on performed actions.
- **Account -** protected premises, vehicle, person or vending machine. Multiple devices can be assigned to an account.

### Logging into the system

To log into the system a unique login and password is used. Access rights (at various levels) are assigned by system administrator.

The Security Agency Console is started by entering a link to the main system in a web browser.

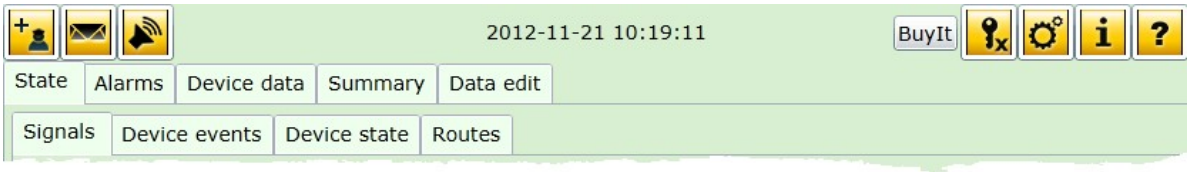
In case of local installation a default link will be created on the desktop: http://localhost/SecurityAgencyConsole/

After the console is launched and is connected to the Policy File and Security Agency Console drivers the following login window appears:


The console must be connected to the access policy file driver, and with the Security Agency Console driver run by the distributor. For this reason the outgoing TCP ports **943** and **4509** (default) must be open for the application.

Access to the system for a user is set up in the Distributors Console by creating a login and password while creating a new Security Agency. Multiple users can be added. (Adding a new user)

## Top menu




Add mobile patrol icon


Send manual SMS text message icon


Volumne icon - sounds muted


Volumne icon - sounds enabled


Error icon (if there are no errors the icon does not appear)

Redirect button to the BuyIt webpage



Login/logout icon

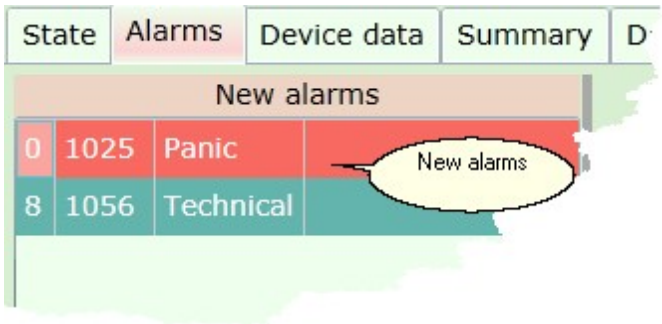

Settings icon


Programme information icon


Help icon

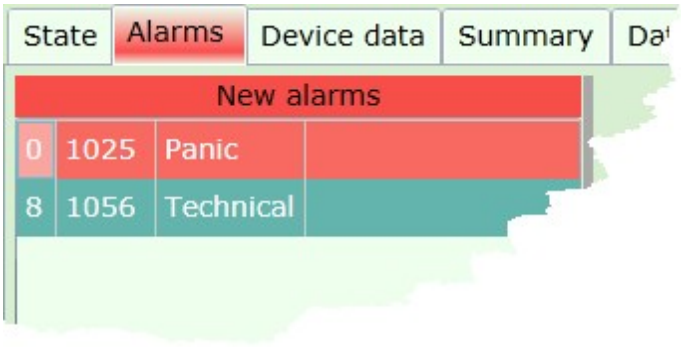
## New alarm

1. Alarm is taken over for handling by double clicking on the alarm list .




2. After the above selection the basic data is displayed.

3. To display another alarm's data it needs to be double clicked on the active alarm list.




4. Basic device data contains information on the device such as its name, hardware number, account it is assigned to or persons assigned to this account. The tab also displays signal and event list beginning from the start time of the alarm.

## Actions while handling an alarm.

In order to add and register a new action connected with the alarm handling in the System one of the icons from 'the comic' can be used.
Following actions are available:


List of persons to be notified will be displayed. After selection OK button can be pressed which will record the action of notifying the person.


List of assigned security guards will be displayed. After selection OK button can be pressed which will record the action of notifying the person.

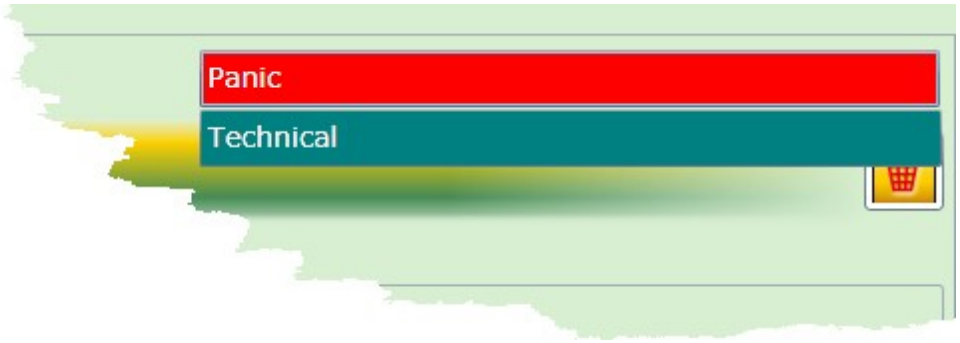

True alarm.


False alarm.


Alarm end.


Additional actions.

During alarm handling, alarm account data and the type of alarm can also be displayed.




You can view a full list of alarms by moving the cursor over the list.

Basic data - basic data about the device where the alarm originated, the signals that have been sent so far, and a list of people related to the device.

Account maps and floorplans

People - people related to the account

Comments - important comments relating to the account

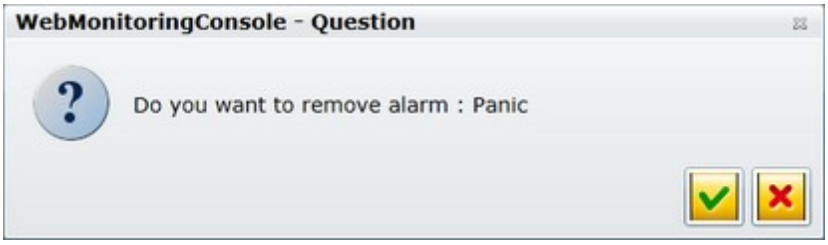
Routes - planned account routes

## Closing an alarm.

To close an alarm the Alarm Close button needs to be pressed.

Alarm Close icon.

and then the alarm removal must be confirmed:



Signals and events are stored in the system database. Relevant summaries can be made on the Account Data and Summaries tabs.

## 3.2 Adding an account and assigning devices

The chapter deals with adding an account in the Security Agency Console.

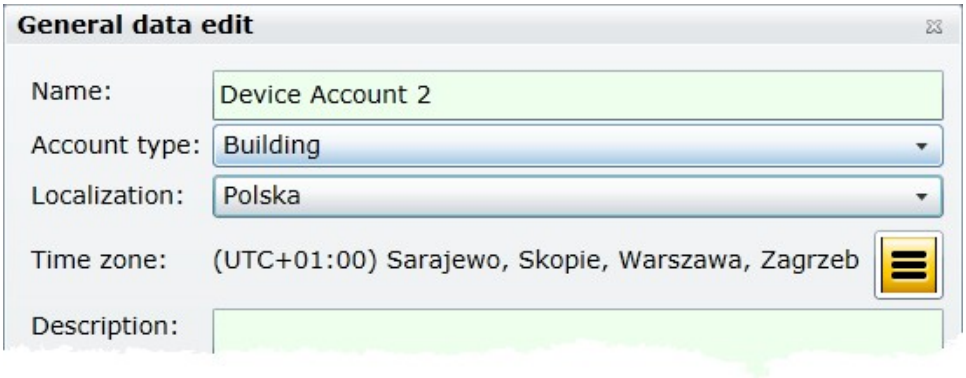
### Terminology

- **Device -** physical guard tour device, that can be assigned to one or multiple accounts.
- **Point -** a unique tag assigned to an account that can be read by the Device.
- **Person** - a person or firm related to a given account that must be notified of an alarm, or who has authorisation to be present at the account.

### Adding a new account

To add a new account click on the *plus* icon in data editing.


1. Fill in the name, type and description of the account.

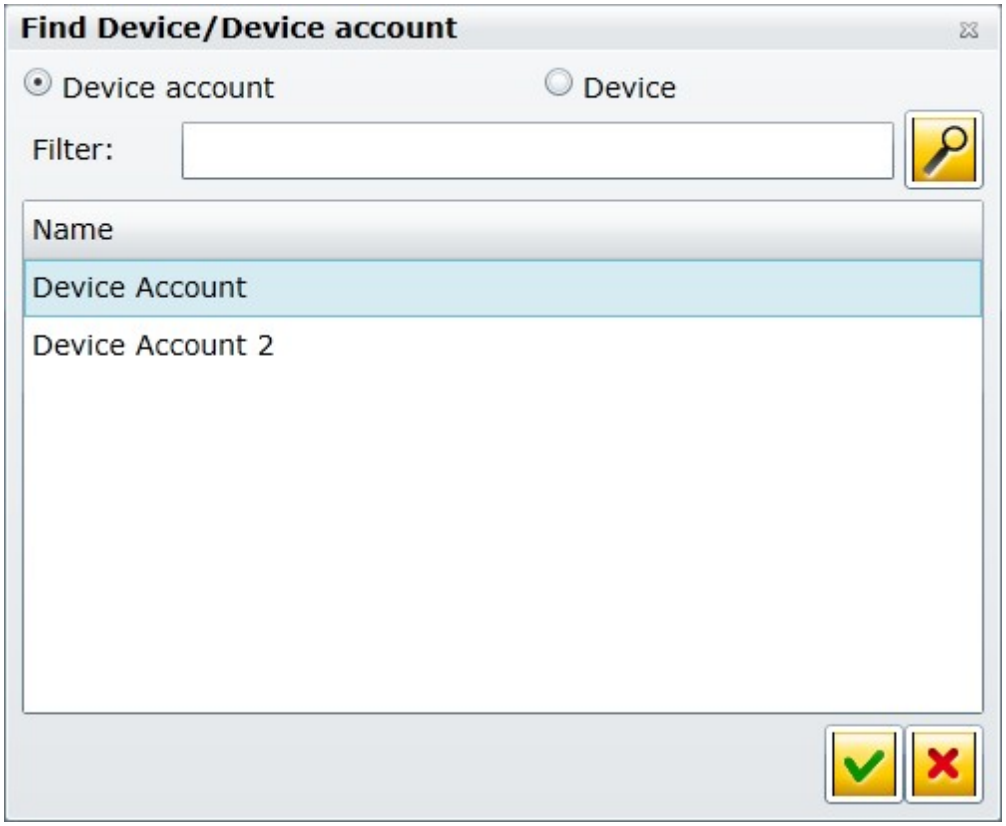




and the additional data:

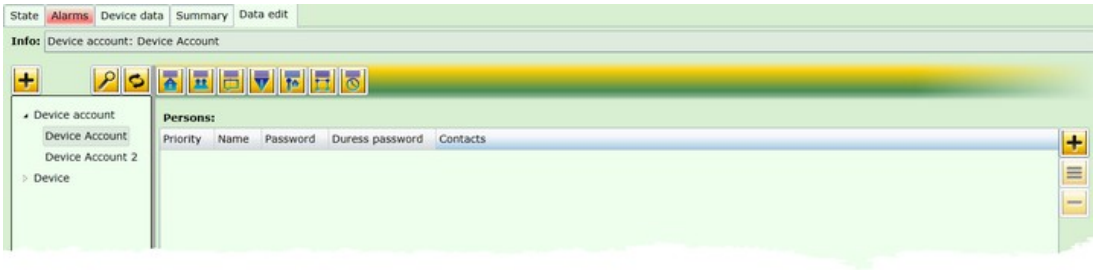
- for a building: street, city etc.
- for a car: licence plate, model etc.
- for a person: name, sex etc.
- for a vending machine: address data, serial number etc.

## Adding a person

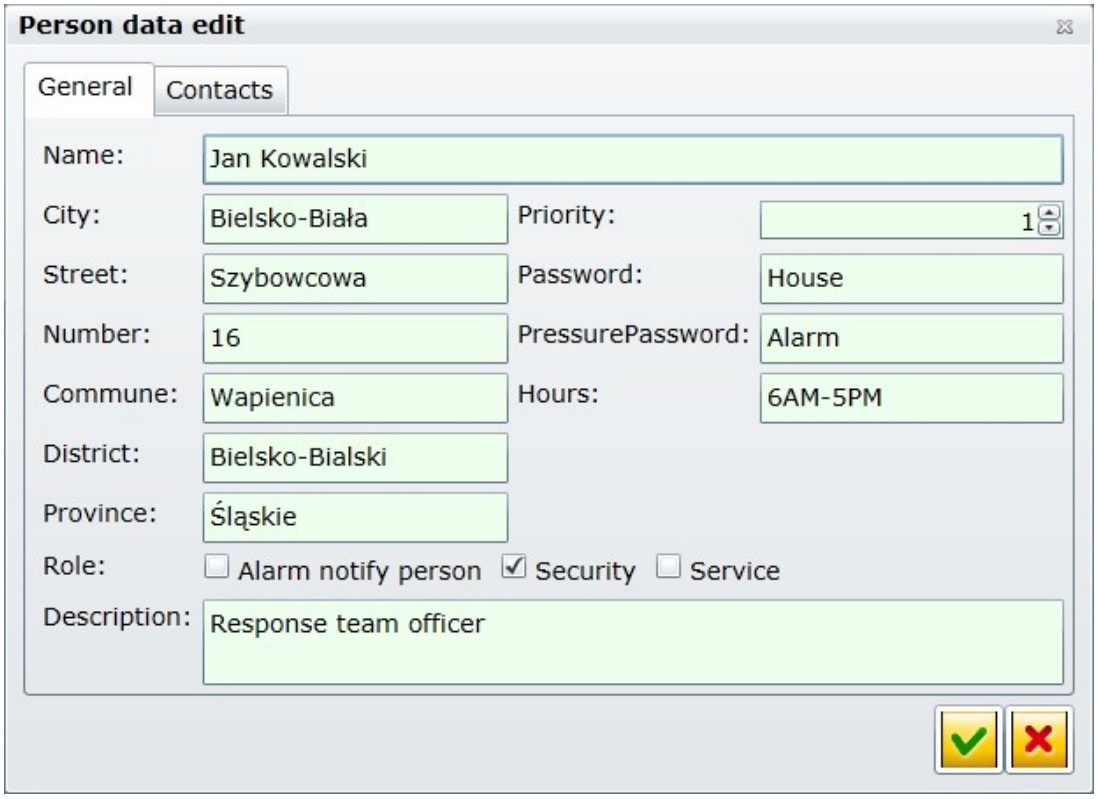
On the Data Edit tab choose the account to which the person will be added.




On the Persons sub tab a new person can be added by clicking on the *plus* icon.

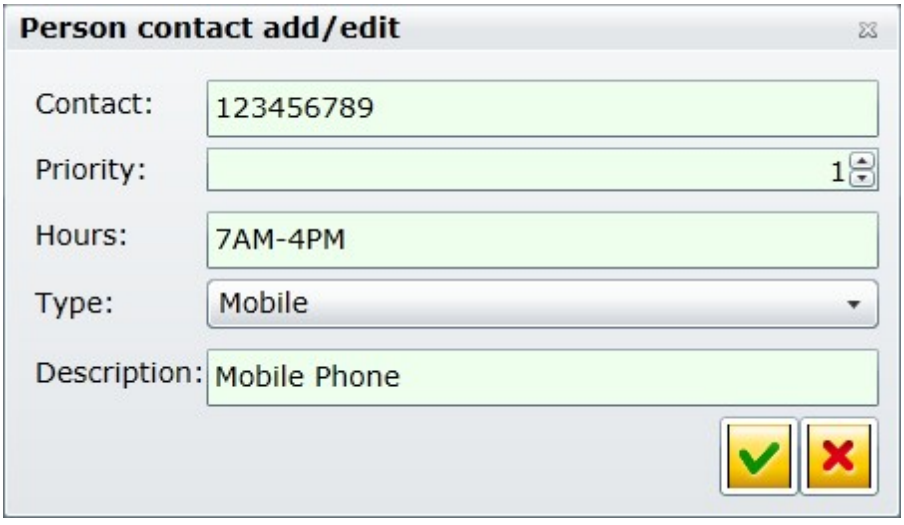



On the General tab data about the person, passwords, contacts etc is filled in.




Contact data is filled in on the Contacts tab.

By clicking on the *plus* icon we add the desired contact data, set a priority (one person can have multiple contacts), the hours within which contact is active and the contact type.

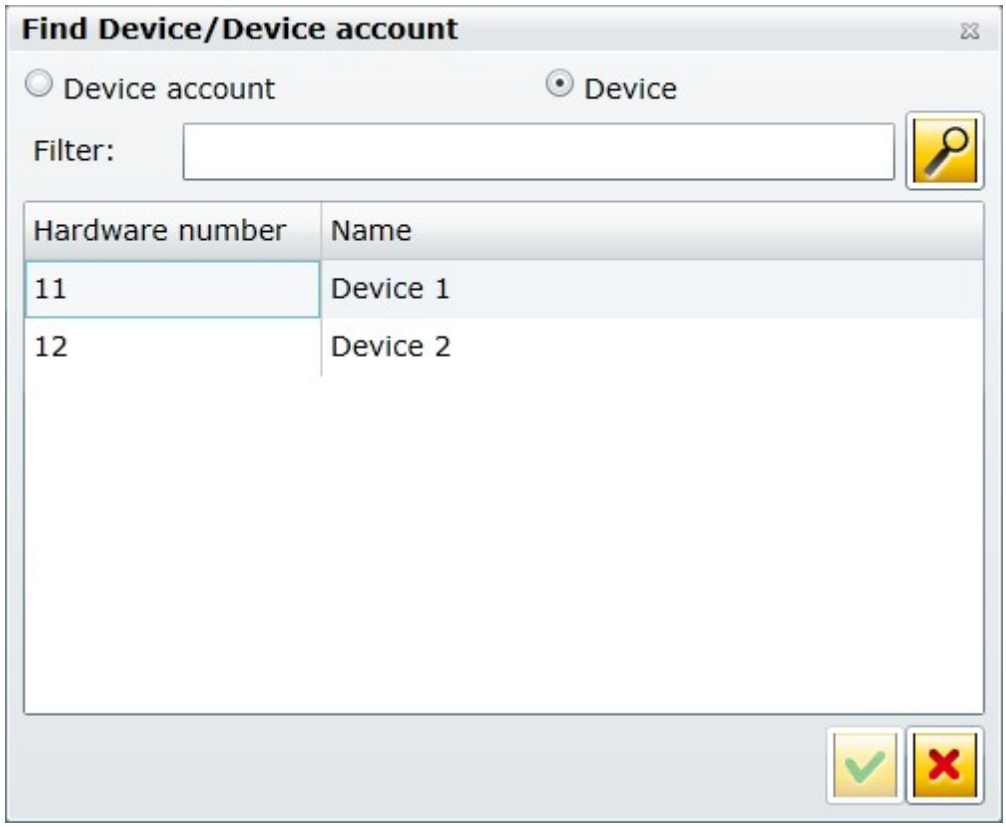



Confirm the data.

## Assigning an existing device to an account.

Assign an existing device by clicking on the *plus* icon from assigned devices.

Find a device by clicking on the *search* icon.




The list will show devices assigned to a Security Agency and new ones that are not assigned to any Security Agency.

Confirm your choice.

## Adding a point to a path.

A point can be added by clicking on the *plus* icon on the Signals tab.

Choose a signal from the list with the assigned point number, add the description and point type.


The list will show unassigned points from the device account.
A point is added to a device automatically after its first readout. By default the first readout time will be found in the description field.
A new point can also be added manually by providing its ID and name.

Confirm your choice.

## 3.3 New patrol

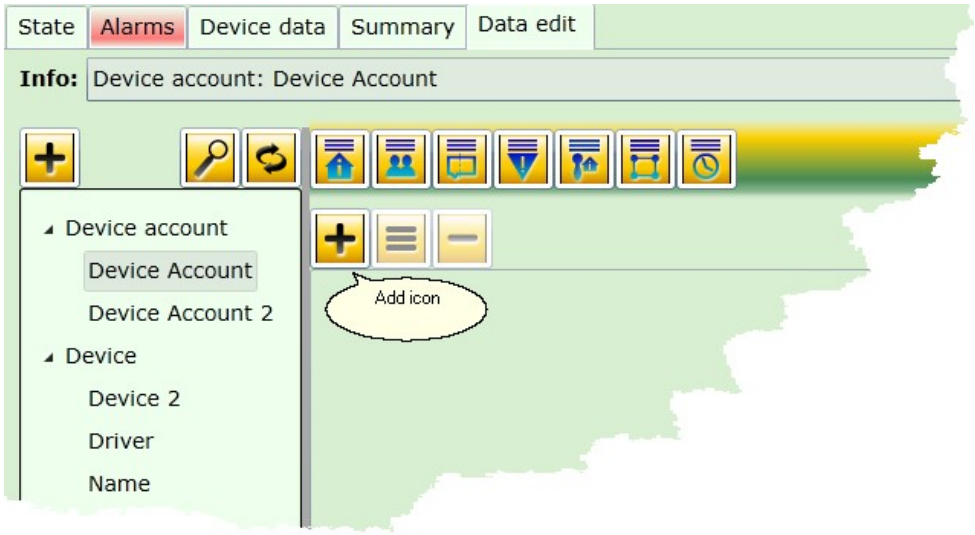
This chapter describes defining paths.

### Terminology

- **Path -** a sequence of points on the patrol route.

### New patrol

In Data Edit add a new path by clicking on the *plus* icon.




Fill in the following:

- name,
- generated alarm type in case of path breach,
- type:
  - *simple* - all points should be checked within provided period in any sequence.
  - *advanced* - sequence and exact times (with time slots allowance) of point checks can be set.
- calendar type.
- start and end time of the path.
- days on which the path is valid.

By choosing mobile calendar type, the option is created of adding a mobile patrol activated by a System User request.

It is also possible to define the validity period of both the path and the path start command.

Confirm entered data.

A path can be created based on any device assigned to the account.

Such created path can be looked up in the device data assigned to an account to which the path was added and an alarm if it occurred. A path can be delayed, stopped and resumed.

## 3.4 Mobile patrol

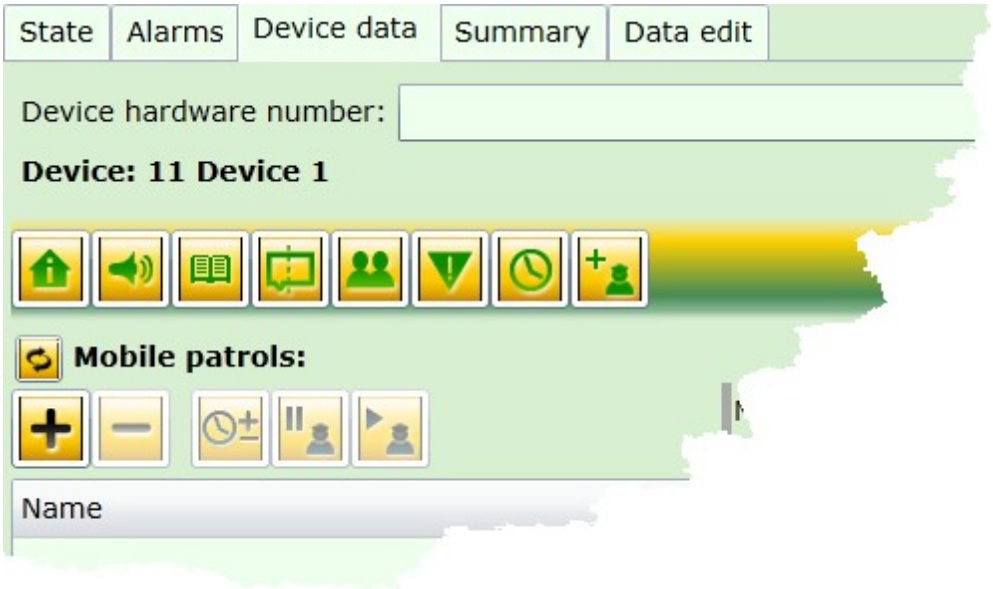
This chapter deals with mobile patrols.

### Terminology

- **Mobile patrol -** a path that is based on multiple accounts. Started manually, by the user.
- **Account -** protected premises, vehicle, person or vending machine. Multiple devices can be assigned to an account.

### Mobile patrol

On the device data tab choose a device.



On the Mobile Patrols tab add a new patrol by clicking on the *plus* icon.

Or add a mobile patrol by clicking on an icon in the main console window (additionally choose a specific device).

On the General tab provide data for the patrol: name, start and end time (device is added automatically).


On the Path tab add the ones that will be serviced by the mobile patrol by choosing an account and mobile patrol path.

Only already defined (as mobile patrol) paths can be added. They have to be defined for the accounts used. (see details in New path).

Confirm the choice.

Confirm mobile patrol creation.

## 3.5 Notifications

This chapter deals with notification settings, i.e. adding actions to devices.

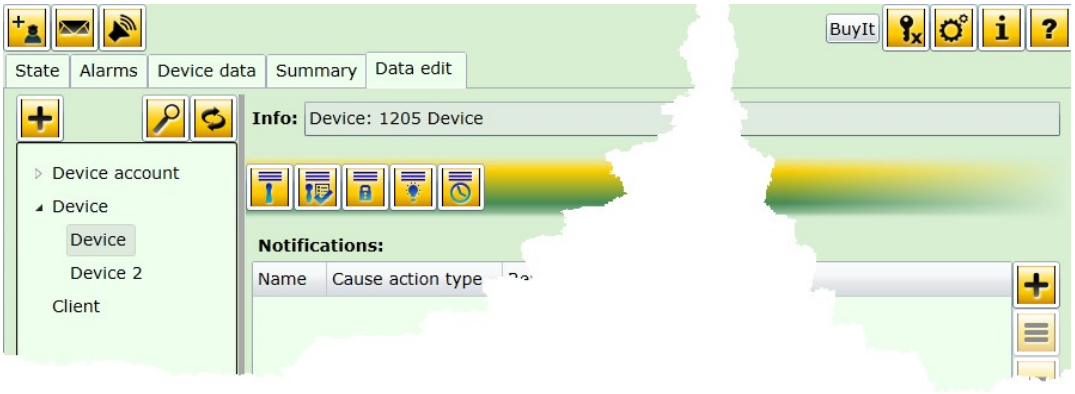
## Terminology

- **Notification -** automatically generated reaction (sending SMS or E-mail) to an event or alarm in the System.

## Notifications

On the Data Edit tab choose the device for which an action will be created.

On the Notifications tab the *plus* icon needs to be clicked.




Fill in:
Notification name.
Notification type:
- signal received:

choose account and point,
- technical signal:

choose technical signal,
- generated alarm:

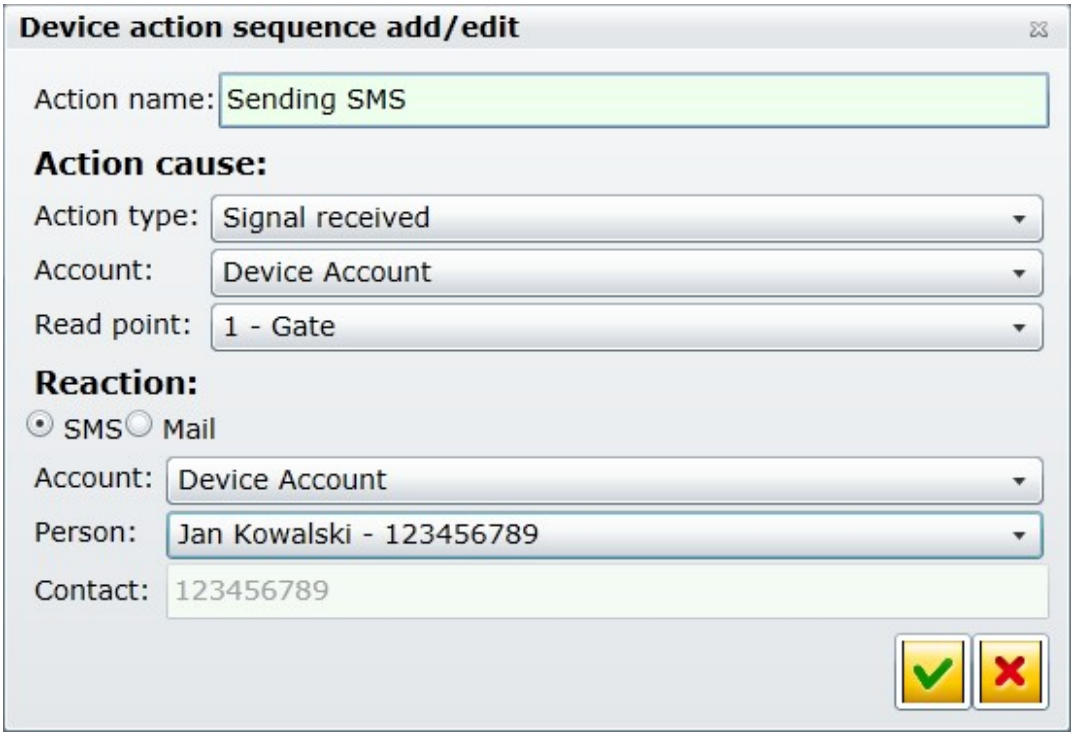
choose alarm.

Choose notification channel:

- E-mail:

choose account and person (if the person is not on the list choose *other* and manually provide email address, otherwise E-mail will be added automatically).
- SMS:

choose account and person (if the person is not on the list choose *other* and manually provide phone number, otherwise phone number will be added automatically).




Confirm creation of a notification.

## 3.6 Adding a new user

This chapter describes adding a new user in the Security Agency Console.

### Adding a new user

To add a new user in the Settings (upper right hand corner of the Console) on the logins tab, click on the *plus* icon.

Fill in data: name, login.


and password.


> The login must be unique system wide.

Add desired rights:

- View and operate alarms.
- Edit device or account data.
- Edit Security Agency data.

Confirm.

# Chapter IV

# 4 Quick start - client

This tutorial is for clients to quickly familiarise themselves with the 4TimeWEB system. The instructions in the following chapters are purposefully brief so as to allow users to start using the system as quickly as possible. The aim is not to teach every small detail, but to make users aware of the basic principles and how the system functions.

For more details on the functions described in the tutorial, please refer to the chapters relating to individual functions and modules. These contain further useful information and an explanation of the 4TimeWEB system advanced functions.

The Client Console is run directly from a browser and does not require installation or configuration by the user.

To run the Client Console you need an internet browser and access to the internet. Using the browser, enter the appropriate link to the Client Console supplied by the manufacturer.

## 4.1 System access

### Terminology

- **Client -** an end user who has authorised access to the devices and accounts in the system.
- **Devices -** a representation of a physical round control device.
- **Device number -** a device identification number

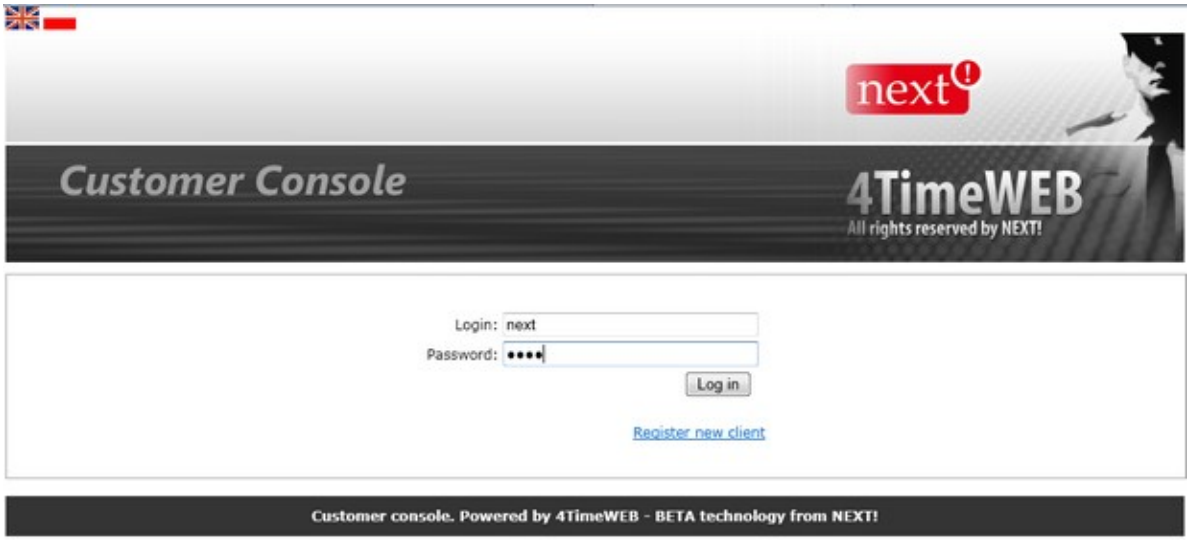
Users log on to the system using their unique login and password.
The Client Console is run by entering the web address provided by the manufacturer into your web browser.

For local installations the default link for running the Console appears on the desktop: http://localhost/CustomerConsole/

## Logging on to the system

After launching the Client Console, log on using:

- the unique user login and password
- click the *Log in* button



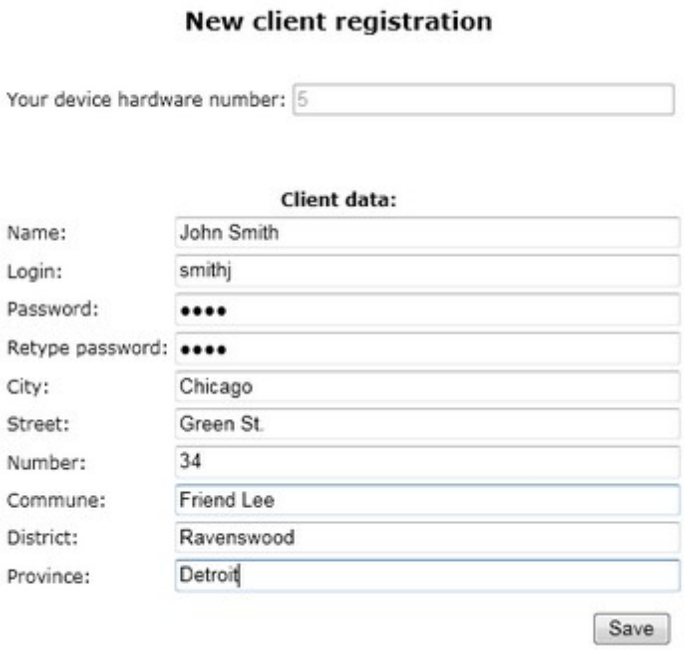

## Registering a new client

To register a new client in the system:

- select the *Register new client* option in the login window
- enter the *device identification number*

> The device must be registered in the system and not assigned to any of the clients. After initial launch of a correctly configured device, the device is automatically registered in the system.

- enter the client data:
  - name
  - the unique login and password used when logging in
  - the correspondence address:
    - town
    - street and house number
    - district
    - region
    - province




- click on the *Save* button.

> Managing and adding new clients can also be done by the distributor from the Administrator Console.

## 4.2 Adding accounts and assigning devices

This chapter describes how to add new devices and device accounts using the Client Console.

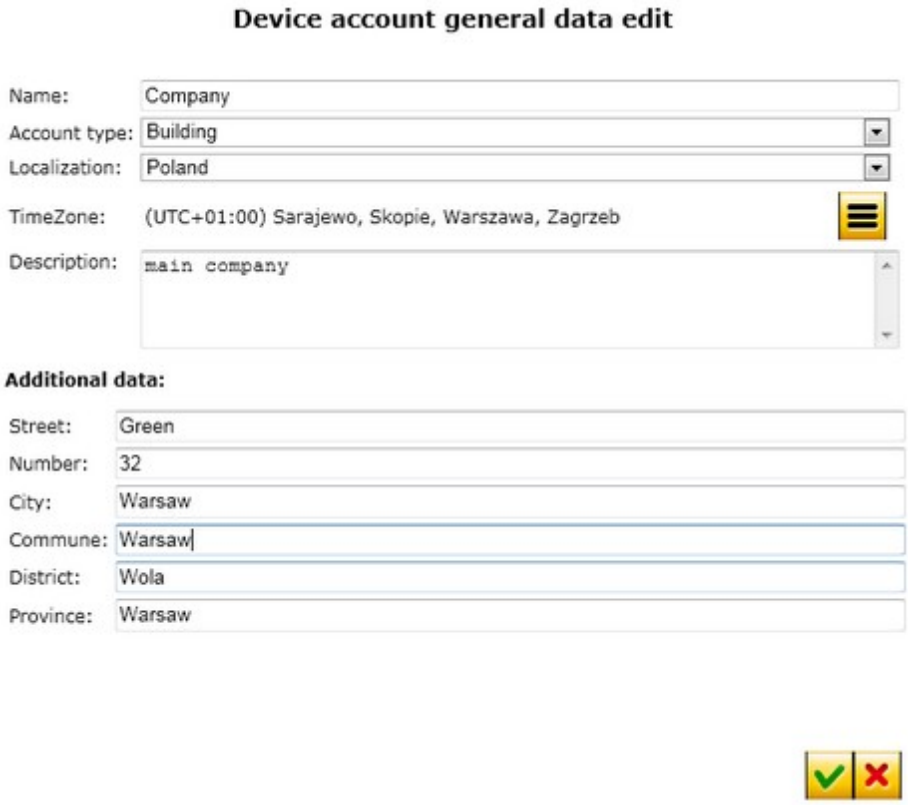
### Terminology

- **Account -** a protected building, vehicle, person or vending machine connected to the system. Several different devices can be assigned to one account.
- **Person -** a person or firm related to a given account who must be notified of any alarms, or who is authorised to be present at the account.
- **Point -** a tag assigned to an account with a unique identification number that can be read by the device.

## Adding a new device account

Select *Device accounts* from the menu and click on the *plus* icon.

Enter the account data:
- name
- account type
- select the location from a pre-defined list
- time zone
- description
- additional information depending on the type of account (e.g. address, vehicle data, personal data).




Click confirm to add the device account

## Adding a person to an account

Select *Device accounts* from the menu select *Person data* for any given device account.

Click on the *plus* icon and enter the following data on to the *General* tab:
- the person's name
- address details (town, street, house number, district, region, province)

- the person's priority
- the password confirming the person's identity and the password used during danger.
- the person's role
  - to be notified of alarms
  - security
  - service personnel
- description


On the *Contacts* tab:

Click on the *plus* icon and enter the following data:

- contact details (e.g. telephone number, email address etc.)
- contact priority
- contact time
- contact type
- description


## Registering a new device

Select *Devices* from the menu and click on the *plus* icon.

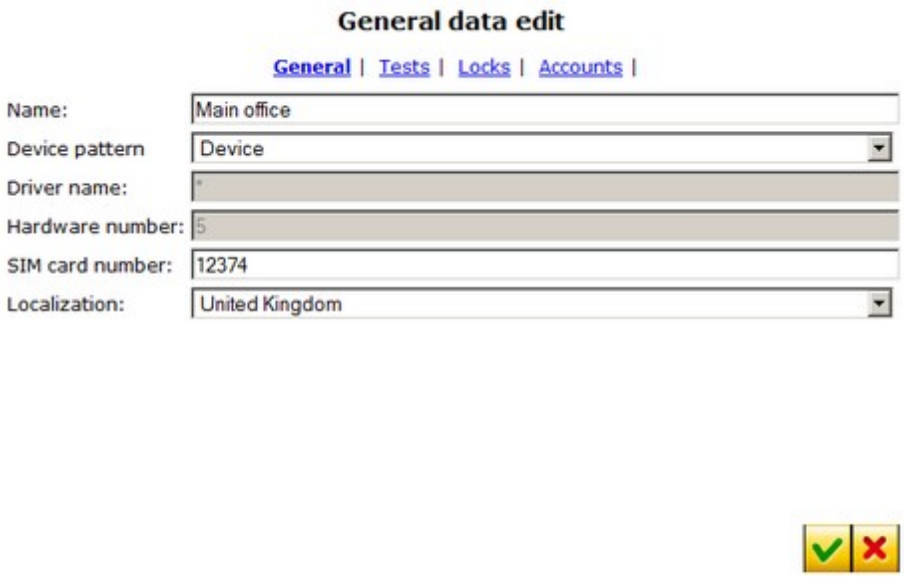
- Enter the device identification number for the device to be added.

> The device must be registered in the system by activation at any RFID point, and must not be assigned to any client. After initial launch of a correctly configured device, registration in the system is carried out automatically.

Select *General data edit* for the device added

The *General* tab can be used to define:

- device name
- device template
- SIM card number
- the location, which affects the language in which the signal and alarm descriptions are displayed.




Confirm to add the device

## Assigning a client device to an account

Select the *Devices* option from the menu. Then click on *General data edit* for any given device.

The device can be assigned to an account by clicking on the *plus* icon on the *Accounts* tab.

## Describing points on a device account

Select *Device accounts* from the menu and click on *Edit points* for any given account.

Click on the *plus* button, select the signal with the assigned point number from the list, then add a description and the signal type.


The points list shows unassigned points from account devices. A point is automatically added to the device after the first reading. The point description in this case contains by default the time when it was received.
A new point can also be added manually by entering its identification number and name.

Confirm to enter the signal.

## 4.3 Routes

This chapter describes the steps required to add a new route to an account.

### Terminology

- **Route -** an area monitored by a guard which has reflection points distributed around it.
- **Reflection point -** a point with its own unique identification number located along a route.
- **Alarm -** the account status indicated in the Security Agency Console

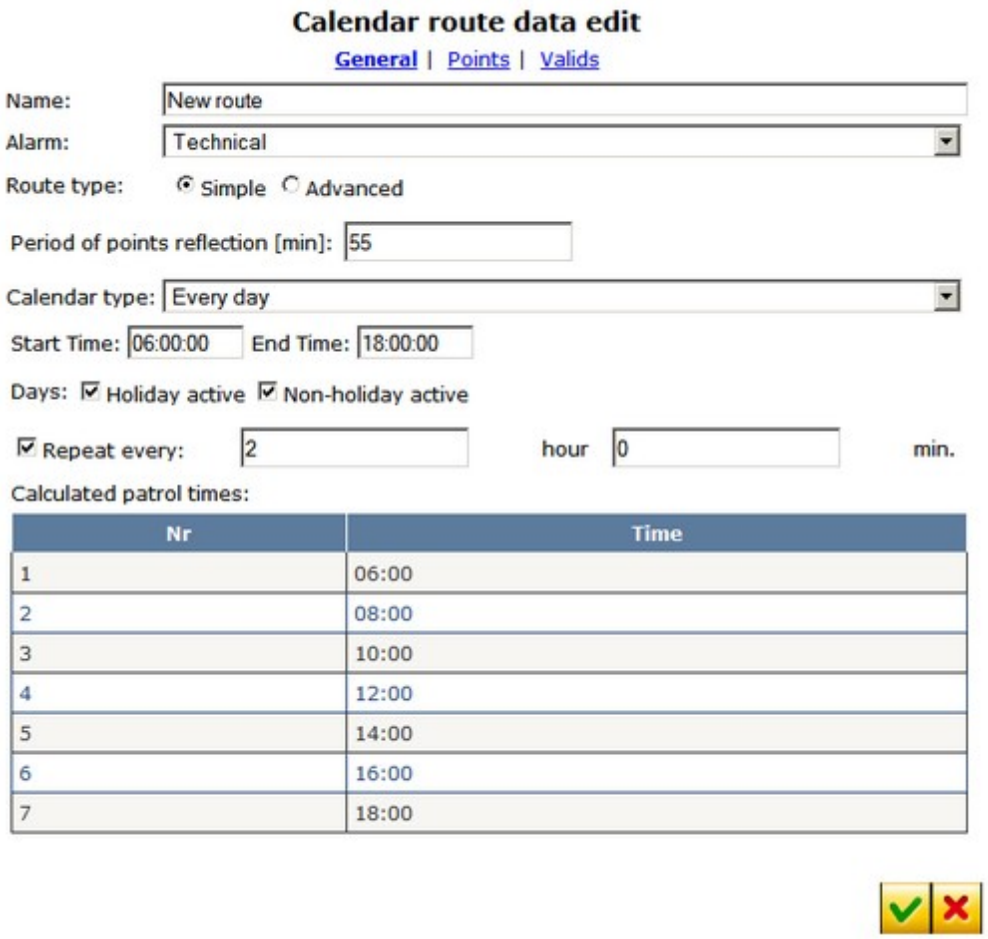
on receipt of an alarm signal.

## New route

Select *Devices* from the menu and click on the *Route edit* icon for any given device.

Click on the *plus* icon and enter the data:

- name
- the type of alarm generated if the route is not completed
- route type:
  - simple - all points should be reflected within the set *point reflection time* but the order of reflections is not important
  - advanced - this allows you to define the order of the reflection points and the time when individual route points should be reflected
- calendar type
- route start and end time
- days on which the route is to be conducted
- at what time period in hours the route should be repeated




Confirm the route.

## 4.4 Device service

This chapter describes how to view historical device data.

### Terminology

- **Signal -** information sent by the device and received by the 4TimeWeb system driver
- **Event -** information generated by the user or by the system on the basis of actions taken relating to account service

## Viewing device signals and events

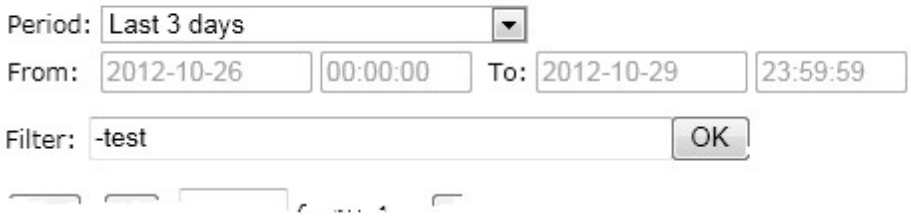
To view summaries:

- select the *Devices* option from the menu.
- Click on the appropriate icon for the chosen device:


*Signal summary*


*Event summary*

- A summary can be generated for any time period. It is also possible to limit the summary displayed by using the signal or event filter.




Each day of the summary is on a separate page. There is an additional tool for viewing individual days of the summary with arrow buttons for changing the day.


## Signal and event filters

The filter is used for refining queries. It works by searching all the data of a defined type in the system for items that include, or do not include, the phrase given.

- The symbol „+” corresponds to the logical *or,* and entering this symbol in front of the phrase means that the phrase is required in items on the list.
- The symbol „-” is for *negation*, and excludes items containing the phrase.
- The symbol „*” means *common section*
- The space symbol„ ” is equivalent to the symbol „+”.

Example 1:
query „+alarm-technical”
searches for **all** alarms **except for** technical (the equivalent of „alarm-technical”).

Example 2:
query "alarm*technical"
searches **only** for technical alarms.

Example 3:
query "alarm technical"

searches for all alarms **and** all technical signals.

If speech marks are used, the special symbols are ignored and the system searches the database for items containing the text exactly as it was entered.

Entering the text *alarm - burglary* is not the same as *alarm-burglary* (where there are no spaces between the special symbol and the text). The system will change the first to alarm+-+burglary (spaces are equivalent to the plus symbol), which changes the meature of the filter.

## 4.5 Notifications

This chapter describes the steps required to enable the SMS text message or email notification function.

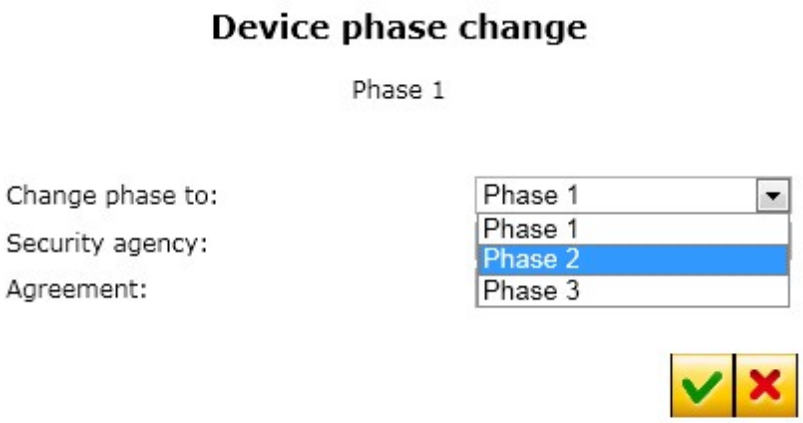
### Terminology

- **Phase -** a device status, which governs access to individual system functions (notification, or device monitoring by an agency).
- **Notification -** information about an alarm or signal sent to a specified contact (telephone number or email address).
- **E-mail summary -** a list of signals, events or payments for a given time period sent to a specified email address.

### Changing device phases

To be able to create SMS text message or email notifications, the device must be set to phase 2 or 3. To change from phase 1 to phase 2:

Select *Devices* from the menu, click on the *Change phase* icon for any given device, and set the appropriate phase.




Phase 2 enables both alarm signals to be received from devices, as well as allowing notifications, for example about an alarm, to be sent to a selected person.

Confirm the device phase change.

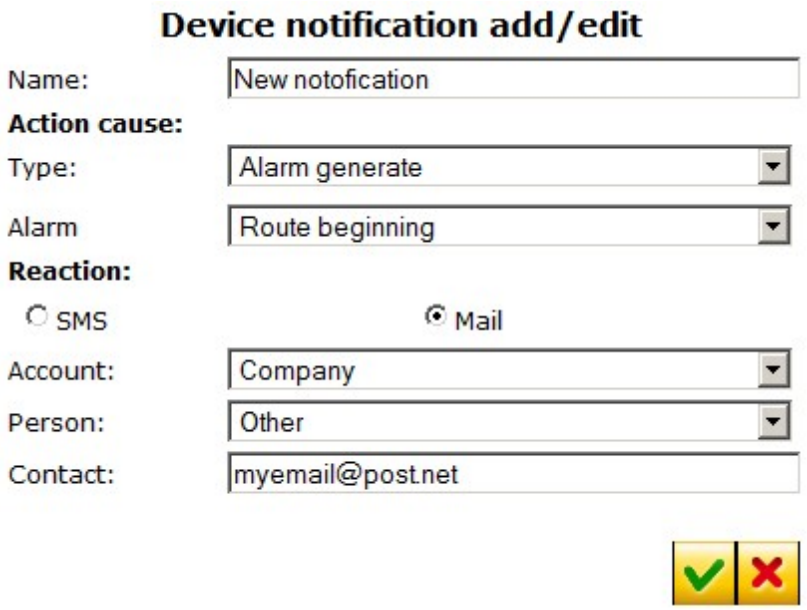
## New notification

After changing the device phase to 2 or 3:

Select *Devices* from the menu and select the *Notification edit* icon for the device.

Click on the *plus* icon and enter:

- notification name
- notification type:
  - signal receiving - select the account name and signal
  - technical signal - select the signal
  - alarm generate - select an alarm
- means of sending notification (SMS text message, e-mail)
- select or enter the telephone number or email address of the person receiving the notification.




Confirm the new notification.

## New email summary

Select *Summaries* from the menu.

Click on the *plus* icon and enter the following data on to the *General* tab:

- name and type of summary
- the period for which the summary is to be generated
- the filter can be used to limit the number of results in the summary
- the email address to which the summary is to be sent

On the *Devices* tab, select the devices the summary is to be generated for.


The time that summaries are sent is defined by the distributor.

Confirm the new summary.

## 4.6 Device monitoring by agencies

This chapter describes the steps required to ensure client device monitoring by a chosen security agency.

### Terminology

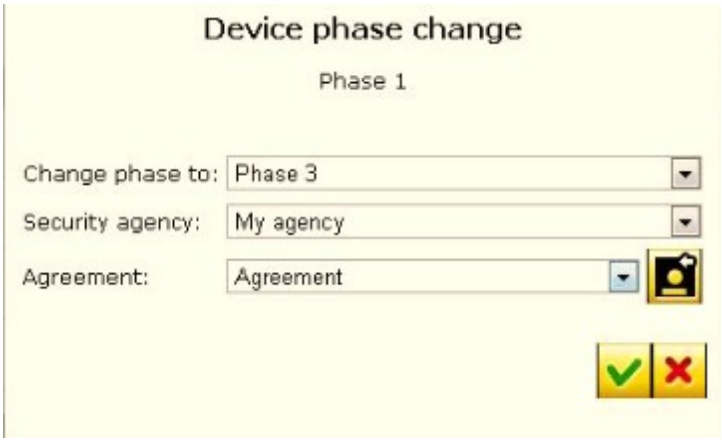
- **Phase -** a device status, which governs access to individual system functions (notification, or device monitoring by an agency).
- **Alarm -** account status displayed on the Console after an alarm signal is received.

### Changing device phases

A device must be set to phase 3 to ensure it is monitored.
To change the phase from 1 to 2 or 3:

Select *Devices* from the menu,click on the *Change phase* icon for any given device, and set:

- the appropriate phase
- the security agency that will be responsible for monitoring the device, in particular for alarm handling.
- the agreement that has been signed between the client and the agency monitoring the device.




Phase 3 enables both alarm signals to be received from devices, as well as allowing SMS text message or email notifications, for example about an alarm, to be sent to a selected person. Phase 3 also enables alarm handling by a chosen security agency.

Confirm the device phase change.