# TS1000 SMARTair™ user manual

Lockwood: *no worries*®

www.assaabloy.co.nz

# Contents

# A – Introduction to the TS1000 manual

# A – INTRODUCTION TO THE TS1000 MANUAL

## A.1 CHAPTERS OF THE TS1000 MANUAL

This manual describes how to install and use the TS1000 Management Software. It is divided into several chapters, whose content is briefly described below, to facilitate its use and consultation. These are the following:

**A Introduction to the TS1000 manual**

This chapter.

**B System description**

Presentation of the different components and structure of the system; useful information for the System Administrator.

**C Licence**

Presentation of the elements provided, as well as the scope of the licence acquired.

**D Setup**

Step by step description of the setup procedure for the TS1000 software.

**E Running the programme for the first time**

There is an explanation on how to proceed the first time the programme is run (Operator Name and Password), as well as the configuration of some initial settings in the “Setup” menu.

**F Creating the Locking Plan**

The Locking Plan defines *Who* can enter, *Where* they can enter and *When* they can enter. This chapter explains how to create it. For this purpose, it is necessary to work with several menus of the TS1000:

- “Users” menu, to define *Who* can enter.
- “Doors” menu, to define *Where* the users will be able to enter.
- “Hours” menu, to create the allowable access hours, that is to say, *When*.
- “Matrix” menu, which, by means of a table, relates *Who*, *Where* and *When*.

Finally, there is an explanation on how to store and transfer the locking plan created.

**G Operators and Operator Levels**

An Operator is a User of the system, who, in turn, can access the TS1000 software to manage the system. It is possible to define Operators with different grants to carry out different management operations in the system, that is to say, different Operators Levels can be defined.

- The different Levels are defined in the “Setup” menu.
- The Operators are added and the Level is assigned to them by means of the “Operators” menu.

### H Grants

The Grants allow granting or denying the access of a user to a door, modifying only the credential of said user, having to neither modify the locking plan nor go to the doors to update such a plan. This is very useful on many occasions.

The Grants are managed by means of three menus:

– Firstly, the grants have to be defined by means of the “Setup” menu.

– Then, the grants have to be assigned to the doors by means of the “Doors” menu.

– Finally, by means of the “Users” menu, the grants are assigned to the users.

### I Programming Credentials and Doors

Once the locking plan, the grants, etc., have been defined, it is necessary to transmit the information both to the credentials of the users (keys, cards, etc.) and to the doors (cylinders, locks, readers, walls, etc.).

It is highly advisable to carry out the programming of the doors before the encoding of the credentials, particularly in Reading/Writing or UoC systems, so that the credentials are not loaded with data unnecessarily.

– The programming of the users credentials is carried out by means of the “Users” menu, using the corresponding device connected to the computer (Portable Programmer, Magnetic Stripe Encoder, Proximity Encoder).

– The doors are programmed on the spot using the Portable Programmer. Previously, it is necessary to have connected the Portable Programmer to the computer and transferred the locking plan to it by means of the “PP” menu (Portable Programmer).

### J Wireless System

The wireless system allows the wireless devices of the doors to communicate with the computer via radio through hubs connected to it. This allows carrying out many operations without having to go physically to the doors with the Portable Programmer

After installing and connecting the hub/s which will connect the computer with the locks by radio, it is necessary to do the following:

– To configure the hubs by means of the “InitHubIP” software.

– To incorporate the hubs and wireless devices of the doors into the system by means of the “Setup” menu of the TS1000.

– To manage the wireless devices of the doors by means of the “Wireless” menu of the TS1000.

### K Site management

After installing the system, once the users start using it, it is time to manage it. This involves the following:

– Reading and deleting user credentials by means of the “Cards” menu.

– Reading and managing the record of openings or events of the doors by means of the “Openings” menu.

– Generating and printing different reports by means of the “Reports” menu. These can be, for example, user lists, door lists, hours, locking plan, etc.

– Managing the record of the operations carried out by the Operators in the system by means of the “Auditor” menu.

### L Other Functions

There are also less common functions which in certain cases can be very useful. They can be found in the “Setup” menu and, in short, they are the following:

– Special functions.

– Deactivation of the Authorisation Key.

– Other credentials: blocking key or card, High Traffic cancelling card, Init Wireless card.

## A.2 TS1000 MAIN FORM

The TS1000 main form, which displays after installing and running the programme, is shown below.

This form allows accessing all the menus which have been mentioned above.

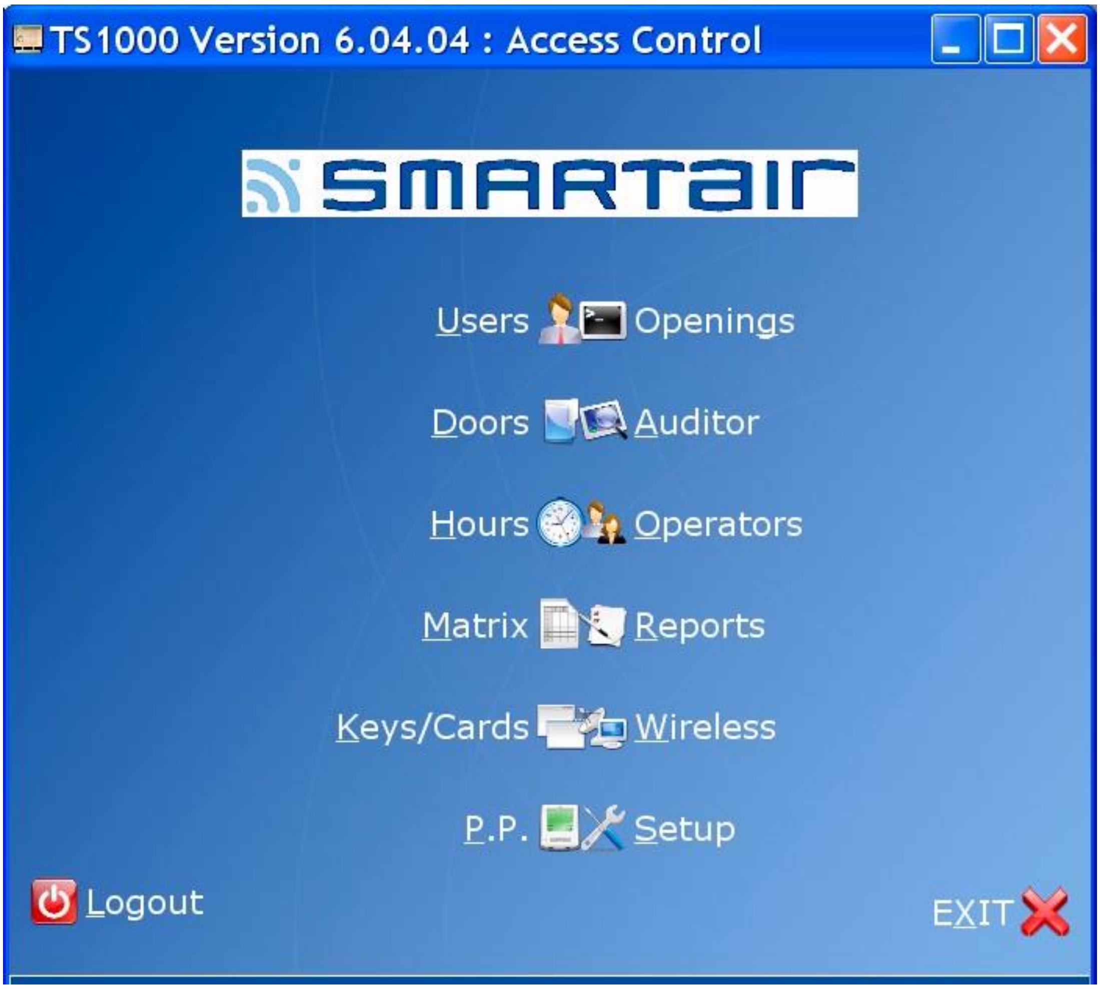


**Fig. 1** TS1000 main form

# B – System description

# B – SYSTEM DESCRIPTION

## B.1 SMARTair TS1000 PLATFORM

The SMARTair TS1000 platform is made up of a server and one or more guests that access it.

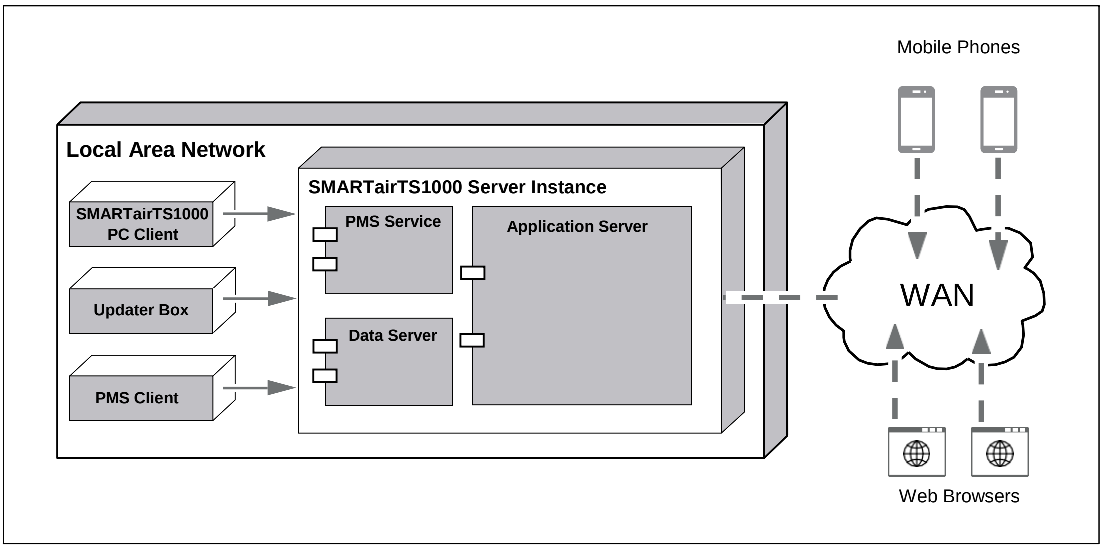


**Fig. 2** System overview

The server, in turn, is made up of 3 components:

- **PMS Service:** this is an autonomous PMS Service which is run in the server. By default, it uses the TCP Port 7779.
- **Data Server:** this is the database system in charge of providing data to the guests through the LAN network. By default, it uses the TCP Port 3050.
- **Application Server:** this is the application in charge of running the applications on the server side. By default, it uses the TCP Port 8181.
- **TimeService:** this is a Service which is configured during setup, and allows synchronising the date and time between the *updaters* and the PCs of the system. It uses port 10101.

The applications on the server side are in charge of running the centralised logic, for example:

- Wireless System management
- Database backup and purge
- E-mail alerts

The application server offers two types of interface, which can be accessed either from inside or outside the LAN network, through the HTTPS secure protocol:

- HTML for access by WEB browser
- SOAP web service interface

# C – Licence

# C – LICENCE

## C.1 INTRODUCTION

The licence of the TESA Access Control system is made up of the following elements:

- Customised TS1000 management software with initial DATA file.
- Authorisation Key.

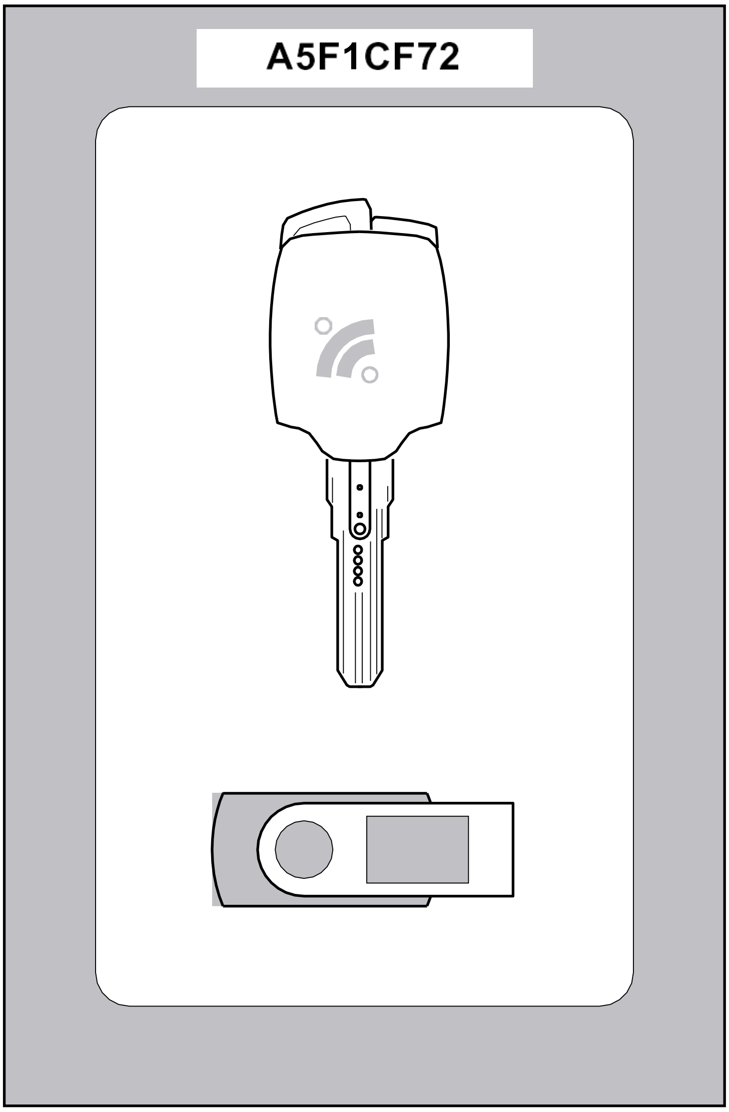


**Fig. 3** Authorisation Key and pen-drive with the Software

## C.2 TS1000 MANAGEMENT SOFTWARE-GUEST

This is the computer application through which the locking plan of the site is scheduled and managed. Therefore, it basically allows making a decision on to whom, where and when access can be granted.

The main features of the TS1000 V6.04 software are the following:

- Easy to use.
- It allows managing all the access control products: electronic cylinders, electronic locks and wall readers (on/off-line).
- It can be run on any PC with Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows Server 2010 or Windows Server 2012 installed.
- Network connection possibility.

## C.3 CUSTOMISED DATA FOLDER

The data related to each site is stored in a file called *Data.fdb* which is saved in a folder called “Data”. This is the data referring to the users, doors, time zones, etc., and it is customised and exclusive for each site.

Therefore, the aforementioned “Data” folder and the files it contains make up the locking plan of a site.

The “Data” folder is created by Talleres de Escoriaza, S. A. and each Data folder is assigned a unique and exclusive System Code.

A System Code is an 8 digit code made up of letters (A-F) and/or numbers (0, 1, ..., 9), such as, for example: A5F1CF72.

When a Data folder is created, it is relatively empty of information. There are no doors, users or time zones defined. Only the System Code is assigned to it.

The distributor or final user is the party who must create the specific locking plan for the site, as described in the corresponding chapter of this manual.

Once the customised locking plan has been created, it is advisable to make a backup of it. In order to make a manual backup, stop the services, copy the *Data.fdb* file to a secure destination and start the services again.

## C.4 AUTHORISATION KEY

The Authorisation Key is a security element which allows preventing possible undesired interventions in the system by third parties.

The Authorisation Key is encoded with the System Code of the locking plan it belongs to.

By default, the Authorisation Key is required in the following cases:

- Data transmission from the Portable Programmer to the cylinders, locks and/or readers.

  In the initialisation, updating and opening operations carried out from the Portable Programmer, the Authorisation Key must be entered in it. Otherwise, the data transmission is not carried out.

  In this way, it is guaranteed that only the person having the Authorisation Key is able to carry out such operations.

  Therefore, it is understood that the Authorisation Key will have to be in the possession of the individual responsible for the security and/or management of the system.

- Authorisation of the keys.

  This function is only available in the STX series, Electronic Cylinders.

  When the user keys are encoded, they do not directly become operative in the system; they are in a non-operative state referred to as “unauthorised key”.

  So as to become operative, the keys require an activation process, which is carried out by means of the Authorisation Key.

  In this way, it is possible to prevent third parties from encoding keys without the consent of the individual responsible for the security and/or management of the system.

## C.5 LICENCE TYPES

The TESA Access Control system, so as to better adapt to the real needs of each site, offers several licence types, based on the following features:

- number of doors: 10, 30, 75 and unlimited
- system type: Off-line, Update On Card, Wireless
- “mobile” licence, which includes the package of functions: Remote opening by mobile, antipassback, e-mail alerts

In the event of having a licence with a door limit, but the number required exceeds the limit specified by the licence, the software will not allow adding more doors. In order to add more doors, it will be necessary to expand the licence.

## C.6 LICENCE EXPANSION

In the event of requiring a licence expansion, it is necessary to contact the distributor and place a licence expansion order.

The licence expansions requiring placement of an order are the following: Antipassback, opening by mobile App, NFC management, System change and Expansion of the number of doors. Contact your distributor if you wish to acquire any of these expansions.

- The order must be accompanied by a copy of the “licence.zip” file which is in the “Data” folder containing the locking plan. The “licence.zip” file is imported and exported by means of the “Tools” application.

  This file can either be sent by e-mail or burnt to a CD.

- Once the order has been placed, a new “licence.zip” file will be sent to you by Talleres de Escoriaza, S.A.
  The new “license.zip” file must be imported with the “Tools” application.

  As from that moment, it will not only be possible to run the management software as you did before, but also to keep adding doors to the site.

# D – Setup

# D – SETUP

## D.1 EXECUTABLE FILE

There is only one executable file for installing both the server as well as the guests. During setup, the installer asks the user if this is a Guest or Server setup.

If the Guest is going to manage wireless devices, the Server will be installed with GlassFish. Otherwise (Guest which is not to manage wireless), the Server will be installed without GlassFish.

It is mandatory to install GlassFish on the server in the event of using wireless management and/or browser management (the wireless system is explained in *"J.1 Wireless system architecture"* on page 131).

If GlassFish is installed on an Update on Card system, the system works in the same way, but with a Java service added to it (the Update on Card system is explained on page 61).

In the event of having only one PC for the setup of the system, the server and the guest will be installed together on the same machine. In a multiuser setup, there will be one complete setup (server + guest) and several guest setups being run on several other machines.

## D.2 SYSTEM REQUIREMENTS

The minimum recommended requirements so as to be able to run the setup (complete setup with guest and server) are the following:

- PC with Pentium 4 or higher.
- 1 GB of free RAM.
- 1 GB of hard disk space.
- Windows operating system (32 bits or 64 bits) with support for services (setup is NOT possible on the Windows 95, Windows 98 and Windows Me platforms).
- The Server communicates through UDP in the range of ports 7780 to 7781 in order to communicate with the wireless devices. These ports must be available and not blocked by the Windows firewall. It also uses the UDP 7790, TCP 7890 and TCP 7881 ports.
- The Server communicates through TCP by means of port 3050 (this port can be configured during the setup process) in order to communicate with the database server. This port must be available and not blocked by the Windows firewall.
- The Server communicates through TCP by means of port 8181 (this port can be configured during the setup process) in order to communicate with the web applications. This port must be available and not blocked by the Windows firewall.
- Communication by means of UDP port 10101 for the Time Service, which allows synchronising the date and time between the PCs and updaters of the system.
- The Software can be run with minimum requirements, but it is important to point out that the server needs to have free RAM available so as to run properly. As a result, it is advisable to have 1GB of free RAM memory for the server.

## D.3 SETUP PREPARATION

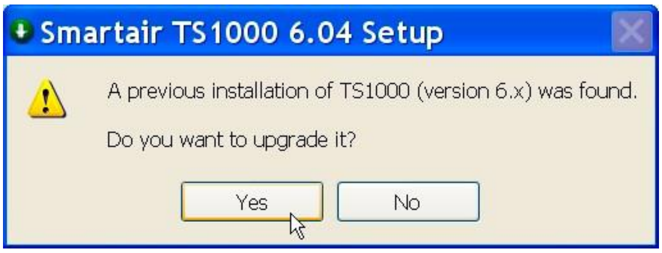
Before starting with the setup, a series of points have to be considered. One of the most important points is the selection of the PC where the Server is to be installed. Consider the following:

- The Server will be the PC where the *data* is installed. The option Server necessarily has to be chosen for that PC.
- The PC used as a Server has to be always on to allow the guest PCs not only to access both the database and the services, but also to deal with the wireless hubs and doors.
- Try to choose the PC with the largest capacity as the server so that it is able to manage in the best possible way communications with the rest of the guest PCs.

## D.4 UNINSTALLING OLDER VERSIONS OF THE TESA APPLICATION - SMARTair TS1000

The installer verifies the system, trying to find older versions of the application. Before proceeding to the setup of the application, it asks whether you wish it to be updated to a more recent version or not.

When updating a version of the software 5.x or higher, the installer asks whether you wish to replace the existing version or not before proceeding to the setup of the application.


Smartair TS1000 6.04 Setup

A previous installation of TS1000 (version 6.x) was found.

Do you want to upgrade it?

- If you choose the option “YES”, to replace the older version, it will be uninstalled from the system and replaced by the new version.
- If you choose “NO”, not to replace, version 5.x will not be uninstalled and the new version will be installed in parallel. In this way, it is possible to have both versions installed on the same PC.

When versions 5.x and 6.x are installed on the same PC, take into account that the same ports will be shared by both versions (for example, the ports of the system of wireless communications or the ports of PMS communications). It will not be possible to run both versions simultaneously.

In order to be able to run version 6.x of the SMARTair TS1000 application, version 5.x must be closed if both versions are being run in the same PC. The same rule has to be followed if you want to run version TESA - SMARTair TS1000 5.x: the services “TESA_APPSERVER Glassfish Server” and “TESA_APPSERVER PMS Service” must be stopped before being able to run it.

## D.5 SETUP PROCESS

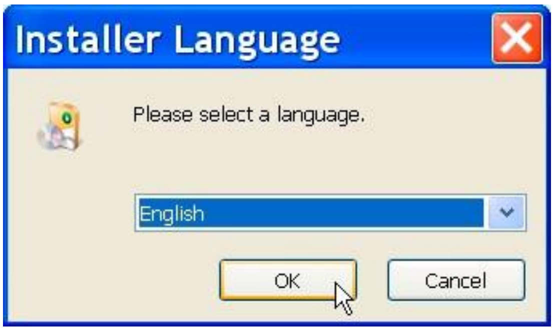
□Administrator rights are necessary so as to be able to install the application. For more information, contact your system administrator.

1 Insert the Pen-Drive. It is advisable to copy the “TS1000 6.04 Setup.exe” file to the PC which will work as a Server to run it from there.

2 Run the “TS1000 6.x Setup.exe” programme (the one you have copied to the PC which will work as a Server).

3 Select the language to be used during the setup.

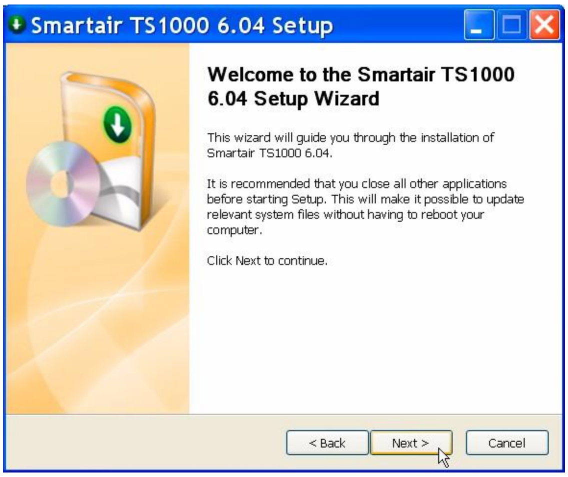
Click “OK” to continue.



Please select a language.

4 A welcome message is displayed.

Click “Next” to continue with the setup.



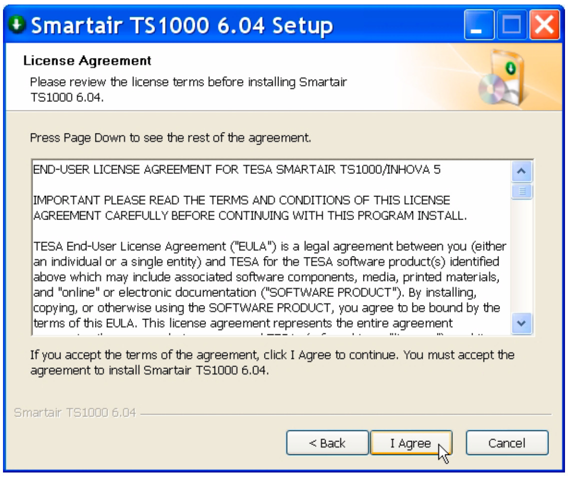
**Welcome to the Smartair TS1000 6.04 Setup Wizard**

This wizard will guide you through the installation of Smartair TS1000 6.04.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

5 Read and accept the licence terms.



**License Agreement**

Please review the license terms before installing Smartair TS1000 6.04.

Press Page Down to see the rest of the agreement.

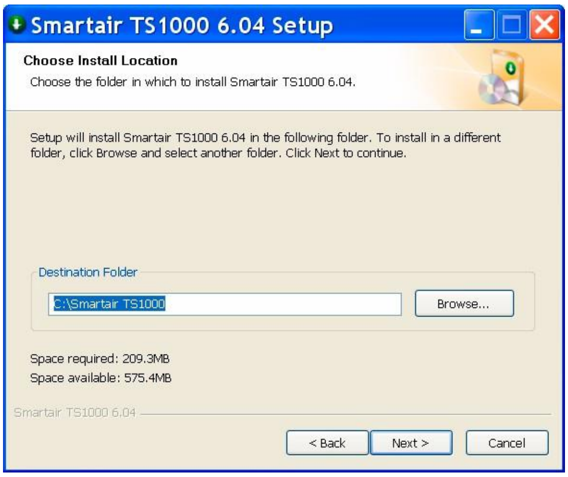
END-USER LICENSE AGREEMENT FOR TESA SMARTAIR TS1000/INHOVA 5

IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL.

TESA End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and TESA for the TESA software product(s) identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Smartair TS1000 6.04.

**6** Specify the path for the setup.



Smartair TS1000 6.04 Setup

**Choose Install Location**

Choose the folder in which to install Smartair TS1000 6.04.

Setup will install Smartair TS1000 6.04 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Smartair TS1000

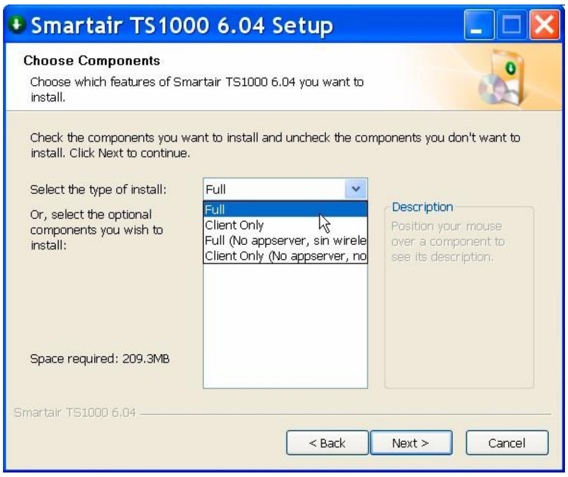
Space required: 209.3MB

Space available: 575.4MB

**7** Select the setup type:

- “Complete (Server+Guest) with Wireless”,
- “Guest Only, with Wireless”,
- “Basic, without Wireless” (server without GlassFish service),
- “Guest Only, without Wireless” (without GlassFish service),

and click “Next” (the last two options are used in Update on Card systems which do not require wireless support, when, in addition, you do not want to use the system through a web browser).



Smartair TS1000 6.04 Setup

**Choose Components**

Choose which features of Smartair TS1000 6.04 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full

Or, select the optional components you wish to install:

Full
Client Only
Full (No appserver, sin wirele
Client Only (No appserver, no

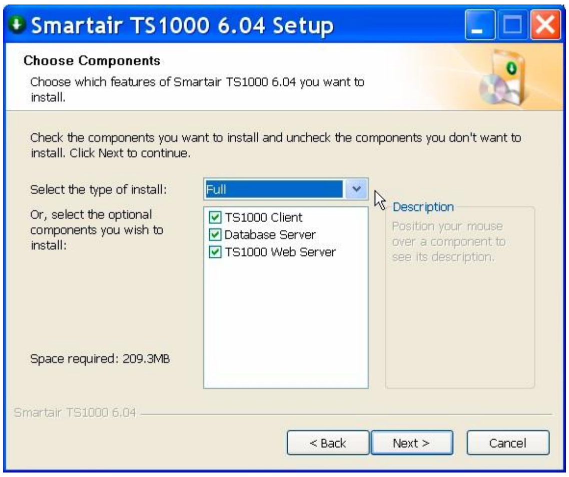
Space required: 209.3MB

Description
Position your mouse over a component to see its description.
Smartair TS1000 6.04
< Back
Next >
Cancel

## Complete Setup

The option “Complete Setup” installs the files both of the Server and the Guest on the PC selected.

**1** After selecting the option “Complete Setup”, click the “Next” button to continue.



Smartair TS1000 6.04 Setup

**Choose Components**

Choose which features of Smartair TS1000 6.04 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full

Or, select the optional components you wish to install:

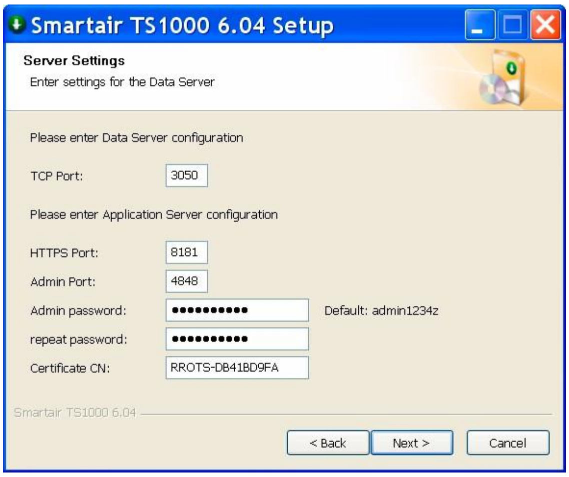
☑ TS1000 Client
☑ Database Server
☑ TS1000 Web Server

Space required: 209.3MB

Description
Position your mouse over a component to see its description.
Smartair TS1000 6.04
< Back
Next >
Cancel

2 The “Server Settings” screen is displayed, which allows you to configure the parameters of the server.
Configure the parameters (see the table below) and click “Next” to continue.

Afterwards, each time you want to make changes to the Server settings, you will need the Administrator password. It is advisable to keep a written copy of the password in a safe place in case it is necessary to consult it in the future.


Smartair TS1000 6.04 Setup

Server Settings
Enter settings for the Data Server

Please enter Data Server configuration

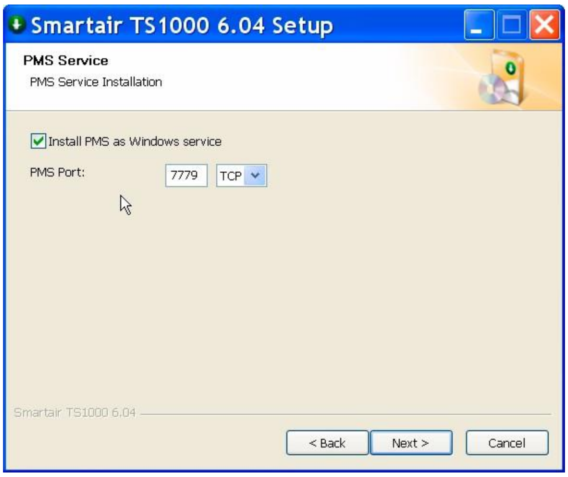
TCP Port: 3050

Please enter Application Server configuration

HTTPS Port: 8181
Admin Port: 4848
Admin password: •••••••••• Default: admin1234z
repeat password: ••••••••••
Certificate CN: RROTS-DB41BD9FA

| Server settings | Default value | Description |
|---|---|---|
| TCP port of the data server | 3050 | TCP communication port of the application with the dataserver |
| HTTPS port | 8181 | HTTPS communication port with the application server |
| Communication port for the PMS protocol | 7779/TCP | Port by means of which the PMS communicates with the PMS service |
| TimeService port | 10101 | |
| Administrator port | 4848 | Administrator communication port with the application server |
| Admin Password | admin1234z | Password to access the Web Server configuration module as an administrator |
| Certificate CN | | Name which will appear in the SSL certificate of the server. It must coincide with the IP or machine name used in the browser for web access. |

3 Configure the PMS service and click “Next” to continue.
By default, the PMS service is off.



Smartair TS1000 6.04 Setup

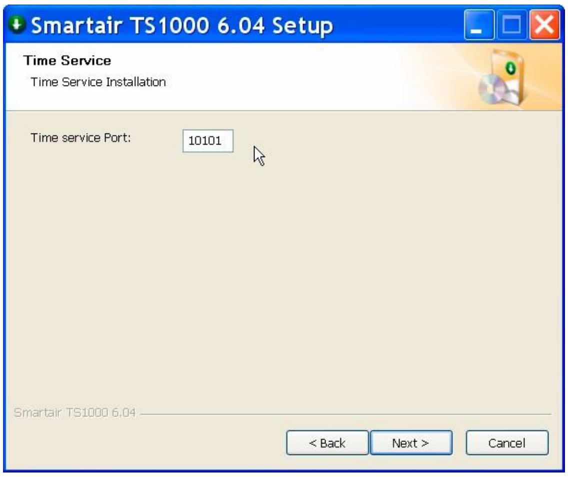
**PMS Service**

PMS Service Installation

☑ Install PMS as Windows service

PMS Port: 7779 TCP

4 Configure the port for the Time service and click “Next” to continue.



Smartair TS1000 6.04 Setup

**Time Service**

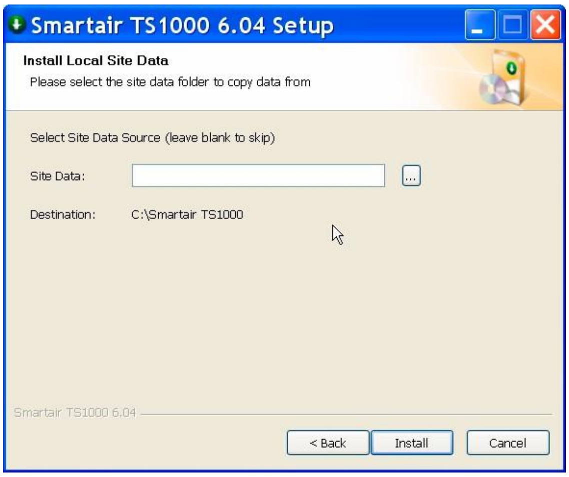
Time Service Installation

Time service Port: 10101

5 Data folder: source (physical unit and path) where the database (Data.fdb) to be used is hosted.

□It is necessary to use the database provided in the *Pen-Drive*, as it has been customised according to your order.

The database will be copied to the internal local directory of the database server.



Smartair TS1000 6.04 Setup

**Install Local Site Data**

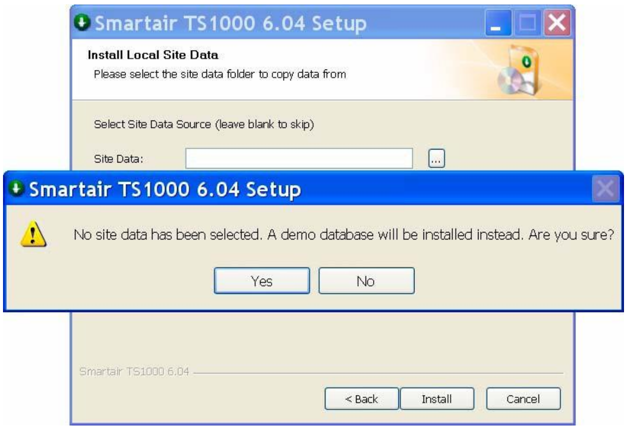
Please select the site data folder to copy data from

Select Site Data Source (leave blank to skip)

Site Data:

Destination: C:\Smartair TS1000

- □ If you have not selected the source of the database, a “demo” database is installed by default. **THE “demo” OPTION MUST NOT BE USED ON A REAL SITE, as its features are limited and it is not customised according to your order. The “demo” option is appropriate only for tests and demonstrations.**



Smartair TS1000 6.04 Setup

Install Local Site Data

Please select the site data folder to copy data from

Select Site Data Source (leave blank to skip)

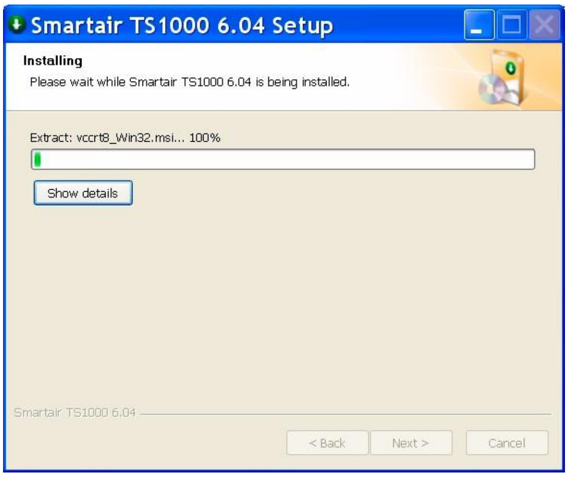
Site Data:

Smartair TS1000 6.04 Setup

No site data has been selected. A demo database will be installed instead. Are you sure?

6 In order to configure the fields, click “Install” to continue with the setup.

The setup files will be copied to the PC in the following step. Click “See Details” if you wish to view the setup process.



Smartair TS1000 6.04 Setup

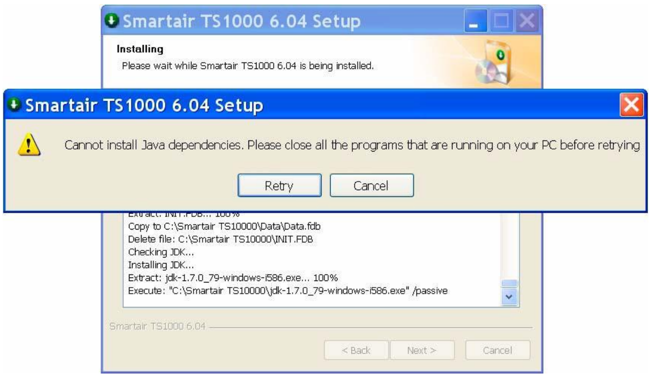
Installing

Please wait while Smartair TS1000 6.04 is being installed.

Extract: vccrt8_Win32.msi... 100%

7 The setup begins.

If the PC used does not have Java, or it does not have the required version, the setup will be carried out. In such a case, a message pointing this out is displayed. Follow its instructions and click “Try again”.



Smartair TS1000 6.04 Setup

Installing

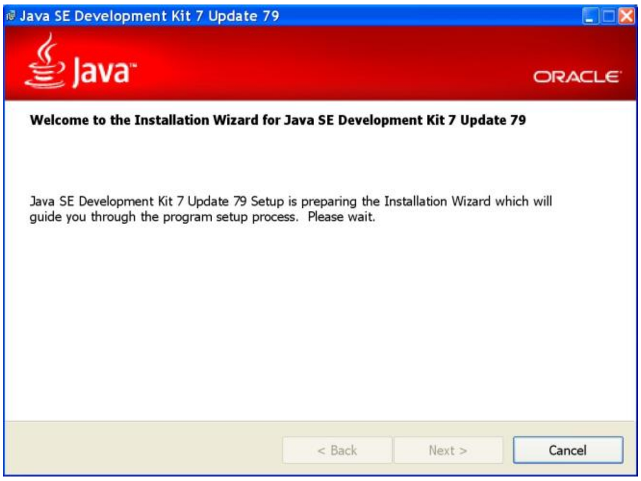
Please wait while Smartair TS1000 6.04 is being installed.

Smartair TS1000 6.04 Setup

Cannot install Java dependencies. Please close all the programs that are running on your PC before retrying

```
Extract: INIT.FDB... 100%
Copy to C:\Smartair TS10000\Data\Data.fdb
Delete file: C:\Smartair TS10000\INIT.FDB
Checking JDK...
Installing JDK...
Extract: jdk-1.7.0_79-windows-i586.exe... 100%
Execute: "C:\Smartair TS10000\jdk-1.7.0_79-windows-i586.exe" /passive
```

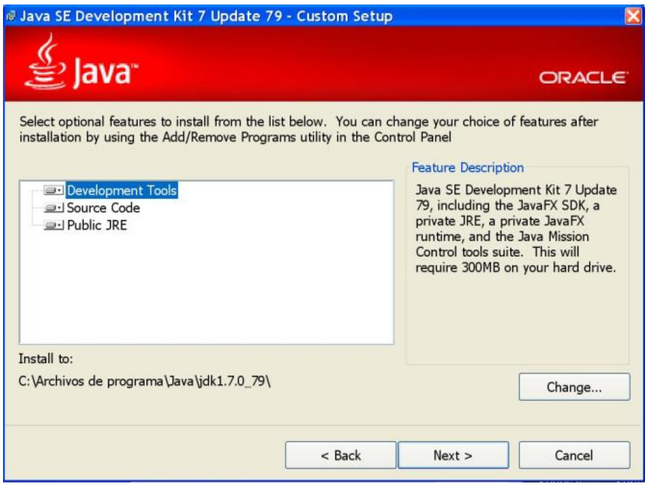
8 Java is installed.



Java SE Development Kit 7 Update 79

**Welcome to the Installation Wizard for Java SE Development Kit 7 Update 79**

Java SE Development Kit 7 Update 79 Setup is preparing the Installation Wizard which will guide you through the program setup process. Please wait.



Java SE Development Kit 7 Update 79 - Custom Setup

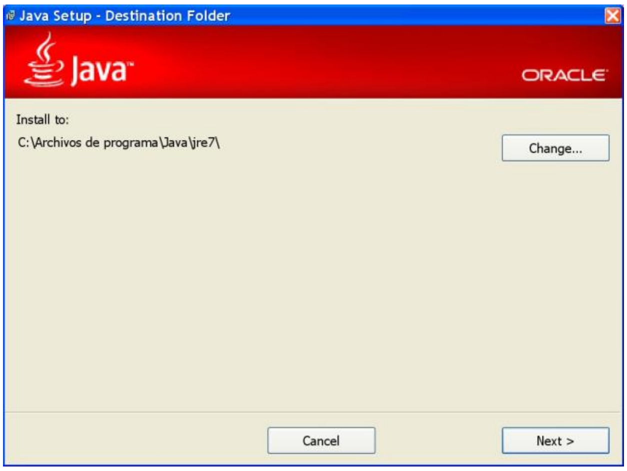
Select optional features to install from the list below. You can change your choice of features after installation by using the Add/Remove Programs utility in the Control Panel

Feature Description

Java SE Development Kit 7 Update 79, including the JavaFX SDK, a private JRE, a private JavaFX runtime, and the Java Mission Control tools suite. This will require 300MB on your hard drive.

Install to:

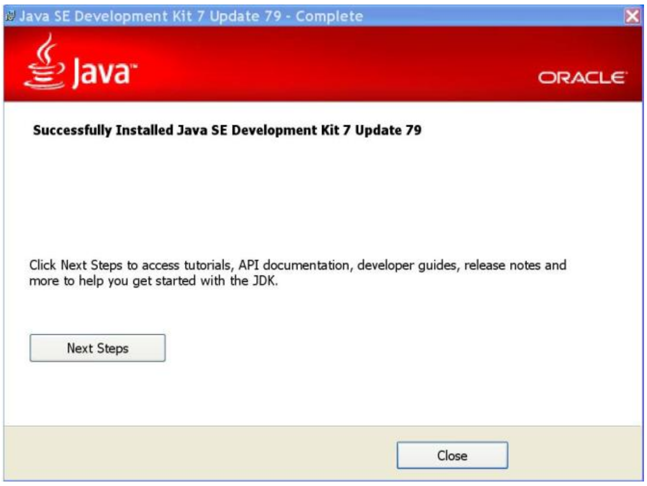
C:\Archivos de programa\Java\jdk1.7.0_79\



Java Setup - Destination Folder

Install to:

C:\Archivos de programa\Java\jre7\

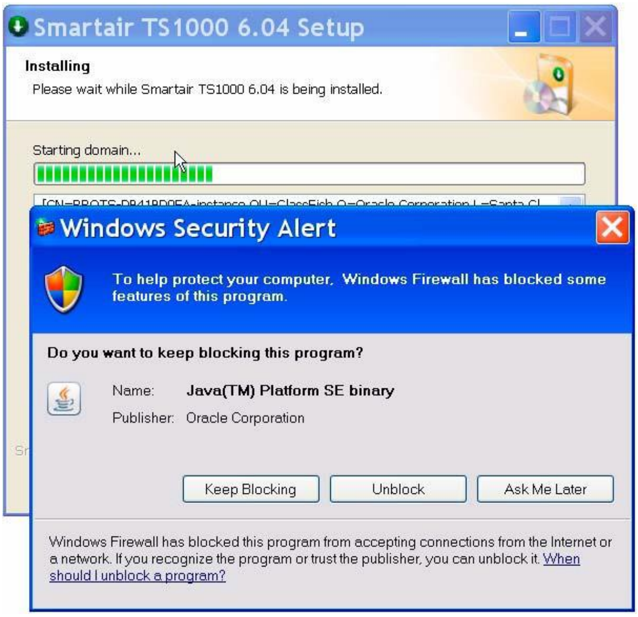


Java SE Development Kit 7 Update 79 - Complete

**Successfully Installed Java SE Development Kit 7 Update 79**

Click Next Steps to access tutorials, API documentation, developer guides, release notes and more to help you get started with the JDK.

**9** A warning is displayed indicating that the port which was previously configured in the Windows firewall will be opened. Click “Unblock”.



Smartair TS1000 6.04 Setup

**Installing**

Please wait while Smartair TS1000 6.04 is being installed.

Starting domain...

```
[CN=PROTS-DB418D0FA-instance,OU=GlassFish,O=Oracle Corporation,L=Santa Cl
```

Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

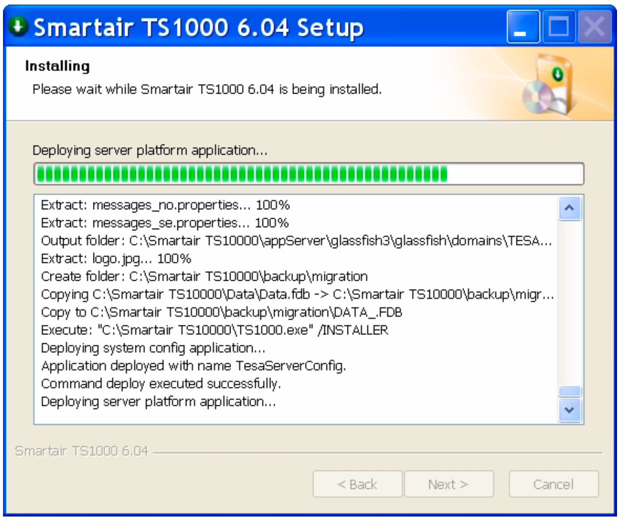
**Do you want to keep blocking this program?**

Name: **Java(TM) Platform SE binary**

Publisher: Oracle Corporation

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

**10** The setup continues.



Smartair TS1000 6.04 Setup

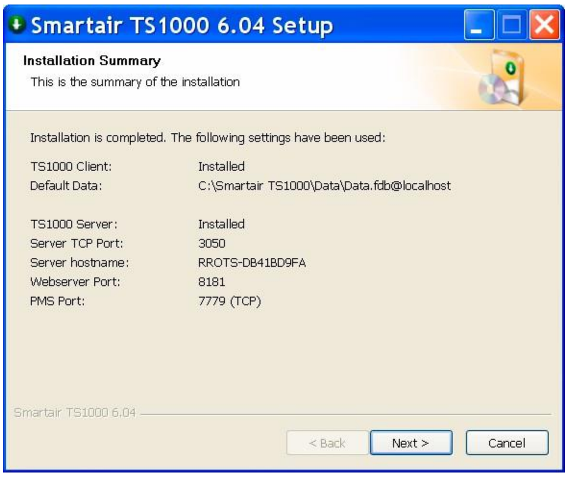
**Installing**

Please wait while Smartair TS1000 6.04 is being installed.

Deploying server platform application...

```
Extract: messages_no.properties... 100%
Extract: messages_se.properties... 100%
Output folder: C:\Smartair TS10000\appServer\glassfish3\glassfish\domains\TESA...
Extract: logo.jpg... 100%
Create folder: C:\Smartair TS10000\backup\migration
Copying C:\Smartair TS10000\Data\Data.fdb -> C:\Smartair TS10000\backup\migr...
Copy to C:\Smartair TS10000\backup\migration\DATA_.FDB
Execute: "C:\Smartair TS10000\TS1000.exe" /INSTALLER
Deploying system config application...
Application deployed with name TesaServerConfig.
Command deploy executed successfully.
Deploying server platform application...
```

**11** The setup summary is shown. Note down the data in case you need them in the future.
Click “Next” to continue.



Smartair TS1000 6.04 Setup

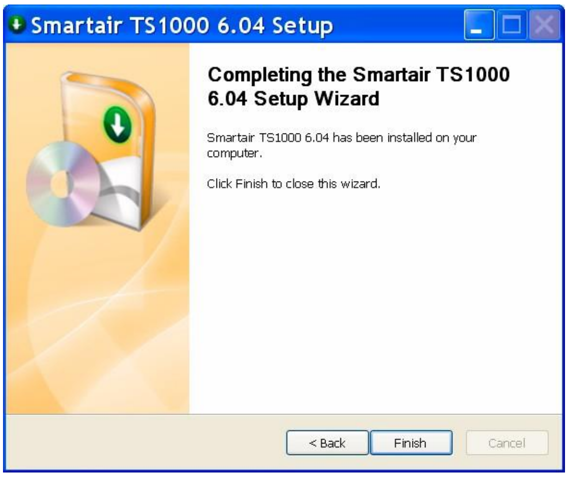
Installation Summary
This is the summary of the installation

Installation is completed. The following settings have been used:

TS1000 Client: Installed
Default Data: C:\Smartair TS1000\Data\Data.fdb@localhost

TS1000 Server: Installed
Server TCP Port: 3050
Server hostname: RROTS-DB41BD9FA
Webserver Port: 8181
PMS Port: 7779 (TCP)

**12** The server setup is completed.
Click “End”.



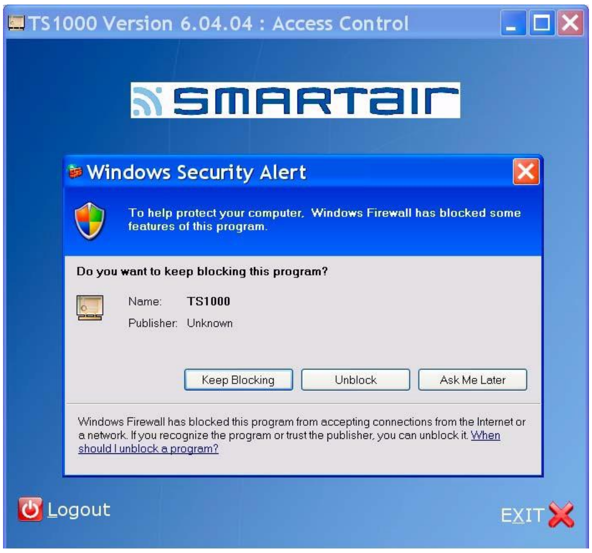
Smartair TS1000 6.04 Setup

Completing the Smartair TS1000 6.04 Setup Wizard

Smartair TS1000 6.04 has been installed on your computer.

Click Finish to close this wizard.

**13** If the firewall warning shown is displayed, click “Unblock”.



TS1000 Version 6.04.04 : Access Control

Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

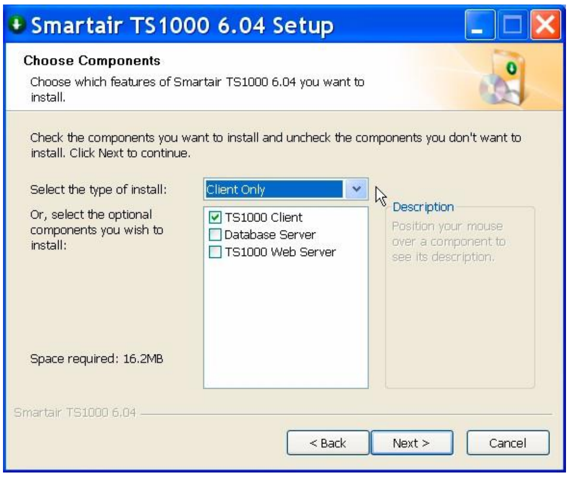
Name: TS1000
Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

## Setup of the Guest Only, with Wireless mode

A setup of type Guest Only with Wireless installs the application in the Guest Only mode on the PC, which allows managing wireless devices. A PC with the TESA SMARTair TS1000 application in the Guest Only mode communicates with the application server through TCP/IP to access the database and services.

1 Select the setup type "Guest Only" and click "Next".



Smartair TS1000 6.04 Setup

Choose Components

Choose which features of Smartair TS1000 6.04 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Client Only

Or, select the optional components you wish to install:

☑ TS1000 Client
□ Database Server
□ TS1000 Web Server

Description

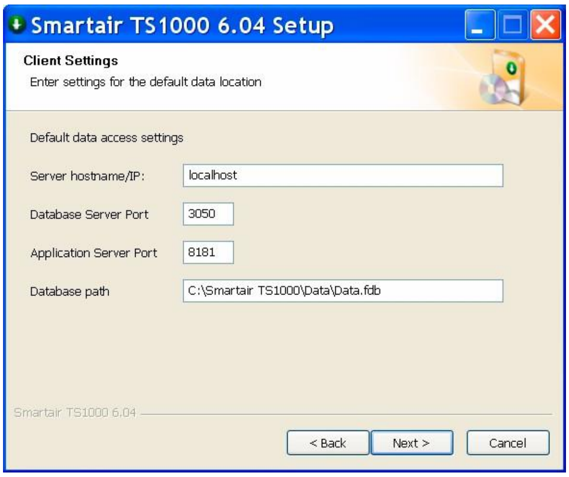
Position your mouse over a component to see its description.

Space required: 16.2MB

Smartair TS1000 6.04

2 Apply the Guest Settings, which involves configuring the parameters of the Server for the Guest PCs.

Once you have finished, click "Next" to continue.



Smartair TS1000 6.04 Setup

Client Settings

Enter settings for the default data location

Default data access settings

Server hostname/IP: localhost

Database Server Port: 3050

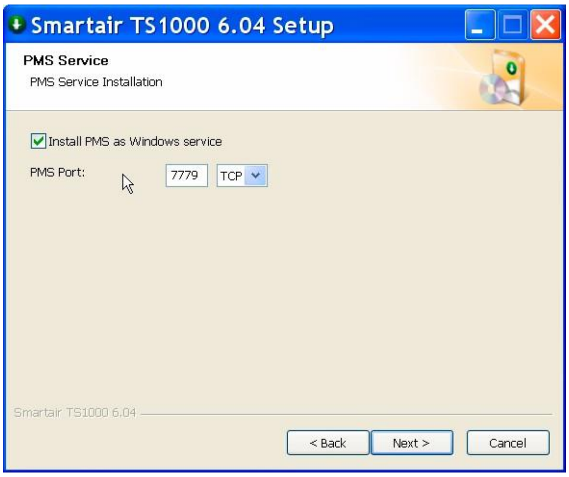
Application Server Port: 8181

Database path: C:\Smartair TS1000\Data\Data.fdb

Smartair TS1000 6.04

| Server settings | Description |
|---|---|
| Name of the Server PC on the network/IP | Name of the Server PC on the network itself or, otherwise, the IP address on the network |
| Port of the Database Server | TCP port through which a communication is established with the Server which contains the Database |
| Port of the application Server | TCP port through which a communication is established with the application Server |
| Target address of the Database | Directory where the Database is located |

**3** Configure the PMS service (in the event of being necessary in your site).
By default, the PMS service is off.



Smartair TS1000 6.04 Setup

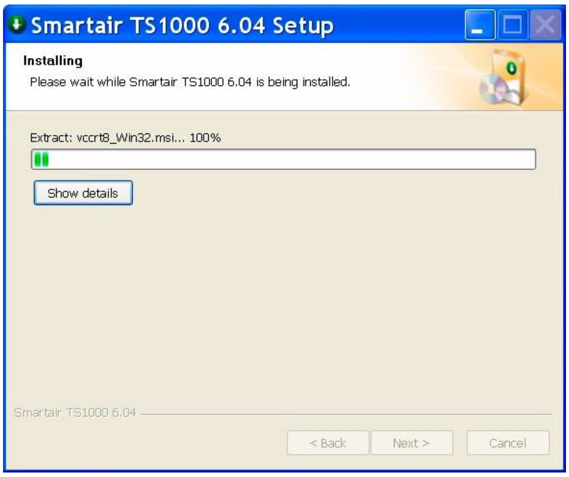
PMS Service

PMS Service Installation

☑ Install PMS as Windows service

PMS Port: 7779 TCP

**4** The setup is carried out.



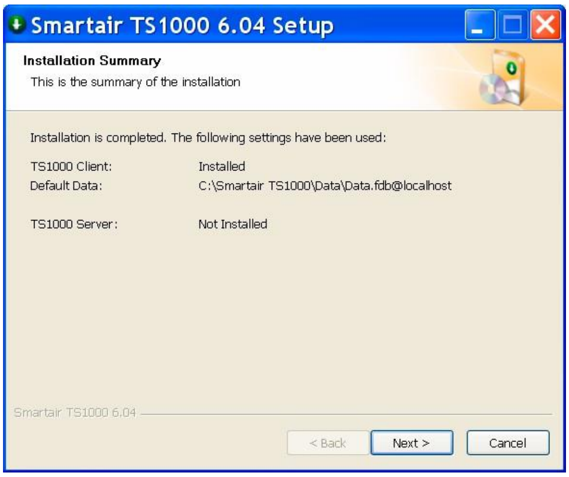
Smartair TS1000 6.04 Setup

Installing

Please wait while Smartair TS1000 6.04 is being installed.

Extract: vccrt8_Win32.msi... 100%

**5** Once the setup has been finished, the application displays a summary screen.



Smartair TS1000 6.04 Setup

Installation Summary

This is the summary of the installation

Installation is completed. The following settings have been used:

| | |
|---|---|
| TS1000 Client: | Installed |
| Default Data: | C:\Smartair TS1000\Data\Data.fdb@localhost |
| TS1000 Server: | Not Installed |

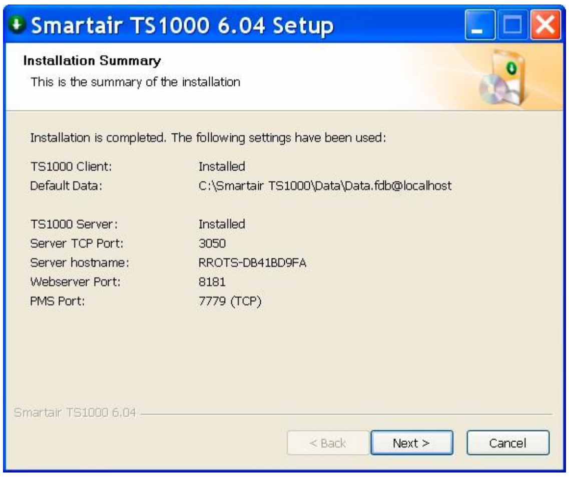
## Summary and end of the application setup

In order to finish the setup process (either Server+Guest or Guest Only), a summary screen is displayed with the parameters defined.

It is advisable to keep a copy of the configuration parameters of the computer working as Server+Guest. These data could be useful as a reference for future setups or configurations.

Furthermore, an "Instal.log" file is generated, which is stored in the setup directory. This file provides valuable information for Technical Service, for example, in order to solve possible issues during the setup.

Click the "Next" button to continue.



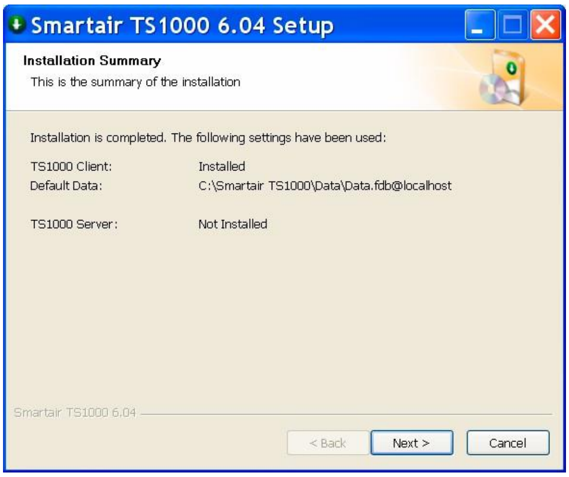
Smartair TS1000 6.04 Setup

Installation Summary

This is the summary of the installation

Installation is completed. The following settings have been used:

| | |
|---|---|
| TS1000 Client: | Installed |
| Default Data: | C:\Smartair TS1000\Data\Data.fdb@localhost |
| TS1000 Server: | Installed |
| Server TCP Port: | 3050 |
| Server hostname: | RROTS-DB41BD9FA |
| Webserver Port: | 8181 |
| PMS Port: | 7779 (TCP) |



Smartair TS1000 6.04 Setup

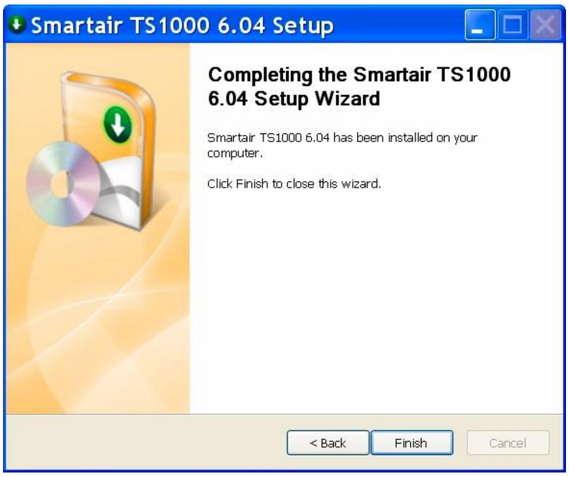
Installation Summary

This is the summary of the installation

Installation is completed. The following settings have been used:

| | |
|---|---|
| TS1000 Client: | Installed |
| Default Data: | C:\Smartair TS1000\Data\Data.fdb@localhost |
| TS1000 Server: | Not Installed |

The application setup finishes at this point. Click the "End" button to finish the setup.



Smartair TS1000 6.04 Setup

Completing the Smartair TS1000 6.04 Setup Wizard

Smartair TS1000 6.04 has been installed on your computer.

Click Finish to close this wizard.

Once the complete setup has been finished, the Server generates two web applications which can be accessed through the web browser:

| Application | URL[a] |
|---|---|
| TESA - SMARTair TS1000 Web Application | https://host:8181/TesaSmartairPlatform |
| Web Server Settings Application | https://host:8181/TesaServerConfig |

[a] replace host by the IP address of the server

## Windows services installed

The Web Server installs several Windows services on the system, depending on the selections made during the setup.

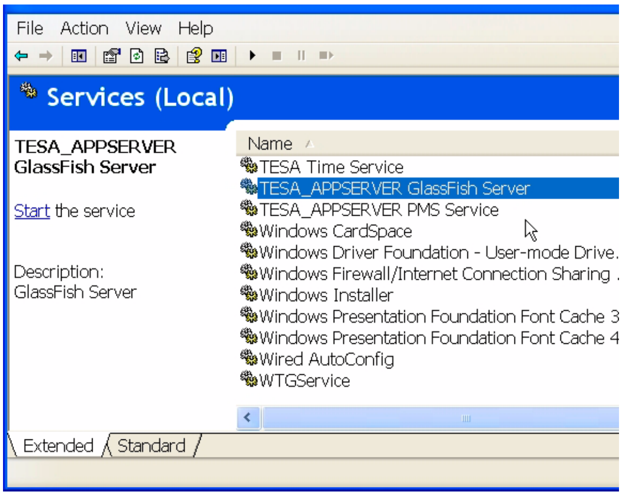
All the possible services are shown below, in spite of the fact that only the ones selected are installed:

| Name of the Windows service | Description |
|---|---|
| Firebird Server TESA_DATASERVER_6 | Database server<br>This is always installed |
| TESA Time Service | Service for synchronising the Date and Time with updaters |
| TESA_APPSERVER GlassFish Server | Application server<br>This is not installed in the Basic (without wireless) and Guest Only (without wireless) options |
| TESA_APPSERVER PMS Service * | PMS service (TCP only) |

* TESA_APPSERVER PMS Service is only installed if during the setup process, in the step related to the configuration of the PMS service, the "Install as a Windows service" option has been selected.

By default, all these Services are run automatically when the PC is powered on. It is possible to specify that the services be run manually or disable them directly.

They are standard Windows Services, and therefore they can be stopped or started using the services.msc Windows utility (from the Run menu of Windows).



Services (Local)

TESA_APPSERVER GlassFish Server

Start the service

Description:
GlassFish Server

Name
TESA Time Service
TESA_APPSERVER GlassFish Server
TESA_APPSERVER PMS Service
Windows CardSpace
Windows Driver Foundation - User-mode Drive.
Windows Firewall/Internet Connection Sharing .
Windows Installer
Windows Presentation Foundation Font Cache 3
Windows Presentation Foundation Font Cache 4
Wired AutoConfig
WTGService

## D.6 CONFIGURATION OF THE GUEST PC

Configuration to connect the Guest PCs to the Server can be carried out by editing the `Config.ini` file which is in the directory where the executable files of the application are located in the Guest PC. By default, the folder is “C:\SMARTair TS1000”.

The lines to be edited are the ones displayed under the heading [SERVER].

| Parameter | Description |
|---|---|
| DataServer | IP address or name of the Server PC on the network |
| DataServerPort | TCP port by means of which the Database Server communicates |
| DatabasePath | Complete path with physical unit to the file of the database (*.fdb file).<br>By default: “C:\SMARTair TS1000\Data\Data.fdb” |
| WebServer | IP address or name of the Server PC on the network |
| WebServerPort | HTTPS port by means of which the application Server communicates |

Example of `config.ini` file:

```
[SERVERS]
DataServer=210.110.20.28
DataServerPort=3050
DatabasePath=C:\Data\Data.fdb
WebServer=210.110.20.28
WebServerPort=8181
```

□ If there is a firewall on the Guest PC, make sure the TCP entry ports 3050 and 8181 (standard ports) are open and not in use.
These standard ports can only be modified during the server setup. These ports are applicable to the server and to all the guests installed.

## D.7 CONFIGURATION OF THE SERVER PC

The Server PC must be configured to work with the database intended to be used.

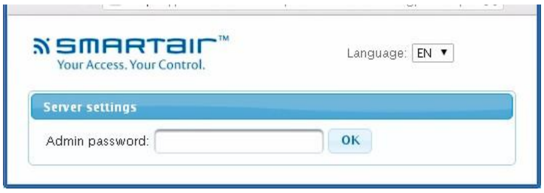
In the event of selecting a local database during the setup process, the Server is configured automatically; therefore, this step is not necessary.

The Server settings can be accessed through the following direct access to the Server configurator:

https://host:8181/TesaServerConfig

*replace host by the IP address of the server.

An administrator password is requested to access the configuration (this password was configured during the application setup, see *"Admin Password"* on page 25):



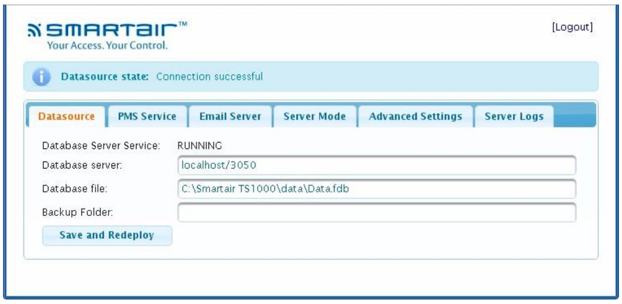
### Configuration of the datasource

The data of the database server and the location of the database on the server are defined in the Datasource tab of the "Datasource state".

The following parameters have to be configured:

| Parameter | Description | Example |
|---|---|---|
| Database server | Name of the PC which contains the DATA and its Communication port.<br>Format: Server name/port or IP/port<br>This must always coincide with the path written in the config.ini file of the guests and the server. | host/3050 |
| Database file | Path to the FDB Database file | C:\Data\Data.fdb |

Click the "Save and Deploy" button to save the changes. This operation can take several minutes (wait).

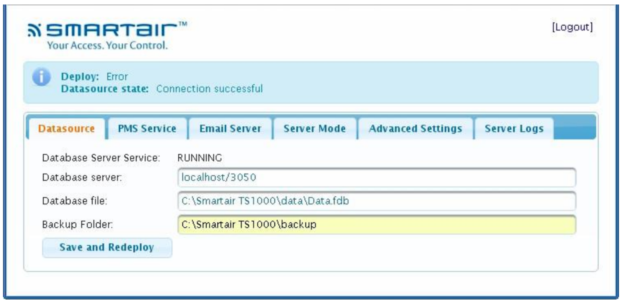


Datasource state: Connection successful

Database Server Service: RUNNING
Database server: localhost/3050
Database file: C:\Smartair TS1000\data\Data.fdb
Backup Folder:

Once the operation has been completed, the messages “Deployment: OK” and “Datasource state: Connection successful” will be displayed.

The deployment does not always end when the OK message appears. This depends on the stabilisation of the *java.exe* processes and, depending on the server, it can take several minutes. It is necessary to wait or confirm that the *java.exe* processes are stable with the Task Manager of Windows.



Deploy: Error
Datasource state: Connection successful

Database Server Service: RUNNING
Database server: localhost/3050
Database file: C:\Smartair TS1000\data\Data.fdb
Backup Folder: C:\Smartair TS1000\backup

If it is not possible to connect to the database, the following error message will be displayed: “Datasource state: Cannot communicate”.

In this case, verify whether the data are correct: the server name, the communication port and the location of the database.

After verifying these data, try to communicate again.

## Configuration of the PMS Service

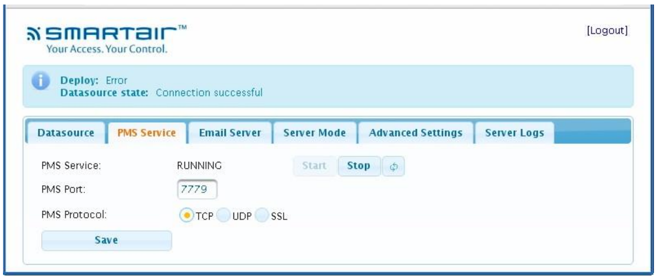
In order to configure the PMS Service, access the “PMS Service” tab and configure the following settings (this tab only appears if, during the setup, the option “Install as a Windows service” has been selected, on the screen “PMS service setup”):

| Server | Description |
|---|---|
| PMS Port | Port number for the PMS requests |
| PMS Protocol | Type of communication with the PMS: TCP, UDP or SSL |

The SSL protocol allows a high degree of encryption over the TCP protocol, and ensures the integrity and confidentiality of data.

It is advisable to use the SSL protocol if the PMS guest is compatible.

Click the “Save” button to save the changes made.



Deploy: Error
Datasource state: Connection successful

PMS Service: RUNNING
PMS Port: 7779
PMS Protocol: ● TCP ○ UDP ○ SSL

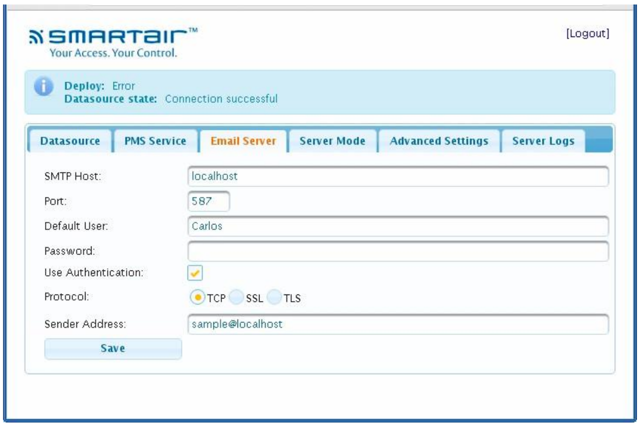
## Configuration of the E-mail Server

The Server can be configured to connect to an Internet SMTP server and send warning/alarm e-mails. The configuration of the SMTP server is carried out in the “E-mail Server” tab and it has the following fields to be configured:

| Server property | Description |
|---|---|
| SMTP Host | Name of the E-mail Server or IP address of the SMTP Mail Server |
| Port | TCP port of the SMTP Server |
| User | User for SMTP authentication |
| Password | Password for SMTP authentication (optional) |
| Authentication | Use Authentication in the SMTP server |
| Protocol | Protocol of the SMTP server |
| Sender Address | Sender address for the outgoing messages: (it does not have to be a real address, for example, noreply@TesaSMARTAIR TS1000_warning) |

Click “Save” to save the changes. If a new E-mail Server is configured, it is necessary to restart the service for the changes to be applied.

In order to restart the service, access “services.msc” in Windows, find the service TESA APPSERVER Glassfish Server and restart it. Wait for the *java.exe* process to stabilise (depending on the server, this can take several minutes; you can confirm that the *java.exe* processes are stable with the Task Manager of Windows).



Deploy: Error
Datasource state: Connection successful

SMTP Host: localhost
Port: 587
Default User: Carlos
Password:
Use Authentication: ☑
Protocol: ● TCP ○ SSL ○ TLS
Sender Address: sample@localhost

NOTE: to enable the e-mail service, it is necessary for the licence to have this option enabled or to request the corresponding licence expansion (see *“C.6 Licence expansion”* on page 17).

### Configuration example: typical configuration for SMTP of GMAIL

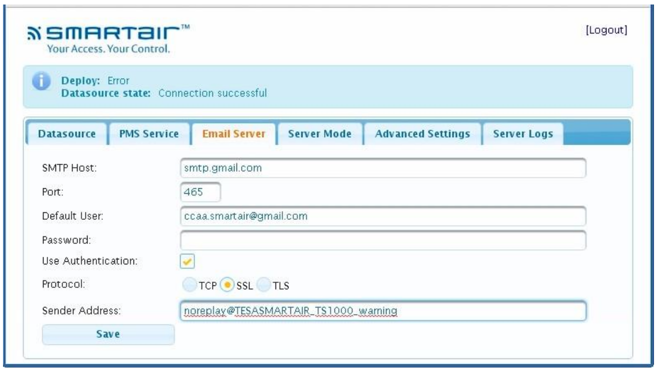
In the event of not having an SMTP server of your own available, it is possible to open an e-mail account with a free service provider on the Internet, such as, for example, GMAIL, and use their own SMTP server to send messages securely.

The following table shows the configuration to be carried out in the event of using a Gmail account. It is possible to access the SMTP server of GMAIL through the SSL or TLS protocols.

Both protocols use a secure connection through their encrypted communications.

## Gmail through SSL protocol

| Server property | Description |
|---|---|
| SMTP Host | smtp.gmail.com |
| Port | 465 |
| User | Your Gmail e-mail account, for example, youraccount@gmail.com |
| Password | Password of your Gmail account |
| Authentication | ENABLED |
| Protocol | SSL |
| Sender Address | Sender address for outgoing messages. This can be your Gmail account or an invented address. For example, noreply@TesaSMARTAIR TS1000_warning |



Deploy: Error
Datasource state: Connection successful

SMTP Host: smtp.gmail.com
Port: 465
Default User: ccaa.smartair@gmail.com
Password:
Use Authentication: ☑
Protocol: ○ TCP ● SSL ○ TLS
Sender Address: noreplay@TESASMARTAIR_TS1000_warning

## Gmail through TLS protocol

| Server property | Description |
|---|---|
| SMTP Host | smtp.gmail.com |
| Port | 587 |
| User | Your Gmail e-mail account. For example, youraccount@gmail.com |
| Password | Password of your Gmail account |
| Authentication | ENABLED |
| Protocol | TLS |
| Sender Address | Sender address for outgoing messages. This can be your Gmail account or an invented address. For example, noreply@TesaSMARTAIR TS1000_warning |

## Server mode

There may be cases where it is necessary to configure more than one server for a site with the wireless system, for example, to connect hubs on different PCs. Each server configured will be assigned a number of specific hubs. This particular mode of operating is only necessary when the data packet traffic in communications between the server and the hubs in the network is too high and generates long waiting times at the hubs.

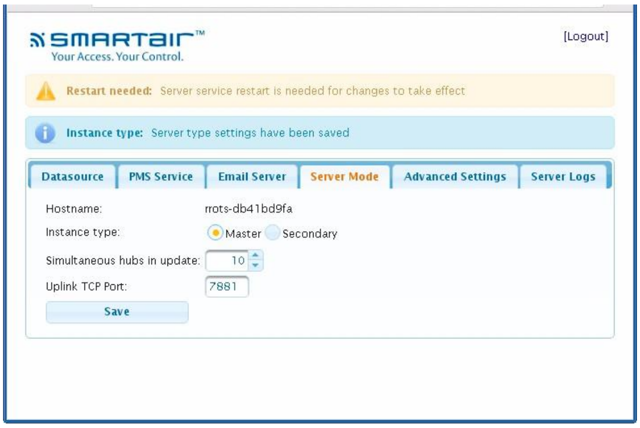
It is also useful for segmenting the network, placing an external server in a segment which can be accessed from the Internet and another internal server, with the “data”, in an internal segment having a more restricted access.

When there are several servers for the site, one of them must be configured as Master and the rest as Secondary.

- The server configured as “Master” will be in charge of making the backups, purging the database and sending the warning/alarm e-mails within the working logic of the hubs in a wireless system. The database will also be stored on the Master server.
- The rest of the servers must be configured as “Secondary”. These secondary points will only be in charge of managing the normal operation of the hubs assigned to them.

It is important to take into account that all the “servers” will access the same database stored on the “Master” server. The servers must have constant access to the database and, in addition, the communications through the high-speed LAN network must be stable.

Once the Server Mode has been configured, click the “Save” button to save the data. If a new Server Mode is configured, it is necessary to restart the service for the changes to be applied.



**Restart needed:** Server service restart is needed for changes to take effect

**Instance type:** Server type settings have been saved

Hostname: rrots-db41bd9fa

Instance type: ● Master ○ Secondary

Simultaneous hubs in update: 10

Uplink TCP Port: 7881

In order to restart the service, access “services.msc” in Windows, find the service TESA APPSERVER Glassfish Server and restart it. Wait for the *java.exe* process to stabilise (depending on the server, this can take several minutes; you can confirm that the *java.exe* processes are stable with the Task Manager of Windows).

NOTE: to see how to configure this mode in detail, see *“Multiple Wireless Server mode”* on page 147.

## Advanced settings

The expiry of the HTTP sessions and the administrator password are configured in this tab.

### Expiry of the HTTP sessions

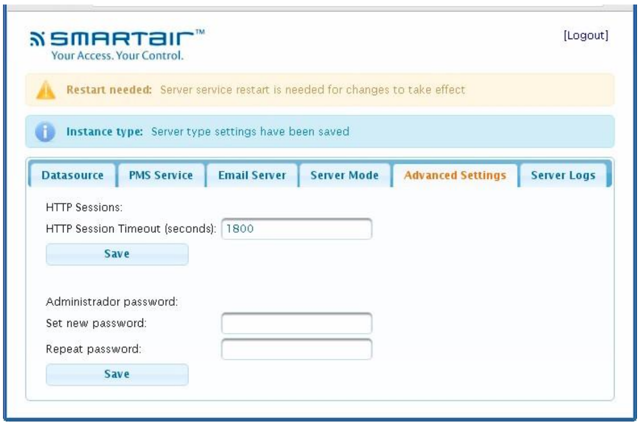
The value in seconds of the expiry of the HTTP session defines after how many seconds of inactivity the system automatically ends the session of the web application. The default value for session expiry is 1,800 seconds (30 minutes), but it can be customised to the desired value. After configuring the value in seconds, click the "Save" button to save the changes made. It is necessary to restart the web application for the changes to be applied.

In order to restart the service, access "services.msc" in Windows, find the service TESA APPSERVER Glassfish Server and restart it. Wait for the *java.exe* process to stabilise (depending on the server, this can take several minutes; you can confirm that the *java.exe* processes are stable with the Task Manager of Windows).

### Administrator Password

The Administrator Password is requested when the configuration of the web application is accessed. The default password is the one configured during the application setup and it can be modified in this tab.

Set the new password (and confirm it in the subsequent field) and click the "Save" button for the changes to be made.



**Restart needed:** Server service restart is needed for changes to take effect

**Instance type:** Server type settings have been saved

HTTP Sessions:

HTTP Session Timeout (seconds): 1800

Administrador password:

Set new password:

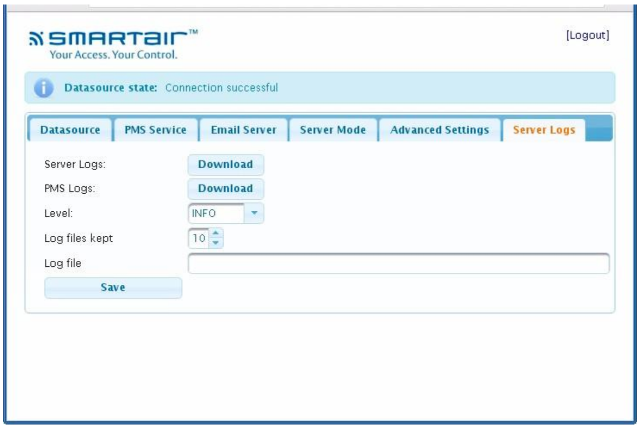
Repeat password:

## Configuration of the Server Logs

It is possible to download the information of the latest records of the server through the Server Logs tab. There are 5 configurable levels for the records to be downloaded. From the OFF mode (without records) to the FINE mode (detailed information on records). The mode set by default after the application setup is the INFO (Information) mode.

| Record level | Description |
|---|---|
| OFF | Without record |
| SEVERE | Only errors are recorded |
| WARNING | Errors and alarms are recorded |
| INFO | The information on actions, errors and alarms is recorded |
| FINE | Detailed information on actions, errors and alarms<br>Information for Technical Service in the event that any problem arises<br>Whenever necessary, you will be requested to set this mode and subsequently reproduce the incident so that the data are reflected in the file. |

In order to save the changes made in the configuration of the Server Logs, click the "Save" button.



Datasource state: Connection successful

Server Logs:

PMS Logs:

Level: INFO

Log files kept 10

Log file

## Notes to be considered in relation to the Windows firewall

If a Server setup is run in a Windows system where the *firewall* is enabled, make sure the communication ports of the server and the guests are not blocked.

The ports which, by default, the system requires to be enabled and open once its setup has been carried out are the following:

- TCP 3050 (database server)
- TCP 8181 (application server)
- UDP ports 7780 and 7781 (communication with the wireless hubs)
- PMS Service port (by default, 7779)
- TimeService port (UDP 10101)
- UDP 7790, TCP 7890, TCP 7881

## D.8 SETUP AND VALIDATION OF THE SERVER CERTIFICATE

A Certificate is necessary to identify the Server and ensure communications in secure mode.

All the server certificates which belong to the system are issued by the TESA CA Certificate Authority, which must be identified by the browser as a trusted authorised certificate. For this purpose, the TESA CA certificate must be installed in the list of trusted Authorised Certificates of the browser, in the list of “root” certificates.

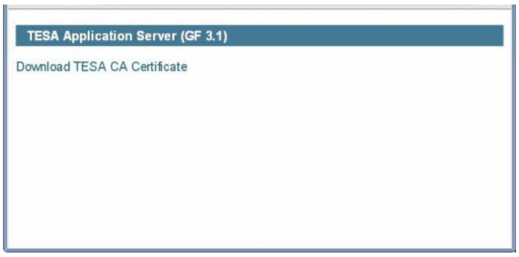
The following list shows the properties and values of the valid TESA CA certificate:

| TESA CA Certificate property | Value |
|---|---|
| Serial number | 00 f3 74 bc 60 6a ee 0e f8 |
| SHA-1 hash | e1 13 16 37 c8 fe f6 ba 5a 87 dd 9a 7a 70 1d f5 61 5f 60 c2 |

The TESA CA certificate can be found in the ca.crt file.

This file is located in the root directory of the application setup (for example, C:\ SMARTair TS1000).

In addition, it can be downloaded through the browser, from the URL address of the Server location (for example, https://host:8181/) by clicking the link Download TESA CA Certificate.



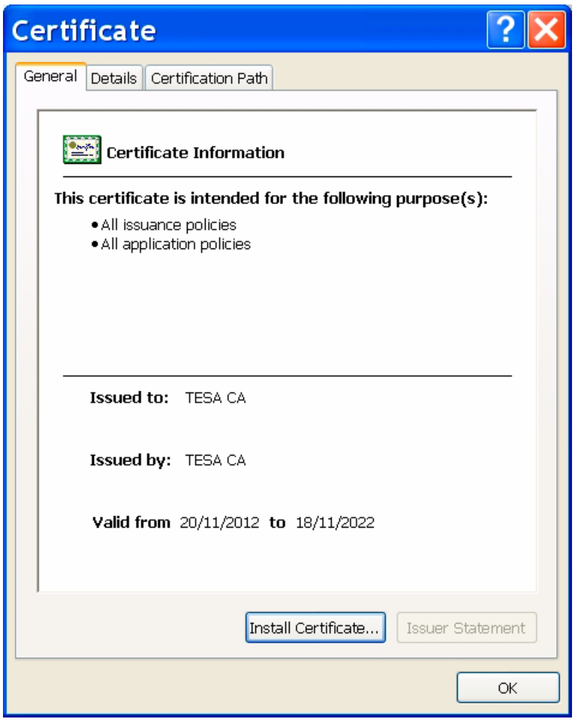
TESA Application Server (GF 3.1)

Download TESA CA Certificate

Once it has been clicked, save the file with the name ca.crt.

## Setup of the TESA CA certificate with Internet Explorer

Double-click the ca.crt file. The following screen will be shown:



Certificate Information

This certificate is intended for the following purpose(s):

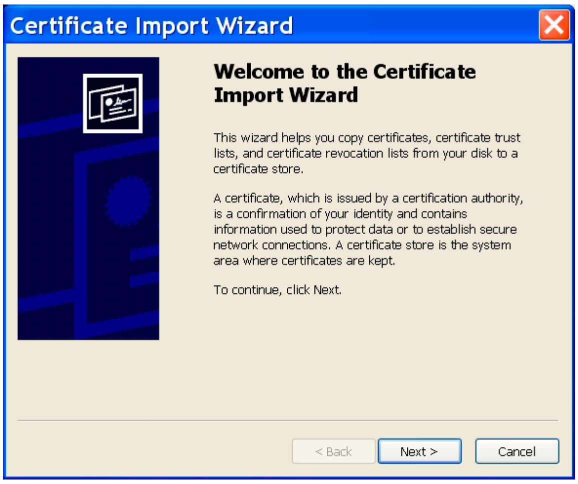
- All issuance policies
- All application policies

Issued to: TESA CA

Issued by: TESA CA

Valid from 20/11/2012 to 18/11/2022

Click the “Install Certificate” button. A setup wizard is run.



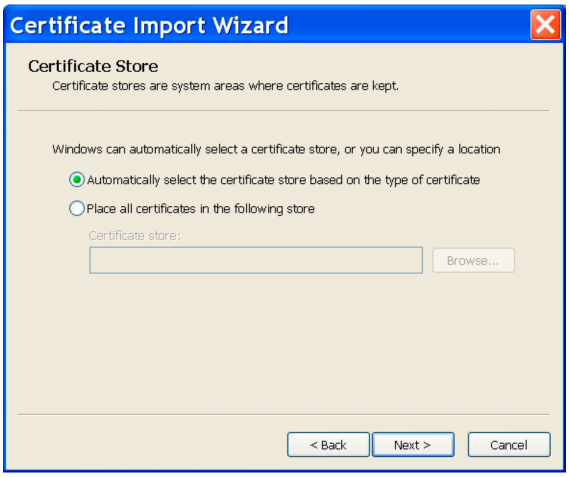
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Click the “Next” button successively on each screen until the last step of the process.



Certificate Store

Certificate stores are system areas where certificates are kept.

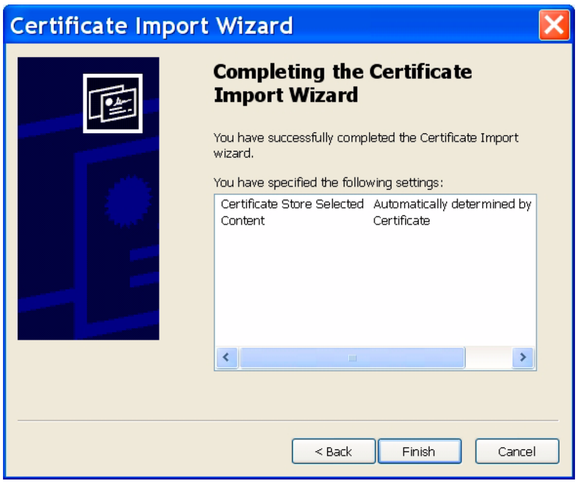
Windows can automatically select a certificate store, or you can specify a location

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

In the last step, click “Finish”.



Certificate Import Wizard

Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

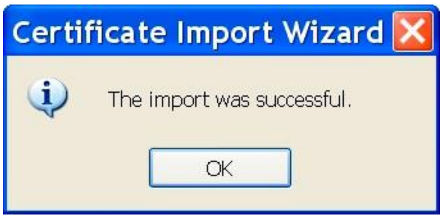
You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected | Automatically determined by |
| Content | Certificate |

A “Security warning” screen will then be displayed for accepting the setup of the certificate.

Click the “Yes” button. Be careful since the “No” button is underlined by default.

Finally, a message confirming that this has been done correctly is displayed.



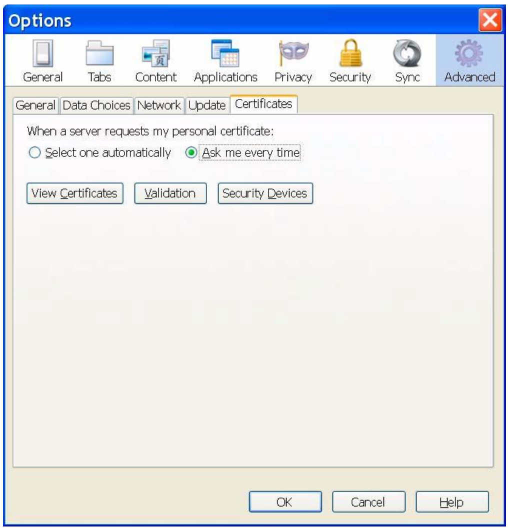
Certificate Import Wizard

The import was successful.

## Setup of the TESA CA certificate with Mozilla Firefox

Open the Options menu (Tools -> Options) of the browser.

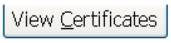
Click the “Advanced” menu in the “Certificates” tab.

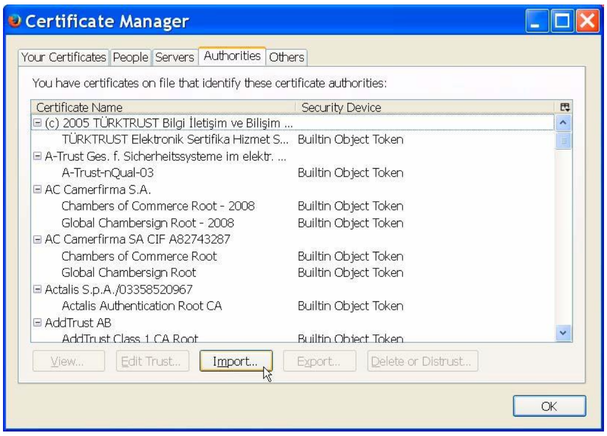


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

Click the “See certificates” button and select the “Authorities” tab.



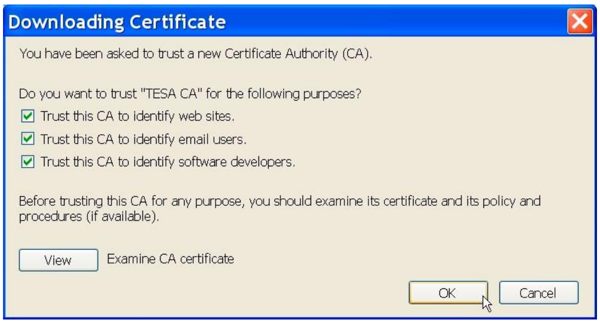


You have certificates on file that identify these certificate authorities:

| Certificate Name | Security Device |
|---|---|
| ⊟ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim ... | |
| TÜRKTRUST Elektronik Sertifika Hizmet S... | Builtin Object Token |
| ⊟ A-Trust Ges. f. Sicherheitssysteme im elektr. ... | |
| A-Trust-nQual-03 | Builtin Object Token |
| ⊟ AC Camerfirma S.A. | |
| Chambers of Commerce Root - 2008 | Builtin Object Token |
| Global Chambersign Root - 2008 | Builtin Object Token |
| ⊟ AC Camerfirma SA CIF A82743287 | |
| Chambers of Commerce Root | Builtin Object Token |
| Global Chambersign Root | Builtin Object Token |
| ⊟ Actalis S.p.A./03358520967 | |
| Actalis Authentication Root CA | Builtin Object Token |
| ⊟ AddTrust AB | |
| AddTrust Class 1 CA Root | Builtin Object Token |

Click the “Import” button and select the *ca.crt* file from its location in the system.

Confirm that the three check boxes validating all the purposes are selected and click the “OK” button.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "TESA CA" for the following purposes?

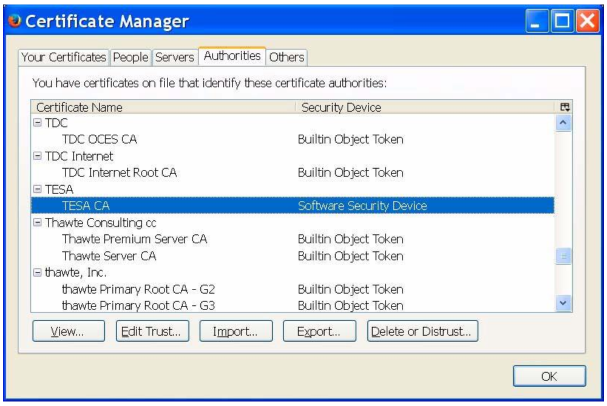
☑ Trust this CA to identify web sites.

☑ Trust this CA to identify email users.

☑ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

The authorisation of the TESA CA certificate will be added to the list of authorised certificates.



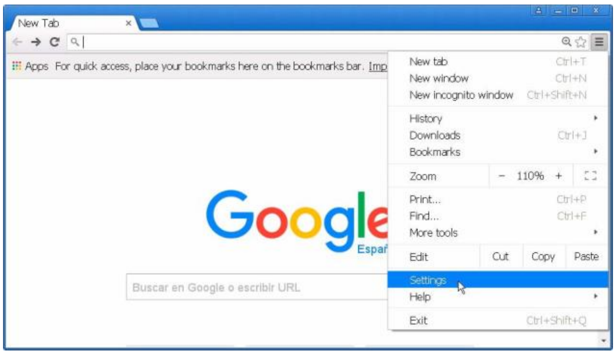
You have certificates on file that identify these certificate authorities:

| Certificate Name | Security Device |
|---|---|
| ⊟ TDC | |
| TDC OCES CA | Builtin Object Token |
| ⊟ TDC Internet | |
| TDC Internet Root CA | Builtin Object Token |
| ⊟ TESA | |
| TESA CA | Software Security Device |
| ⊟ Thawte Consulting cc | |
| Thawte Premium Server CA | Builtin Object Token |
| Thawte Server CA | Builtin Object Token |
| ⊟ thawte, Inc. | |
| thawte Primary Root CA - G2 | Builtin Object Token |
| thawte Primary Root CA - G3 | Builtin Object Token |

## Setup of the TESA CA certificate with Google Chrome

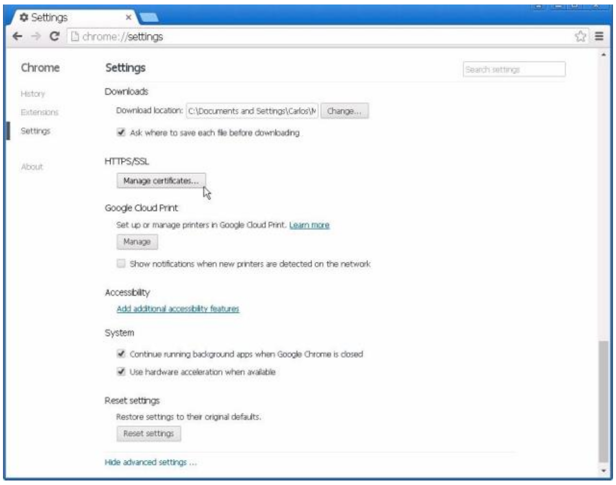
Open the Google Chrome browser and proceed as follows:

1 Click the “Customise and control Google Chrome” button (upper right-hand corner) and, in the menu which is displayed, click “Configuration”.

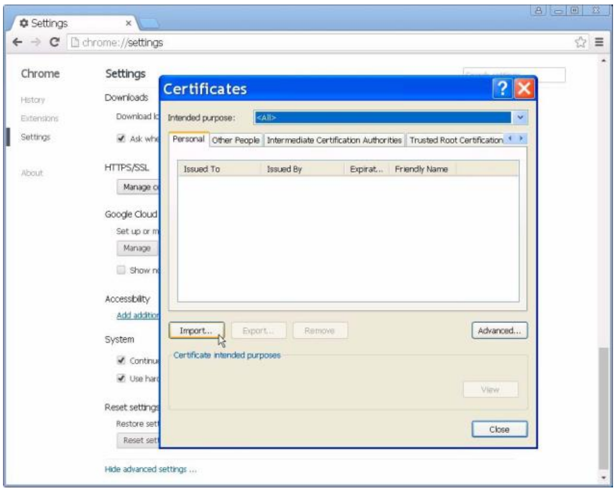


2 Scroll down, through the Advanced Settings, until you reach HTTPS/SSL.

Click the “Manage certificates” button.

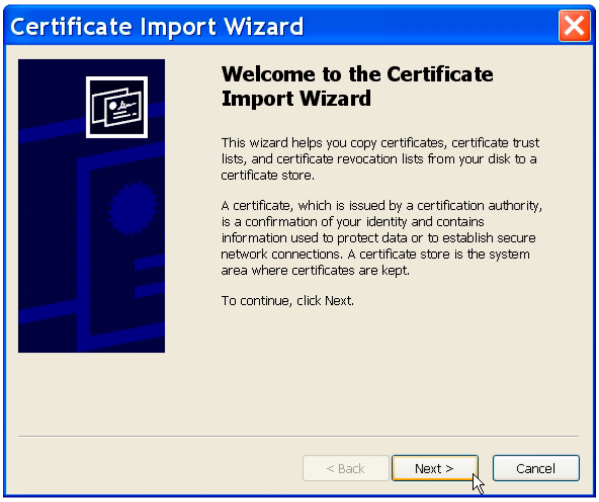

Settings
chrome://settings
Chrome
History
Extensions
Settings
About
Settings
Search settings
Downloads
Download location: C:\Documents and Settings\Carlos\M
Change...
Ask where to save each file before downloading
HTTPS/SSL
Manage certificates...
Google Cloud Print
Set up or manage printers in Google Cloud Print. Learn more
Manage
Show notifications when new printers are detected on the network
Accessibility
Add additional accessibility features
System
Continue running background apps when Google Chrome is closed
Use hardware acceleration when available
Reset settings
Restore settings to their original defaults.
Reset settings
Hide advanced settings ...

3 In the window which is displayed, click the “Import” button.



**4** The "Certificate import wizard" is displayed.

Click the "Next" button.



Certificate Import Wizard

**Welcome to the Certificate Import Wizard**

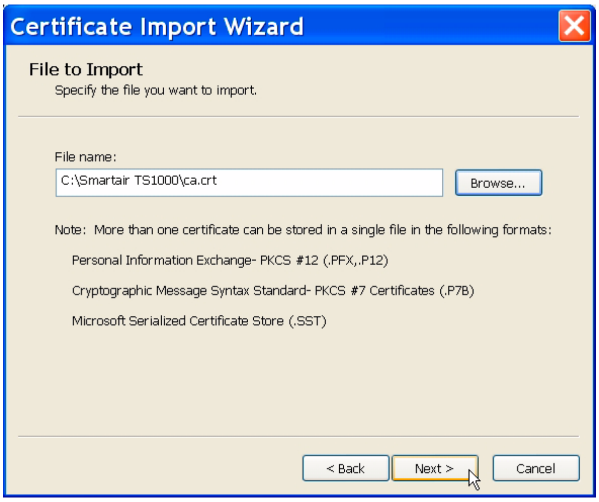
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

**5** In the dialogue box, enter the name of the file containing the certificate (*ca.crt)* with the complete path (*C:\Smartair TS1000\ca.crt*).

Click the "Next" button.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name: C:\Smartair TS1000\ca.crt

Note: More than one certificate can be stored in a single file in the following formats:

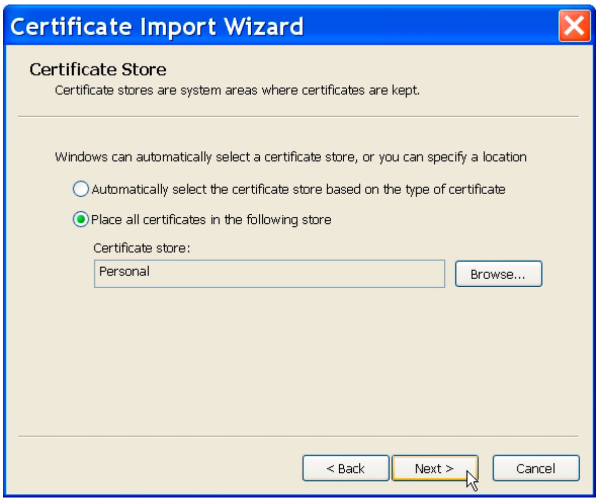
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

**6** The wizard requests a location to store the certificate.

Leave the default option and click "Next".



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location

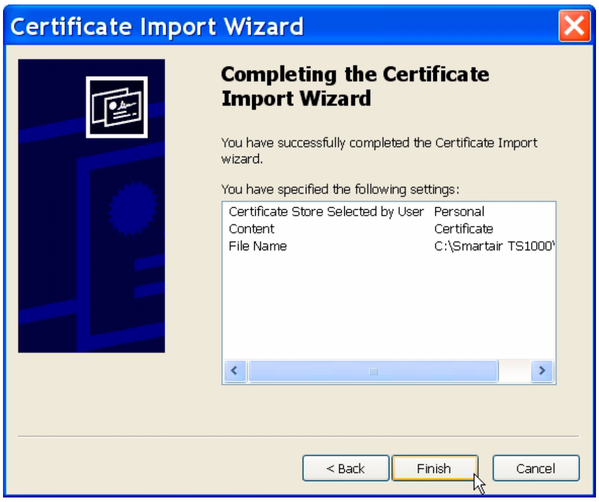
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal

7 A window is displayed showing a box with the properties of the certificate imported.

Click “OK”.



Certificate Import Wizard

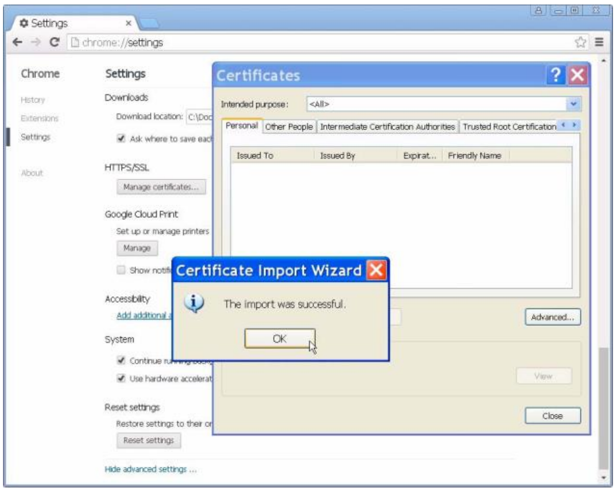
**Completing the Certificate Import Wizard**

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected by User | Personal |
| Content | Certificate |
| File Name | C:\Smartair TS1000\ |

8 A box is displayed confirming that the certificate has been correctly imported.



Certificate Import Wizard

The import was successful.

## D.9 IMPORT OF A DATABASE FROM AN OLDER VERSION OF THE TESA - SMARTair TS1000 APPLICATION

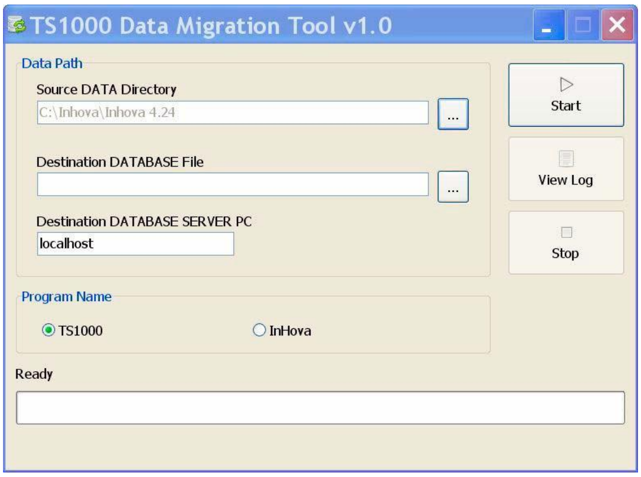
### Import of a database from a 4.x version

This process can only be carried out if the engines of both databases, Paradox and Firebird, are installed x (both versions installed on the PC).

The resulting file is directly compatible with the 5.x versions, but not with the 6.x. It is necessary to open it with a 5.6 so that it can then be opened with a 6.x. If the guest has a 6.x version, it will not be able to open the database even if it manages to import it.

In order to import a *data* from a SMARTair TS1000 4.x version, to a SMARTair TS1000 5.00 version, it is necessary to use the "ParadoxToFirebird.exe" tool, installed together with the application on its Server PC. Afterwards, from version 5.00, it is necessary to update to the desired version.

**1** Select the source database you wish to update.



TS1000 Data Migration Tool v1.0

Data Path

Source DATA Directory: C:\Inhova\Inhova 4.24

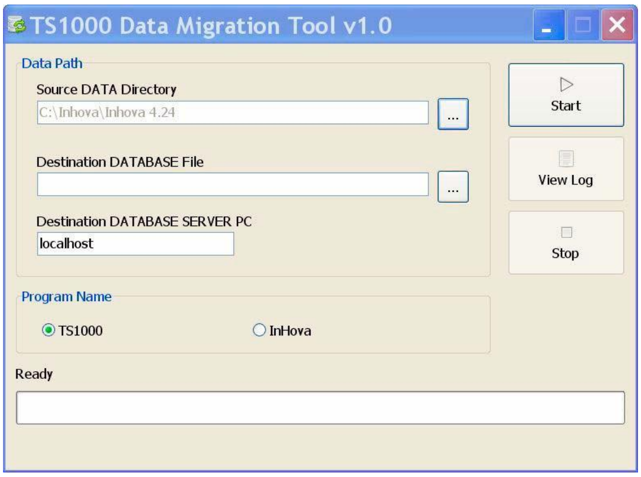
Destination DATABASE File:

Destination DATABASE SERVER PC: localhost

Program Name: ● TS1000 ○ InHova

Ready

**2** Select the name of the target database (for example, Data.fbd) in the server. If the database does not exist, type a new name.



TS1000 Data Migration Tool v1.0

Data Path

Source DATA Directory: C:\Inhova\Inhova 4.24

Destination DATABASE File:

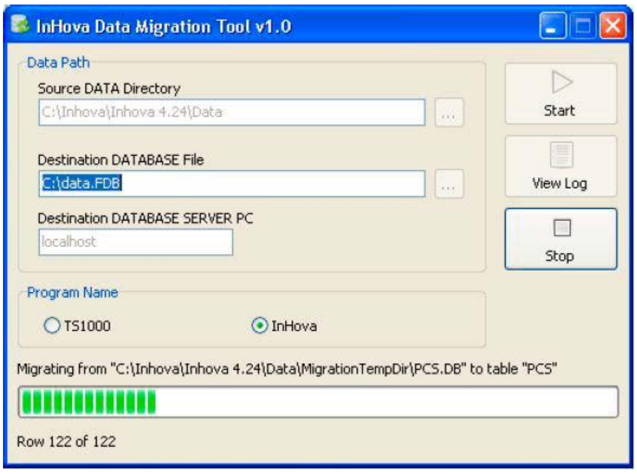
Destination DATABASE SERVER PC: localhost

Program Name: ● TS1000 ○ InHova

Ready

**3** Click the "Start" button.

**4** Wait while the process is carried out.



InHova Data Migration Tool v1.0

Data Path

Source DATA Directory: C:\Inhova\Inhova 4.24\Data

Destination DATABASE File: C:\data.FDB

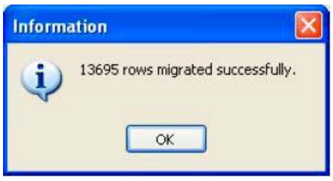
Destination DATABASE SERVER PC: localhost

Program Name: ○ TS1000 ● InHova

Migrating from "C:\Inhova\Inhova 4.24\Data\MigrationTempDir\PCS.DB" to table "PCS"

Row 122 of 122

**5** When the process ends, a message similar to this one will be displayed:



Information

13695 rows migrated successfully.

**6** Open the database converted by means of the TESA - SMARTair TS1000 6.0 application on the PC to complete the migration process.

It is possible that, when trying to migrate the database to *Firebird*, the version of SMARTair TS1000 is too old, so that, before using the migration tool, you would have to update the database to a higher version of SMARTair TS1000, nearer to v4.25 (last official version of the system under *paradox*).

## Import of a database from a 5.x version

The possibility of migrating databases from a 5.x version is integrated into the executable file itself of the 6.x version.

When a 5.x version is updated to a 6.x version, the TESA - SMARTair TS1000 application is run during the update process and a dialogue box is displayed asking for permission to update the database tov6.x.

If the request is accepted, the update process of the application updates the database at the same time, so that when the former process ends, both are automatically configured.

To convert a data to version 6, importing it from version 5, it is not possible to do this from version 5.00; it is advisable to have the data in version 5.06 so as to update it from there to version 6.

## D.10 TROUBLESHOOTING

### Errors or alerts from the security certificate

**Possible cause:**
The TESA CA Security Certificate has not been installed in the list of authorised certificates of the browser or the server name does not coincide with the name specified in the address bar.

**Solution:**
Install the TESA CA Certificate as explained in point *"D.8 Setup and validation of the Server Certificate"* on page 43 of this manual, and make sure that the name specified in the address bar of the browser to access the web application server is the correct one and is not its IP address or an alias.

### Message from the TESA - SMARTair TS1000 Guest: "The Web Server is not running or it is not available"

**Possible cause:**
The TESA APPSERVER Glassfish Server service is not running or the platform has not been correctly deployed.

**Solution:**
Restart the service. For this purpose, access "services.msc" in Windows, find the service TESA APPSERVER Glassfish Server and restart it. Wait for the *java.exe* process to stabilise (depending on the server, this can take several minutes; you can confirm that the *java.exe* processes are stable with the Task Manager of Windows).
Afterwards, it may be necessary to set the database server again using the web configurator application https://host:8181/TesaServerConfig/views/index.xhtml as shown in point *"D.7 Configuration of the server PC"* on page 36 of this manual.

### Message from the TESA - SMARTair TS1000 Guest: "The TESA – SMARTair TS1000 database and the location of the database do not coincide"

**Possible cause:**
The TESA - SMARTair TS1000 Guest PC and the Server PC are accessing different databases, or the Server uses the *localhost* name rather than the real name of the machine in the network, or a different redirection is taking place from the web service and the *config.ini* (IP in one and name in the other, etc.).

**Solution:**
Set the same name both for the application server and the database server, in the server PC as well as in the guest PCs. Use the real PC names rather than *localhost* (*localhost* is the name set by default when installing the application).
That is to say, the lines "DataServer" and "Webserver" of the file *config.ini* and the field "Database server" do not coincide. It is necessary to put the name in both or the IP in both, and never "localhost", unless there is only one PC and it is both guest and server.

## The TESA - SMARTair TS1000Platform web application is not being run

**Possible cause:**
The location of the database on the Server is not correctly configured.

**Solution:**
Configure the location of the database in the Server correctly. The TESA - SMARTair TS1000Platform application is only available at the URL address
https://host:8181/TesaSmartairPlatform/views/login.xhtml
after configuring the location of the database correctly. Follow the steps of point *"Configuration of the datasource"* on page 36 of this manual to configure the location of the database.

## The ServerConfig application shows the "Deployment Error" message when setting the location of the database

**Solution:**
Restart the TESA_APPSERVER GlassFish Server Windows service as shown in point *"Windows services installed"* on page 34 and, afterwards, set the database server again using the web configurator application https://host:8181/TesaServerConfig/views/index.xhtml as shown in point *"D.7 Configuration of the server PC"* on page 36 of this manual.

# E – Running the programme for the first time

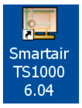
# E – RUNNING THE PROGRAMME FOR THE FIRST TIME

## E.1 OPERATOR NAME AND PASSWORD

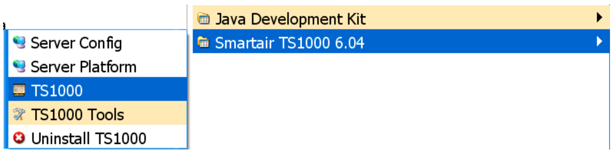
After installing the software as described in the corresponding chapter, the programme is now ready to be run.

1 Run the programme. You can proceed in two different ways:

- Double-clicking the shortcut created in the Windows desktop, or,

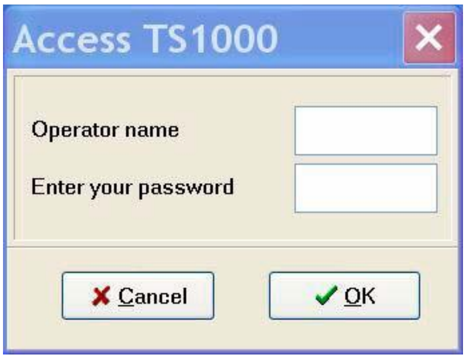


- In the event of a local setup, running it from the TS1000 entry of the “Programmes” menu of Windows.



2 Once it has been run, the programme requests the “Operator Name” and “Password”, which are necessary to access the system.

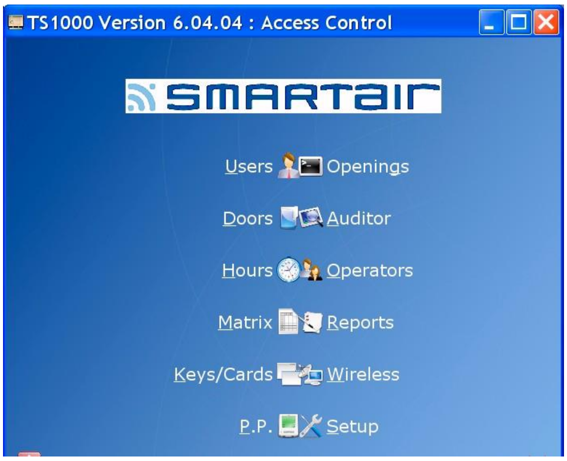
Enter the Operator Name and Password. If you do not know these, request them from the SMARTair Technical Service, indicating the 8 digit alphanumeric code which is labelled in the licence.



□ Once you have accessed the programme, you will be able to add as many operators as you wish, with the same or different rights and with their corresponding passwords, according to your needs. For more information, refer to section *“G.3 Operators”* on page 95.

3 After entering the correct Operator Name and Password, click “OK”.

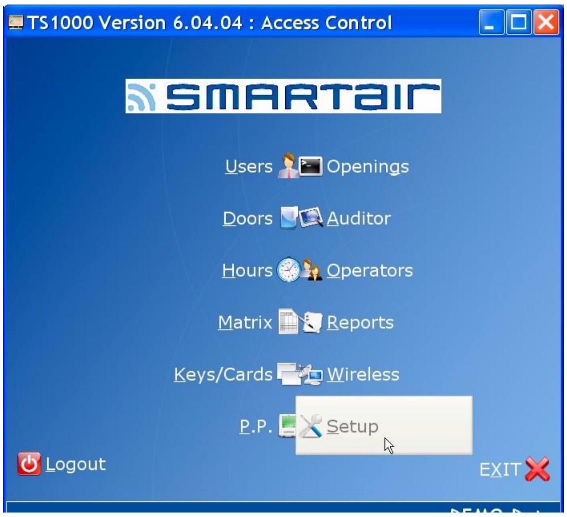
The main screen of the TS1000 programme is displayed and, as a result, it is possible to start configuring the locking plan.



## E.2 “SETUP” MENU

Before starting to programme the locking plan (defining users, doors, etc.), it is necessary to configure the site, defining aspects such as the language, etc.

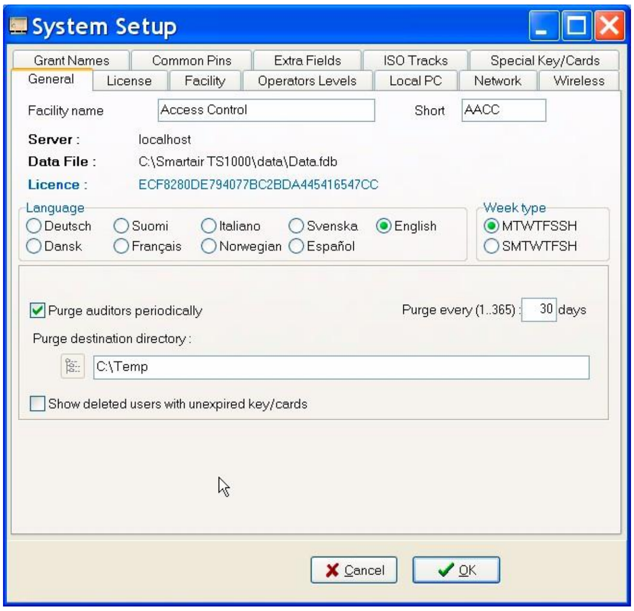
Access the “Setup” menu, clicking the corresponding button on the main screen of the TS1000 software.



### “General” tab

In the “General” tab of the “Setup” menu, the following fields are displayed:

- Facility name
- Short
- Language
- Week type
- Purge auditors periodically
- Show deleted users with non-expired card/key



Facility name: Access Control  Short: AACC

**Server :** localhost

**Data File :** C:\Smartair TS1000\data\Data.fdb

**Licence :** ECF8280DE794077BC2BDA445416547CC

Language: ○ Deutsch ○ Suomi ○ Italiano ○ Svenska ● English ○ Dansk ○ Français ○ Norwegian ○ Español

Week type: ● MTWTFSSH ○ SMTWTFSH

☑ Purge auditors periodically  Purge every (1..365) : 30 days

Purge destination directory : C:\Temp

□ Show deleted users with unexpired key/cards

Each of the fields is described below.

**Facility name:** this is the name which will be displayed on the main screen of the TS1000, after the programme version.

**Short:** this is the name used to identify the locking plan of the site in the Portable Programmer. This field is particularly useful when managing more than one site with the same PP, since the screen of the Programmer is small, preventing the full facility name from being seen if it is too long. When only one site is managed with the Programmer, this field is less important.

**Language:** this is the language used in the TS1000 software and in the messages of the Portable Programmer. The language can be changed whenever desired, as many times as you want, without losing as a result any data or configuration. Select the language you prefer and click “OK” to confirm.

**Week type:** this allows selecting the first day of the week as Monday (Europe) or Sunday (America).

**Purge auditors periodically:** the Auditor is a file where all the operations carried out in the TS1000 are recorded. Each record provides information making reference to the date and time when an operation is carried out, who the operator carrying it out is, which operation is carried out, and which user, door or time zone was the subject of the operation. That is to say, it is a file with which you can always know which operations have been carried out in the software and who did so.

This file has no capacity limit. In order to prevent it from becoming too large, the function “Purge auditors periodically” is available. This function deletes or saves the records of the auditor file automatically in an ASCII file after a given number of days.

When this function is enabled, the option “Purge after (1...365) days” is also enabled, where you indicate in the box the number of days you wish to wait until the new cleaning of the auditor takes place.

The field “Purge target folder” is also enabled, which allows selecting the folder where we want the purge to be carried out.

The record of openings is also purged in this process, in the same way and at the same time, in another file. The resulting files have names with a given format “EventOldAAMMDD.txt” for the record of openings and “SistOldAAMMDD.txt”, where AAMMDD is the date of the last record stored, and can be consulted from the “Openings” and “Auditor” windows using the “Open” button (see sections *“K.3 Openings”* on page 156 and *“K.5 Auditor”* on page 168).

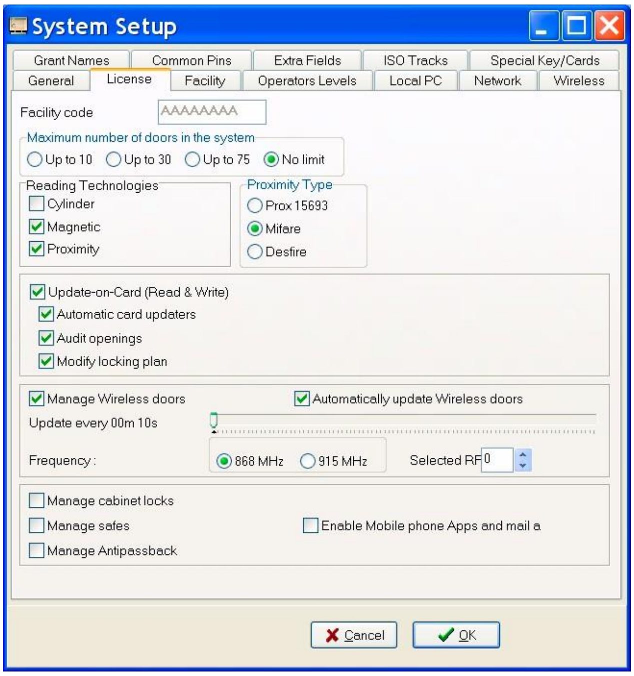
**Show deleted users with non-expired card/key:** the users who have been deleted, whose card has not yet expired, are also shown on the list of users. They are indicated with their names crossed out.

## “Licence” tab

Only the “Reading technologies” parameters and the parameters of the wireless management can be modified in this tab (the latter if a wireless licence is available).

The rest of the fields are shown in “Read-only” mode. For the modification of the values, it is necessary to carry out an update process by means of the export, delivery to Tesa and import of the *license.zip* file.

This tab is only visible during the start-up of the system. Once the basic configuration has been programmed, this tab disappears, since the data included must not be subsequently modified, under normal conditions.



Facility code AAAAAAAA

Maximum number of doors in the system

○ Up to 10 ○ Up to 30 ○ Up to 75 ● No limit

Reading Technologies

□ Cylinder

☑ Magnetic

☑ Proximity

Proximity Type

○ Prox 15693

● Mifare

○ Desfire

☑ Update-on-Card (Read & Write)

☑ Automatic card updaters

☑ Audit openings

☑ Modify locking plan

☑ Manage Wireless doors ☑ Automatically update Wireless doors

Update every 00m 10s

Frequency : ● 868 MHz ○ 915 MHz Selected RF 0

□ Manage cabinet locks

□ Manage safes □ Enable Mobile phone Apps and mail a

□ Manage Antipassback

The following fields are viewed in the “Licence” tab:

- Facility code (unique and not editable in any case)
- Maximum number of doors
- Update on Card and its parameters
- Manage wireless doors
- Manage cabinet locks
- Manage safes
- Manage Antipassback
- Enable applications for mobiles and sending of e-mails

Each of the fields is described below.

**Facility code:** this is the System Code. It is the unique and exclusive code which has been assigned to your site. By means of the System Code, it is guaranteed that there are no two identical sites. This code can also be found in the identification labels of the licence folder (see *“Licence”* on page 15).

**Reading technologies:** the TESA Access Control system offers the possibility of working with different product ranges: electronic cylinders (whose identification technology is a contact chip), locks and wall readers with magnetic stripe card, and locks and wall readers with contactless chip technology (proximity). The product type to be installed is decided in this field. This is extremely important since, based on the reading technology selected, the communication with doors and credentials (keys or cards) will be different.

- In the case of electronic cylinders, the encoder of keys is the Portable Programmer itself.
- In the case of magnetic stripe products, the encoder required is the encoder of magnetic stripe cards.
- In the case of using contactless chip technology (proximity), the encoder to be used is the encoder of contactless chip credentials.
- In the case of doors, the data transferred to the Portable Programmer, depending on whether they are assigned to Cylinders, Magnetic Stripe Locks or Proximity Locks, will be different and specific.

Of course, it is possible to select two or even all three technologies, if so required by the site, as a result of having installed more than one different product.

In addition, in the event of selecting “Proximity” as the reading technology, it is necessary to select the type of chip used. For this purpose, the fields “Prox 15693”, “Mifare” and “Desfire” are enabled, which represent the three types of chips available:

- **Prox 15693:**
  Contactless read-write chips according to the ISO 15693 standard.

- **Mifare:** Contactless read-write Mifare Classic chips, 1k or 4k (ISO 14443 A). Also compatible with Mifare Ultralight. In the event of selecting this type of chip, the configuration of the sectors involved must be determined, especially if the credentials to be programmed are already being used or are going to be used for any other application which requires the reservation of any of the sectors.

- **Desfire:** Compatible with Desfire EV1.

**Update on Card (Read & Write):** this allows defining whether updaters will be installed, in addition to readers and/or locks. And, in turn, whether the credentials will be carriers of information related to the locking plan of the user they belong to (openings and crosses).

The Update on Card (UoC) system allows updating the information related to the doors without having to go to them. For this purpose, there is a Reader-Updater available, which is connected to the PC over Ethernet. In this way, when any piece of data is updated in the TS1000 software, the information is transmitted to the Reader-Updater over Ethernet, which updates the user's card when it is held within range of the Reader-Updater. Afterwards, when the user holds the card by the door, that door will be updated with the new information contained in the card.

**Manage wireless doors:** in the event of having wireless equipment on the site, it is possible to define how often, and whether automatically or not, the software should connect to the Hubs to update the locks/readers and capture the opening records. For more information on the wireless system, see *"Wireless system architecture"* on page 131.

**Manage cabinet locks/Manage safes:** it is also possible to have *Mifare* cabinet locks and safes, in addition to locks, readers and wireless readers and locks. In order to manage this type of device, it is necessary for these boxes to be enabled. Otherwise, it will be necessary to send the exported *license.zip* file by means of the application "Tools" for updating by Tesa, and then importing it with the same application.

**Manage Antipassback:** if you enable this option, a new tab is displayed in the "Setup" menu, which we are describing in this section: the "Antipassback" tab. To learn how this option works, refer to section *"Antipassback" tab* below.

**Enable applications for mobiles:** this allows wireless door opening by means of the mobile App. The possibility of sending alerts by mail is also enabled by this. In order to select this function, it must be enabled in the licence acquired.

## "Antipassback" tab

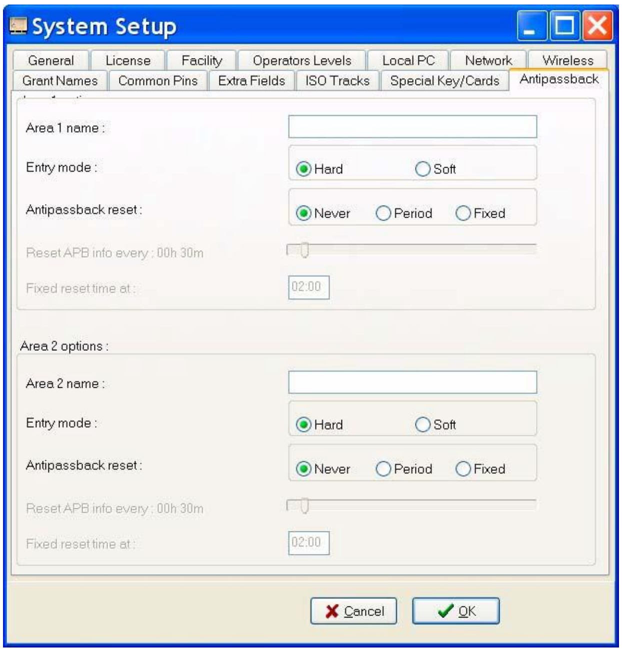
NOTE: this tab is only displayed if the option "Manage Antipassback" is enabled in the "Licence" tab of the "Setup" menu, which is described in this section.

The Antipassback system can be used to prevent multiple accesses with the same credential and it works as follows:

- A number of doors are defined, some of them as "antipassback entry" and some others as "antipassback exit".
- When a user goes through an "antipassback entry" door, a signal is activated in their credential, which prevents the user going through any other "antipassback entry" door.
- This signal is deactivated when that user goes through an "antipassback exit" door or else after a given period of time. Once the signal has been deactivated, the user can go through an "antipassback entry" door again.

The configuration is carried out in the "Antipassback" tab of the "Setup" menu.

This tab allows defining one or two *antipassback* areas, by means of the following fields:



Area 1 name :

Entry mode : ● Hard ○ Soft

Antipassback reset : ● Never ○ Period ○ Fixed

Reset APB info every : 00h 30m

Fixed reset time at : 02:00

Area 2 options :

Area 2 name :

Entry mode : ● Hard ○ Soft

Antipassback reset : ● Never ○ Period ○ Fixed

Reset APB info every : 00h 30m

Fixed reset time at : 02:00

- **Area name:** name which defines the controlled *antipassback* area. If two areas are created, it is necessary to assign a different name to each of them.
- **Entry mode:** this offers two options: "Hard" and "Soft".
  - "Hard" mode: the locks defined as *antipassback entry* will not let a user whose signal is activated go through.
  - "Soft" mode: the locks defined as *antipassback entry* will let a user go through even if the signal is activated, but they will generate an alert event for the site manager.
    Depending on the technology used, the event will be collected by the Portable Programmer at the door itself, by means of the updaters when the credential is passed through them or by the Hubs in the wireless system.
- **Reset antipassback:** this allows configuring how the *antipassback* signal is deactivated when it has been activated in the user credential:
  - Never: the signal remains activated indefinitely until the user goes through an *antipassback exit*.
  - Fixed: the signal is deactivated every day at the same time (fixed *reset* hour).
  - Period: the signal is deactivated a certain time after having gone through the *antipassback entry* door (*reset* APB info after...).

After having defined at least one antipassback area, in the "Doors" menu, for each door, a field is displayed which allows selecting whether the door is "entry", "exit" or "neither". If "entry" or "exit" is selected, another field is displayed to select the area.

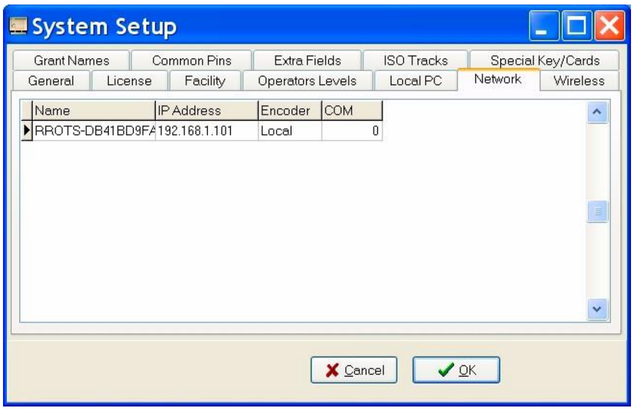
In addition, in the "Settings" tab of the "Users" menu, an option is displayed, for each user, which allows choosing whether the user will be affected or not by the *antipassback* mode.

## “Network” tab

The TS1000 system can be installed on a network of PCs.

In the “Network” tab of the “Setup” menu of the TS1000 programme, all the network computers where the programme is installed and has been run are shown, including their name, their IP address in the network, the way in which the Encoder is used (local or remote) and which COM port they use to communicate with the Portable Programmer.

**NOTE:** it is possible for a PC which is not currently in the system, even if it has been present in previous phases, to appear on the list. If desired, it is possible to remove all these obsolete PCs from the list, by means of the TOOLS programme.



| Name | IP Address | Encoder | COM |
|---|---|---|---|
| RROTS-DB41BD9FA | 192.168.1.101 | Local | 0 |

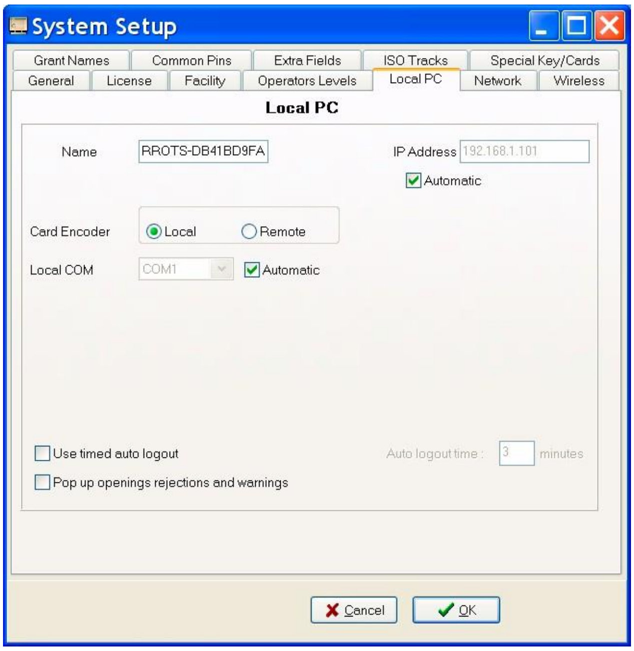
## “Local PC” tab

Using the “Local PC” tab of the “Setup” menu, it is possible to view the data related to the communications and to the computer from which the TS1000 programme is being run.

The following data are shown:

- Name
- IP Address
- Card Encoder
- Local COM
- Use timed auto logout
- Pop up openings rejections and warnings

Each of the fields is described below.



**Local PC**

Name RROTS-DB41BD9FA

IP Address 192.168.1.101

☑ Automatic

Card Encoder ● Local ○ Remote

Local COM COM1 ☑ Automatic

□ Use timed auto logout

Auto logout time : 3 minutes

□ Pop up openings rejections and warnings

**Name:** this is the network identification name of the computer itself. This field is filled in automatically with the name assigned to the local PC in the Operating System. If it is empty, it can be filled in by means of the option “System” of the “Computer Control Panel”. In the option “System”, click the “Computer name” tab and verify the field “Full computer name”. If this field is empty, issues may arise when communicating with the Portable Programmer and, therefore, it is necessary to enter an identification name, clicking the “Change” button. Contact your distributor if you need assistance.

**IP Address:** this is also automatically filled in. If it is blank, contact your distributor.

**Card Encoder:** if the TS1000 system is installed on a single PC, the card encoder will always have to be connected to that through the RS-232 serial port or a USB port. That is to say, it will be a “local” connection. As a result, the option “Local” must be selected for this field.

### Sharing an encoder amongst various PCs

If the access control system is installed on a PC network, the system offers the possibility of sharing an encoder. That is to say, the encoder can be connected by means of RS-232 to one of the PCs and the rest will be able to use it remotely. This is valid for:

- Encoder of magnetic stripe cards
- SMARTair Encoder
- Portable Programmer (when working as an electronic key encoder)

Proceed as follows:

1 On the computer where the encoder is installed locally via RS-232, select the option “Local” in the field “Card Encoder”.

2 On the network computers where you want to use the encoder remotely, select the option “Remote”. Once this has been selected, a drop-down field is displayed, which shows the list of network computers. In this field, select the computer where the encoder is connected locally.

**Local COM:** this refers to the serial port of the computer through which the TS1000 software will communicate with the Portable Programmer and/or the Encoder. It is advisable to maintain the option “Automatic”, which automatically searches for the port the device is connected to.

When the TS1000 software is installed, the *drivers* for communicating with the portable programmer and the encoder are also installed. Once these devices have been connected to the computer by means of the USB cable, the system will generate the corresponding COM ports, which can be consulted in the Device Manager. If the automatic detection check box (“Automatic” option) is selected, the software itself will locate them.

If issues arise when generating these COM ports, it is possible to install the *drivers* again manually, running the file contained in the “Drivers” folder which is included in the software setup folder.

If your devices have RS232 entries rather than USB, it is possible to provide you with approved RS232-USB adaptor cables.

**Timed auto LOGOUT:** this is an automatic security blocking system. If the option “Use timed auto LOGOUT” is selected, every time the software is fully inactive for a set period of time, it will be blocked. It will be necessary to enter a valid operator name and password again to reactivate it. The “Timed auto LOGOUT” is set in minutes and it can be modified as desired.

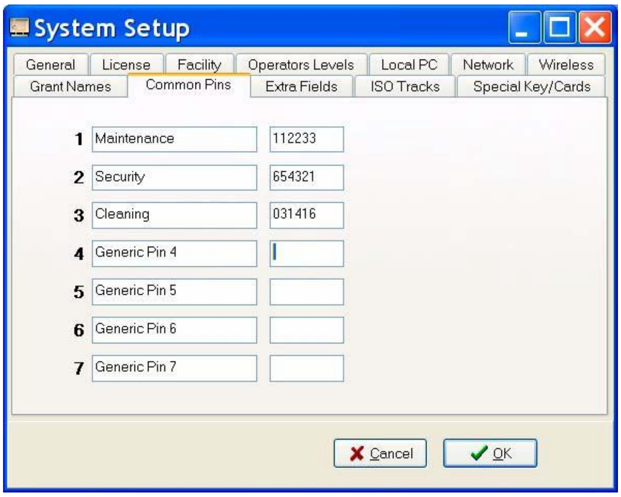
**Pop up openings rejections and warnings:** if this option is selected, when the “Openings” menu is accessed from the PC which has the TS1000 installed, a “Pop up” will be displayed showing the rejections and warnings of the doors.
A “Pop up” is a pop-up window located in the lower right-hand area of the screen, which is only displayed when a new alert is generated, provided that the software is open and the openings window is displayed.

## “Common PINs” tab

The Common PINs are keypad codes, from 4 to 6 figures, which can be used by several users to open the doors. In this way, it is possible to define groups of users (for example, by departments) with the same *common PIN* for all of them.

The Common PINs are defined by means of their identification name, followed by the “PIN” number.

It is necessary to assign the Common PINs to the doors where they will be used (see *F.3 “Doors” menu* on page 74).



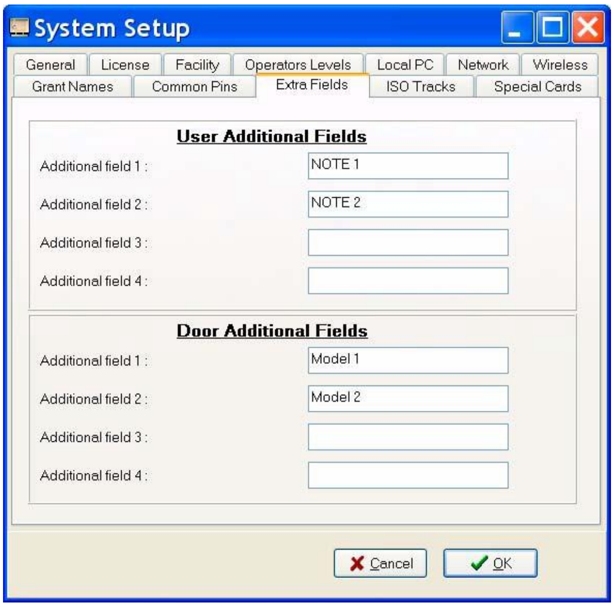
| | | |
|---|---|---|
| 1 | Maintenance | 112233 |
| 2 | Security | 654321 |
| 3 | Cleaning | 031416 |
| 4 | Generic Pin 4 | |
| 5 | Generic Pin 5 | |
| 6 | Generic Pin 6 | |
| 7 | Generic Pin 7 | |

## “Extra Fields” tab

The “Extra Fields” tab allows defining a maximum of 4 additional fields for the user forms and the same number for the door forms. This information is transmitted neither to doors nor to credentials: it is only useful for making data management in the software easier.

These fields can be used later on for multiple selection of users or doors.

By means of these fields, it is possible to add customised data, according to your preferences and needs, to the information related to the users and doors. For example, different departments can be defined for users, and buildings, floors, etc., can be defined for doors.



**User Additional Fields**

| | |
|---|---|
| Additional field 1 : | NOTE 1 |
| Additional field 2 : | NOTE 2 |
| Additional field 3 : | |
| Additional field 4 : | |

**Door Additional Fields**

| | |
|---|---|
| Additional field 1 : | Model 1 |
| Additional field 2 : | Model 2 |
| Additional field 3 : | |
| Additional field 4 : | |

## Other tabs and functions

The other tabs and functions are explained in chapter *“L – Other Functions”* on page 179.

# F – Creating the Locking Plan

# F – CREATING THE LOCKING PLAN

## F.1 INTRODUCTION

The locking plan allows making a decision on to whom, where and when access can be granted.

The creation of the locking plan consists of the following steps:

1. Creating the user list, by means of the “Users” menu.
2. Creating the door list, by means of the “Doors” menu.
3. Creating the access hours, by means of the “Hours” menu.
4. Saving the locking plan.

Once the locking plan has been created, it is necessary to encode the credentials of the users and load it into the Portable Programmer to initialise the locks, readers and/or cylinders, as will be seen in the corresponding chapters.

F

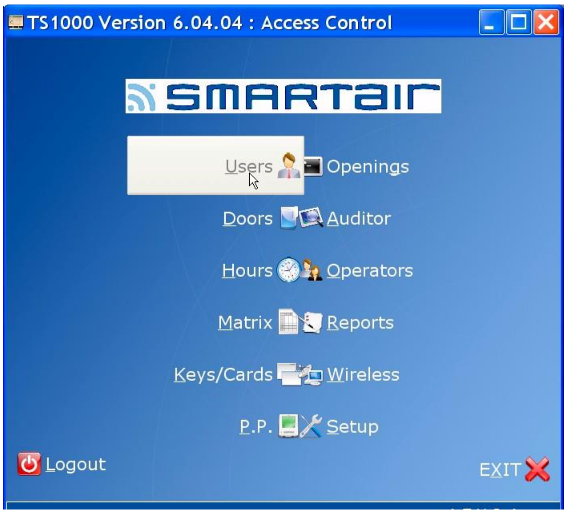
□ Before proceeding to the creation of the locking plan, it is advisable to configure some of the settings of the system by means of the “Setup” menu, as described in chapter “E – Running the programme for the first time”.

□ In UoC systems (Update on Card), **it is VERY IMPORTANT to previously configure the distribution of data on the cards** (see *“Proximity setup”* on page 181).

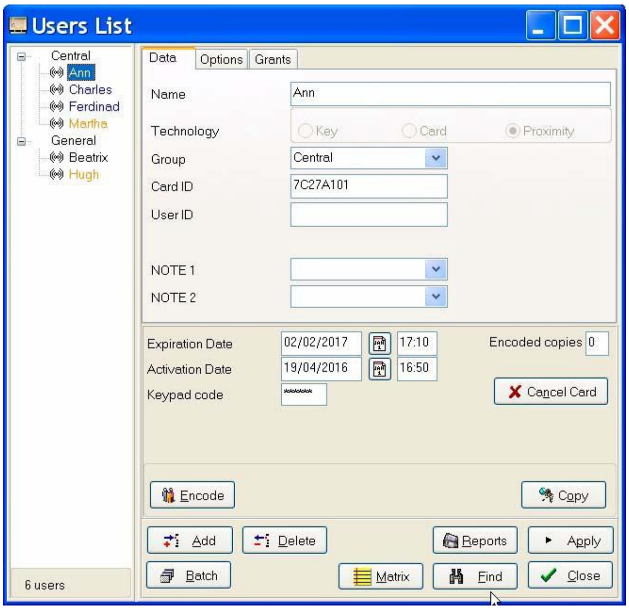
## F.2 “USERS” MENU

The first step in creating a locking plan is creating the user list in the “Users” menu.

In order to access the “Users” menu, click this option on the main screen of the TS1000.



In the “Users” menu, the following fields are displayed:



Central
- Ann
- Charles
- Ferdinad
- Martha

General
- Beatrix
- Hugh

6 users

Name: Ann

Group: Central

Card ID: 7C27A101

User ID:

NOTE 1:

NOTE 2:

Expiration Date: 02/02/2017 17:10

Activation Date: 19/04/2016 16:50

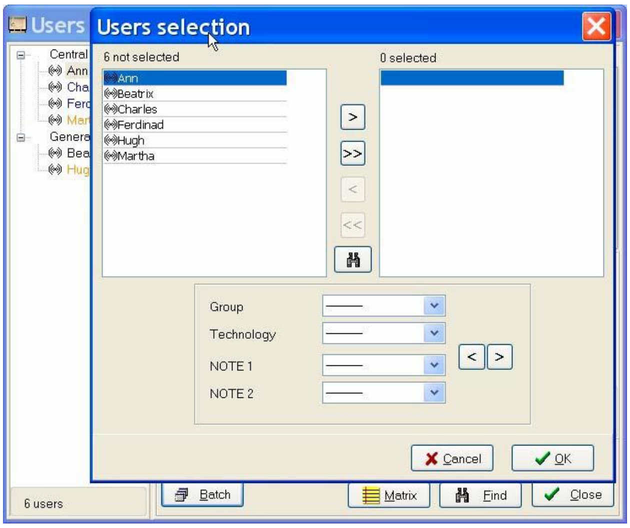
Keypad code: ******

Encoded copies: 0

- **Name:** user name.
- **Group:** name of the group the user belongs to.
- **Card ID:** identification number incorporated into all the source credentials, which is read and recorded when the user card is encoded.

  It is also possible to carry out the process the other way around: writing the ID manually if this is known, distributing the credentials which are not encoded, and delegating the encoding to an automatic updater which is connected to the database and made available to the users.
- **User ID:** additional information you wish to add in relation to the user.
- **NOTE 1, NOTE 2:** customised fields. It is possible to define a maximum of 4 customised fields, which can be configured in the “Extra Fields” tab of the “Setup” menu, as shown in section *“Extra Fields” tab*on page 65.
- **Expiry Date:** date when the credential of the user ceases to be valid on the site and from which, therefore, the user is no longer able to access the doors authorisation was held for.
- **Activation Date:** date when the credential of the user becomes valid on the site and from which, therefore, the user is able to access the doors authorisation is held for.
- **Keypad Code:** code (from 4 to 6 digits) for opening the door if it is in the state “Card + PIN” or “PIN + Card”. Refer to *“States”* on page 82.
- **“Encode” button:** this allows encoding the credentials of the user (see chapter *“I – Programming Credentials and Doors”*).
- **“Copy” button:** this allows making a copy of *master* cards. It is only displayed if the option “Manage staff card copies” is enabled in the “Facility” tab of the “Setup” menu. For more information, see *“Manage staff card copies”* on page 184.
- **“Add” button:** this allows adding new users. This button must always be clicked before you start to enter data related to a new user, as otherwise, the data of an existing user are overwritten.
- **“Delete” button:** this allows removing the user from the locking plan.

- **“Multi” button:** this allows modifying the properties of different users at the same time, by selecting them and clicking “OK”.



Users selection

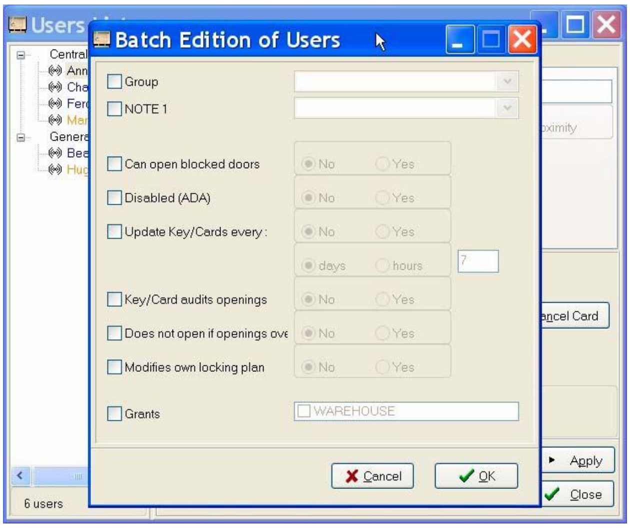
6 not selected

Ann
Beatrix
Charles
Ferdinad
Hugh
Martha

0 selected

Group ———
Technology ———
NOTE 1 ———
NOTE 2 ———

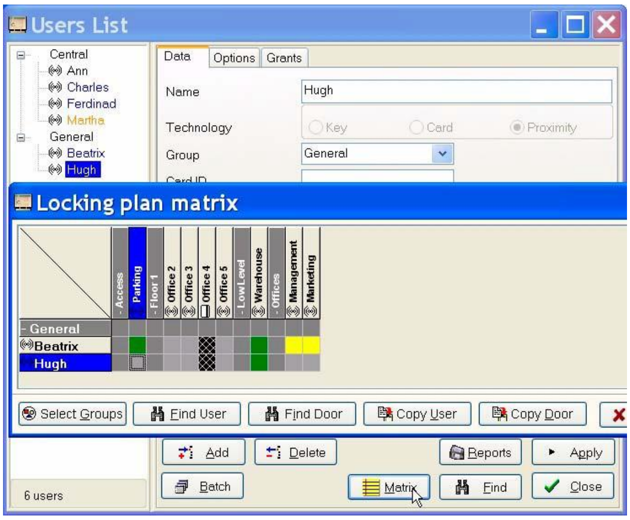
Finally, the settings to be modified are selected and you click “OK”.



Batch Edition of Users

□ Group
□ NOTE 1
□ Can open blocked doors ● No ○ Yes
□ Disabled (ADA) ● No ○ Yes
□ Update Key/Cards every : ● No ○ Yes
● days ○ hours 7
□ Key/Card audits openings ● No ○ Yes
□ Does not open if openings ove ● No ○ Yes
□ Modifies own locking plan ● No ○ Yes
□ Grants □ WAREHOUSE

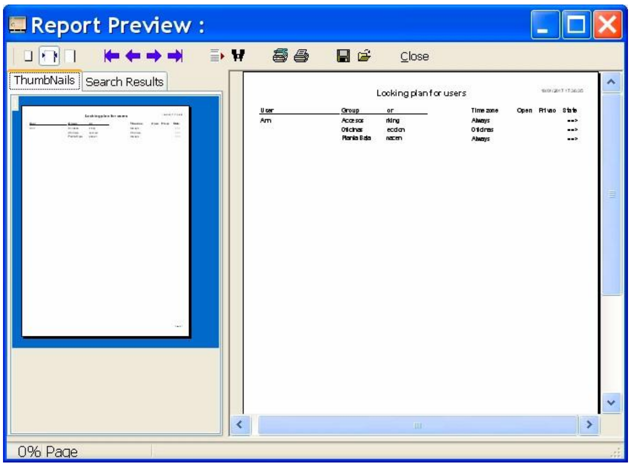
- **“Matrix” button:** this allows accessing the matrix menu directly, but showing only the user selected and those who belong to the same group.



Users List

Name: Hugh
Technology: ○ Key ○ Card ● Proximity
Group: General

Locking plan matrix



Locking plan for users

| User | Group | or | Time zone | Open | Privac | State |
|---|---|---|---|---|---|---|
| Ann | Accesor | rking | Always | | | ==> |
| | Oficinas | ecdon | Oficinas | | | ==> |
| | Planta Baja | nacen | Always | | | ==> |

- **“Reports” button:** this allows consulting and exporting the information related to the users.

  The information shown by the reports is the following:

  – *User*: user name.

  – *Group*: name of the group the user belongs to.

  – *Door*: name of the door they have access to.

  – *Time Zone*: hours when the user has access to the door.

  – *Open*: if the “@” symbol is displayed, then the user can leave the door in open mode. For more information on the “Can leave door open” concept, see *“F.5 Matrix”* on page 86.

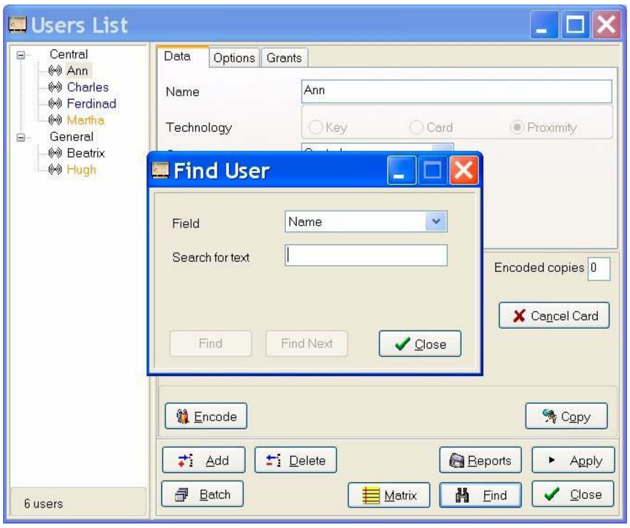
  – *Privac*: if the “@” symbol is displayed, then the user overrides privacy. For more information on the “Overrides privacy” concept, see *“F.5 Matrix”* on page 86.

  – *State*: this indicates the situation which the encoding process of a user is in.
  An arrow pointing to the right (==>) indicates that the changes made in the locking plan of a user have NOT yet been transferred to the credential of the user.
  An arrow pointing to the left (<==) indicates that the changes made in the locking plan of a user have already been transferred to the credential.
  A blank space ( ) indicates that the changes in the locking plan have already been transferred to the lock and, then, the credential has been passed through an updater reader or has been read from the TS1000.

  □ **IMPORTANT:** it is advisable to transfer the information related to the locks to the system. In a site without updater readers, this will be carried out by means of the Portable Programmer. It is enough to connect the programmer to the computer once the initialisation of the locks/cylinders has finished, and read the openings.

- **“Find” button:** this allows finding a user, making this task easier when the list is long.

  The search can be conducted by *Name*, by *User ID* or by any of the extra fields which have been defined.



Name: Ann

Technology: ○ Key ○ Card ● Proximity

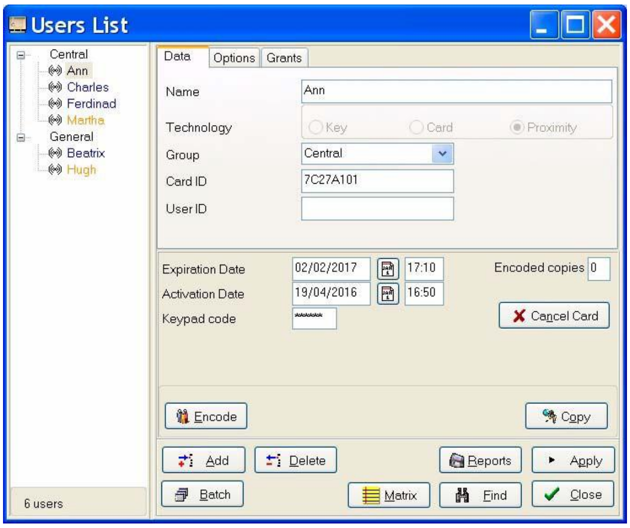
Field: Name

Search for text:

Encoded copies: 0

- **“Apply” button:** this saves the latest changes made.

- **“Close” button:** this closes the users window and saves the changes made.



Central
- Ann
- Charles
- Ferdinad
- Martha

General
- Beatrix
- Hugh

6 users

Name: Ann

Technology: ○ Key ○ Card ● Proximity

Group: Central

Card ID: 7C27A101

User ID:

Expiration Date: 02/02/2017 17:10

Activation Date: 19/04/2016 16:50

Keypad code: ******

Encoded copies: 0

On the left of the window, the list of users who are in the system is displayed, sorted according to the group they belong to.

The user colour can be orange, blue or black:

- **ORANGE** indicates that the credential of the user has not been encoded yet.

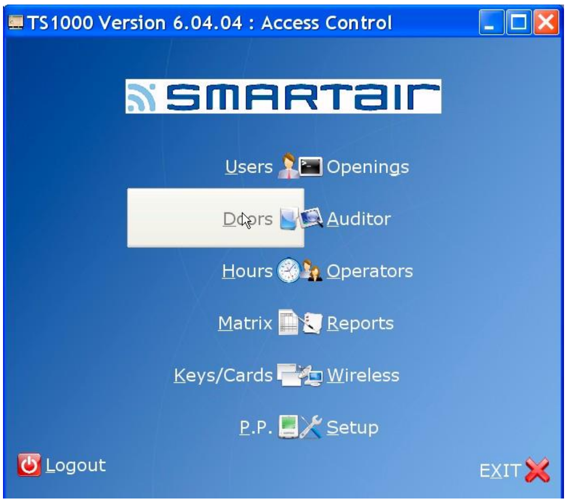
- **BLUE** indicates that there are pending modifications and, therefore, the card has to be encoded again.

- **BLACK** indicates that the credentials of the user have already been encoded or the pending modifications have already been transferred to the locks/cylinders.

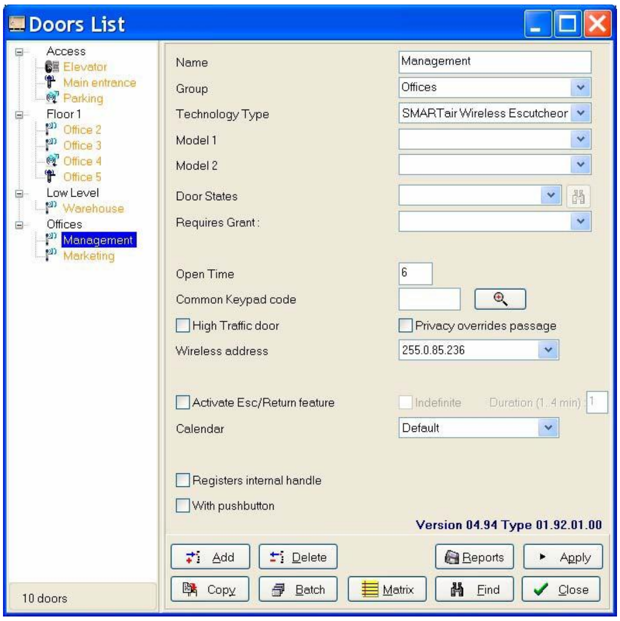
## F.3 “DOORS” MENU

After creating the user list, the next step involves creating the door list, by means of the “Doors” menu.

In order to access the “Doors” menu, click this option on the main screen of the TS1000.



The “Doors” menu presents the following fields (all the possible fields are shown here, but, at any given time, only those which correspond to the type of door selected are displayed):


Doors List

- Access
  - Elevator
  - Main entrance
  - Parking
- Floor 1
  - Office 2
  - Office 3
  - Office 4
  - Office 5
- Low Level
  - Warehouse
- Offices
  - Management
  - Marketing

10 doors

| | |
|---|---|
| Name | Management |
| Group | Offices |
| Technology Type | SMARTair Wireless Escutcheor |
| Model 1 | |
| Model 2 | |
| Door States | |
| Requires Grant : | |
| Open Time | 6 |
| Common Keypad code | |
| □ High Traffic door | □ Privacy overrides passage |
| Wireless address | 255.0.85.236 |
| □ Activate Esc/Return feature | □ Indefinite Duration (1..4 min) : 1 |
| Calendar | Default |
| □ Registers internal handle | |
| □ With pushbutton | |

Version 04.94 Type 01.92.01.00

- **Name:** door name.

- **Group:** name of the group the door belongs to.

- **Technology Type:** this allows selecting the type of door available in the system.

- **Model 1, Model 2:** customised fields. It is possible to define a maximum of 4 customised fields, which can be configured in the “Extra Fields” tab of the “Setup” menu, as shown in section *“Extra Fields” tab*on page 65.

- **Door States:** the states are automatic behaviours of the doors, based on the day of the week and the time. It is possible to define up to 256 different states for the doors in the state tables, with a maximum of 20 zones. For more information, see *“States”* on page 82.

- **Requires Grant:** a grant is an additional parameter which can be assigned to a door, in order to restrict the passage of users, allowing passage only to those who hold this grant. For more information, see *“Grants”* on page 103.

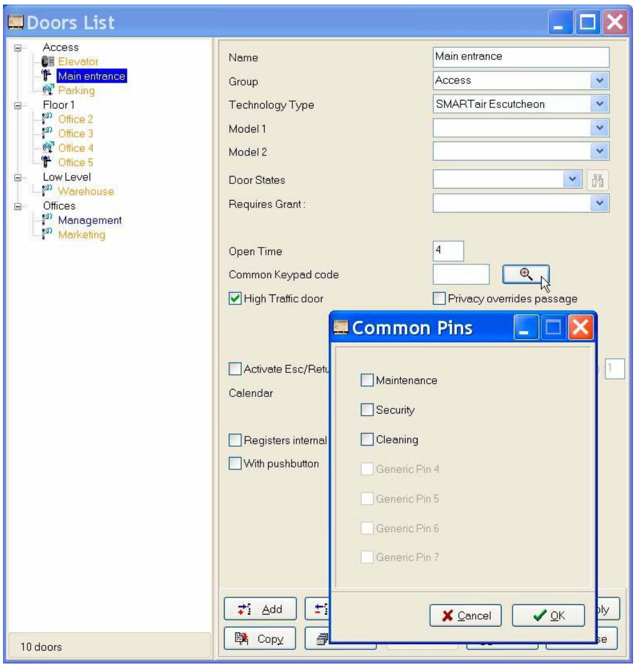
- **Open Time:** time in seconds a door remains open from when a valid credential is brought near to it. The standard time is 4 seconds. The maximum is 15 seconds.

- **Common Keypad:** code ranging from 4 to 6 digits for opening the door if it is in the state "Common Keypad": refer to *"States"* on page 82.

- **Common PINs:** the Common PINs are identification numbers which can be used by several users. In this way, it is possible to define groups of users (for example, by departments) with the same *common PIN* for all of them.

  The Common PINs are defined in the "Setup" menu, "Common PINs" tab, by means of their identification name, followed by the "PIN" number, as shown in section *"Common PINs" tab*on page 65.

  The Common PINs are assigned to the doors desired, by means of the "Magnifier" icon, which opens the window that allows them to be assigned.



Name: Main entrance
Group: Access
Technology Type: SMARTair Escutcheon
Model 1
Model 2
Door States
Requires Grant :
Open Time: 4
Common Keypad code
☑ High Traffic door
□ Privacy overrides passage
□ Activate Esc/Retu
Calendar
□ Registers internal
□ With pushbutton

□ Maintenance
□ Security
□ Cleaning
□ Generic Pin 4
□ Generic Pin 5
□ Generic Pin 6
□ Generic Pin 7

- **High Traffic Door:** see section *"High Traffic Door"* on page 77.

- **Close without card:** only for cabinet locks.

- **RF Address:** this is automatically filled in when the wireless doors are initialised. It is advisable not to modify it.

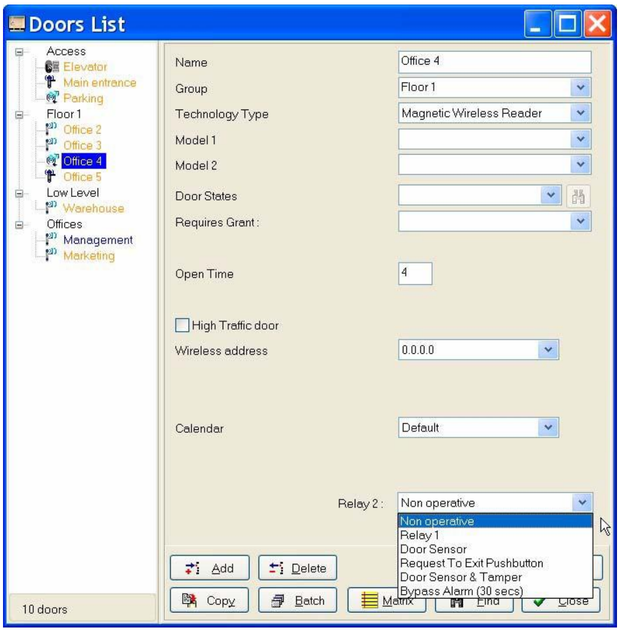
- **Updater:** if the door is of the updater reader type, the list of updaters of the system is displayed to associate it to one of them.

- **Calendar:** this allows selecting the calendar desired, from amongst those which have been defined by means of the "Calendar" tab of the "Hours" menu.

- **Registers internal handle:** this saves the record of the number of times the internal handle is used.

- **With pushbutton:** this allows opening by means of a pushbutton or "Request To Enter".

- **Relay 2:** in the Wall Reader type doors with a 2 relay board, it is possible to configure the operation of relay 2, so that it is either a copy of relay 1 or different and with diverse configurations, which can be selected by means of the corresponding drop-down menu. It is also possible to configure relay 2 by means of the DIPs of the 2 relay board. For more information, refer to the instructions for that board.
  The software always has priority over the DIPs of the board. The DIPs are only decisive when the software version is lower than 6.03.



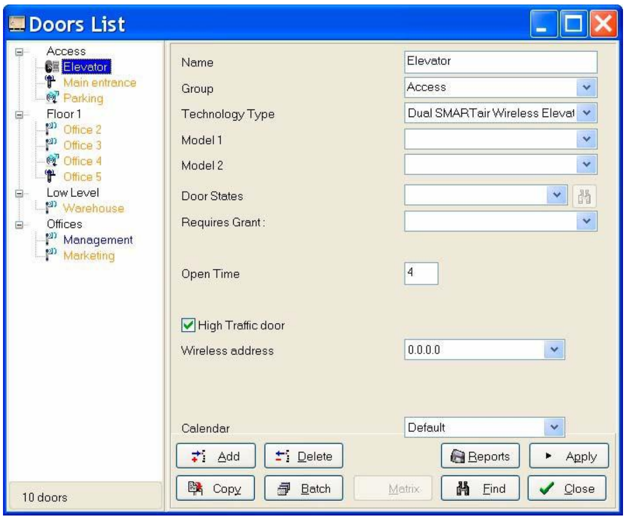
Name: Office 4
Group: Floor 1
Technology Type: Magnetic Wireless Reader
Model 1:
Model 2:
Door States:
Requires Grant :
Open Time: 4
□ High Traffic door
Wireless address: 0.0.0.0
Calendar: Default
Relay 2 : Non operative

- **"Add" button:** this adds a door. This button must always be clicked before you start to enter data related to a new door, as otherwise, the data of an existing door are overwritten.
- **"Copy" button:** this allows adding a new door, by copying an already existing one, which makes the task of adding doors easier.
- **"Delete" button:** this deletes a door.
- **"Multi" button:** this modifies the properties of several doors at the same time: see section *"Multi"* on page 78.
- **"Matrix" button:** see section *"Matrix"* on page 80.
- **"Reports" button:** see section *"Reports"* on page 78.
- **"Find" button:** see section *"Find"* on page 80.
- **"Apply" button:** this saves the latest changes made.
- **"Close" button:** this closes the doors menu and saves the changes made.

On the left of the window, the list of doors which are in the system is displayed, sorted according to the group they belong to.

The door colour can be orange, blue or black:

- **ORANGE** indicates that the door has not been initialised yet; it is necessary to initialise it.
- **BLUE** indicates that the door is initialised, but there is still information which has to be transmitted to it, either by means of the Portable Programmer or through wireless.
- **BLACK** indicates that the door is initialised and there is no information which has to be transmitted to it.



Name: Elevator
Group: Access
Technology Type: Dual SMARTair Wireless Elevat
Model 1:
Model 2:
Door States:
Requires Grant :
Open Time: 4
☑ High Traffic door
Wireless address: 0.0.0.0
Calendar: Default

## High Traffic Door

The cylinders, as well as the locks and readers, have the capacity to recognise up to 1,500 different users. For more information on the limitations of the devices, see *"Lock's Audit trail"* on page 181.

For doors where it is necessary to provide access to more than 1,500 users, the TS1000 system offers the option "High Traffic Door".

The High Traffic Door can be combined with *grants*.

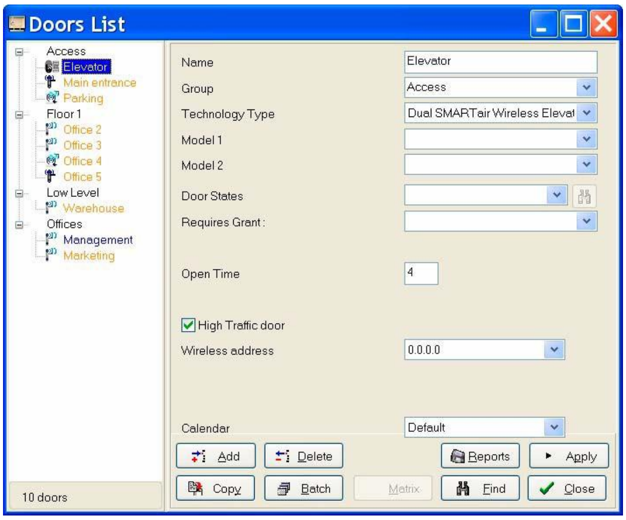
When a door is defined as a "High Traffic Door", the product installed on the door (a cylinder, a lock and/or a reader) is instructed that, in order to grant or reject access, it only has to take into account the system code, the activation and expiry dates, and the grants. That is to say, a high traffic door allows access to all the users whose credentials belong to the system, whose activation and expiry dates are correct, and who have the appropriate grants (for more information, refer to the chapter "Grants").

Therefore, a high traffic door is not displayed on the *Matrix* of the system, since it does not require any other condition for granting access or not.

For a door to operate as a high traffic door, do the following:

1 Select the door and tick the option "High Traffic Door".

2 Click the "Apply" button to save the changes.
The "Matrix" button ceases to be operative for this door.



Name: Elevator
Group: Access
Technology Type: Dual SMARTair Wireless Elevat
Model 1:
Model 2:
Door States:
Requires Grant :
Open Time: 4
☑ High Traffic door
Wireless address: 0.0.0.0
Calendar: Default

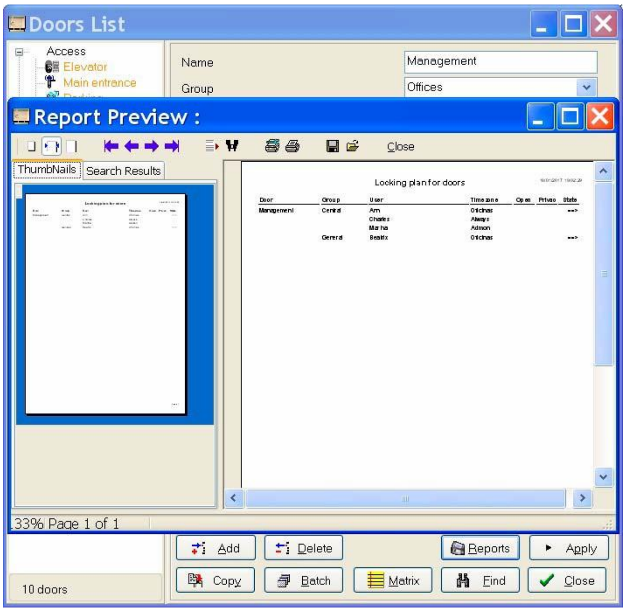
For high traffic doors, it is important to consider that a user with a credential belonging to the site, but without an expiry date, will always have access to the high traffic doors and, in principle, there is no way to cancel such a credential.

In order to solve this problem, there exists a "High Traffic Cancelling Card" credential.

For more information, see the corresponding chapter (*"High Traffic Cancelling Card"* on page 194).

## Reports

The “Reports” button allows consulting and exporting the information related to the users.



Locking plan for doors

| Door | Group | User | Time zone | Open | Privac | State |
|---|---|---|---|---|---|---|
| Management | Central | Ann | Oficinas | | | ==> |
| | | Charles | Always | | | |
| | | Martha | Admon | | | |
| | General | Beatrix | Oficinas | | | ==> |

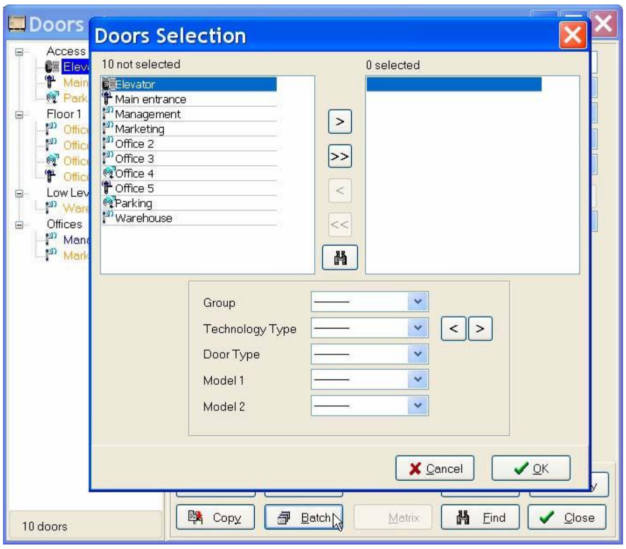
The information shown by the reports is the following:

- **Door:** door name.
- **Group:** name of the group the door belongs to.
- **User:** user name.
- **Time Zone:** this indicates whether the user is granted access or not and whether this is restricted to a time zone.
- **Open:** if the “@” symbol is displayed, then the user can leave the door in open mode. For more information on the “Can leave door open” concept, see *“F.5 Matrix”* on page 86.
- **Privac:** if the “@” symbol is displayed, then the user overrides privacy. For more information on the “Overrides privacy” concept, see *“F.5 Matrix”* on page 86.
- **State:** this indicates the situation which the user is in at the door.
  - An arrow pointing to the right (==>) indicates that the changes made in the locking plan of a user in that door have NOT been transferred yet to the credential of the user.
  - An arrow pointing to the left (<==) indicates that the changes made in the locking plan of a user in that door have already been transferred to the credential.
  - A blank space ( ) indicates that the changes in the locking plan of that door have been transferred to the TS1000 system.

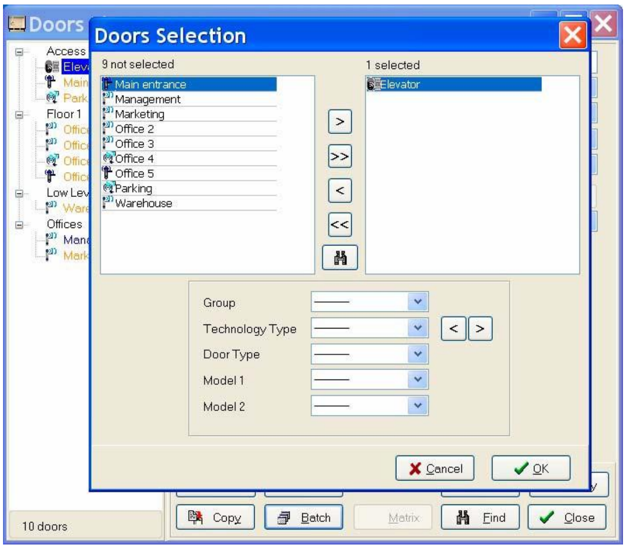
## Multi

The “Multi” button allows modifying the properties of several doors at the same time.

1 Click the “Multi” button; the following screen is displayed:



2 Select the doors whose properties you want to modify and click “OK”.



Doors Selection

9 not selected

- Main entrance
- Management
- Marketing
- Office 2
- Office 3
- Office 4
- Office 5
- Parking
- Warehouse

1 selected

- Elevator

Group ———

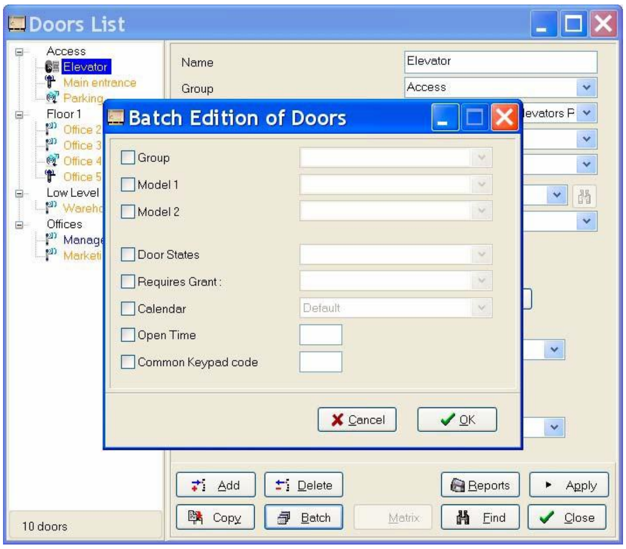
Technology Type ———

Door Type ———

Model 1 ———

Model 2 ———

3 Select the settings you need and click “OK” to accept the changes.



Doors List

Name: Elevator

Group: Access

Batch Edition of Doors

☐ Group

☐ Model 1

☐ Model 2

☐ Door States

☐ Requires Grant :

☐ Calendar: Default

☐ Open Time

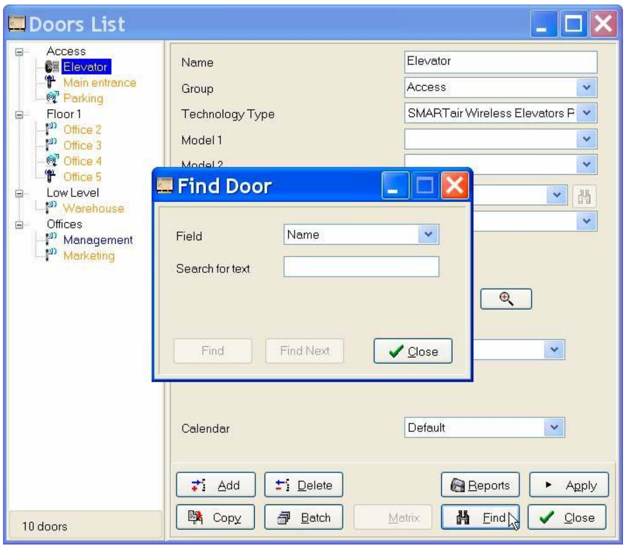
☐ Common Keypad code

## Find

The “Find” button allows conducting quick searches, which is very useful if the door list is too long.

When this button is clicked, a window is displayed which allows selecting the lookup field (door name or door ID) and entering the name or ID sought.

The search can be conducted by *Name*, by *Door ID* or by any of the *Door Extra Fields* which have been defined.



Doors List

- Access
  - Elevator
  - Main entrance
  - Parking
- Floor 1
  - Office 2
  - Office 3
  - Office 4
  - Office 5
- Low Level
  - Warehouse
- Offices
  - Management
  - Marketing

10 doors

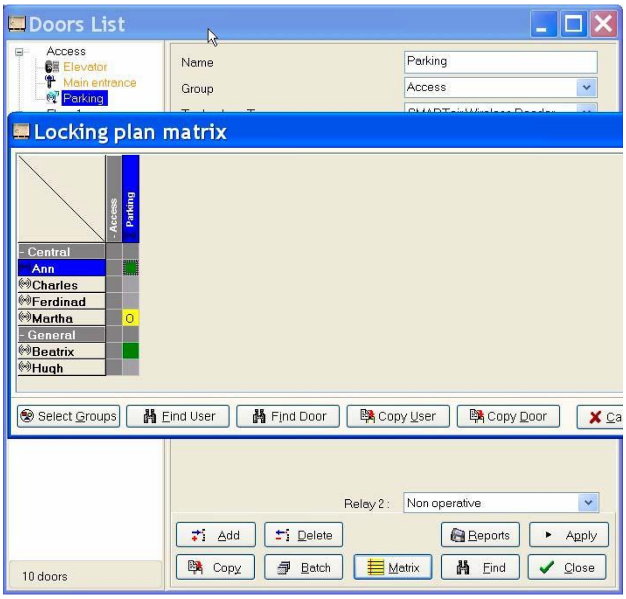
Name: Elevator
Group: Access
Technology Type: SMARTair Wireless Elevators P
Model 1:
Model 2:
Calendar: Default

Find Door

Field: Name
Search for text:

## Matrix

By clicking the “Matrix” button, the “Matrix” menu is accessed directly, but only the doors which belong to the same group as the door selected will be displayed.
If, for example, the door “Management” is selected, which belongs to the “Offices” group, only the doors belonging to the “Offices” group will be displayed.



Doors List

- Access
  - Elevator
  - Main entrance
  - Parking

10 doors

Name: Parking
Group: Access

Locking plan matrix

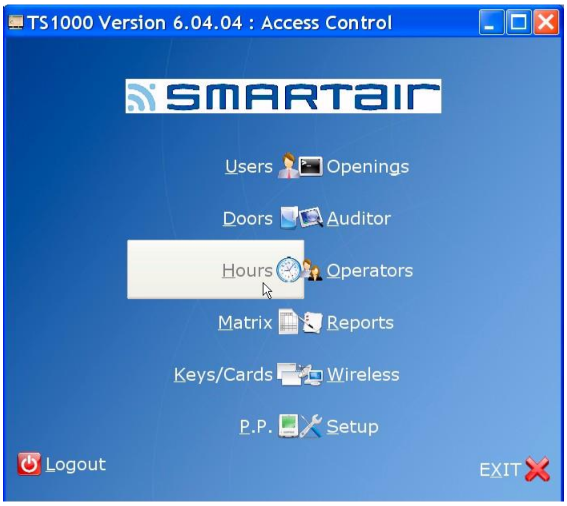
| | Access | Parking |
|---|---|---|
| - Central | | |
| Ann | | 🟩 |
| Charles | | |
| Ferdinad | | |
| Martha | | O |
| - General | | |
| Beatrix | | 🟩 |
| Hugh | | |

Relay 2 : Non operative

## F.4 “HOURS” MENU

After defining both users and doors, we should to define the access hours, even though this is not essential in order to create a locking plan.

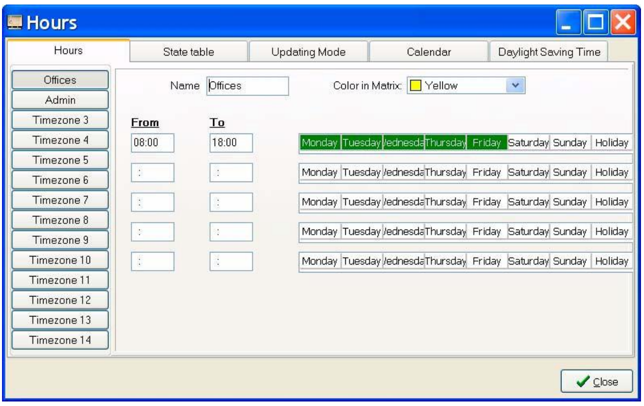
In order to access the “Hours” menu, click this option on the main screen of the TS1000.



In the “Hours” menu, there are 5 configuration tabs:

- Hours
- States
- Update Mode
- Calendar
- Time Changes

These tabs are described in the following sections.



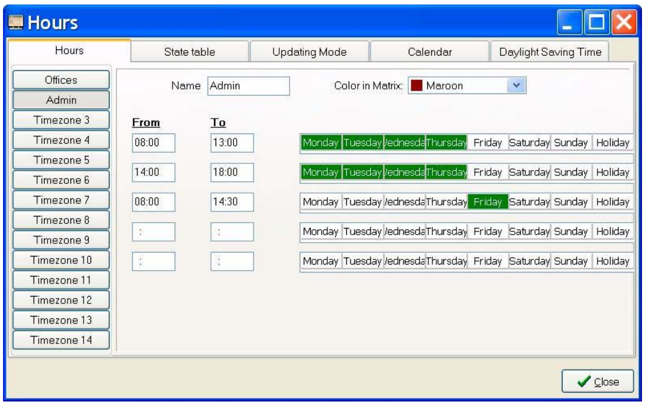
Name: Offices
Color in Matrix: Yellow

| From | To | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 08:00 | 18:00 | [✓ Monday] | [✓ Tuesday] | [✓ /ednesda] | [✓ Thursday] | [✓ Friday] | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |

### “Hours” tab

The “Hours” tab allows defining up to 14 different time zones with a maximum of 5 periods of time.

For example, it is possible to define a time zone called “Admin”, with an access time from 08:00 to 13:00 and from 14:00 to 18:00 from Mondays to Thursdays, and from 08:00 to 14:30 on Fridays.

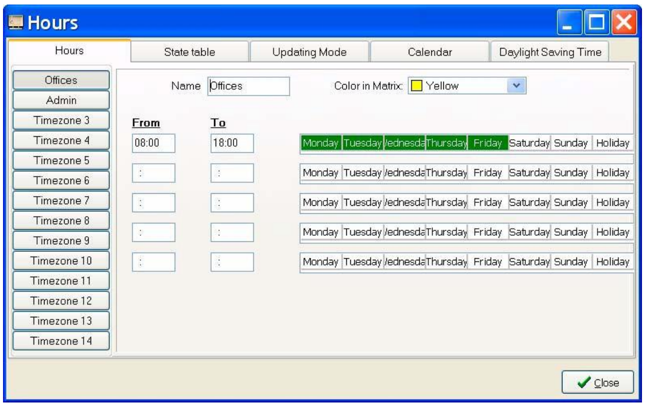


Name: Admin
Color in Matrix: Maroon

| From | To | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 08:00 | 13:00 | [✓ Monday] | [✓ Tuesday] | [✓ /ednesda] | [✓ Thursday] | Friday | Saturday | Sunday | Holiday |
| 14:00 | 18:00 | [✓ Monday] | [✓ Tuesday] | [✓ /ednesda] | [✓ Thursday] | Friday | Saturday | Sunday | Holiday |
| 08:00 | 14:30 | Monday | Tuesday | /ednesda | Thursday | [✓ Friday] | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |

Another time zone could also be defined, called “Offices”, with permitted access from 08:00 to 18:00 from Mondays to Fridays.

In order to define a time zone, write its name in the field “Name”, the limit hours in the fields “From” and “To”, and select the days by double-clicking the day desired. Finally, click “Close” to accept and save the changes.



Name: Offices  Color in Matrix: Yellow

| From | To | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 08:00 | 18:00 | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| : | : | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |

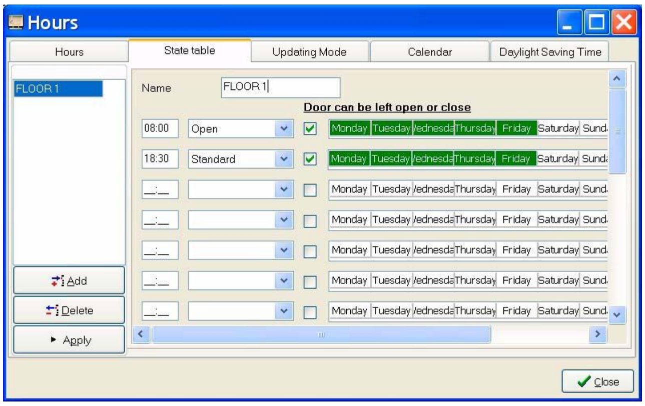
Once the hours have been defined, they have to be assigned to the corresponding locking plan crosses in the matrix.

□ As can be seen, each timetable has a different colour, which allows the timetable assigned to each user-door combination to be quickly distinguished in the matrix.

## States

These are only available for Electronic Locks and Wall Readers.

The states, defined in the state tables, are automatic behaviours of the doors, based on the day of the week and the time.



Name: FLOOR 1

Door can be left open or close

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 08:00 | Open | ☑ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |
| 18:30 | Standard | ☑ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |
| __:__ | | □ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |
| __:__ | | □ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |
| __:__ | | □ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |
| __:__ | | □ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |
| __:__ | | □ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sund. |

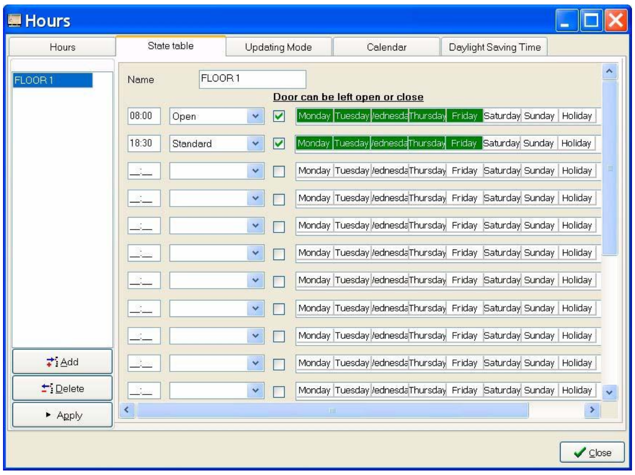
It is possible to define up to 256 different states for the doors in the state tables, with a maximum of 20 zones.

The doors can be programmed in any of the following states:

- **Open:** the door passes to open mode at the time scheduled.
- **First User:** the door operates in standard mode until the first user with granted access goes through it, as from the time indicated. As from that moment, the door passes to open mode.
- **Common Keypad:** all the users open a door by typing the same code (from 4 to 6 digits) or one of the 8 common PINs defined and valid for that door. This code is programmed in the “Doors” menu.
  This operation mode is only available for locks with a built-in keypad (magnetic stripe and proximity readers and locks).
- **Standard:** the door operates in standard mode, that is to say, it is necessary for each user to pass their credential to open it.
- **Card + PIN:** in order to open the door, it is necessary to pass an authorised card through and then type the code (from 4 to 6 digits) assigned to that card. This code is programmed in the “Users” menu.
  This operation mode is only available for locks with a built-in keypad (magnetic stripe readers and locks).
  It is only compatible with wireless devices; it is incompatible with the UoC system.
- **Dual User:** the door opens only if two credentials from authorised users are brought near to the lock successively.

- **PIN + Card:** in order to open the door, it is necessary in the first place to type the access code and then pass through the card associated to that code. This code is programmed in the "Users" menu.
  This is the only dual identification option available in UoC (Update On Card) systems.
  It is also compatible with wireless systems.

In order to create a new State, click "Add" and enter the desired data in the corresponding fields. The days are selected by double-clicking the corresponding day. Once you have finished, click "Apply" to encode the data.



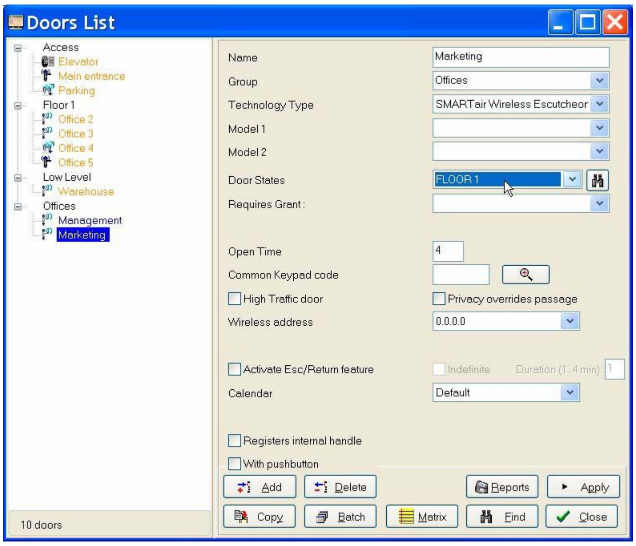
Name: FLOOR 1

**Door can be left open or close**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 08:00 | Open | ☑ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| 18:30 | Standard | ☑ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | ☐ | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |

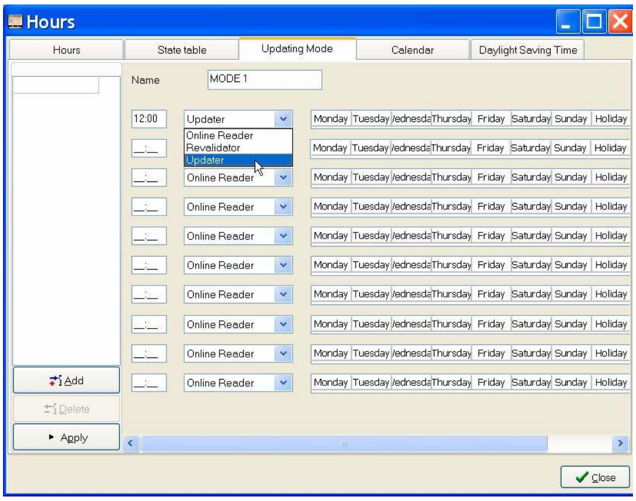
For example, the state FLOOR 1 is defined in such a way that the door opens at 08:00 and closes automatically at 18:30. In addition, the possibility of leaving the door open has been enabled by means of the corresponding check box. This check box allows prioritising the automatic or manual change of state during the corresponding period.

Once a door state has been created, a new Door States field is displayed in the "Doors" menu:



Name: Marketing
Group: Offices
Technology Type: SMARTair Wireless Escutcheor
Model 1:
Model 2:
Door States: FLOOR 1
Requires Grant :
Open Time: 4
Common Keypad code:
☐ High Traffic door ☐ Privacy overrides passage
Wireless address: 0.0.0.0
☐ Activate Esc/Return feature ☐ Indefinite Duration (1..4 min): 1
Calendar: Default
☐ Registers internal handle
☐ With pushbutton

## "Update Mode" tab



Name: MODE 1

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 12:00 | Updater | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |
| __:__ | Online Reader | Monday | Tuesday | /ednesda | Thursday | Friday | Saturday | Sunday | Holiday |

This tab allows defining how the updater type door can be programmed. It allows disregarding certain features for the purpose of optimising the response time of the device:

- **Online Reader:** it is only a reader, which simply reads the card.
  This is the fastest response mode. It neither updates data nor collects openings. It is only used in updaters with door control, since it only manages the opening of the door associated to the device.

- **Revalidator:** reads and encodes the dates and grants of the cards.
  This is the intermediate response mode.
  It neither collects the stored events nor loads the locking plan crosses still not encoded on the credential, but it allows renewing the expiry of the credentials and modifying the grants assigned to the user.
  It can equally be used in updaters with or without door control.

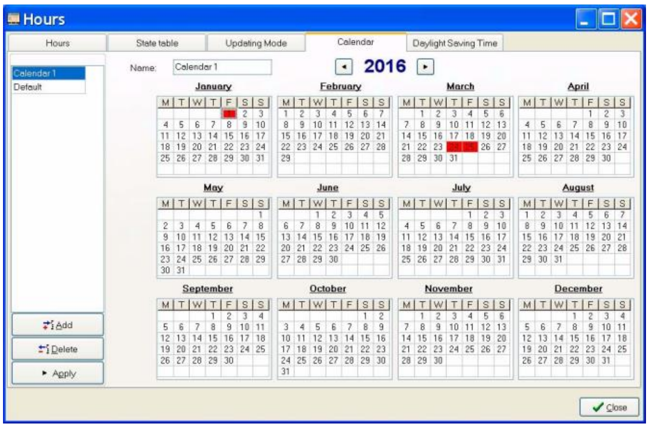
- **Updater:** reads the card, collects the events and writes the modifications of the matrix for that user.
  This is the most complete mode, but the processing time is longer. It collects events, writes the locking plan crosses still to be encoded, renews the expiry of the credential and modifies the grants.
  It can equally be used in updaters with or without door control.

## Calendar

It is possible to define the holidays for each site, by means of the "Calendar" tab.

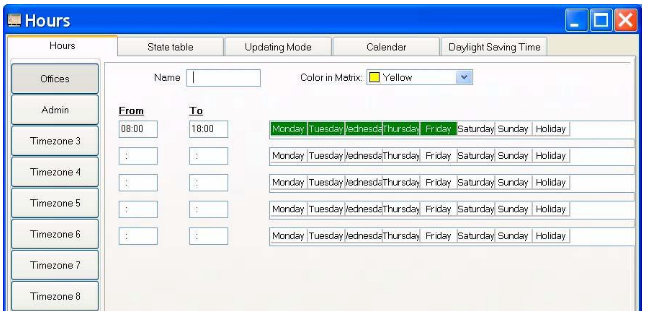
For this purpose, double-click the holidays for them to turn red.

It is possible to define different calendars of holidays. In order to define a new calendar, click "Add" and write a name in the field "Name". Select the holidays by double-clicking the corresponding days. Once you have finished, click "Apply". The new calendar is displayed in the column on the left.



Name: Calendar 1

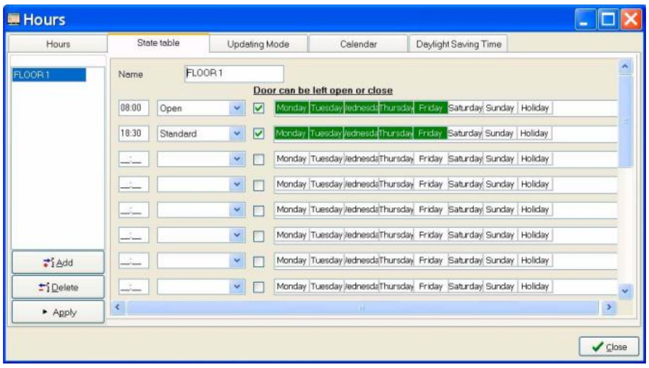
After setting the holidays by means of the “Calendar” tab, it is possible to restrict the access to the users on holidays, both in the “Hours” tab as well as in “States”, by clicking on “Holidays”, which is after “Sunday”.



Name:

Color in Matrix: Yellow

From: 08:00 To: 18:00



Name: FLOOR 1

Door can be left open or close

08:00 Open ☑

18:30 Standard ☑

## “Time Changes” tab

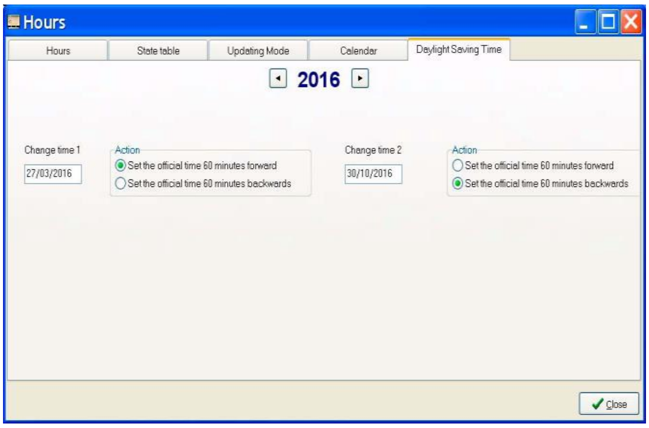
This allows setting the time changes for summer and winter.

The specific dates are taken from those defined by Windows.

Even though the database allows configuring all the years desired, each device stores only the two forthcoming changes (valid for the next 12 months); therefore, it is necessary to update the information in the doors at least once a year.

In the off-line and UoC systems, it is necessary to update it manually with the portable programmer.

In the wireless systems, this information is sent automatically on the 1st of each month.



2016

Change time 1: 27/03/2016

Action:
- ● Set the official time 60 minutes forward
- ○ Set the official time 60 minutes backwards

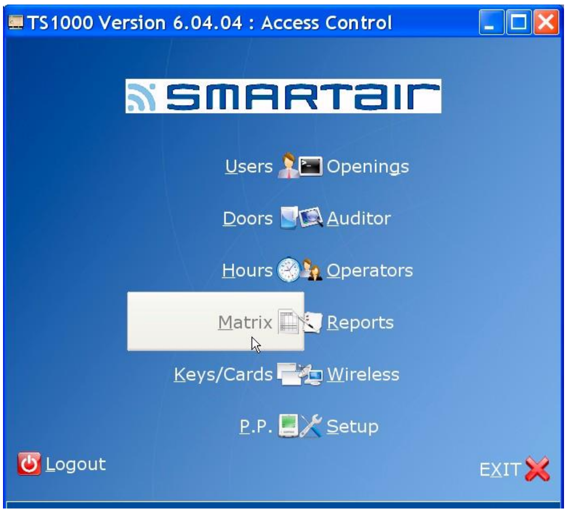
Change time 2: 30/10/2016

Action:
- ○ Set the official time 60 minutes forward
- ● Set the official time 60 minutes backwards

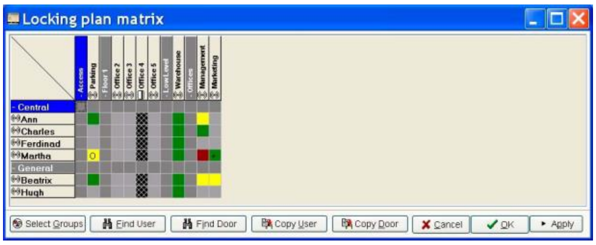
## F.5 MATRIX

Once the users (who), the doors (where) and the hours (when) have been created, it is time to define the locking plan. The matrix allows the three things to be tied together.

In order to access the “Matrix” menu, click this option on the main screen of the TS1000.

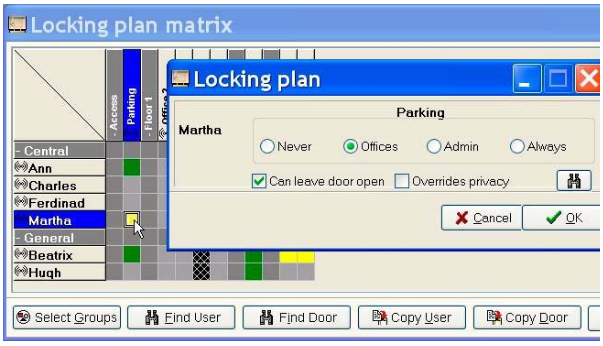


The matrix relates a user to a door, by means of a square. This square is referred to as a “Cross”.



By double-clicking the *Cross*, it is possible to define the access properties:

It is possible to define whether the user *Miren* enters through the Car Park: “Never”, “Always” or according to one of the timetables defined (Offices and Admin). Between “Never” and “Always” there will be as many timetables as you have defined in the Hours menu.



Parking

Martha

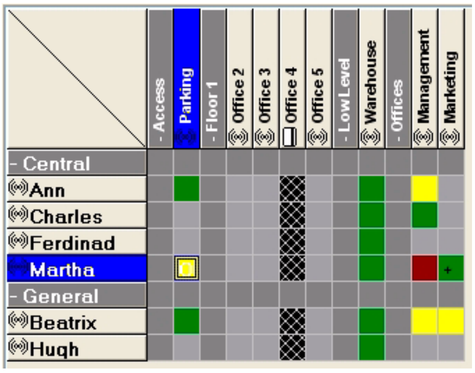
○ Never ● Offices ○ Admin ○ Always

☑ Can leave door open □ Overrides privacy

- **Can leave door open check box:** if this check box is enabled, the user can leave the door open, by acting as follows: passing their credential through the door once and, immediately afterwards, passing it through once again, while the light is still green. In this way, the door remains open permanently. For the door to be closed again (for example, at night), it is necessary to define a *State* (see *“States”* on page 82).
- **Overrides privacy check box:** if this check box is enabled, the user can access a door which they are authorised to access, even if its privacy thumb turn is engaged. Otherwise, they cannot gain access to it, even if authorised to do so, because the privacy thumb turn is engaged.

From the colour of the *cross*, it is possible to tell the access type:

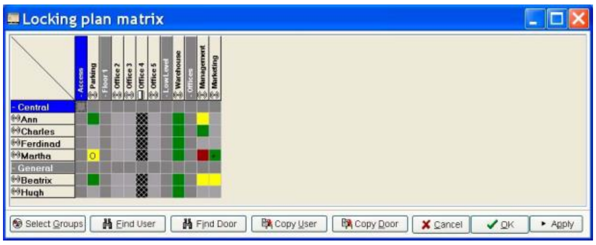
- **Never:** grey colour
- **Always:** green colour
- **Hours:** the colour of the timetable set. In order to see the properties of the hours, click the 🔍 button. For this button to be displayed, it is necessary to double-click the cross and show the cross definition window. It can also be seen by right-clicking the corresponding cross.



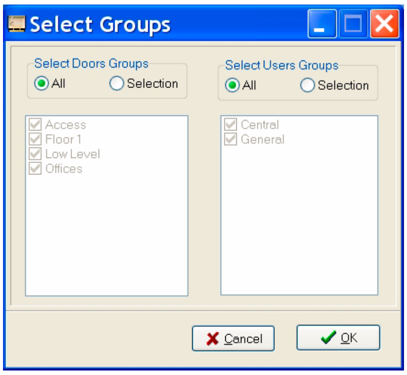
| | - Access | Parking | - Floor 1 | Office 2 | Office 3 | Office 4 | Office 5 | - Low Level | Warehouse | - Offices | Management | Marketing |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - Central | | | | | | | | | | | | |
| Ann | | 🟩 | | | | ▩ | | | 🟩 | | 🟨 | |
| Charles | | | | | | ▩ | | | 🟩 | | 🟩 | |
| Ferdinad | | | | | | ▩ | | | 🟩 | | | |
| Martha | | 0 | | | | ▩ | | | 🟩 | | 🟥 | + |
| - General | | | | | | | | | | | | |
| Beatrix | | 🟩 | | | | ▩ | | | 🟩 | | 🟨 | 🟨 |
| Hugh | | | | | | ▩ | | | 🟩 | | | |

- **+:** indicates that the user Overrides privacy.
- **0:** indicates that the user can leave the door open.

The following buttons are available at the bottom:


Locking plan matrix

- **Select Groups:** this allows defining which groups of doors and users are displayed on the screen, which is very useful when the matrix is large.


Select Groups

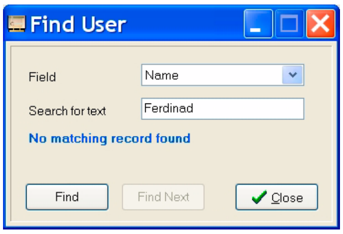
Select Doors Groups: ● All ○ Selection

☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Select Users Groups: ● All ○ Selection

☑ Central
☑ General

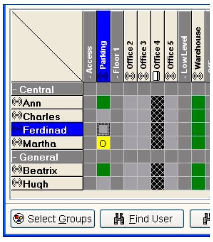
- **Find User:** a window is displayed when this button is clicked, which allows finding a user quickly. The marker is placed on the name of the user sought. The search can be conducted by *Name*, by *User ID* and by any of the *User Extra Fields* which have been defined.


Find User

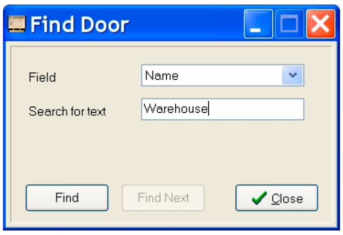
Field: Name

Search for text: Ferdinad

No matching record found

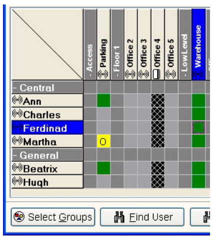


- **Find Door:** this allows finding a door easily, by means of a search window, in a large-sized matrix. The marker is placed on the name of the door sought. The search can be conducted by Name, by Door ID and by any of the Door Extra Fields which have been defined.

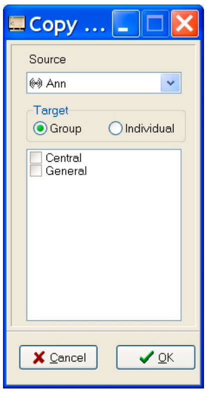

Find Door

Field: Name

Search for text: Warehouse



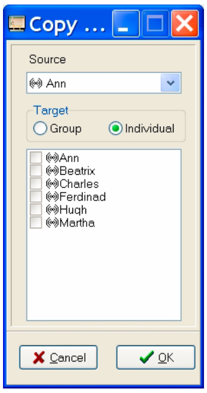
- **Copy User:** allows copying the accesses of one user to a series of individual users, or to one or several groups of users.



Source: Ann

Target: ● Group ○ Individual

□ Central
□ General

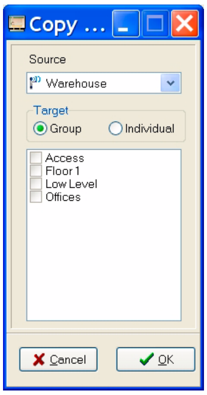


Source: Ann

Target: ○ Group ● Individual

□ Ann
□ Beatrix
□ Charles
□ Ferdinad
□ Hugh
□ Martha

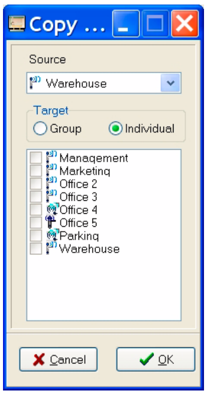
- **Copy Door:** allows copying the accesses of one door to a series of individual doors, or to one or several groups of doors.



Source: Warehouse

Target: ● Group ○ Individual

□ Access
□ Floor 1
□ Low Level
□ Offices



Source: Warehouse

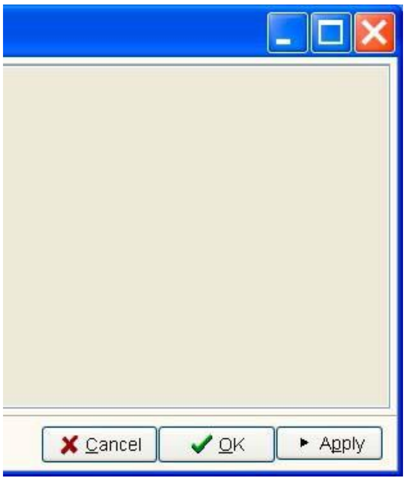
Target: ○ Group ● Individual

□ Management
□ Marketing
□ Office 2
□ Office 3
□ Office 4
□ Office 5
□ Parking
□ Warehouse

- **Cancel:** exits the "Matrix" menu without saving the changes made.

- **OK:** saves the changes made to the matrix and closes the "Matrix" menu.

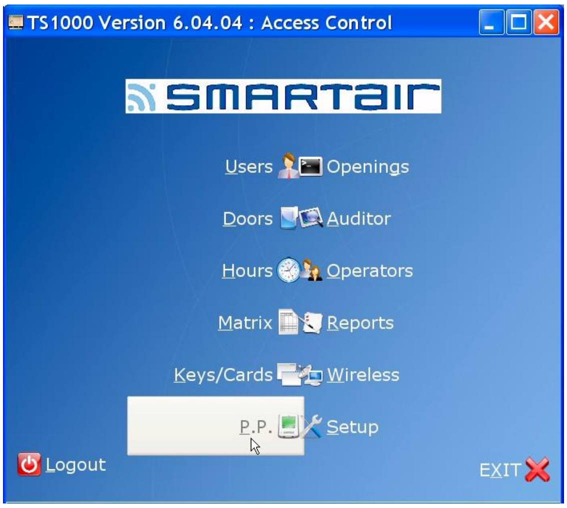
- **Apply:** saves the changes made to the matrix, without exiting the menu.



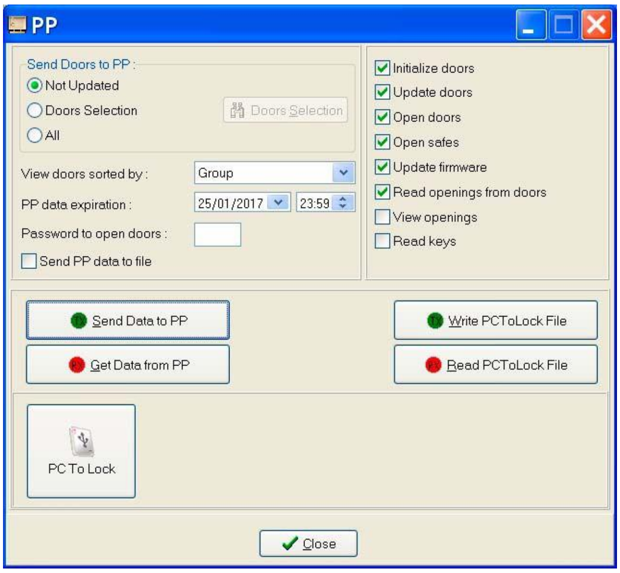
## F.6 SAVING AND TRANSFERRING THE LOCKING PLAN

Once the locking plan has been created, it is necessary to transfer this information to the portable programmer and, subsequently, initialise the locks, readers and/or cylinders.

In order to access the Portable Programmer menu, click “PP” on the main screen of the TS1000.



□The most common way is to click “Send Data to PP”, as detailed in section *“I.2 Transmitting data to the Portable Programmer”* on page 114.
However, it is also possible to store the data in a file, without sending them to the Portable Programmer for the moment, although this option is not currently used.



Send Doors to PP :
● Not Updated
○ Doors Selection
○ All

View doors sorted by : Group
PP data expiration : 25/01/2017 23:59
Password to open doors :
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

# G – Operators and Operator Levels

# G – OPERATORS AND OPERATOR LEVELS

## G.1 INTRODUCTION

In order to access the TS1000 software for the first time, it is necessary to use the “Operator Name” and “Password” provided by your distributor.

This Operator Name and Password can be modified as desired. In addition, it is possible to register as many Operators as there are Users in the system.

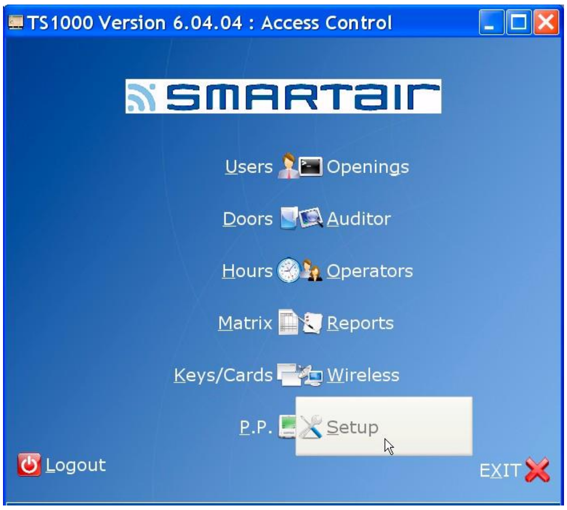
The difference between a “User” of the system and an “Operator” of the system is the following:

- **User:** any individual holding a credential allowing them to open the different doors where a cylinder, lock and/or reader are installed.
- **Operator:** this is a user of the system, who, in addition, has access to the TS1000 management software. That is to say, they have an identification name (Operator Name) and password, which allow them to access the software and carry out some or all of the operations which the software allows.

The access of the operators to the TS1000 software may have certain operations restricted. That is to say, there are “Operator Levels”.

## G.2 OPERATOR LEVELS

On the TS1000 main screen, access the “Setup” menu, clicking the corresponding button.



In the “Setup” menu, click the “Operator Levels” tab.

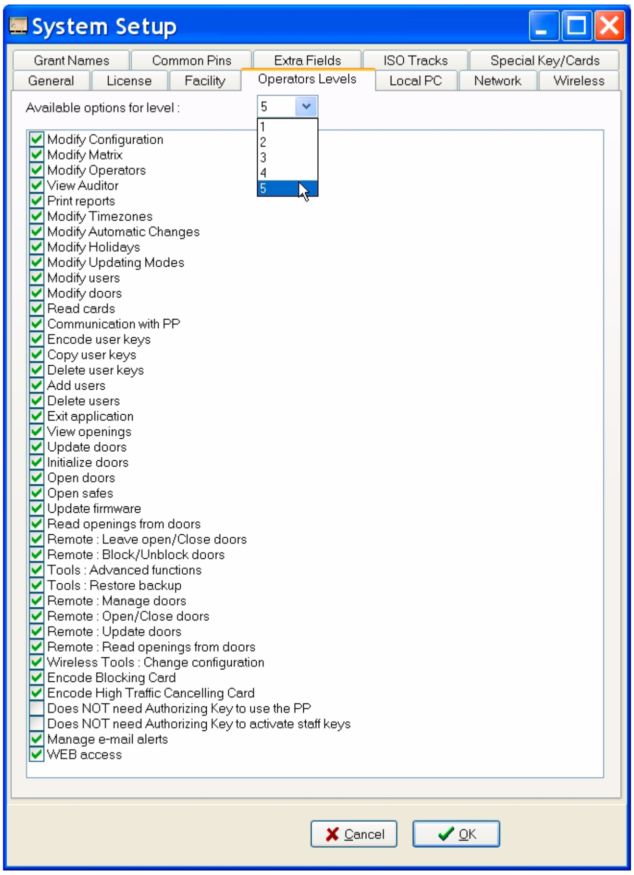
As can be seen, there are 5 different Operator Levels.

It is possible to define which functions will be available for each of the 5 levels.

For this purpose, select one of the levels from the drop-down menu (for example, 5, which is the highest and has the most functions allowed) and, in the list, select the Functions available for that level.

You can do the same for the other 4 levels.

Afterwards, each Operator should be assigned the Level which is considered appropriate.



Available options for level : 5

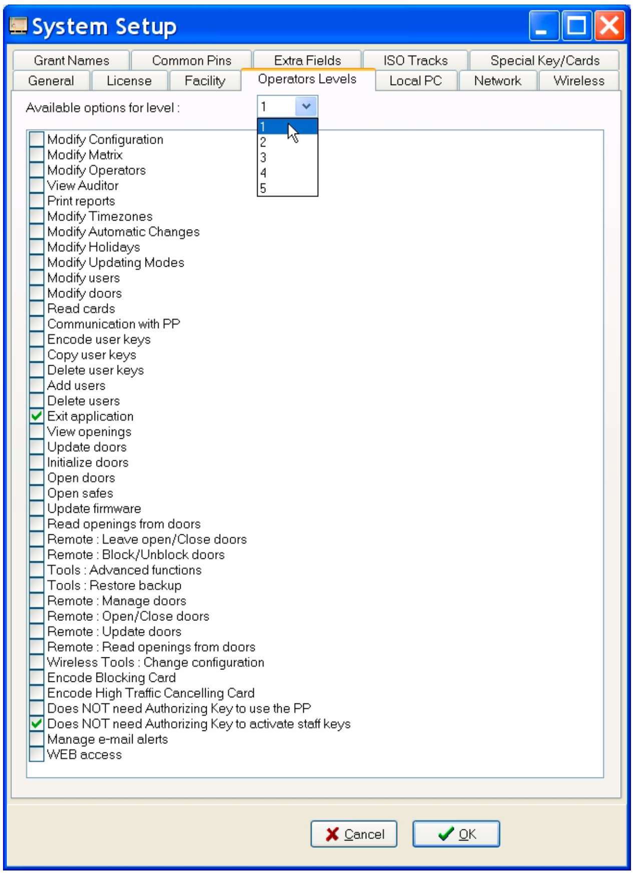
☑ Modify Configuration
☑ Modify Matrix
☑ Modify Operators
☑ View Auditor
☑ Print reports
☑ Modify Timezones
☑ Modify Automatic Changes
☑ Modify Holidays
☑ Modify Updating Modes
☑ Modify users
☑ Modify doors
☑ Read cards
☑ Communication with PP
☑ Encode user keys
☑ Copy user keys
☑ Delete user keys
☑ Add users
☑ Delete users
☑ Exit application
☑ View openings
☑ Update doors
☑ Initialize doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
☑ Remote : Leave open/Close doors
☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
□ Does NOT need Authorizing Key to use the PP
□ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

The Functions selected for Level 1, which has the fewest functions allowed, are shown in this example.

By default, the levels ranging from 1 to 4 have the option “Close Programme” enabled, in order to avoid a situation where an operator, who has been assigned by mistake to one of these levels without this having been defined in advance, is left with the programme open without being able to log out. The other options can be selected as desired, so creating different profiles according to needs. There is no need to go from fewer to more functions allowed.

The functions “Does NOT need Authorising Key to...” involve a special process for their activation, which is explained in section *“L.3 Deactivation of the Authorisation Key”* on page 188.

Once the Operator Levels have been defined, it is necessary to define the System Operators.

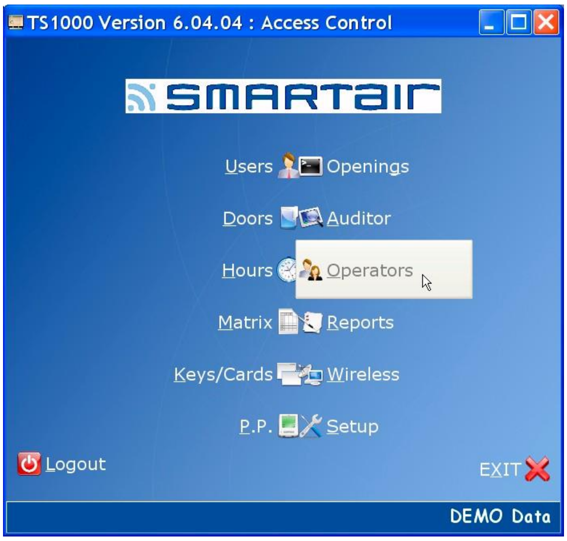


Available options for level : 1

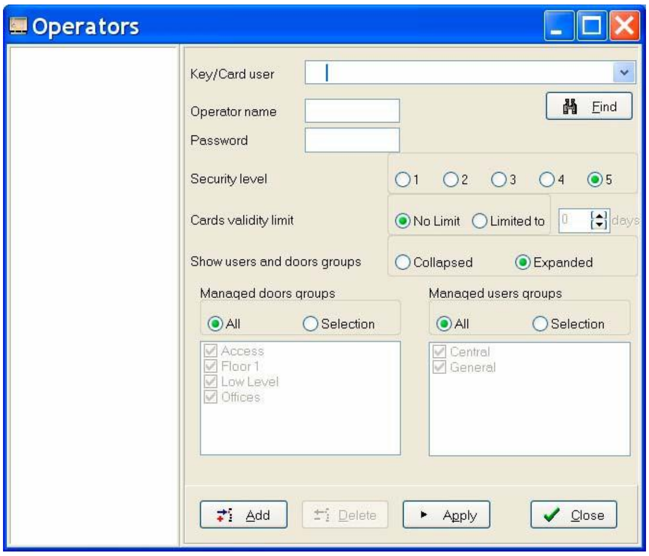
□ Modify Configuration
□ Modify Matrix
□ Modify Operators
□ View Auditor
□ Print reports
□ Modify Timezones
□ Modify Automatic Changes
□ Modify Holidays
□ Modify Updating Modes
□ Modify users
□ Modify doors
□ Read cards
□ Communication with PP
□ Encode user keys
□ Copy user keys
□ Delete user keys
□ Add users
□ Delete users
☑ Exit application
□ View openings
□ Update doors
□ Initialize doors
□ Open doors
□ Open safes
□ Update firmware
□ Read openings from doors
□ Remote : Leave open/Close doors
□ Remote : Block/Unblock doors
□ Tools : Advanced functions
□ Tools : Restore backup
□ Remote : Manage doors
□ Remote : Open/Close doors
□ Remote : Update doors
□ Remote : Read openings from doors
□ Wireless Tools : Change configuration
□ Encode Blocking Card
□ Encode High Traffic Cancelling Card
□ Does NOT need Authorizing Key to use the PP
☑ Does NOT need Authorizing Key to activate staff keys
□ Manage e-mail alerts
□ WEB access

## G.3 OPERATORS

On the TS1000 main screen, access the "Operators" menu, by clicking the corresponding button.



The "Operators" screen is displayed:



Key/Card user

Operator name

Password

Security level ○ 1 ○ 2 ○ 3 ○ 4 ● 5

Cards validity limit ● No Limit ○ Limited to 0 days

Show users and doors groups ○ Collapsed ● Expanded

Managed doors groups ● All ○ Selection

☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Managed users groups ● All ○ Selection

☑ Central
☑ General

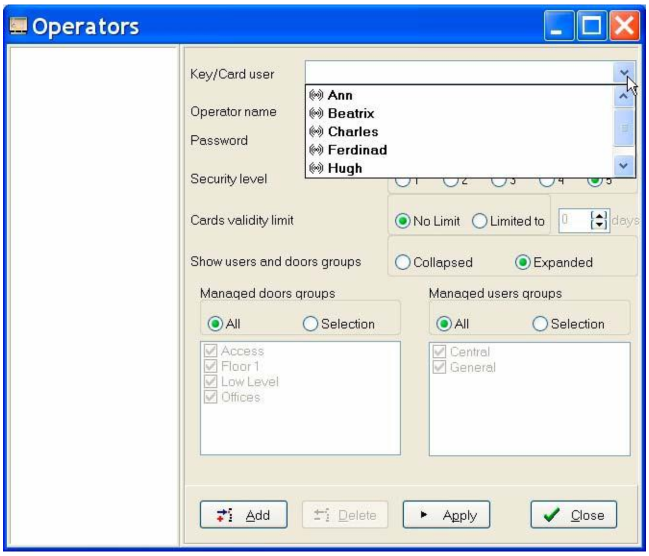
This screen allows adding the Operators to the system.

The meaning of the different fields is explained below.

## “Card User” field

This field allows selecting, from among all the Users of the system, the one who is to be added as an Operator.

By clicking the user list, all of them are displayed, except for those who have already been added as operators.



Key/Card user:
- Ann
- Beatrix
- Charles
- Ferdinad
- Hugh

Operator name

Password

Security level: ○1 ○2 ○3 ○4 ●5

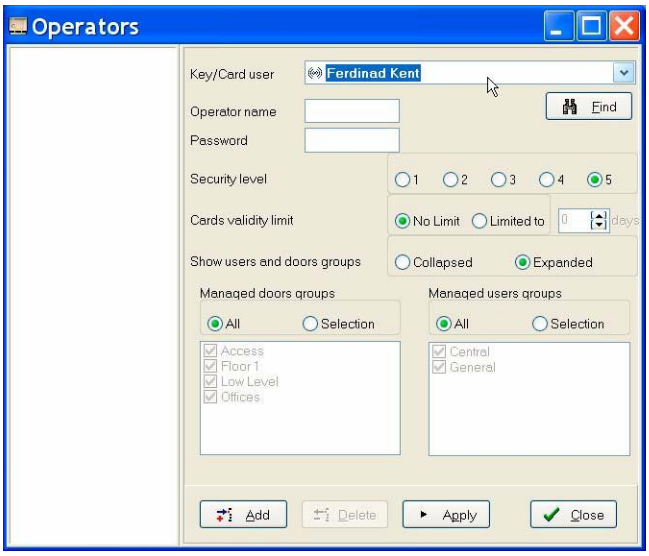
Cards validity limit: ● No Limit ○ Limited to 0 days

Show users and doors groups: ○ Collapsed ● Expanded

Managed doors groups: ● All ○ Selection
☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Managed users groups: ● All ○ Selection
☑ Central
☑ General

Select a user from the list, and their name will be displayed in the field “Card User”.



Key/Card user: Ferdinad Kent

Operator name

Password

Security level: ○1 ○2 ○3 ○4 ●5

Cards validity limit: ● No Limit ○ Limited to 0 days

Show users and doors groups: ○ Collapsed ● Expanded

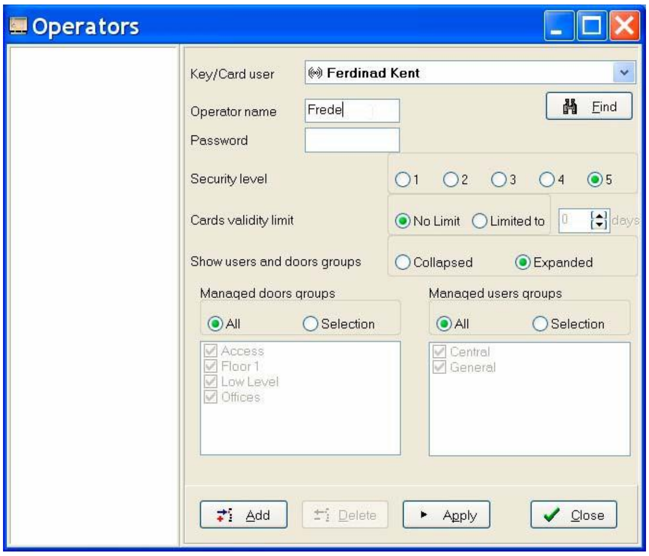
Managed doors groups: ● All ○ Selection
☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Managed users groups: ● All ○ Selection
☑ Central
☑ General

## “Operator Name” field

This field allows assigning an Identification Name to the Operator who is being added. This name need not match the User name.

Type the Operator name in the corresponding field.



Operators

Key/Card user: Ferdinad Kent

Operator name: Frede

Password:

Security level: ○ 1 ○ 2 ○ 3 ○ 4 ● 5

Cards validity limit: ● No Limit ○ Limited to 0 days

Show users and doors groups: ○ Collapsed ● Expanded

Managed doors groups: ● All ○ Selection

☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Managed users groups: ● All ○ Selection

☑ Central
☑ General

It is possible to choose an “alias” from 1 to 10 digits for the Operator name, whereas the User name tends to be their first name and both surnames.

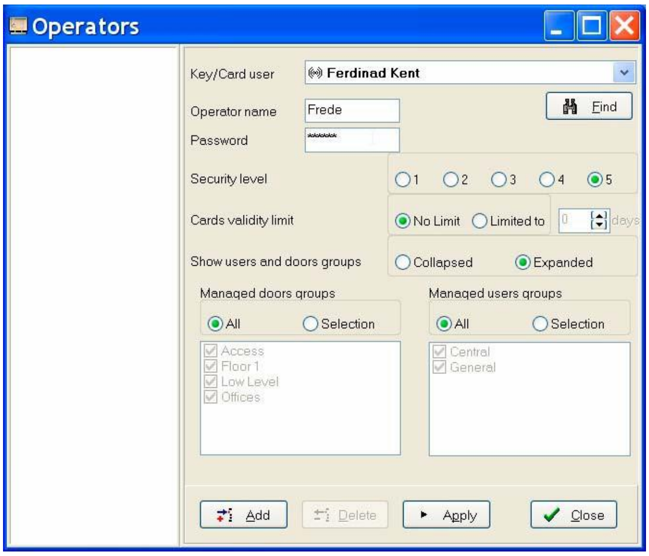
Either capital or lower case letters may be used in the Operator name.

Once the Operator has been added, they will be displayed in the column on the left with the assigned Operator name in this field.

## “Password” field

The password must have at least 6 characters, including a capital letter and a digit.

When entering the password, for security, this is shown as asterisks on the screen.



Operators

Key/Card user: Ferdinad Kent

Operator name: Frede

Password: ******

Security level: ○ 1 ○ 2 ○ 3 ○ 4 ● 5

Cards validity limit: ● No Limit ○ Limited to 0 days

Show users and doors groups: ○ Collapsed ● Expanded

Managed doors groups: ● All ○ Selection

☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

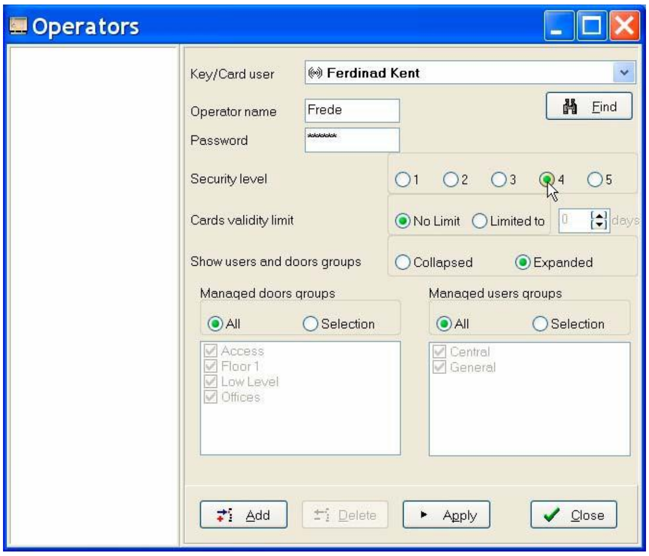
Managed users groups: ● All ○ Selection

☑ Central
☑ General

## "Security Level" field

This field allows selecting the Security Level, from among the 5 existing ones.

In the previous section, *"G.2 Operator Levels"* on page 93, it was explained how to define the operations allowed for each level.



Key/Card user: Ferdinad Kent
Operator name: Frede
Password: ******
Security level: ○ 1 ○ 2 ○ 3 ● 4 ○ 5
Cards validity limit: ● No Limit ○ Limited to 0 days
Show users and doors groups: ○ Collapsed ● Expanded
Managed doors groups: ● All ○ Selection
☑ Access
☑ Floor 1
☑ Low Level
☑ Offices
Managed users groups: ● All ○ Selection
☑ Central
☑ General

## "Cards Validity Limit" field

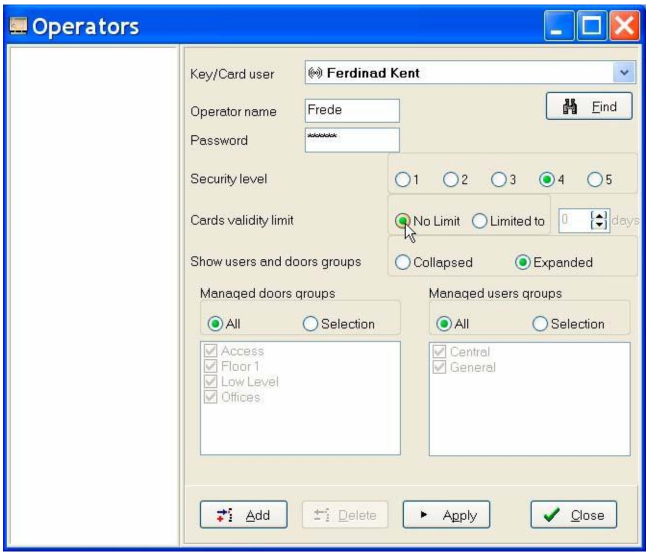
This field allows preventing certain operators from encoding user cards with no expiry limit.

When encoding a user card, it is possible to set an expiry date for it. If the field is left blank, this means that it will never expire. If a date is entered, the card will stop working from then.

There are two settings: No Limit and Limited to.

"No Limit" setting:

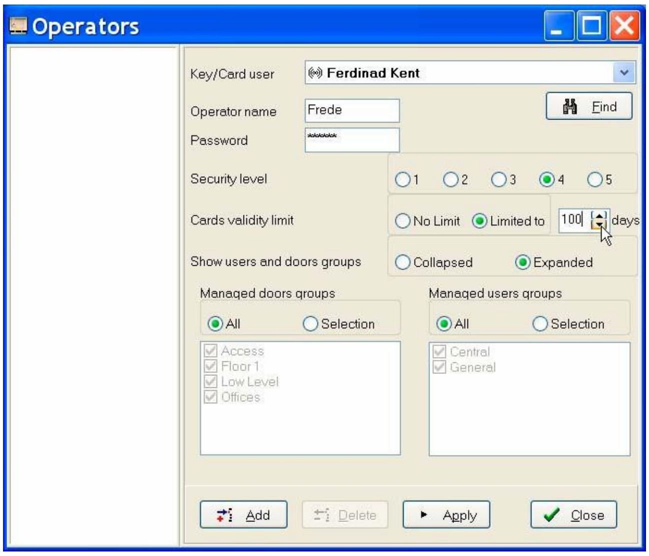
This option allows this Operator to encode user cards without indicating an expiry date and, as a result, these cards will NEVER expire.



Key/Card user: Ferdinad Kent
Operator name: Frede
Password: ******
Security level: ○ 1 ○ 2 ○ 3 ● 4 ○ 5
Cards validity limit: ● No Limit ○ Limited to 0 days
Show users and doors groups: ○ Collapsed ● Expanded
Managed doors groups: ● All ○ Selection
☑ Access
☑ Floor 1
☑ Low Level
☑ Offices
Managed users groups: ● All ○ Selection
☑ Central
☑ General

"Limited to" setting:

This option allows entering a number of days (from 1 to 730; 100 in the example) after which the card will expire, even if the operator had not entered an expiry date when encoding it.



Key/Card user: Ferdinad Kent
Operator name: Frede
Password: *****
Security level: ○ 1 ○ 2 ○ 3 ● 4 ○ 5
Cards validity limit: ○ No Limit ● Limited to 100 days
Show users and doors groups: ○ Collapsed ● Expanded

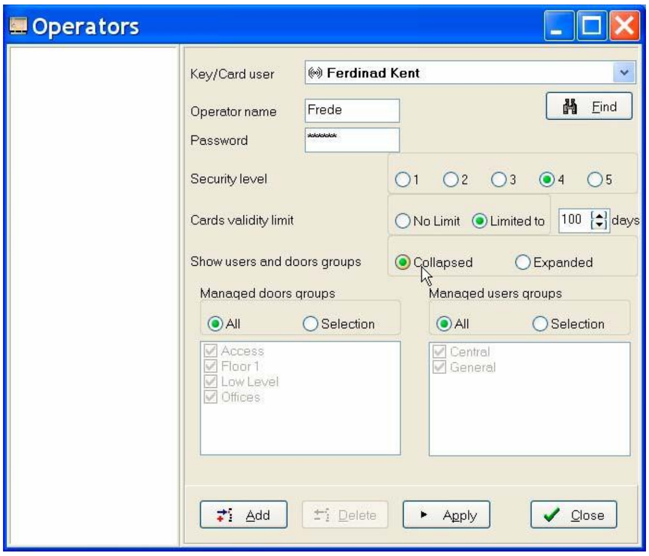
Managed doors groups: ● All ○ Selection
☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Managed users groups: ● All ○ Selection
☑ Central
☑ General

## "Show user and door groups" field

This field allows choosing between the "Collapsed" or "Expanded" view. This refers to the initial view of the matrix with user and door groups.

If the matrix is too large, it is impossible to view all of it on the computer screen; only a part can be seen. In this case, it is preferable to initially use the "Collapsed" view for the groups and then expand them one by one as required.



Key/Card user: Ferdinad Kent
Operator name: Frede
Password: *****
Security level: ○ 1 ○ 2 ○ 3 ● 4 ○ 5
Cards validity limit: ○ No Limit ● Limited to 100 days
Show users and doors groups: ● Collapsed ○ Expanded

Managed doors groups: ● All ○ Selection
☑ Access
☑ Floor 1
☑ Low Level
☑ Offices

Managed users groups: ● All ○ Selection
☑ Central
☑ General

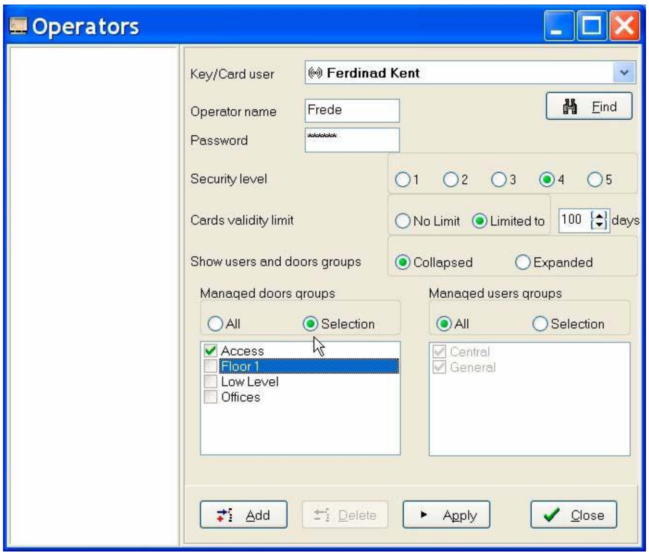
## “Manage door groups” and “Manage user groups” fields

This option allows restricting (for this Operator) the possibility of viewing and managing some groups of doors and/or users.

If you do not want to restrict any group, select the option “All”, either for the door groups, the user groups or both.

If you want to apply a restriction, tick the option “Selection” in the corresponding group (doors, users or both) and tick the groups which the operator is going to manage (“Accesses” in the example).

This option is very useful in some cases, when, for example, a site is divided into several buildings with a management team in each. In this way, it is possible for each Operator to manage only the users from their own building, preventing them from providing credentials to users from others.



Operators

Key/Card user: Ferdinad Kent

Operator name: Frede

Password: ******

Security level: ○ 1 ○ 2 ○ 3 ● 4 ○ 5

Cards validity limit: ○ No Limit ● Limited to 100 days

Show users and doors groups: ● Collapsed ○ Expanded

Managed doors groups: ○ All ● Selection

- ☑ Access
- □ Floor 1
- □ Low Level
- □ Offices

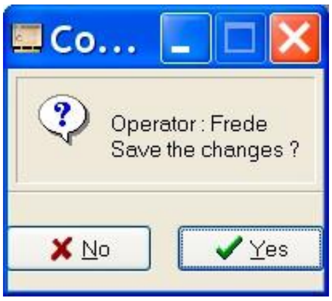
Managed users groups: ● All ○ Selection

- ☑ Central
- ☑ General

## “Add” and “Close” buttons

After filling in all the fields, click “Add”, if you want to keep adding operators, or “Close”, if you do not want to add any other.

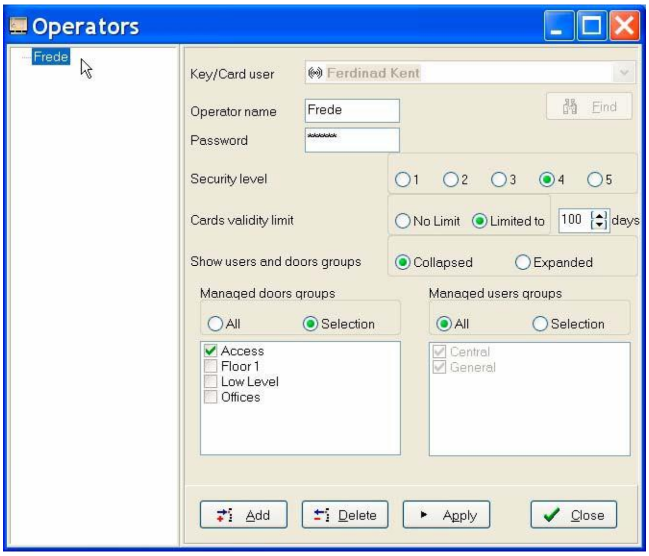
In both cases, a screen is displayed which asks whether you want to save the changes.



Co...

Operator : Frede
Save the changes ?

From that moment, when opening the “Operators” window, the new operator will be displayed in the column on the left:



Operators

Frede

Key/Card user: Ferdinad Kent

Operator name: Frede

Password: ******

Security level: ○ 1 ○ 2 ○ 3 ● 4 ○ 5

Cards validity limit: ○ No Limit ● Limited to 100 days

Show users and doors groups: ● Collapsed ○ Expanded

Managed doors groups: ○ All ● Selection

- ☑ Access
- □ Floor 1
- □ Low Level
- □ Offices

Managed users groups: ● All ○ Selection

- ☑ Central
- ☑ General

# H – Grants

# H – GRANTS

## H.1 INTRODUCTION

One of the functions of the "TESA Access Control" system is managing electronic cylinders, electronic locks and/or wall readers "off-line".

In an "off-line" system, once it is in operation, each time a modification is made to the locking plan, the data must be transmitted to the affected doors using the Portable Programmer.

The "TESA Access Control" system allows defining certain special parameters by means of which it is possible to grant or deny the access of a user to a door (or group of doors) precisely at the moment when the credential of that user is encoded. This avoids the need to go to the door.

These special parameters are called "Grants".

## H.2 OPERATION WITHOUT GRANTS

Once the system is in operation, when working without grants, the operation sequence of the cylinders, locks and/or readers is the following:

- The cylinders, locks and/or readers have the locking plan stored in the memory of their control unit.

- When a user uses their credential in a door, the reader module reads the information stored in the credential and transmits it to the control unit.

- For the user to be able to open the door, the control unit must check that the credential meets the following requirements:

  **System code**
  The system code encoded in the credential must match that of the site.

  **Activation and expiry dates**
  If the credential has an activation date encoded in it, this must be prior to the date and time when the door opening is attempted.

  If the credential has an expiry date encoded in it, this must be subsequent to the date and time when the door opening is attempted.

  **Matrix**
  The user must hold authorised access in the system matrix (locking plan). Either Always or based on one of the Time Zones set.

  If the credential meets all these requirements, the user will be able to open the door. Otherwise, the opening will be denied.

In this operation mode, each time you want to authorise or deny the access of a user to a door, the following steps are necessary:

**1** To modify the locking plan: User/Door locking plan cross on the matrix.

**2** To transmit the data to the Portable Programmer (this step is not necessary for wireless doors). For an Update on Card system, it is also possible to encode the credential of the affected user (in the encoder or updater) for the pending modification to be loaded.

**3** To bring the Portable Programmer to the door and update it. That is to say, to update the locking plan stored in the control unit of the door (this step is not necessary for wireless doors). If the system is Update on Card and the credential has been encoded in the previous step, the user will themselves update the information when passing the card through the lock.

**4** To collect the data from the Portable Programmer by means of the corresponding button on the "PP" menu in the TS1000, for the database to be updated with the information about the doors already updated and for the system to close the process. If the system is Update on Card and the modification has been made by means of the credential of the user, the card will have to be read again, either using the encoder or in an updater, in order to capture the confirmation of the update and for the database to close the update process.

This process may end up becoming burdensome when it must be carried out relatively often (frequent changes of permissions). Grants allow this situation to be avoided.

## H.3 OPERATION WITH GRANTS

A Grant is an additional parameter which can be entered into the system voluntarily.

This parameter will be an additional condition that a door or group of doors will demand of users. That is to say, a user intending to open a door which requires a Grant will have to be in possession of that Grant.

The Grants held are stored in each user's credential and therefore can be determined at the moment of encoding it.

The operation sequence is as follows:

- The cylinders, locks and/or readers have the locking plan stored in the memory of their control unit.

- When a user uses their credential in a door, the reader module reads the information stored in the credential and transmits it to the control unit.

- For the user to be able to open the door, the control unit must check that the credential meets the following requirements:
  - System code
  - Activation and expiry dates
  - Matrix
  - Grant: the credential of the user must be in possession of the grant required by that door

In this way, if you want to withdraw the access of a user to a door, you only need to encode the credential again, having cancelled the corresponding grant beforehand. It is neither necessary to modify the locking plan nor to go to the door with the Portable Programmer.

If the system is Update on Card, the card can be encoded in the encoder or simply in an updater connected to the database.

## H.4 USING GRANTS

Using grants requires taking the following steps:

1 “Defining the Grants”

2 “Assigning grants to the doors”

3 “Updating the matrix”

4 “Updating the doors”

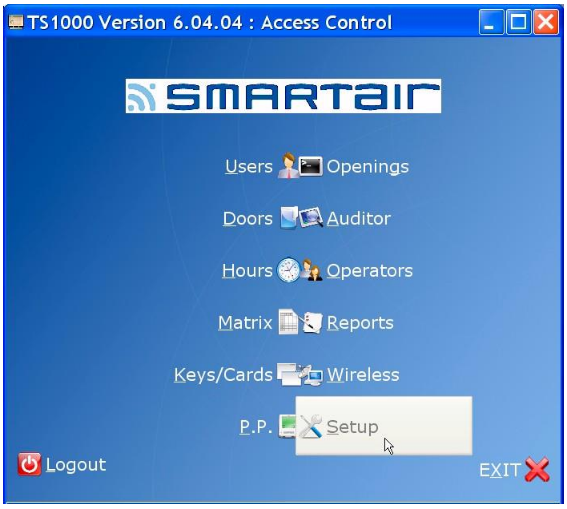
5 “Assigning the grants to the users”

These steps are described in the following sections.

### Defining the Grants

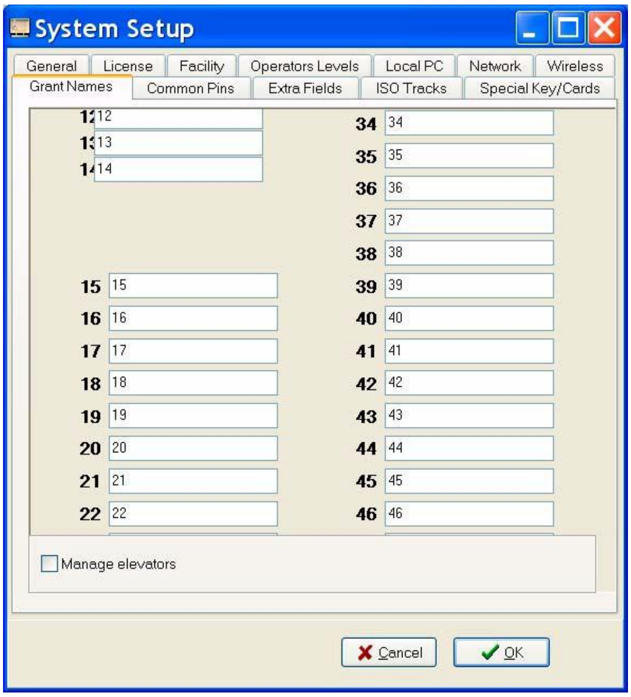
In order to use the grants, in the first place, it is necessary to define the grants desired.

For this purpose, first of all, access the “Setup” menu, on the TS1000 main screen.



In the “Setup” menu, select the “Grant Names” tab.

It is possible to define up to 48 different grants.

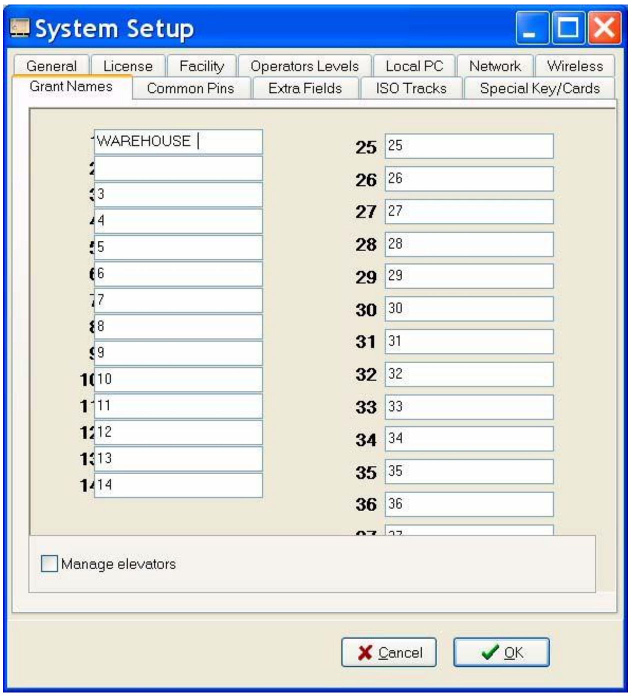


12
13
14
15 15
16 16
17 17
18 18
19 19
20 20
21 21
22 22

34 34
35 35
36 36
37 37
38 38
39 39
40 40
41 41
42 42
43 43
44 44
45 45
46 46

□ Manage elevators

EXAMPLE: in order to create a grant for the “Warehouse” door of a site, write the word WAREHOUSE in the field 1.



WAREHOUSE

3
4
5
6
7
8
9
10
11
12
13
14

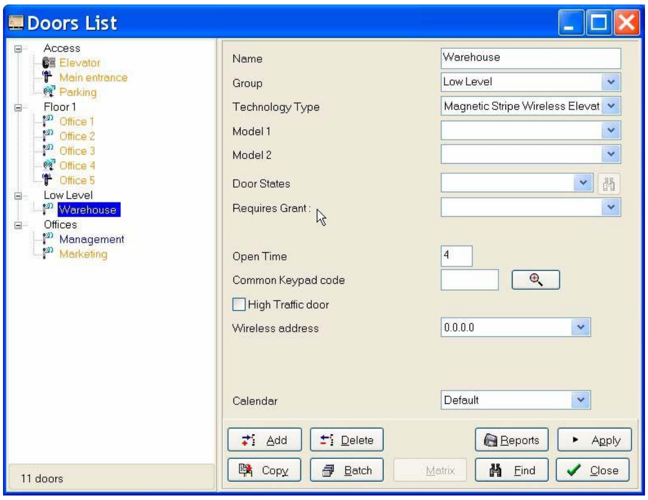
25 25
26 26
27 27
28 28
29 29
30 30
31 31
32 32
33 33
34 34
35 35
36 36

□ Manage elevators

## Assigning grants to the doors

Once a grant has been created, a new field called “Requires Grant” is displayed in the “Doors” menu.

If this field is blank, it means that that door does not require any grant and, therefore, its operation mode will be like the one explained in section *“H.2 Operation without Grants”* on page 103.

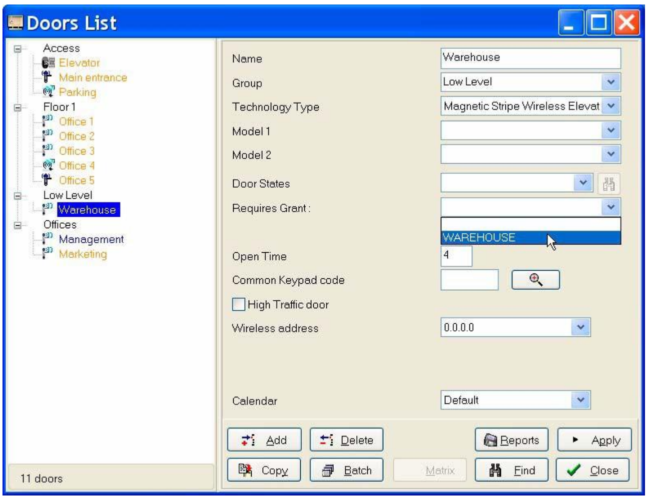


Name: Warehouse
Group: Low Level
Technology Type: Magnetic Stripe Wireless Elevat
Model 1:
Model 2:
Door States:
Requires Grant :
Open Time: 4
Common Keypad code:
□ High Traffic door
Wireless address: 0.0.0.0
Calendar: Default

If you want to assign a grant to a door, in the first place, the door is selected (for example, the “Warehouse” door).

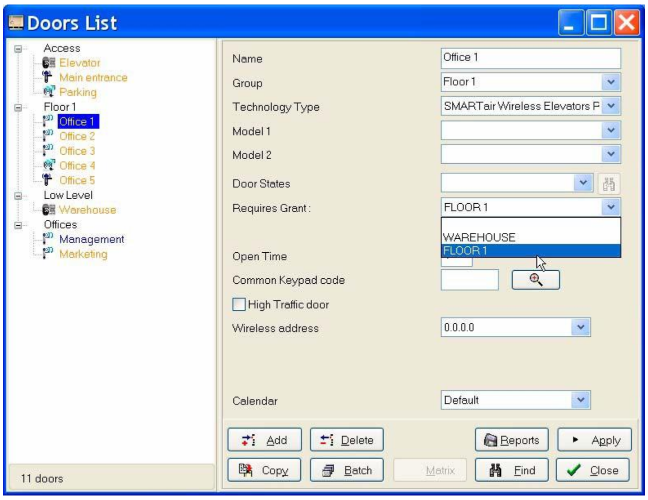
Afterwards, in the drop-down menu of the field “Requires Grant”, the required grant is selected (“WAREHOUSE” in the example).

Finally, the “Apply” button is clicked.



Name: Warehouse
Group: Low Level
Technology Type: Magnetic Stripe Wireless Elevat
Model 1:
Model 2:
Door States:
Requires Grant :
Open Time: 4
Common Keypad code:
□ High Traffic door
Wireless address: 0.0.0.0
Calendar: Default

If desired, the same grant can be assigned to several different doors. For example, if there are 5 different offices on a floor (Floor 1), it is possible to define a grant called “Floor 1” and assign it to the 5 doors of the “Floor 1” group.



Name: Office 1
Group: Floor 1
Technology Type: SMARTair Wireless Elevators P
Model 1:
Model 2:
Door States:
Requires Grant : FLOOR 1
Open Time:
Common Keypad code:
□ High Traffic door
Wireless address: 0.0.0.0
Calendar: Default

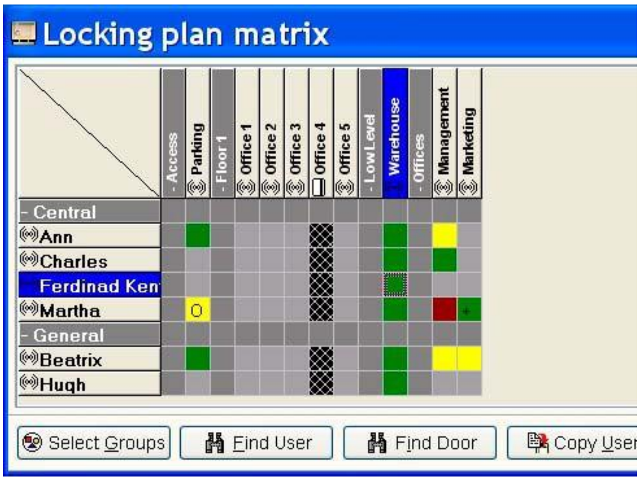
## Updating the matrix

For the use of grants to be really effective, it is advisable to authorise access by all the users of the system to all the doors which require a grant.

The granted access can be according to the time zone “Always” (green colour) or according to any of the Time Zones set in the system.

In this way, authorising or denying the access of a user to a door which requires a grant will only depend on whether the user holds that grant.

In the example, all the users have been provided with granted access to the “Warehouse” door.



Locking plan matrix

| | - Access | Parking | - Floor 1 | Office 1 | Office 2 | Office 3 | Office 4 | Office 5 | - Low Level | Warehouse | - Offices | Management | Marketing |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - Central | | | | | | | | | | | | | |
| Ann | | 🟩 | | | | | ▨ | | | 🟩 | | 🟨 | |
| Charles | | | | | | | ▨ | | | 🟩 | | 🟩 | |
| Ferdinad Ken | | | | | | | ▨ | | | 🟩 | | | |
| Martha | | O | | | | | ▨ | | | 🟩 | | 🟥 | + |
| - General | | | | | | | | | | | | | |
| Beatrix | | 🟩 | | | | | ▨ | | | 🟩 | | 🟨 | 🟨 |
| Hugh | | | | | | | ▨ | | | 🟩 | | | |

## Updating the doors

After the previous steps have been followed, it is necessary to update the affected doors for the grants to start operating. In the event of an initial start-up, rather than updating the doors, it is necessary to initialise them.

This is done in the following steps:

**1** Transmitting the data to the portable programmer

**2** Updating and/or initialising the affected doors

According to the example, the door to be updated would be “Warehouse”.

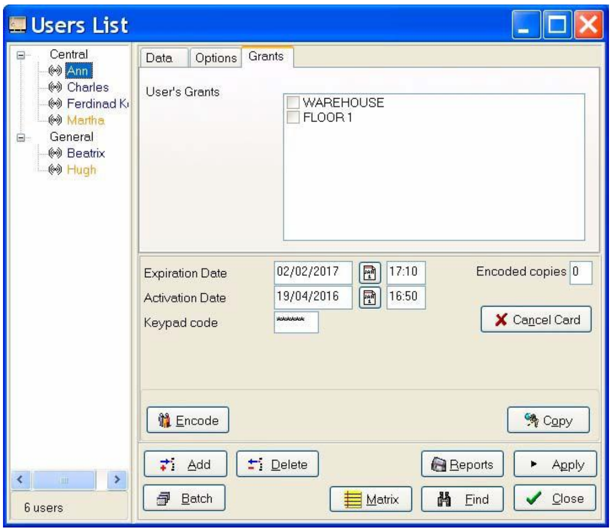
## Assigning the grants to the users

On a similar basis to the Doors menu, when Grants are defined in the system, a new tab called “Grants” is automatically displayed in the Users menu.

In that tab, the list of Grants available in the system is displayed. Each grant has a check box for selection which, if empty, means that the user does not hold that grant.

If you want to assign a grant to a user, you only need to select the user and assign them that grant.

The assignment of grants can be modified as many times as desired; you only need to encode the credential of the user again each time the assignment is modified.


Users List

Central
- Ann
- Charles
- Ferdinad Ki
- Martha

General
- Beatrix
- Hugh

6 users

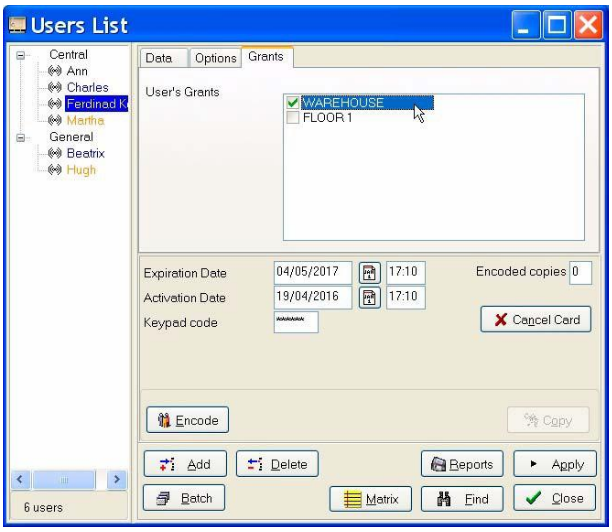
User's Grants
□ WAREHOUSE
□ FLOOR 1

Expiration Date 02/02/2017 17:10
Activation Date 19/04/2016 16:50
Keypad code ******
Encoded copies 0

In the example, the grant WAREHOUSE has been assigned to the user Fernando.

Once the credential of Fernando has been encoded, he will be able to access the Warehouse without carrying out any other process.

In order to prevent Fernando from accessing the warehouse, you only need to remove the selection from the grant WAREHOUSE and encode his credential again.


Users List

Central
- Ann
- Charles
- Ferdinad Ki
- Martha

General
- Beatrix
- Hugh

6 users

User's Grants
☑ WAREHOUSE
□ FLOOR 1

Expiration Date 04/05/2017 17:10
Activation Date 19/04/2016 17:10
Keypad code ******
Encoded copies 0

If the system is Update on Card, the encoding can be carried out manually in an encoder or when the user goes through an updater.

## H.5 EXAMPLES OF APPLICATION OF THE GRANTS

### Management of the entire site using grants

In a site with up to 48 doors (which is the maximum number of grants which can be defined in the "Grant Names" tab of the "Setup" menu), a grant can be defined for each door.

It is therefore possible to design a matrix where all users have access to all the doors, either Always or based on a Time Zone.

In this way, whether a user has access or not to any door of the site only depends on the assignment of grants and not on the matrix.

In a site with these characteristics, it is only necessary to go to the doors with the Portable Programmer during the initial start-up, when you want to collect the record of openings and/or when you need to add users to the system.

The changes to the accesses of each user will be made by modifying their grants and encoding their credentials again, without the need to go to the doors. If the system is Update on Card and there is an updater, the changes will be automatically applied by the users when passing the credential through the updater.

### Guest management

In general, the issues related to guest management in a site are the following:

- There is no information on "Who" the guest will be
- There is no information on "How many" guests there will be
- There is no information on "Who" the guest is visiting and, therefore, "Where" they need access to
- There is no information on "How much time" they are going to be in the site

Grants can help in the management of this situation. For this purpose, it is possible to define a group of users called "Guests".

We will refer to them as "Guest 1, Guest 2, Guest 3, ..., Guest Z", Z being the maximum number of guests expected per day.

The users of this group will be provided with access according to the time zone to such doors or groups of doors which are deemed appropriate.

These doors or groups of doors will require one of the grants defined.

In this way, when a potential guest arrives, the following is done:

- selecting the user number "Guest X" which is available,
- assigning the necessary grants based on the visit to be paid,
- assigning the expiry date and time, and
- encoding the credential (if the system is Update on Card and there is an updater, the changes can be automatically applied by the users when passing the credential through the updater).

After that expiry date and time, the "Guest X" credential will be available once again for another guest.

The names of the individuals are not managed with this system (changing the name of a credential would affect all the events, both past and future, of that credential).

However, this can be managed in another programme, recording the name of the individual next to the number of the credential assigned, and the entry and exit dates.

# I – Programming Credentials and Doors

# I – PROGRAMMING CREDENTIALS AND DOORS

## I.1 INTRODUCTION

After entering the necessary parameters for the operation of the site into the software, in order to run the system, it is necessary to transfer the information to the credentials (keys or cards) and doors (cylinders, locks or wall readers). In addition, for the case of electronic keys, it is necessary to authorise them after encoding.

In order that the computer can communicate with the credentials and doors, different devices are needed, based on the type of technology used:

- Encoding of credentials:
  - Electronic keys (contact chip): ST Portable Programmer
  - Proximity (cards, key-rings, wristbands, watches…): Proximity Encoder
  - Magnetic Stripe Cards: Magnetic Stripe Encoder

- Encoding of doors:
  - Electronic cylinders: ST Portable Programmer
  - Proximity Locks and Wall Readers: ST Portable Programmer
  - Magnetic Stripe Locks and Wall Readers: IT Portable Programmer

A summary table is shown below:

| | Electronic Key and Cylinder | Proximity | Magnetic Stripe |
|---|---|---|---|
| **1** Encoding credentials | ST Portable Programmer | Proximity Encoder | Magnetic Stripe Encoder |
| **2** Encoding doors | ST Portable Programmer | ST Portable Programmer | IT Portable Programmer |
| **3** Authorising | Key | Not necessary | Not necessary |

**NOTE:** the authorisation of the key can be omitted from the process if its encoding is carried out by an operator of an operator level where the option "Does not need Authorising Key to activate staff keys" has been enabled (see *"Does NOT need Authorisation Key to activate staff keys" option* on page 190).

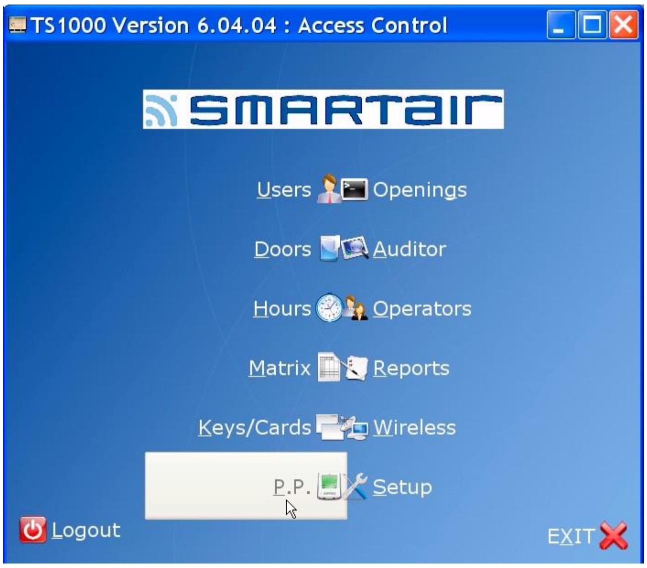
## I.2 TRANSMITTING DATA TO THE PORTABLE PROGRAMMER

After encoding the credentials, the next step in order to run the system is transmitting the data to the Portable Programmer (PP) so as to initialise the cylinders, locks and/or readers with that data.

To send the data to the Portable Programmer, it is necessary to for the Programmer to be connected to and installed on the computer. It will be necessary to have a USB or RS-232 serial port, depending on the Programmer model.

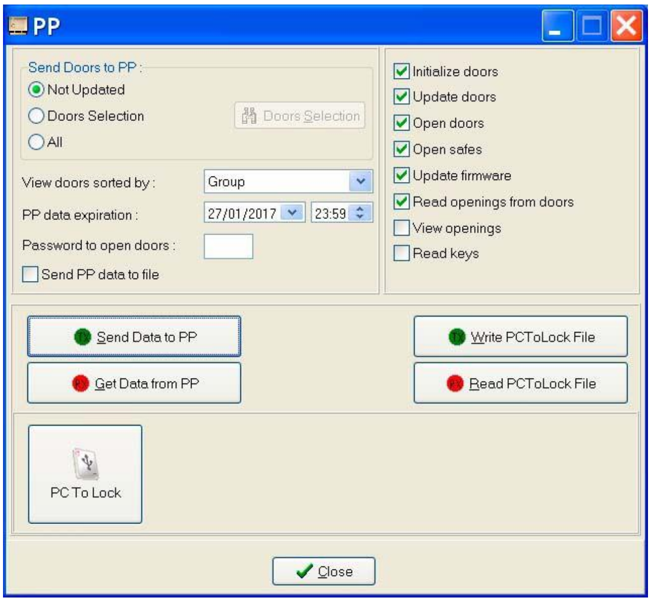
□ Refer to the Instruction Manual of the Programmer used to see how it is connected, installed and managed.

After installing and connecting the Programmer to the PC, click the “PP” button on the TS1000 main screen.



The following screen is displayed:

Before sending the data to the Portable Programmer, it is necessary to select some options in the corresponding fields:



Send Doors to PP :
● Not Updated
○ Doors Selection
○ All

View doors sorted by : Group

PP data expiration : 27/01/2017 23:59

Password to open doors :

□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

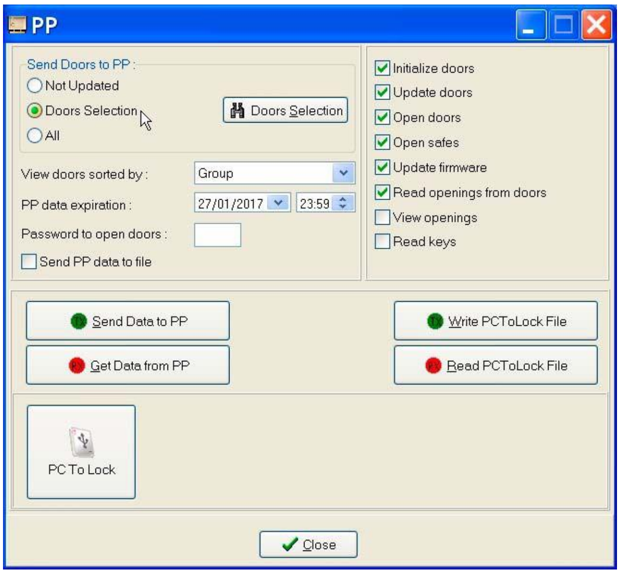
## “Send Doors to PP” field

This field has three settings: “Not Updated”, “Door Selection”, “All”.

- The option “**Not Updated**” is the one selected by default. By selecting this option, the information on those doors whose locking plan or information has undergone some change but which are still not updated will be sent to the Portable Programmer. If this option is used the first time the data are sent to the Portable Programmer, the data related to all the doors will be sent to it, since none of them has received any information from the system.

  This option is very useful in large sites, when it is not clear which doors have been changed, and sending all the doors to the Programmer would occupy too much memory unnecessarily. It is a convenient option, but it entails that the Programmer will only have the doors which have been modified loaded in it and, if you subsequently want to act on another door, it will be necessary to load the data into the Programmer again.

- The option “**Doors Selection**” allows selecting the doors which are needed: this option is selected and then the “Select” button is clicked.



Send Doors to PP:
○ Not Updated
● Doors Selection
○ All

View doors sorted by: Group

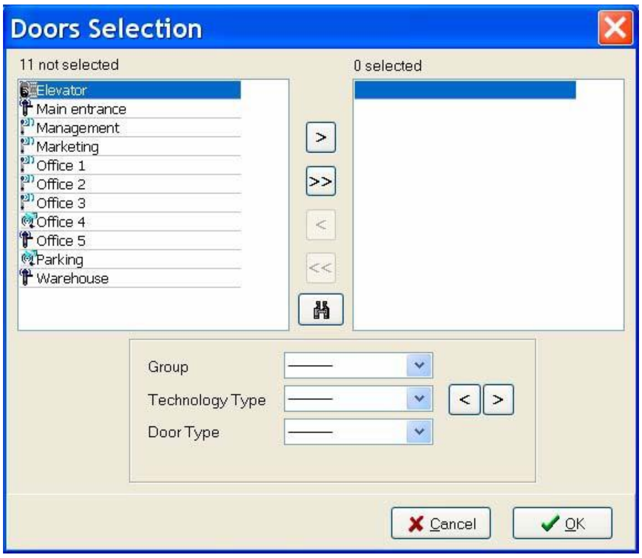
PP data expiration: 27/01/2017 23:59

Password to open doors:

☐ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
☐ View openings
☐ Read keys

When clicking the “Select” button, the following screen is displayed:



11 not selected

Elevator
Main entrance
Management
Marketing
Office 1
Office 2
Office 3
Office 4
Office 5
Parking
Warehouse

0 selected

Group ——
Technology Type ——
Door Type ——

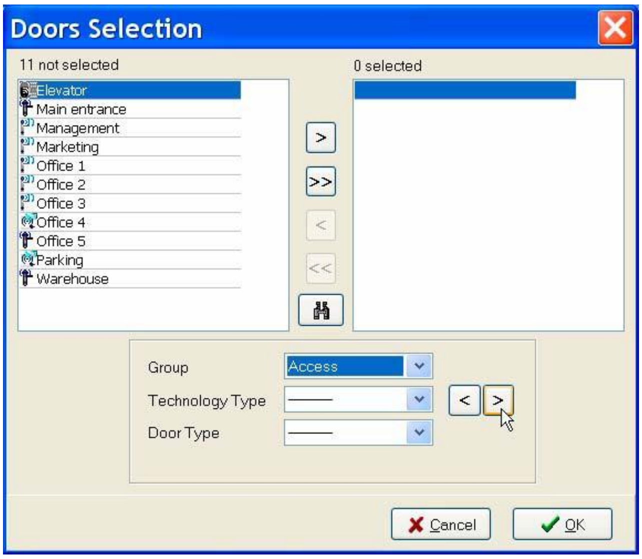
In the column on the left, the doors which are Not selected are displayed and, on the right, there appear the ones which are Selected. In order to move doors from one column to the other, the following buttons are available:

– The “>” button (select door) moves the door which is ticked in the left-hand list to the list on the right.

– The “>>” button (select all) moves all the doors to the list on the right.

– The “<” button (reject door) moves the door which is ticked in the right-hand list to the list on the left.

– The “<<” button (reject all) moves all the doors to the list on the left.



11 not selected

Elevator
Main entrance
Management
Marketing
Office 1
Office 2
Office 3
Office 4
Office 5
Parking
Warehouse

0 selected

Group: Access

Technology Type: ———

Door Type: ———

This screen also allows selecting by “Door Group”, by “Technology Type” or by “Door Type”.

For this purpose, it is necessary, in the first place, to empty the list of selected doors, by clicking on “<<”. Afterwards, it is necessary to click the drop-down list you are interested in (Group, Technology or Type) and select the name identifying the set of doors desired. Finally, you have to click on “>” to send the set selected to the list on the right.

In the example, the group “Accesses” is being selected.

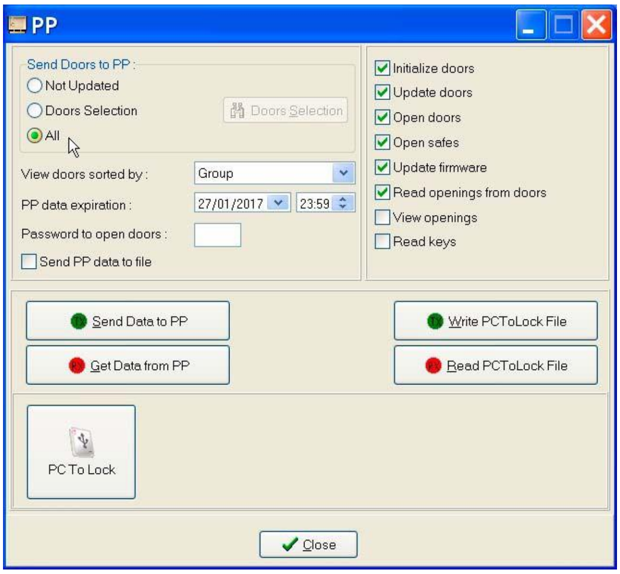
- The selection by “Door Group” allows loading the Portable Programmer with the information on one of the Groups previously created in the “Doors” menu. Depending on the groups created, this is useful, for example, for selecting all the doors on one floor of a building, in a specific department of a company, one unit from a group of buildings, etc.
- The selection by “Technology Type” allows automatically separating out the doors with a given technology, in the event of having several.
- The selection by “Door Type” allows selecting, without having to conduct a search, the doors of type “Access Control”, “Common Access”, “High Traffic Door” and “Safe”.

The selection of doors to be sent to the Portable Programmer may involve several individual selections made successively, that is to say, it is possible to select first the “Accesses” Group and, then, the “Offices” Group.

After selecting the desired doors, you have to click “OK” and you return to the “Portable Programmer” screen.

This option is very useful when the locking plan is very big and, for some reason (security, assignment of zones, simplicity), you want to have partial information on the site available in the Portable Programmer.

- The option “**All**” loads all the doors into the Portable Programmer.



Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

View doors sorted by : Group

PP data expiration : 27/01/2017 23:59

Password to open doors :

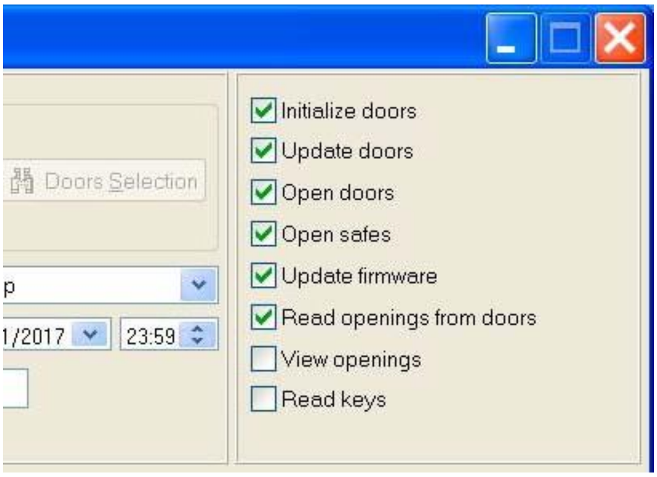
☐ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
☐ View openings
☐ Read keys

## “Available operations” field

After sending the data to the Portable Programmer, it is possible to carry out, using the Programmer, the following operations:

- Initialise doors
- Update doors
- Open doors
- Open safes
- Update firmware
- Read openings from doors
- View openings
- Read keys



Doors Selection

p

1/2017 23:59

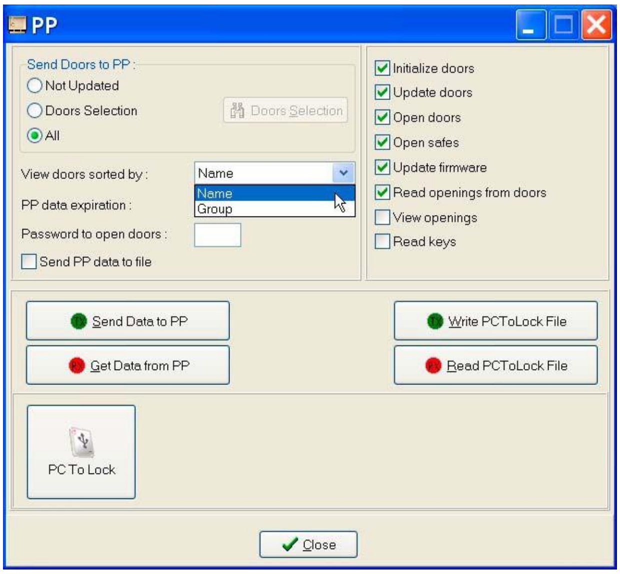
☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

Select only the operations you want to carry out, by ticking the corresponding check box.

## “View doors sorted by” field

After sending the data related to the doors of the site, you can choose how they will be sorted in the Portable Programmer: it is possible to view them sorted by “Group” or “Name”.

- The option “Sort by Group” will arrange the door list in the order in which they are displayed on the “Doors” screen, without taking into account their names, but the group they belong to. For example, the doors of the “Accesses” group first, followed by all the doors of the “Workshops” group.
- The option “Sort by Name” will arrange the doors sorted by alphabetical order, without taking into account the group they belong to.



PP

Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

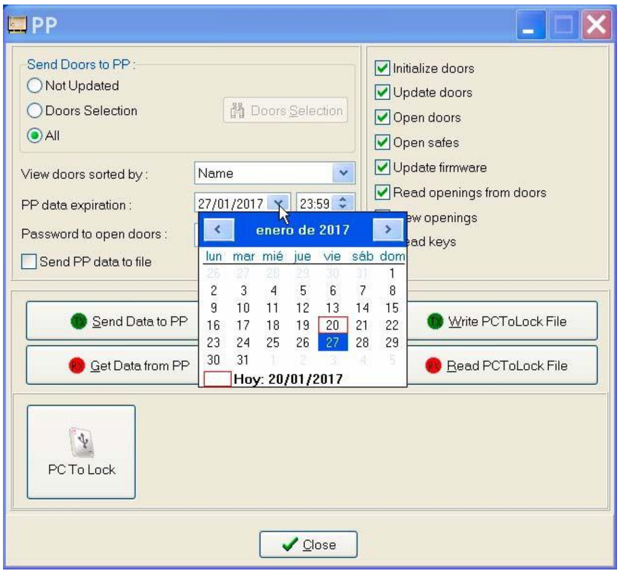
View doors sorted by : Name (Name / Group)
PP data expiration :
Password to open doors :
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

## “PP data expiry” field

The Portable Programmer, loaded with data, allows carrying out actions like Initialise, Update and even Open doors. This could cause security issues in the site if the Programmer happened to be in the possession of non-authorised individuals.

As a result, as a preventive measure, the data in the Programmer expire by default at 23 hours 59 minutes on the same day of the week after the loading of the data. Once the data have expired, the Programmer turns into an inoperative tool.



Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

View doors sorted by : Name

PP data expiration : 27/01/2017 23:59

Password to open doors :

□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
ew openings
ead keys

enero de 2017

| lun | mar | mié | jue | vie | sáb | dom |
|---|---|---|---|---|---|---|
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | 1 | 2 | 3 | 4 | 5 |

Hoy: 20/01/2017

The expiry date and time can be modified as deemed convenient, with a maximum limit of one year, the user assuming the risk posed by the security issue arising in the event of loss.

□WARNING: the date entered in this field is only used at the moment of sending the data to the Programmer, not being recorded in the system. If, after loading the data into the Programmer, the window is closed, when it is opened again, the field will show the default date, although the Programmer will retain the date entered until a different one is sent.

## “Password to open doors” field

From the Portable Programmer, it is possible to carry out emergency openings of the cylinders, as well as of the locks and wall readers. In the Portable Programmer, this function is called “Open doors” and it can be found in the “F2: Doors” menu.

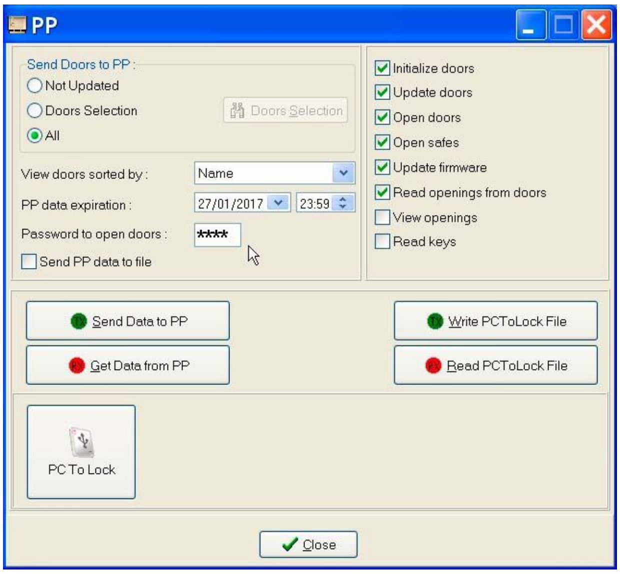
In order to carry out this emergency opening, the Authorising Key of the system must be inserted into the Portable Programmer as a security measure (except when its use has been disabled as explained in *“L.3 Deactivation of the Authorisation Key”* on page 188).

The system allows setting an additional security measure: the “Password to open doors”. In this way, in order to carry out emergency openings with the Portable Programmer, in addition to the Authorising Key, it is necessary to enter a Password.

Thus, it is possible, for example, to give the Portable Programmer to another individual for the purpose of performing maintenance tasks, such as updating doors or collecting openings, knowing that they cannot open the doors without the Password. If necessary, this individual can contact the System Manager, who will provide the Password if so considered appropriate. The door will be opened with no further inconvenience, but the System Manager will be aware of this.

□WARNING: it is important to highlight that the password must be set EACH TIME the data are sent to the Portable Programmer, that is to say, if the Programmer is loaded with a password to open doors, this will be valid until the data expire or the Programmer is loaded again.
If no password is entered when sending the data again, the tasks will be carried out directly, without requesting authorisation.
If a different password is entered, the latter will be the one requested and the former one will be invalidated.

As a matter of security, the password remains hidden, represented by asterisks.



PP

Send Doors to PP :

○ Not Updated

○ Doors Selection

● All

View doors sorted by : Name

PP data expiration : 27/01/2017 23:59

Password to open doors : ****

☐ Send PP data to file

☑ Initialize doors

☑ Update doors

☑ Open doors

☑ Open safes

☑ Update firmware

☑ Read openings from doors

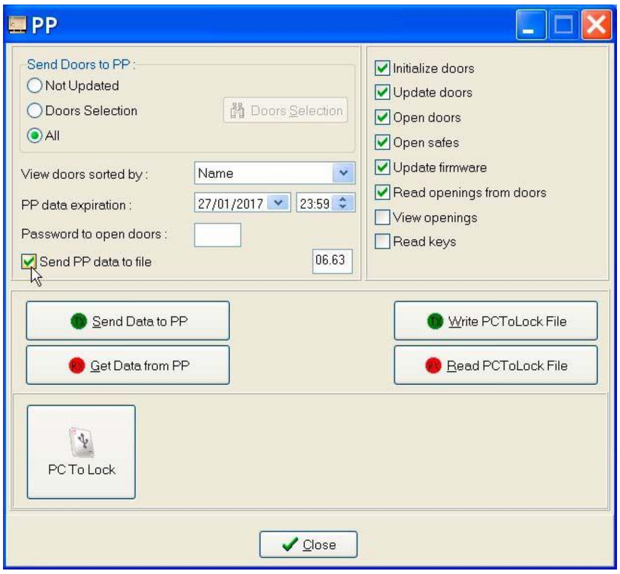
☐ View openings

☐ Read keys

## Send PP data to file

It is possible to create a file with the data to be loaded into the Portable Programmer and save it on the PC.

Nowadays, this option is not used any more.



PP

Send Doors to PP :

○ Not Updated

○ Doors Selection

● All

View doors sorted by : Name

PP data expiration : 27/01/2017 23:59

Password to open doors :

☑ Send PP data to file 06.63

☑ Initialize doors

☑ Update doors

☑ Open doors

☑ Open safes

☑ Update firmware

☑ Read openings from doors

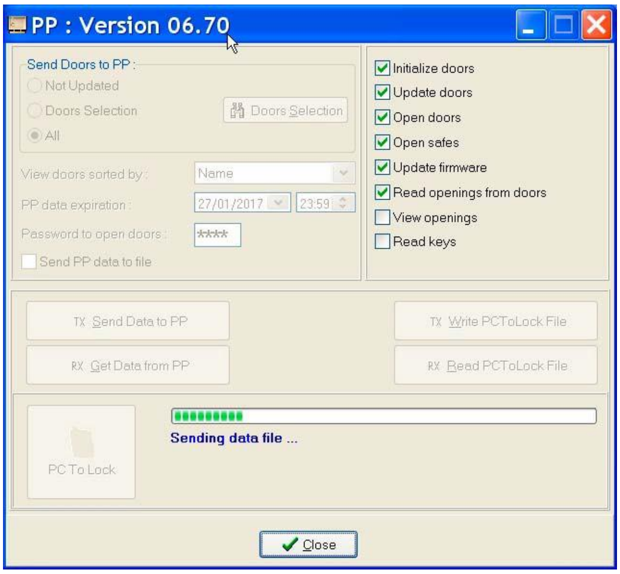
☐ View openings

☐ Read keys

## “Send Data to PP” button

After following the previous steps, it is possible to send the data to the Portable Programmer, by clicking on “Send Data to PP”.

□ Before clicking this button, it is important to make sure that the Portable Programmer is on, since it has a powersaving facility which automatically turns the device off after some minutes of inactivity.


PP : Version 06.70

Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

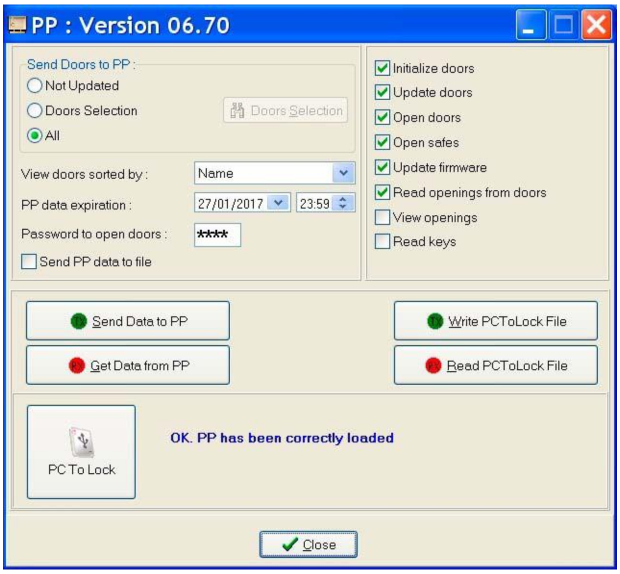
View doors sorted by : Name
PP data expiration : 27/01/2017 23:59
Password to open doors : ****
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

Sending data file ...

Once the loading has been finished successfully, the corresponding confirmation message is displayed.

From this moment, the Portable Programmer contains all the information necessary to carry out the tasks transferred, according to the options selected in the column on the right. One of these is “Initialise doors”, which is described in *“I.3 Initialising the doors of the site”* on page 123.


PP : Version 06.70

Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

View doors sorted by : Name
PP data expiration : 27/01/2017 23:59
Password to open doors : ****
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

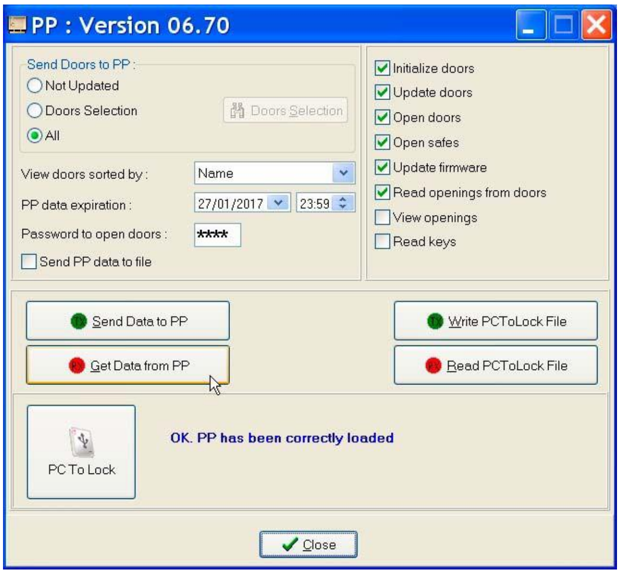
OK. PP has been correctly loaded

## “Get Data from PP” button

With the Portable Programmer, it is possible to carry out various operations on the doors, such as Initialise doors, Update doors, Read events from doors, etc.

In some of these operations, the Programmer collects data from the doors, which can then be analysed by means of the TS1000 software. In order to conduct this analysis, it is necessary to transfer the data collected by the Programmer to the database, which task is carried out by clicking the “Get Data from PP” button in the “PP” menu of the TS1000.

This operation is essential, after having initialised or updated devices, for the system to be notified that the changes have been made to the doors, so that it does not consider these to be pending (orange or blue colour in users and doors).



PP : Version 06.70

Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

View doors sorted by : Name
PP data expiration : 27/01/2017 23:59
Password to open doors : ****
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

OK. PP has been correctly loaded

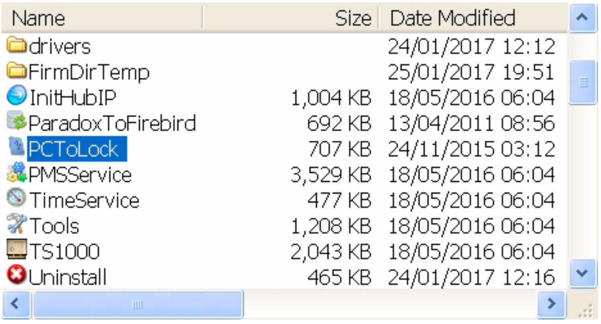
□ Before clicking this button, it is important to make sure that the Portable Programmer is on, since it has a powersaving facility which automatically turns the device off after some minutes of inactivity.

## “PCToLock” button

There is another method, an alternative to the Portable Programmer, to send the data to the doors, initialise and update them, as well as to read their openings. This system is called “PC To Lock”. It consists of the following components:

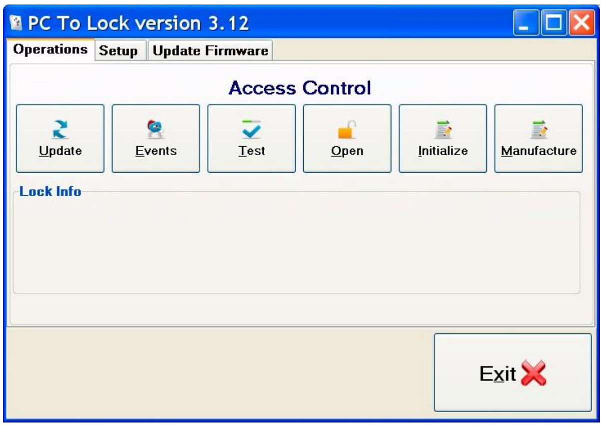
- Electronic device using “USB-KCOM” communication, which connects to a PC through a USB port and to the doors through a cable.
- Portable PC or equivalent device with Windows XP, Vista, Windows 7, Windows 8.1 or Windows 10operating system.
- “PCToLock” software to manage the communication with the doors. This software is automatically installed in the same directory as the TS1000, when installing the latter.

**NOTE:** it is also possible to work with the PCToLock software and the USB-KCOM device without using the TS1000 software. For more information, refer to the instructions for these products.



| Name | Size | Date Modified |
|---|---|---|
| drivers |  | 24/01/2017 12:12 |
| FirmDirTemp |  | 25/01/2017 19:51 |
| InitHubIP | 1,004 KB | 18/05/2016 06:04 |
| ParadoxToFirebird | 692 KB | 13/04/2011 08:56 |
| PCToLock | 707 KB | 24/11/2015 03:12 |
| PMSService | 3,529 KB | 18/05/2016 06:04 |
| TimeService | 477 KB | 18/05/2016 06:04 |
| Tools | 1,208 KB | 18/05/2016 06:04 |
| TS1000 | 2,043 KB | 18/05/2016 06:04 |
| Uninstall | 465 KB | 24/01/2017 12:16 |

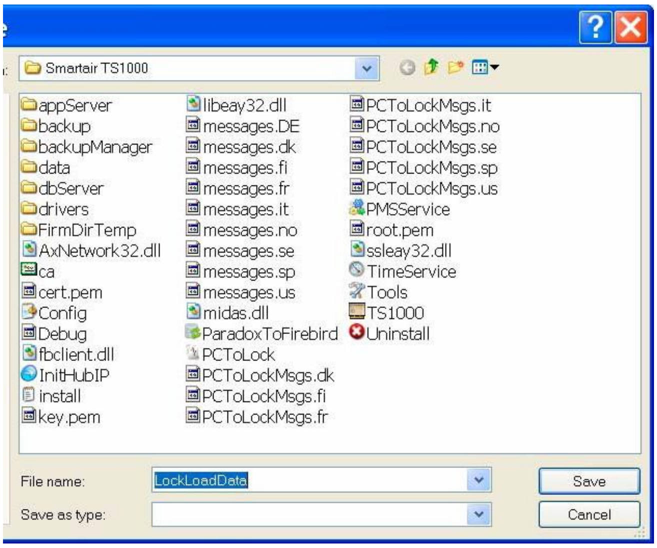
After clicking the “PC To Lock” button on the “PP” screen of the TS1000, the PCToLock software is run, which allows using the “USB-KCOM” device.



PC To Lock version 3.12

□ For more information on the “PCToLock” software and the “USB-KCOM” device, refer to their respective instruction manuals.

## “Write PCToLock File” button


Smartair TS1000

appServer
backup
backupManager
data
dbServer
drivers
FirmDirTemp
AxNetwork32.dll
ca
cert.pem
Config
Debug
fbclient.dll
InitHubIP
install
key.pem
libeay32.dll
messages.DE
messages.dk
messages.fi
messages.fr
messages.it
messages.no
messages.se
messages.sp
messages.us
midas.dll
ParadoxToFirebird
PCToLock
PCToLockMsgs.dk
PCToLockMsgs.fi
PCToLockMsgs.fr
PCToLockMsgs.it
PCToLockMsgs.no
PCToLockMsgs.se
PCToLockMsgs.sp
PCToLockMsgs.us
PMSService
root.pem
ssleay32.dll
TimeService
Tools
TS1000
Uninstall

File name: LockLoadData
Save as type:

If you wish to use the “PCToLock” software in the doors of the site, it is necessary to have a file with its data, called “LockLoadData”.

This file is generated at any TS1000 management console of the site, by clicking the “Write PCToLock File” button of the “PP” menu.

After clicking this button, a message is displayed requesting the location desired for saving the corresponding *.zip file for the site, in order to be able to work with it later on. It is advisable to save it in the same folder as the “PCToLock” software.

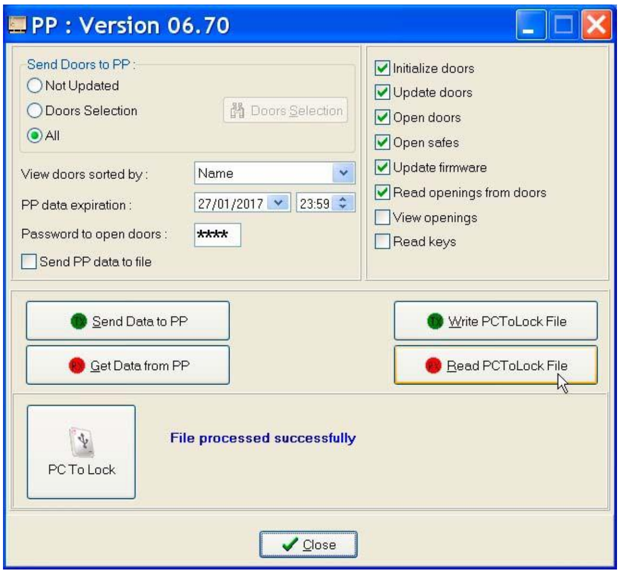
If you want to use the PCToLock software on a Portable PC or *Tablet* where the TS1000 has not been installed, in order to be able to work more conveniently at the doors of the site, it is necessary this device to have a specific folder (for example, C:\PCToLock) to which the PCToLock.exe files and all the “PCToLockMsgs.*" have been previously copied, and, subsequently, transfer the information of the data for the locking devices by copying the file called “LockLoadData.zip”.

## “Read PCToLock File” button

In the “PCToLock” software, it is possible to carry out various operations, such as Initialise doors, Update doors, or collect events recorded in the doors (Auditor) to analyse them with the TS1000, etc.

After carrying out these operations, the data are recorded in the file loaded into the “PCToLock” software, so that, for the database of the site to be updated, it is necessary to process this file using the TS1000 software.

In this way, the system will record the updates, initialisations, firmware changes and events of the doors, so that subsequent management is conducted on the real data of the site.


PP : Version 06.70

Send Doors to PP :
○ Not Updated
○ Doors Selection
● All

View doors sorted by : Name
PP data expiration : 27/01/2017 23:59
Password to open doors : ****
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

File processed successfully

This downloading process is carried out by transferring the data file from the portable PC or tablet to any TS1000 management console and clicking the “Read PCToLock File” button of the “PP” menu.

A window will be opened for you to select the file from the location where it is stored.

Once the file has been processed successfully, the system will have all the data and firmware changes recorded, in addition to the events which have been collected and which can be analysed as usual, using the “Openings” menu of the TS1000 software.

## I.3 INITIALISING THE DOORS OF THE SITE

### Introduction

The initialisation of all the access points is carried out by means of the Portable Programmer or the PCToLock device, after having transmitted the locking plan to it, as has been explained in the previous point.

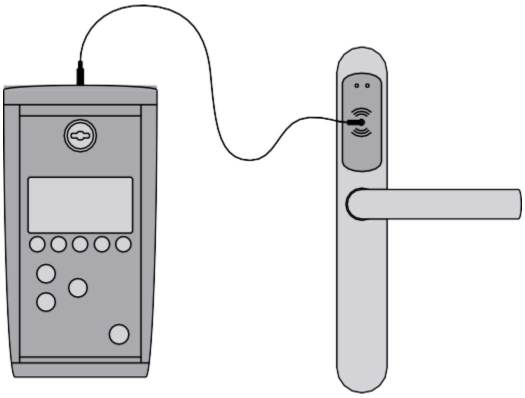
**The initialisation of a door involves assigning a name to it**, as set in the programme, **and transmitting its locking plan to it**, that is to say, how it should respond when presented with each of the credentials of the site.

When it is initialised, the product loses all the information previously stored in it. If still set to factory settings (as delivered from the manufacturer), it will cease to be so.

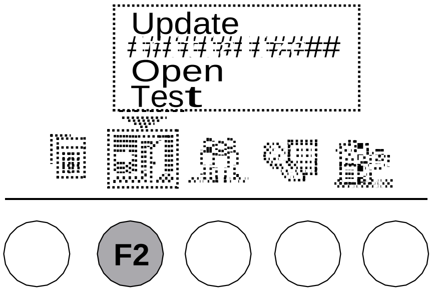
Once a cylinder, lock or wall reader becomes part of a site, it can only be initialised anew with information from another door of the same site. That is to say, once initialised, you can change their location as many times as you wish, but always within the site they were initialised for.

### Initialisation by means of the Portable Programmer

For initialisation using the Portable Programmer, it is necessary to connect it to the Electronic Cylinder, Lock or Wall Reader.

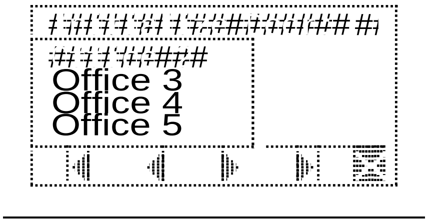


The process is carried out at each door, by means of the Portable Programmer, in the menu “2- Doors” > “Initialise” > “Select Door” > “OK”.



For more information, refer to the instructions for the Portable Programmer.

In addition, it is necessary for the Authorising Key of the system (Blue Key for Electronic and Proximity Cylinders, Green Key for Magnetic Stripe) to be inserted into the Portable Programmer (except when its use has been disabled as explained in *“L.3 Deactivation of the Authorisation Key”* on page 188).

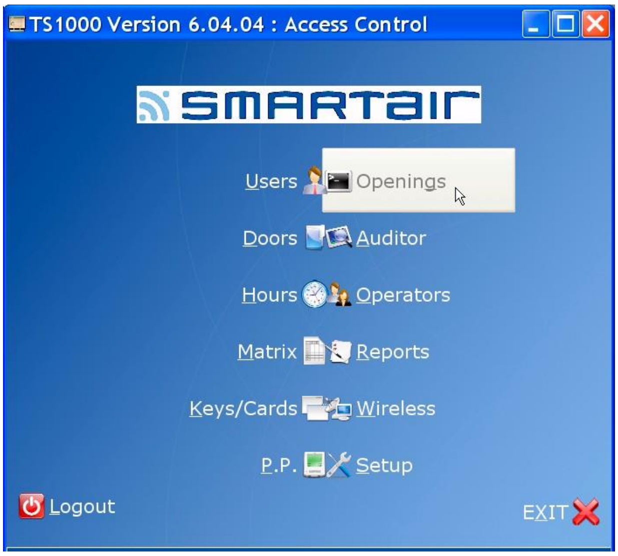


The Authorising Key is a special key which contains the system code, exclusive for the site, and enables its holder to carry out the sensitive functions of the system (particularly, Authorise keys, Programme, Update and Open doors). Therefore, unless otherwise stated (as explained in chapter *"L – Other Functions"*), this key is essential in the execution of this process.

Once the door has been initialised by means of the Portable Programmer, it is necessary to collect the openings.

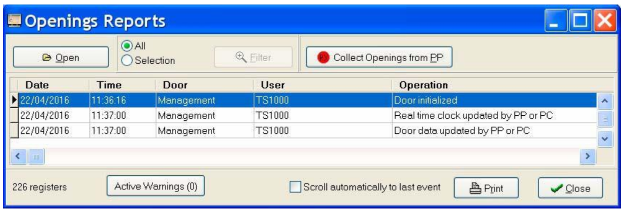
**This last step is very important** for the information of the work done at the doors to be recorded in the database and for the pending actions to be recognised as completed, so that the affected doors and users are highlighted in black, rather than orange or blue, in the corresponding menus.

In order to do this, connect the Portable Programmer to the TS1000 management console and click the "Openings" menu on the main screen of the software.



On the "Openings Reports" screen, click the "Collect Openings from PP" button. It is also possible to update the information by clicking the "Get Data from PP" in the "PP" menu.

After this operation has been carried out, the door initialisation process is finished.



| Date | Time | Door | User | Operation |
|---|---|---|---|---|
| 22/04/2016 | 11:36:16 | Management | TS1000 | Door initialized |
| 22/04/2016 | 11:37:00 | Management | TS1000 | Real time clock updated by PP or PC |
| 22/04/2016 | 11:37:00 | Management | TS1000 | Door data updated by PP or PC |

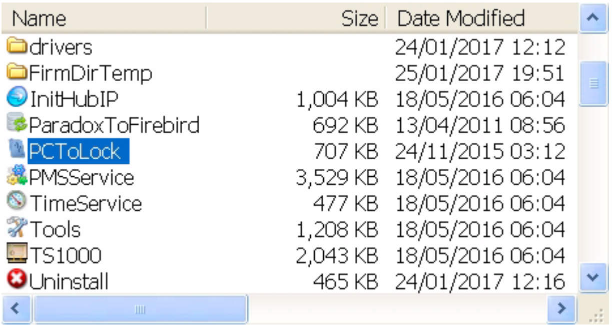
226 registers

☐ Scroll automatically to last event

## Initialisation by means of PCToLock

It is also possible to initialise the door with the “PCToLock” software and the “USB-KCOM” device connected to a portable PC or equivalent device, rather than using the Portable Programmer.

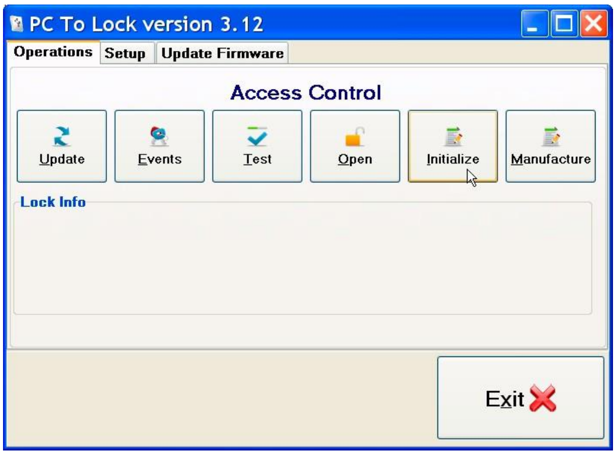
For this purpose, run the “PCToLock” software on the PC where the “USB-KCOM” device is connected.



| Name | Size | Date Modified |
|---|---|---|
| drivers | | 24/01/2017 12:12 |
| FirmDirTemp | | 25/01/2017 19:51 |
| InitHubIP | 1,004 KB | 18/05/2016 06:04 |
| ParadoxToFirebird | 692 KB | 13/04/2011 08:56 |
| PCToLock | 707 KB | 24/11/2015 03:12 |
| PMSService | 3,529 KB | 18/05/2016 06:04 |
| TimeService | 477 KB | 18/05/2016 06:04 |
| Tools | 1,208 KB | 18/05/2016 06:04 |
| TS1000 | 2,043 KB | 18/05/2016 06:04 |
| Uninstall | 465 KB | 24/01/2017 12:16 |

The initialisation of the doors is carried out by means of the “Initialise” button.

For more information, refer to the instructions for the “PCToLock” software and the “USB-KCOM” device.

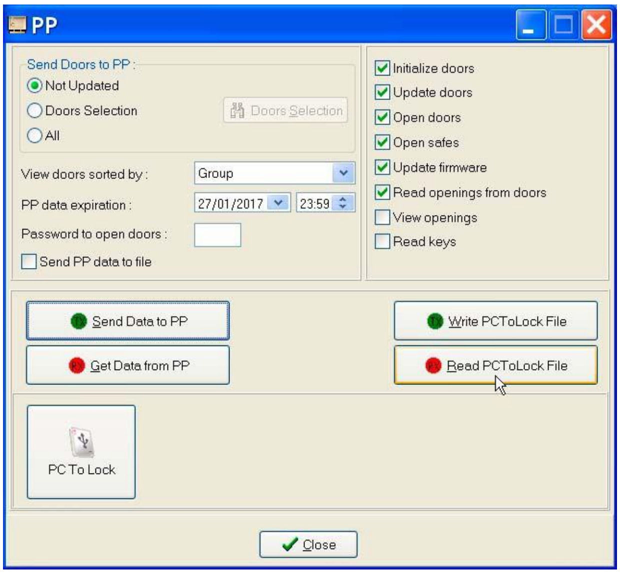


After the initialisation, it is necessary to update the information of the system. For this purpose, click the “Read PCToLock File” button in the “PP” menu of the TS1000.

For more information, refer to *““Read PCToLock File” button”* on page 122.

This step is only necessary if the PCToLock has been used on another PC by means of the option “Write PCToLock File”.

If the “PCToLock” button is clicked, it is carried out automatically.



PP

Send Doors to PP :
● Not Updated
○ Doors Selection
○ All

View doors sorted by : Group
PP data expiration : 27/01/2017 23:59
Password to open doors :
□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

## I.4 ENCODING OF CREDENTIALS

**NOTE:** particularly in Update on Card systems, the encoding of credentials must be carried out once the doors have been initialised and the database updated with the information of that initialisation, in order to minimise the loading of locking plan crosses still not encoded on the credentials.

The encoding of Credentials is always carried out from the "Users" menu of the TS1000 software. The information encoded on each credential is, basically, what can be seen in the Users tab, encrypted.

In order to encode the credentials, it is necessary to have the Credential Management Device connected to and installed on the computer. It will be necessary to have a USB or RS-232 serial port, depending on the device.

□ Refer to the Instruction Manual of the Device used to see how it is connected, installed and managed.

As a guide, the procedure for the different types of technology is shown below:

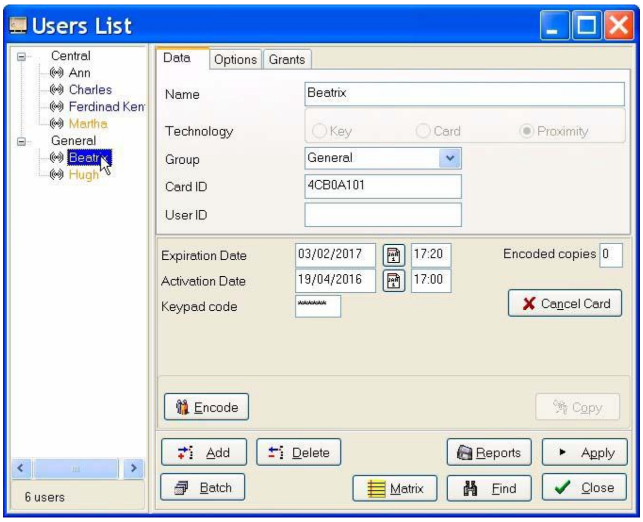
- **Electronic Keys:** connect the Portable Programmer to the PC and click the ON/OFF button to turn it on (after a 2 minute period of inactivity, the Programmer turns off automatically to save battery).

- **Proximity:** connect the Encoder to the PC by means of the USB cable and it will start running, since it is powered by the USB port of the PC (in some models, which are connected to the PC by means of an RS-232 serial cable, it is necessary to use an external adaptor for the Encoder). A red LED will come on on the Encoder, indicating that it is receiving power.

- **Magnetic Stripe:** connect the Encoder to the PC and start it up by plugging in the adaptor supplied with it and turning on the black switch located at the back of the Encoder, on the right. A green LED will come on at the front.

On the "Users" screen of the TS1000, select the user name (highlighted in blue) whose credential you want to encode.

Once the user has been selected, click the "Encode" button.



Users List

Central
- Ann
- Charles
- Ferdinad Ken
- Martha

General
- Beatrix
- Hugh

6 users

Name: Beatrix

Technology: ○ Key ○ Card ● Proximity

Group: General

Card ID: 4CB0A101

User ID:

Expiration Date: 03/02/2017 17:20

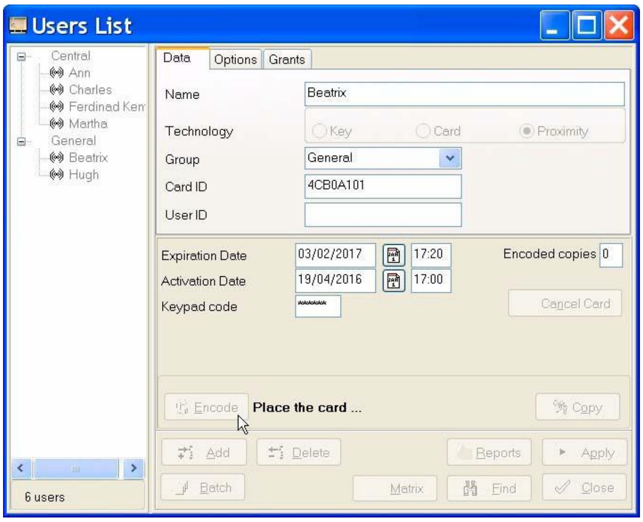
Activation Date: 19/04/2016 17:00

Keypad code: ******

Encoded copies: 0

The software prompts you to present the credential to be encoded:

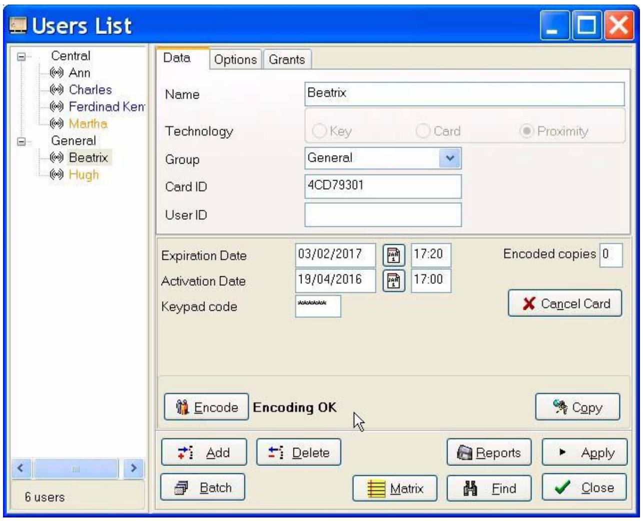
- Electronic Keys: Insert the key...
- Proximity: Place the card...
- Magnetic Stripe: Insert the card...



Name: Beatrix
Technology: ○ Key ○ Card ● Proximity
Group: General
Card ID: 4CB0A101
User ID:
Expiration Date: 03/02/2017 17:20
Activation Date: 19/04/2016 17:00
Keypad code: ******
Encoded copies: 0
Cancel Card
Place the card ...

Finally, if the encoding is successful, the corresponding confirmation message is displayed, indicating that the encoding process of the Credential has been successfully finished.

After encoding the credential, the user name will be displayed in black, indicating that this credential has been encoded.



Name: Beatrix
Technology: ○ Key ○ Card ● Proximity
Group: General
Card ID: 4CD79301
User ID:
Expiration Date: 03/02/2017 17:20
Activation Date: 19/04/2016 17:00
Keypad code: ******
Encoded copies: 0
Cancel Card
Encoding OK

Repeat the same process for every User whose credential you want to encode.

It is not necessary to encode all the credentials at the same time if you are not going to use them. You can return to the “Users” menu later on to encode more credentials when necessary.

When changes are made to the data stored in the software, it is necessary to check the colour of the user name in the Users List. If the name appears in black, this means that it is not necessary to encode the credential of that user again. If the name is displayed in red or blue, this means that it is necessary to encode the credential again for the changes to be applied. For example, in the event of modifying the activation and expiry dates of a user, it will be necessary to encode their credential again.

## I.5 AUTHORISATION AND DENIAL OF ELECTRONIC KEYS

Unlike card-type Credentials (Proximity and Magnetic Stripe), the Electronic Keys of the STX contact electronic keys and cylinders system of TESA have an additional security feature called Authorisation.

Thanks to this feature, an STX Electronic Key, encoded as indicated in *"I.4 Encoding of credentials"* on page 126, will contain in its memory the data related to the user assigned and the clock/calendar correctly set, but it will not yet hold the necessary permission to access the site. An attempt to access with the key in this state will record the event "Key not authorised".

This feature allows the Site Manager to delegate the encoding of the user Keys to another individual, but maintaining control over the keys created, since for a Key which is not authorised to become valid in the site, it will be necessary for the Manager, who is responsible and the holder of the Authorising Key, to carry out a simple, but essential, Authorisation process.

### Authorisation process

This involves approaching any cylinder in the site (it can be a spare cylinder, properly initialised, and kept next to the Authorising Key) and carrying out the following steps:

1. Insert the Authorising Key into the cylinder and verify that the LED of the Key blinks several times, turning from red to green. Once the blinking has stopped, remove the Authorising Key.
2. Insert the Key which is not authorised into the cylinder and verify that the LED of this Key likewise blinks several times. Wait until the blinking stops and remove the Key from the cylinder.

From this moment, the Key will be authorised and it will be possible to use it as established in the Matrix of the programme.

### Denial

Another exclusive feature of the Electronic Cylinder/Key Technology, derived from the possibility of Authorisation of the Key, is the possibility of "Denial" in the event of fraudulent or inappropriate use.

If a user receives six or more consecutive messages related to Access Rejection on their key, either in the same door or in several doors within a site, with no Permitted Access in between, the Key will become Not authorised again, it becoming necessary for the Site Manager to repeat the Authorisation process. As a result, the individual responsible will be informed of the key use irregularity and will be able to take the measures deemed convenient in each case.

Just as the case of the Programming of the Doors, the "Authorisation" process of the Keys is an essential step for the system to operate correctly, unless expressly stated otherwise (see chapter *"L – Other Functions"*). In such a case, the "Denial" function will also be inoperative.

# J – Wireless System

# J – WIRELESS SYSTEM

## J.1 WIRELESS SYSTEM ARCHITECTURE

In a wireless system, the PC can communicate with the wireless devices (locks, wall readers, etc.) by means of radio frequency, both to update them and to collect their events. For this purpose, the following additional elements are required:

- Wireless devices at the doors, with RF module, to communicate with the HUB.
- HUB to communicate with the wireless devices through RF. The HUB is connected to the PC (server) through TCP/IP.

The RF communication is at 868 MHz or 915 MHz. The information sent between the devices is encrypted (AES128 standard encryption).

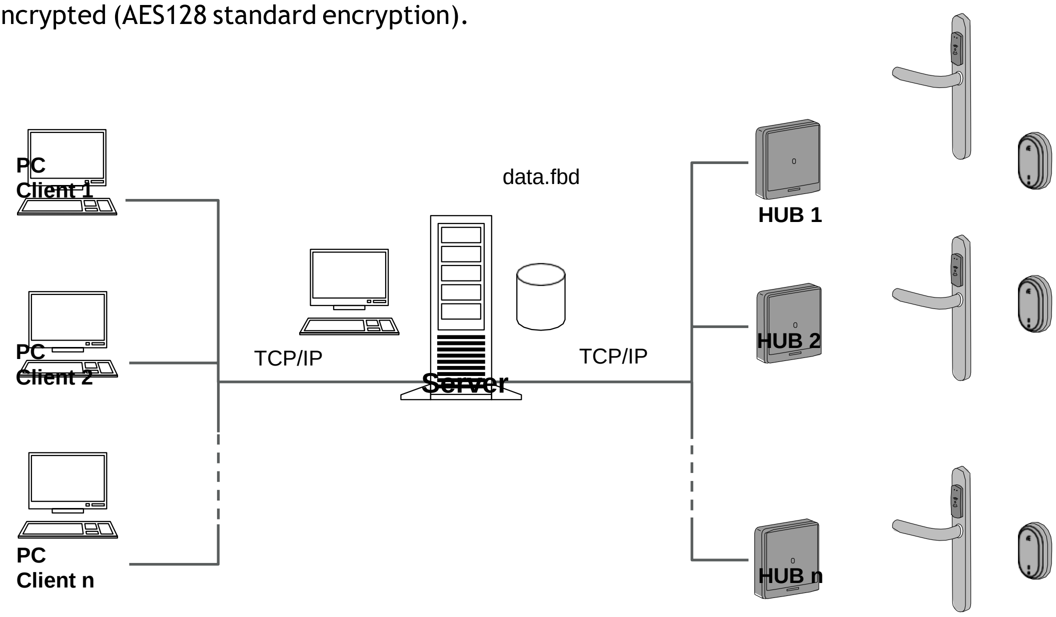


**Fig. 4** Wireless system architecture, with a single centralised server

A computer can control as many Hubs as deemed necessary. A Hub can control up to about 30 wireless locks in a radius of up to 30 meters in a closed environment or up to 100 meters in an open environment. The range is different at each site, according to its construction characteristics (wall thickness, materials used, etc.).

NOTE: the wireless system allows updating the locks and reading their events without the need to bring the Portable Programmer to them. However, their initialisation must always be carried out by means of the Portable Programmer.

## J.2 WIRELESS SYSTEM CONFIGURATION

The main steps for configuring a wireless system are described below.

### Hub setup

Connect and supply power to the Hubs as explained in their corresponding product manuals.

As a summary, and bearing in mind that there may be differences depending on the model of the Hub, the operations to be carried out are the following:

- Connect the Hub to the PC by means of the Ethernet network connector. Use a PC where the TESA - SMARTair TS1000 Server application is installed, as well as the "InitHubIP" tool, which is used to configure the IP parameters of the Hubs and initialise them.
- Connect the power supply of the Hub. In some cases, the power supply arrives through the Ethernet connector and, in some other cases, it is necessary to use an external adaptor. It is possible that you may also have to turn on a switch. Refer to the instructions of the Hub used to clarify this point. Damage may be caused to the Hub if it is not correctly powered.
- Perform the TCP/IP configuration of the Hub for it to be able to communicate with the PC. This is carried out by means of the InitHubIP tool, as described in the following section.

### Configuration and initialisation of the Hubs by means of InitHubIP

The steps to be carried out are the following:

1 Knowing the initial network parameters of the Hub (initialising it, if necessary).

2 Configuring the network parameters of the PC for it to be able to communicate with the Hub.

3 Configuring the Hubs by means of InitHubIP, assigning them the work network parameters, compatible with the network where they are installed, and initialising them for the TS1000 system.

4 Resetting the PC to its initial network parameters for it to operate on its usual network.

These steps are described below.

#### Initial network parameters of the Hub

The factory parameters of the Hub are the following:

| | |
|---|---|
| IP address: | 192.168.1.10 |
| Subnet mask: | 255.255.255.0 |
| Default gateway: | 192.168.1.0 |

□ If the Hub has been used before and the parameters are not known, the factory parameters can be recovered by resetting the Hub. The reset involves, with the Hub off, clicking the Reset button and, without releasing it, turning on the Hub, and keeping the Reset button pressed for approximately 5 seconds. After about 30 seconds, the Hub will have recovered its factory values. For more information, refer to the instructions for the Hub.

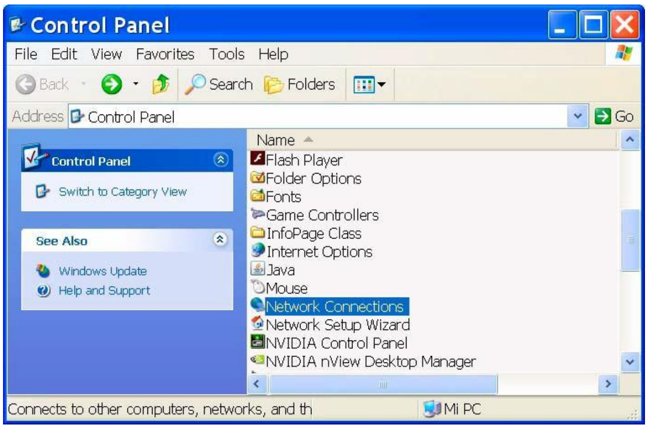
□ If you have previously initialised and configured the Hub to operate in a network, and you know the IP address, subnet mask and gateway, you can use these known parameters, without having to reset the Hub to the factory values.

## Configuring the network parameters of the PC for it to be able to communicate with the Hub

Once the parameters of the Hub are known, it is necessary to configure the corresponding parameters of the PC for it to be able to communicate with the Hub (the IP of the PC has to be configured to lie in the same range as that of the Hub, with the same subnet mask and the same gateway).

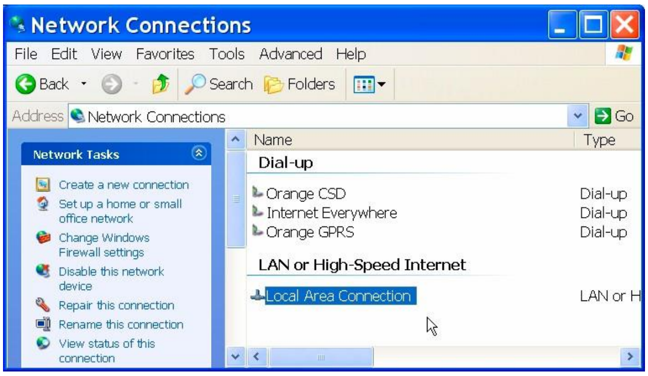
Proceed as follows (these steps may vary depending on the Operating System installed on your computer):

1 Access “Network connections” in the “ControlPanel”.



Connects to other computers, networks, and th

2 In “Network connections”, select “Local areaconnection”.


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Repair this connection
Rename this connection
View status of this connection

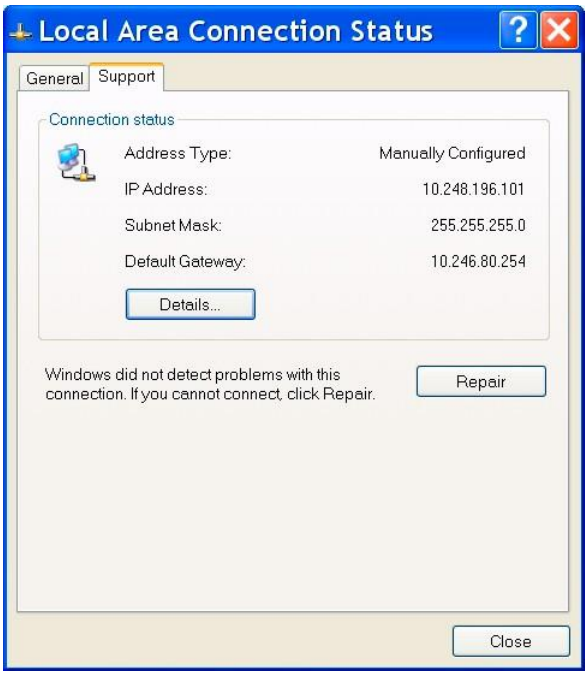
| Name | Type |
|---|---|
| Dial-up | |
| Orange CSD | Dial-up |
| Internet Everywhere | Dial-up |
| Orange GPRS | Dial-up |
| LAN or High-Speed Internet | |
| Local Area Connection | LAN or H |

3 Select the “Support” tab. The current configuration of your PC is displayed. Note it down, since you will have to modify it and then restore it. In the example, the parameters are:

– IP address: 10.248.196.101

– Subnet mask: 255.255.255.0

– Gateway: 10.246.80.254



Address Type: Manually Configured

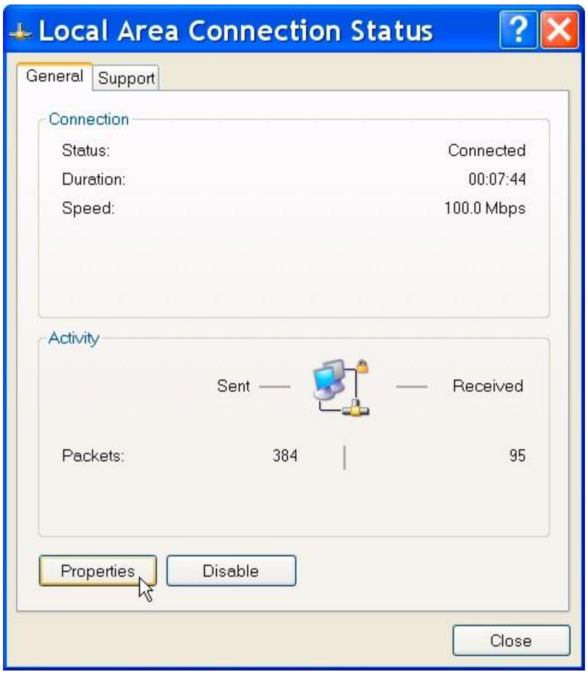
IP Address: 10.248.196.101

Subnet Mask: 255.255.255.0

Default Gateway: 10.246.80.254

Windows did not detect problems with this connection. If you cannot connect, click Repair.

4 In the "General" tab, click the "Properties" button.



Local Area Connection Status

General | Support

Connection

Status: Connected

Duration: 00:07:44

Speed: 100.0 Mbps

Activity

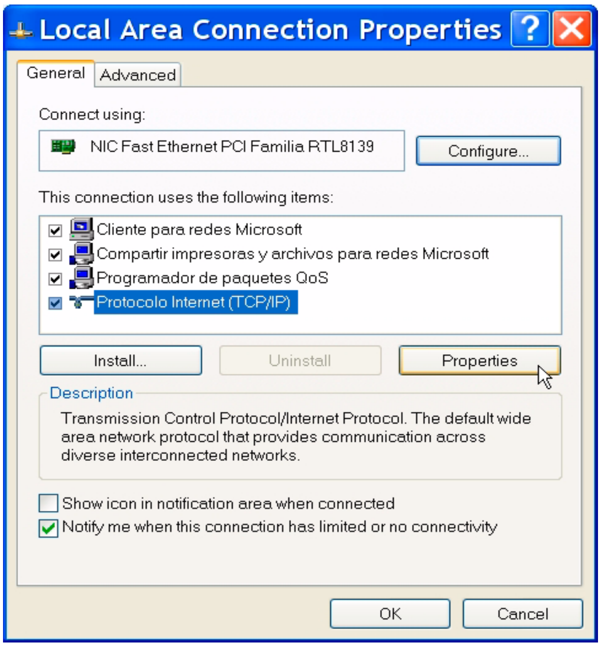
Sent — — Received

Packets: 384 | 95

Properties | Disable

Close

5 Select "Internet Protocol (TCP/IP)" and click the "Properties" button.



Local Area Connection Properties

General | Advanced

Connect using:

NIC Fast Ethernet PCI Familia RTL8139 | Configure...

This connection uses the following items:

☑ Cliente para redes Microsoft

☑ Compartir impresoras y archivos para redes Microsoft

☑ Programador de paquetes QoS

☑ Protocolo Internet (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

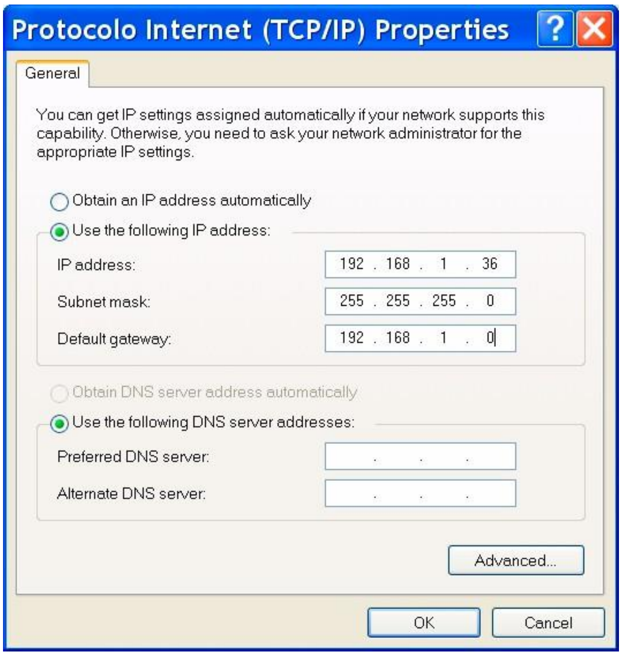
OK | Cancel

6 Change the IP address and enter one which is in the same range as that of the Hub, with the same subnet mask and gateway. For example:

– IP address: 192.168.1.36

– Subnet mask: 255.255.255.0

– Gateway: 192.168.1.0



Protocolo Internet (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 36

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 0

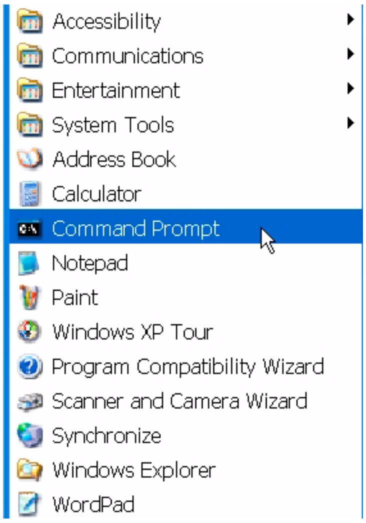
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

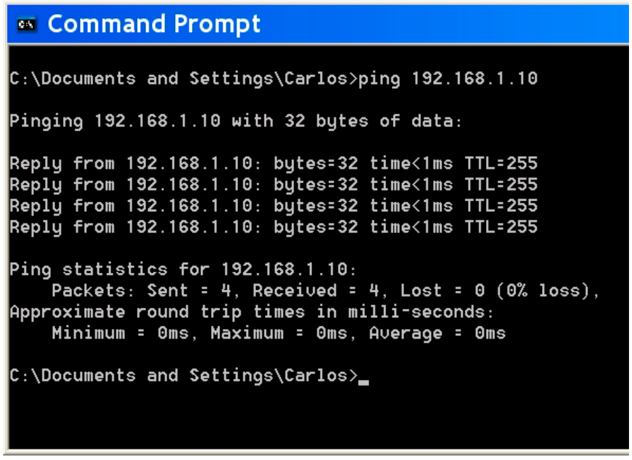
Preferred DNS server: . . .

Alternate DNS server: . . .

7 Verify that the Hub and PC are communicating properly, by means of the PING command. For this purpose, access “Home”, “All Programmes”, “Accessories”, “Command Prompt”.



In “Command Prompt”, write “ping 192.168.1.10”, which is the IP of the Hub. Then, the PC sends 4 data packets to the Hub. If the communication is successful, the Hub will get the 4 packages back and none will be lost, as the message in the example indicates.



Command Prompt

```
C:\Documents and Settings\Carlos>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255
Reply from 192.168.1.10: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Carlos>_
```

At this moment, since the PC and Hub are communicating properly, it is possible to initialise the Hub by means of the “InitHubIP” tool, as explained in the following section.

## Configuration of the Hubs by means of InitHubIP

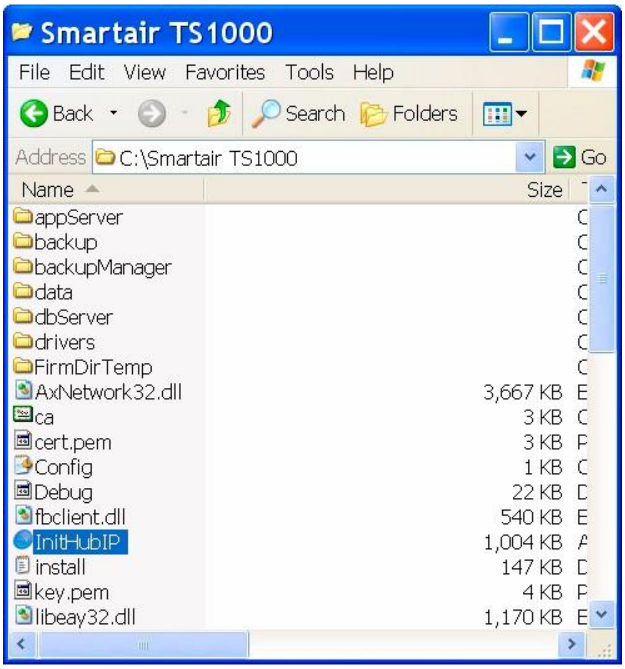
The "InitHubIP" tool is used to configure the network parameters of the Hubs (assigning them a fixed IP address, provided by the network administrator) and to initialise them.

□The "InitHubIP" tool uses the same communication ports with the Hubs as the Glassfish service. To avoid conflict, the programme must be run from the server since, during start-up, it will detect whether the Glassfish service has been launched and it will offer to stop it in order to communicate with the Hubs. From a Guest PC, the application would not be able to stop this service.

Another option is to connect the Hubs directly to a PC external to the network, which does not have the TS1000 installed, where InitHubIP.exe and the messages.* files have already been copied. In this way, there will not be any communication conflicts with the Glassfish service and it will be possible to programme the Hubs without incidents.

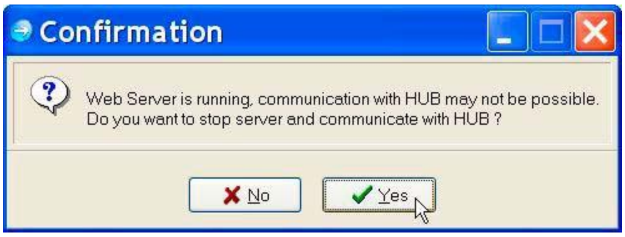
The steps to be followed in order to run the InitHubIP application are shown below, on the same PC where the TESA - SMARTair TS1000 6.x Server application is being run:

**1** Run the InitHubIP application, which is installed in the same folder as the TS1000.



| Name | Size | |
|---|---|---|
| appServer | | C |
| backup | | C |
| backupManager | | C |
| data | | C |
| dbServer | | C |
| drivers | | C |
| FirmDirTemp | | C |
| AxNetwork32.dll | 3,667 KB | E |
| ca | 3 KB | C |
| cert.pem | 3 KB | P |
| Config | 1 KB | C |
| Debug | 22 KB | D |
| fbclient.dll | 540 KB | E |
| InitHubIP | 1,004 KB | A |
| install | 147 KB | D |
| key.pem | 4 KB | P |
| libeay32.dll | 1,170 KB | E |

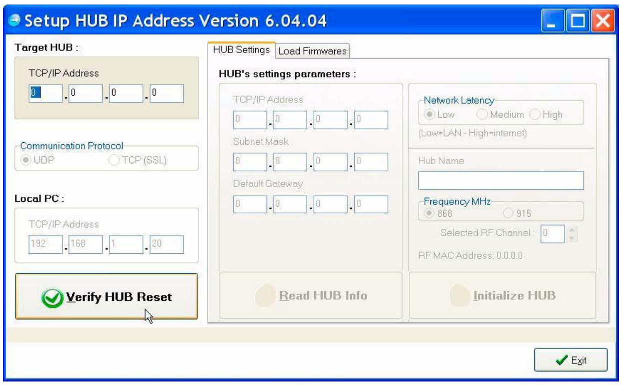
**2** A message is displayed, requesting permission to stop the "TESA_APPSERVER Glassfish Server" service. Confirm this by clicking "Yes".
This window is not displayed if the application is being run from a PC which does not have the TS1000 installed.



Web Server is running, communication with HUB may not be possible.
Do you want to stop server and communicate with HUB ?

3 The InitHubIP application is run, showing the main screen, with the following fields:

- **Target HUB (IP Address of Hub):** allows writing the TCP/IP address of the Hub. If this is not known, it will be necessary to initialise the Hub by means of its corresponding Reset button in order to restore the factory values.



Target HUB :
TCP/IP Address 0 . 0 . 0 . 0
Communication Protocol ● UDP ○ TCP (SSL)
Local PC :
TCP/IP Address 192 . 168 . 1 . 20

HUB's settings parameters :
TCP/IP Address 0 . 0 . 0 . 0
Subnet Mask 0 . 0 . 0 . 0
Default Gateway 0 . 0 . 0 . 0
Network Latency ● Low ○ Medium ○ High
(Low=LAN - High=internet)
Hub Name
Frequency MHz ● 868 ○ 915
Selected RF Channel : 0
RF MAC Address: 0.0.0.0

- **HUB Settings (configuration of the Hub):**

  HUB settings parameters: new valid TCP/IP Address, Subnet Mask and Gateway of the site (to be provided by its network administrator).

  Network Latency: used for remote Hubs, in order to configure the response time of the Hubs when the Ethernet connections are slow.
  For more information, see *"Remote Hubs"* on page 148.

  Hub Name: name assigned to the Hub so as it can be recognised in the locking plan.

  Frequency MHz: allows selecting the working frequency of the RF modules. For more information, see *"Frequency change (from 868 MHz to 915 MHz)"* on page 146.

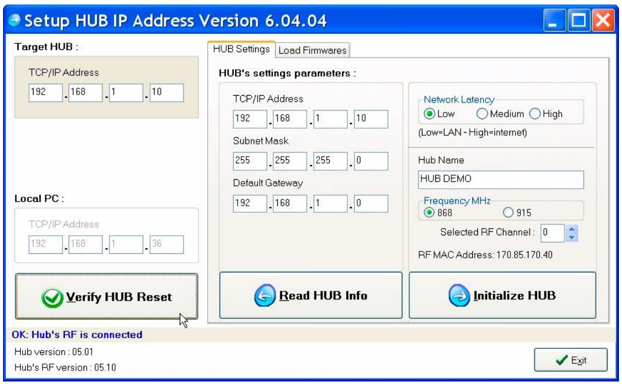
  Select RF channel: allows conflicts with other devices operating at the same frequency in the same site to be avoided.
  For more information, see *"Channel change"* on page 145.

In addition, 3 buttons are shown:

- Verify HUB RESET: verifies that the Hub is operating with the factory parameters.
- Read HUB info: shows the configuration of the Hub.
- Initialise Hub: modifies the parameters of the Hub.

4 Click "Verify HUB Reset" to verify that the Hub is operating with the factory parameters (192.168.1.10). If not, and you do not know the parameters it is operating with, reset the Hub (see *"Initial network parameters of the Hub"* on page 132).

If the Hub is not set to its factory parameters but you know what they are, you can enter them in the field "Target Hub" and click "Verify Hub Reset", thus being able to communicate with the Hub by clicking "Read Hub Info" immediately.



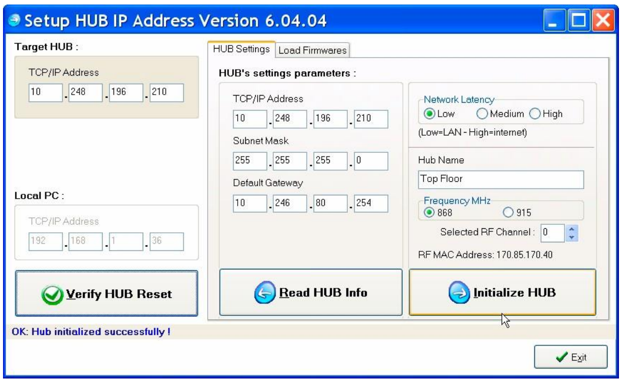
Target HUB :
TCP/IP Address 192 . 168 . 1 . 10
Local PC :
TCP/IP Address 192 . 168 . 1 . 36

HUB's settings parameters :
TCP/IP Address 192 . 168 . 1 . 10
Subnet Mask 255 . 255 . 255 . 0
Default Gateway 192 . 168 . 1 . 0
Network Latency ● Low ○ Medium ○ High
(Low=LAN - High=internet)
Hub Name HUB DEMO
Frequency MHz ● 868 ○ 915
Selected RF Channel : 0
RF MAC Address: 170.85.170.40

OK: Hub's RF is connected
Hub version : 05.01
Hub's RF version : 05.10

**5** Once the connection with the Hub has been verified, enter the new parameters (**the network parameters must be provided by its administrator**).
In the example:
TCP/IP = 10.248.196.210,
Subnet Mask = 255.255.255.0,
Gateway = 10.246.80.254,
Name = Top floor.

Click "Initialise HUB" to confirm. The confirmation message "OK Hub initialised successfully!" will be displayed.


Setup HUB IP Address Version 6.04.04

Target HUB :
TCP/IP Address: 10 . 248 . 196 . 210

Local PC :
TCP/IP Address: 192 . 168 . 1 . 36

HUB's settings parameters :
TCP/IP Address: 10 . 248 . 196 . 210
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 10 . 246 . 80 . 254

Network Latency: ● Low ○ Medium ○ High
(Low=LAN - High=internet)

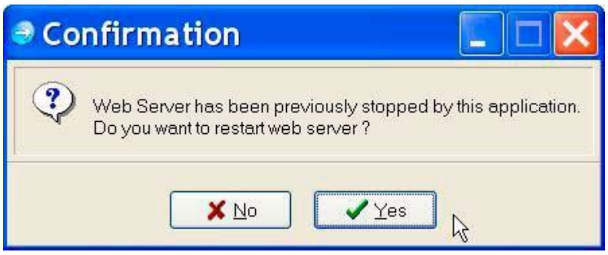
Hub Name: Top Floor

Frequency MHz: ● 868 ○ 915
Selected RF Channel : 0
RF MAC Address: 170.85.170.40

OK: Hub initialized successfully !

**6** When all the Hubs have been configured, close the InitHubIP application by clicking "Exit".

A message is displayed about starting the "TESA_APPSERVER Glassfish Server" service again. Click "Yes" to confirm.
This window is not displayed if we run the application from a PC which does not have the TS1000 installed.

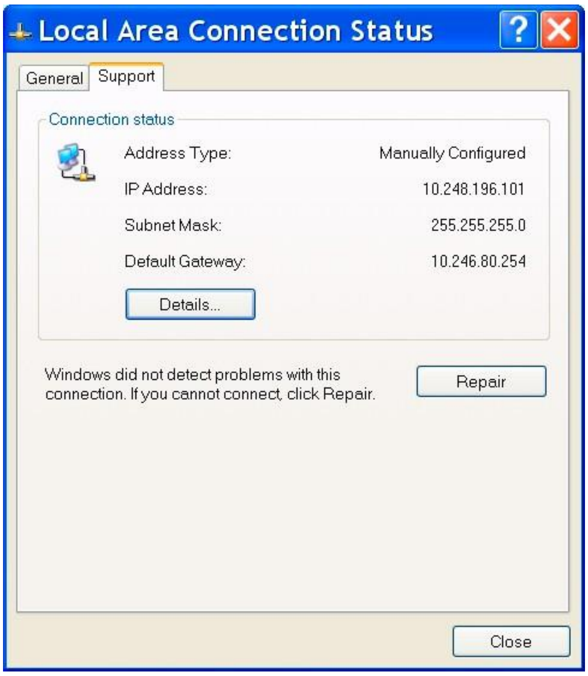

Confirmation

Web Server has been previously stopped by this application.
Do you want to restart web server ?

**7** Repeat these steps for each Hub you want to incorporate into the system, disconnecting the Hubs which are already configured, and assigning a different fixed IP to each one.

## Resetting the network parameters of the PC to the previous configuration

After initialising all the Hubs by means of InitHubIP, as explained in the previous section, it is necessary to reset the PC to its original IP value, since this was modified in section *"Configuring the network parameters of the PC for it to be able to communicate with the Hub"* on page 133.


Local Area Connection Status

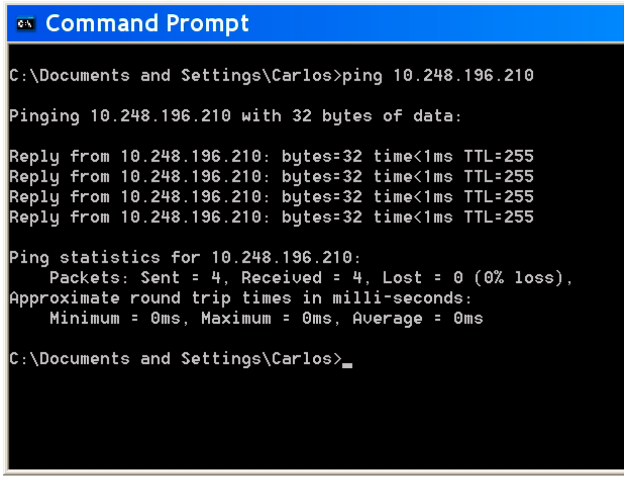
Connection status
Address Type: Manually Configured
IP Address: 10.248.196.101
Subnet Mask: 255.255.255.0
Default Gateway: 10.246.80.254

Windows did not detect problems with this connection. If you cannot connect, click Repair.

After resetting the PC to its original IP values, verify that the PC and Hub are on the same network.

In order to verify that the PC and Hub are on the same network and can communicate properly, ping the Hub (in the example, ping 10.248.196.210). If you receive the 4 packets sent, without losing any (as shown in the example), communication has been successful.

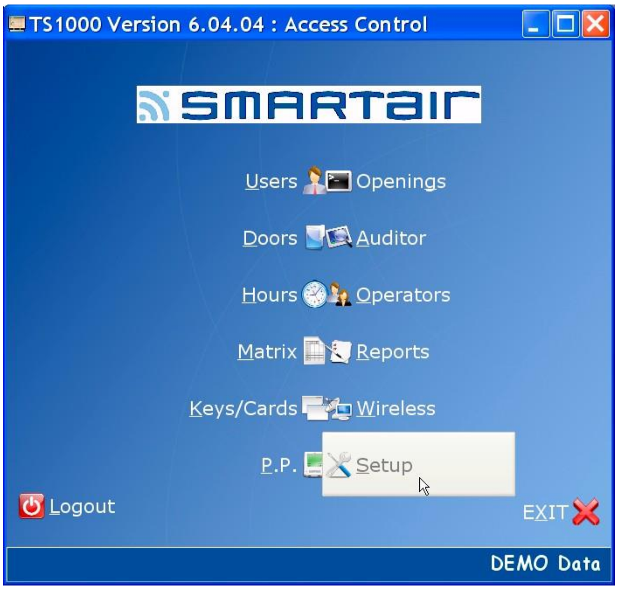
This ping has to be carried out from a PC which is on the network of the system being installed. If the application has been run on an external PC, the ping will be carried out from another machine.



```
C:\Documents and Settings\Carlos>ping 10.248.196.210

Pinging 10.248.196.210 with 32 bytes of data:

Reply from 10.248.196.210: bytes=32 time<1ms TTL=255
Reply from 10.248.196.210: bytes=32 time<1ms TTL=255
Reply from 10.248.196.210: bytes=32 time<1ms TTL=255
Reply from 10.248.196.210: bytes=32 time<1ms TTL=255

Ping statistics for 10.248.196.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Carlos>_
```

## Adding the Hubs to the system

After initialising the Hubs, it is necessary to add them to the system, by means of the TESA - SMARTair TS1000 application, in the "Setup" menu, "Wireless" tab.



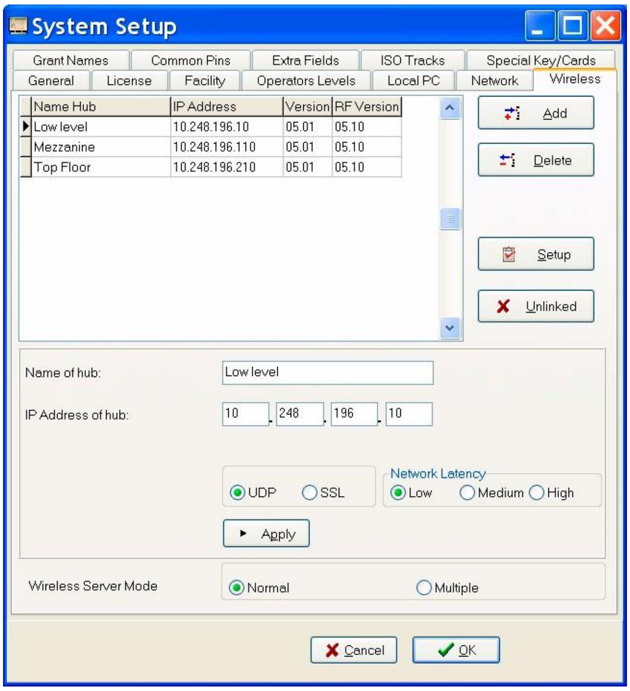
Each Hub is identified with a name or number differentiating it from the rest and a fixed IP address provided by the network administrator (as explained in *"Configuration of the Hubs by means of InitHubIP"* on page 136).

In order to add new Hubs to the site, click the "Add" button and fill in the fields "Hub Name" and "IP Address of Hub". It is necessary to fill in the two fields, entering the same data used when initialising the Hub by means of InitHubIP.

Network Latency field: use the same option applied when initialising the Hub by means of InitHubIP.

Wireless Server mode field:

- Standard mode: the Hubs are managed by a single server. This mode is the most usual one for most sites.
- Multiple mode: Several applications can be running in Server mode. Each server manages a specific number of Hubs. In this mode, each Hub has to be assigned to one of the servers, by selecting one from the drop-down list. It is important to take into account that these servers must be running and have their accesses to the database correctly configured. Otherwise, they will not be displayed in the drop-down list.



| Name Hub | IP Address | Version | RF Version |
|---|---|---|---|
| Low level | 10.248.196.10 | 05.01 | 05.10 |
| Mezzanine | 10.248.196.110 | 05.01 | 05.10 |
| Top Floor | 10.248.196.210 | 05.01 | 05.10 |

Name of hub: Low level

IP Address of hub: 10 . 248 . 196 . 10

● UDP ○ SSL

Network Latency: ● Low ○ Medium ○ High

Wireless Server Mode: ● Normal ○ Multiple

Finally, click the "Apply" button. The Hub will be displayed in the table shown above.

## *Autolink* function

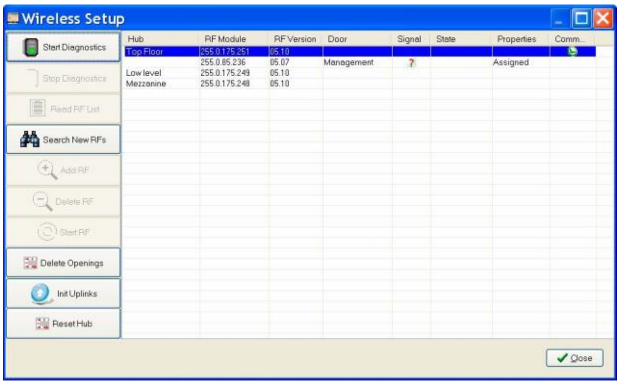
The V3 wireless devices have a function by means of which they try to automatically link to the nearest Hub on their own, under the following conditions:

- When they are turned on/activated (battery change).
- After being initialised or having the time updated with the Portable Programmer (6.70 version or higher) or by means of the PCToLock (V3.11 or higher).
- Every time a New event is generated in a device which has not previously been linked to a Hub.
- If the “Init Wireless” special card is brought close.

For the automatic link to be set up, the Hub must be powered, communicating with the PC and created in the database of the server, as explained in the previous sections.

□ For the automatic link to initialise, it is very important to carry out a diagnostic of the communications to the Hub.
For this purpose, select the Hub and, once it has been highlighted in blue, click “Start Diagnostic”.

Otherwise, it would be necessary to restart the “Glassfish” Web Service or wait an hour (communications for the automatic link are verified every hour, on the hour).



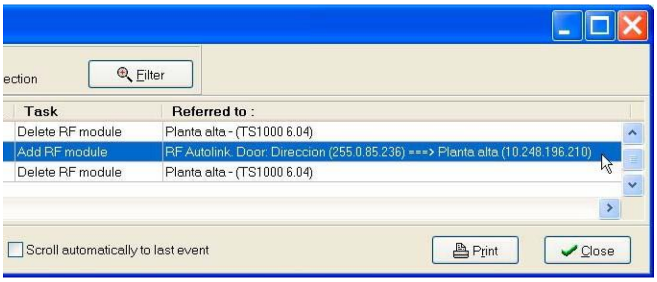
| Hub | RF Module | RF Version | Door | Signal | State | Properties | Comm... |
|---|---|---|---|---|---|---|---|
| Top Floor | 255.0.175.251 | 05.10 | | | | | |
| | 255.0.85.236 | 05.07 | Management | ? | | Assigned | |
| Low level | 255.0.175.249 | 05.10 | | | | | |
| Mezzanine | 255.0.175.248 | 05.10 | | | | | |

For the automatic link process, bear the following in mind:

- When a door device tries to link automatically, it will search for Hubs which are within its coverage range. If more than one Hub is found, it will automatically select the Hub with the strongest coverage signal.
- The device will only link to the Hubs which belong to the same site.
- When a device finds a Hub which meets the preceding requirements, it will send the corresponding information to the Server, by means of the Hub (the Hubs do not store information on the devices assigned in their memory).

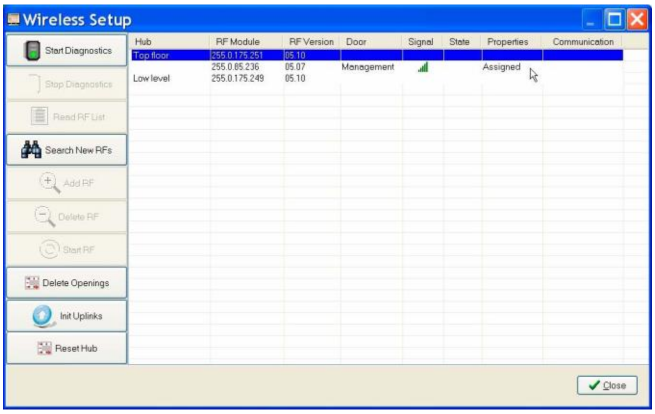
When a device is correctly linked, the following message will be displayed in the system Auditor:

“Add RF module - RF Autolink: Door XXX ===> Hub YYYY”



| Task | Referred to : |
|---|---|
| Delete RF module | Planta alta - (TS1000 6.04) |
| Add RF module | RF Autolink. Door: Direccion (255.0.85.236) ===> Planta alta (10.248.196.210) |
| Delete RF module | Planta alta - (TS1000 6.04) |

The V3 wireless door device will automatically be displayed in the Wireless menu as “Assigned” to the Hub.



| Hub | RF Module | RF Version | Door | Signal | State | Properties | Communication |
|---|---|---|---|---|---|---|---|
| Top floor | 255.0.175.251 | 05.10 | | | | | |
| | 255.0.85.236 | 05.07 | Management | | | Assigned | |
| Low level | 255.0.175.249 | 05.10 | | | | | |

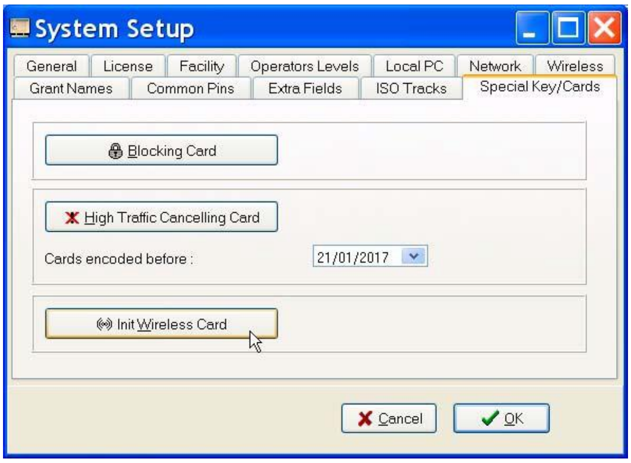
If, during the initialisation of a door device, it does not find any Hubs within its coverage range (communication attempts every 6 seconds), its link to a Hub will remain pending. The link can be established later on in any of the following ways:

- Directly from the software, as explained in *“Adding wireless devices to the Hub (manual link)”* on page 143.

- Bringing the “Init Wireless Card” special card close to the lock.

  This card is encoded in the “Setup” menu, “Other Cards” tab, “Init Wireless Card” button.

- By means of the Update of the lock either with the PP or PCToLock.



Cards encoded before : 21/01/2017

## Adding wireless devices to the Hub (manual link)

After adding the Hubs to the system, it is necessary to assign the wireless devices (locks, wall readers, etc.) with which they will communicate to them.

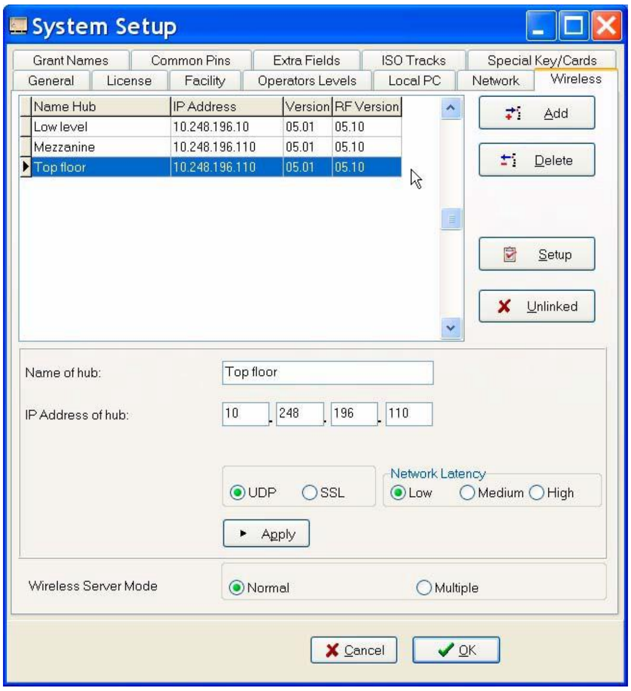
**NOTE:** the devices of the V3 wireless system have the "Autolink" function, which has been explained in the previous section, for adding them to the Hub. Therefore, it is not necessary to apply what has been explained in this section for V3 devices, since they have "Autolink". However, it may be useful in particular cases, for example: if the Hubs were not connected when the doors were initialised and you do not want to go around door by door again with the Init wireless card or the PP.

In order to add a V3 wireless device to the Hub, carry out the following steps:

1 Add the wireless device to the "Doors" menu if it has not been assigned yet (see *"F.3 "Doors" menu"* on page 74 if you do not know how to do this).

2 Initialise the wireless device if it has not been initialised yet (see *"I.3 Initialising the doors of the site"* on page 123 if you do not know how to do this).

3 In the TS1000 programme, in the "Setup" menu, "Wireless" tab, double-click the Hub chosen.



System Setup

| Name Hub | IP Address | Version | RF Version |
|---|---|---|---|
| Low level | 10.248.196.10 | 05.01 | 05.10 |
| Mezzanine | 10.248.196.110 | 05.01 | 05.10 |
| Top floor | 10.248.196.110 | 05.01 | 05.10 |

Name of hub: Top floor

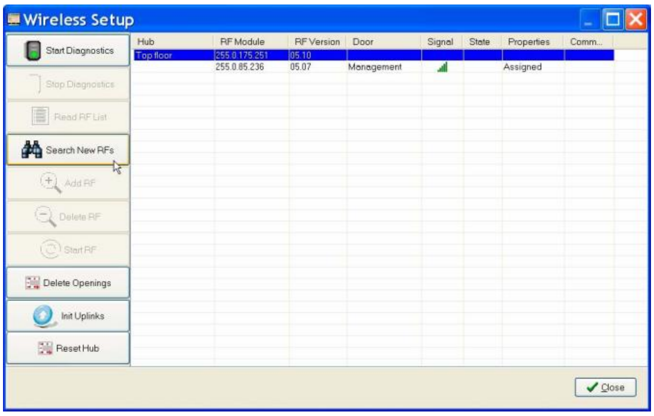
IP Address of hub: 10 . 248 . 196 . 110

● UDP ○ SSL

Network Latency: ● Low ○ Medium ○ High

Wireless Server Mode: ● Normal ○ Multiple

4 The following screen is displayed: Click the "Find New RFs" button.



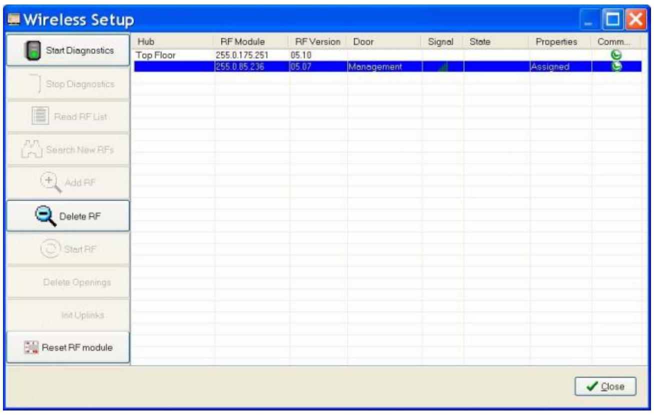
Wireless Setup

| Hub | RF Module | RF Version | Door | Signal | State | Properties | Comm... |
|---|---|---|---|---|---|---|---|
| Top floor | 255.0.175.251 | 05.10 | | | | | |
| | 255.0.85.236 | 05.07 | Management | | | Assigned | |

5 Once it has been found, select it to highlight it in blue and click “Add RF”.

The wireless device is now assigned to the Hub.

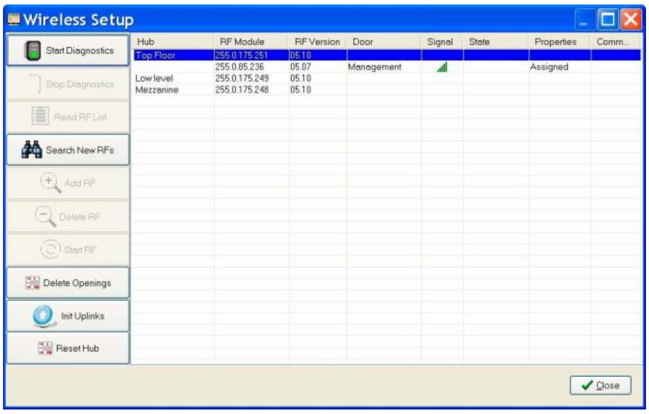
From this moment, it is possible to communicate with the “Management” wireless lock through the PC, by means of the “Wireless” menu of the TS1000 main screen, as explained in *“J.3 Management of wireless devices”* on page 150.



| Hub | RF Module | RF Version | Door | Signal | State | Properties | Comm... |
|---|---|---|---|---|---|---|---|
| Top Floor | 255.0.175.251 | 05.10 | | | | | ● |
| | 255.0.85.236 | 05.07 | Management | | | Assigned | ● |

Before proceeding to the next section, the functions available on the “Wireless Setup” screen are described:

The different configuration functions between the different RF modules and Hubs are available in this menu:



| Hub | RF Module | RF Version | Door | Signal | State | Properties | Comm... |
|---|---|---|---|---|---|---|---|
| Top Floor | 255.0.175.251 | 05.10 | | | | | |
| | 255.0.85.236 | 05.07 | Management | | | Assigned | |
| Low level | 255.0.175.249 | 05.10 | | | | | |
| Mezzanine | 255.0.175.248 | 05.10 | | | | | |

- **Start Diagnostic:** verifies the state of the wireless device.
- **Stop Diagnostic:** stops the diagnostic.
- **Read RF List:** reads the wireless devices.
- **Search New RFs:** it searches the new devices to be added.
- **Add RF:** adds the device selected in blue to the Hub.
- **Delete RF:** removes the device selected from the Hub.
- **Start RF:** enables the RF module so as to be able to carry out remote operations.
- **Delete Openings:** removes the openings from the Hub selected, wiping the memory.
- **Init Uplinks:** forces the doors which communicate with this Hub to connect and send the information they hold (this button is not applicable in the V1 and V2 wireless versions).
- **Reset Hub:** wipes the volatile memory of the Hub, but neither deletes nor alters the configuration data.

## Advanced setup

### Channel change

The default values in the system, for the frequency and the channel, are 868 MHz and Channel= 0, respectively. These values are sent to the Hub and door devices during the initialisation process (both with the InitHubIP application and the Portable Programmer or PCToLock, respectively).

It is also possible for the site to have a wireless SMARTair system, version V1-V2. **In order to avoid conflicts with the devices previously installed, it is advisable not to use channels 1 and 2.**

It is also possible for the communication channel to be in use by other devices from third party systems (such as alarm systems or hospital equipment).

The V3 wireless communication system allows changing the communication channel within values ranging from 0 to 31, in three steps:

**1** Changing the channel in the Hub by means of the InitHubIP application.

**2** Changing the channel in the door devices by means of the TS1000 Software Setup menu.

□Step 1 can be skipped if a diagnostic is conducted for all the Hubs at this point.
During the diagnostic of the Hub, the name, channel and frequency are verified, and they are changed if necessary.

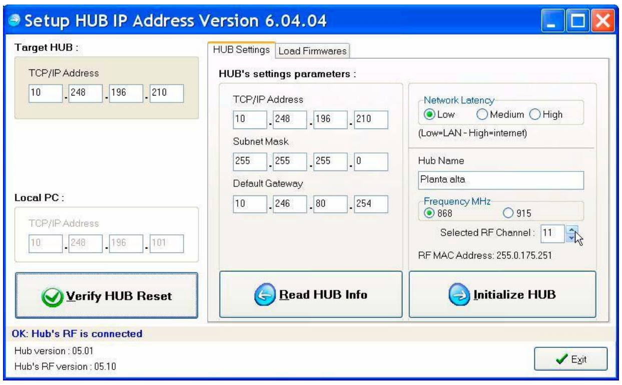
**3** Initialising the door devices, by means of the Portable Programmer or PCToLock.

The three steps are described below:

**1** Changing the channel in the Hubs by means of InitHubIP.

This process can be carried out both the first time the Hub is initialised and subsequently. For this purpose, it is necessary to have access to the Hub through the network or directly through the Ethernet cable.

Select the channel desired (11 in the example) and click the “Initialise Hub” button.


Setup HUB IP Address Version 6.04.04

Target HUB :
TCP/IP Address 10 . 248 . 196 . 210

Local PC :
TCP/IP Address 10 . 248 . 196 . 101

HUB's settings parameters :
TCP/IP Address 10 . 248 . 196 . 210
Subnet Mask 255 . 255 . 255 . 0
Default Gateway 10 . 246 . 80 . 254

Network Latency ● Low ○ Medium ○ High
(Low=LAN - High=internet)

Hub Name
Planta alta

Frequency MHz ● 868 ○ 915
Selected RF Channel : 11

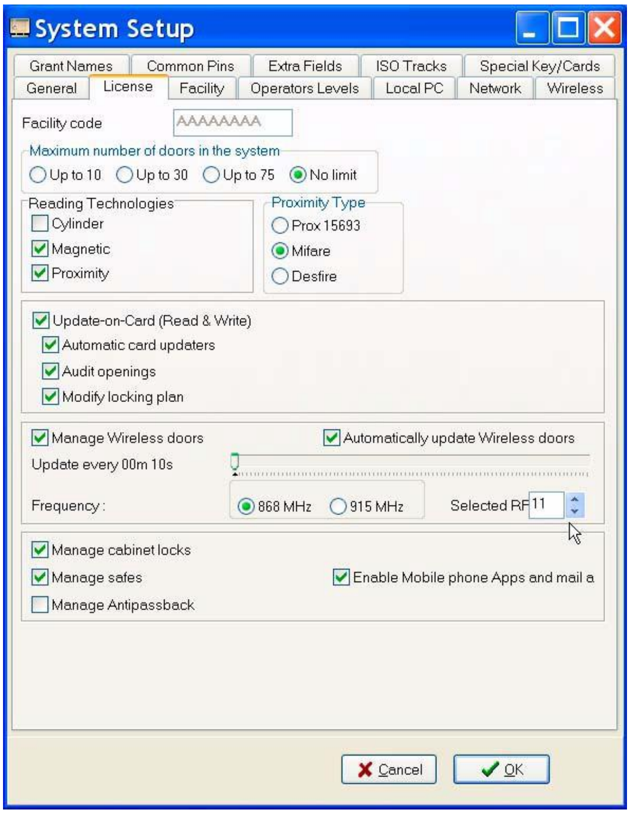
RF MAC Address: 255.0.175.251

OK: Hub's RF is connected
Hub version : 05.01
Hub's RF version : 05.10

**2** Configuring the channel in the door devices.

This is performed in the TS1000 software, in the "Setup" menu, "Licence" tab.

Select **the same channel selected for the V3 Hubs** (11 in the example) and click the "OK" button to confirm.



Facility code AAAAAAAA

Maximum number of doors in the system
○ Up to 10 ○ Up to 30 ○ Up to 75 ● No limit

Reading Technologies
□ Cylinder
☑ Magnetic
☑ Proximity

Proximity Type
○ Prox 15693
● Mifare
○ Desfire

☑ Update-on-Card (Read & Write)
☑ Automatic card updaters
☑ Audit openings
☑ Modify locking plan

☑ Manage Wireless doors
☑ Automatically update Wireless doors
Update every 00m 10s
Frequency : ● 868 MHz ○ 915 MHz
Selected RF 11

☑ Manage cabinet locks
☑ Manage safes
☑ Enable Mobile phone Apps and mail a
□ Manage Antipassback

□ Step 1 can be skipped if a diagnostic is conducted for all the Hubs at this point.
During the diagnostic of the Hub, the name, channel and frequency are verified, and they are changed if necessary.

**3** Initialising the door devices again with the PP or PCToLock. This information cannot be updated by means of RF.

□ Note: any door device which requires a "manual" update (with PP or PCToLock) will be displayed in orange in the programme, indicating that it needs to be updated.

## Frequency change (from 868 MHz to 915 MHz)

Due to the restrictions applicable in several countries, in relation to the frequencies which can be used, it may be necessary to change the radio frequency to 915 MHz (for example, in the USA, Canada, Australia or New Zealand).

This is carried out just like the channel change, explained in the previous section, but in the field corresponding to the frequency:

**1** Changing the frequency of the Hub by means of the InitHubIP application.

**2** Changing the frequency in the door devices by means of the TS1000 Software Setup menu.

**3** Initialising the door devices, by means of the Portable Programmer or PCToLock.

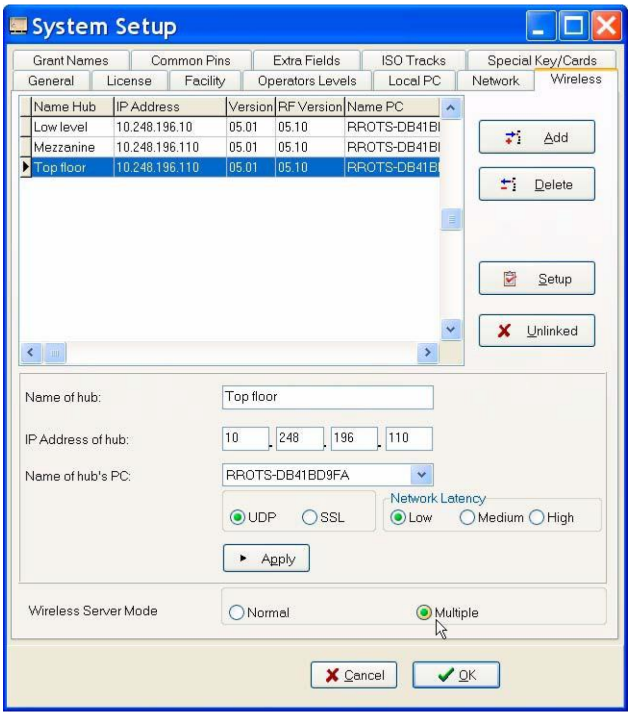
## Multiple Wireless Server mode

Similar to that used in the V1 and V2 wireless systems, it is possible to configure a Multiple Server mode. This allows for more agile management in multi-site systems.

1 **Standard mode:** all the HUBs are managed by a single centralised Server. This mode is advisable for most sites (see *"Fig. 4 Wireless system architecture, with a single centralised server"* on page 131).

2 **Multiple Server mode:** several server instances can be run. Each server manages a particular number of Hubs. In this mode of operation, it is necessary to assign a server to each Hub, by selecting it from the drop-down list. It needs to be borne in mind that the servers must be in operation and the accesses to the database correctly configured. Otherwise, the servers will not be displayed in the drop-down list.

□ Take into account that it is not necessary for the Hubs to be on different machines. It is possible to have all the Hubs connected to the master server and use the secondary server as a DMZ to redirect Internet requests to the site; this is a typical wireless site with an App having a fixed IP.



| Name Hub | IP Address | Version | RF Version | Name PC |
|---|---|---|---|---|
| Low level | 10.248.196.10 | 05.01 | 05.10 | RROTS-DB41BI |
| Mezzanine | 10.248.196.110 | 05.01 | 05.10 | RROTS-DB41BI |
| Top floor | 10.248.196.110 | 05.01 | 05.10 | RROTS-DB41BI |

Name of hub: Top floor

IP Address of hub: 10 . 248 . 196 . 110

Name of hub's PC: RROTS-DB41BD9FA

● UDP ○ SSL

Network Latency: ● Low ○ Medium ○ High

Wireless Server Mode: ○ Normal ● Multiple

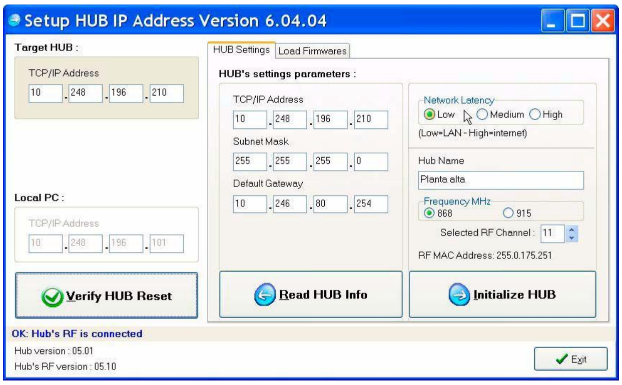
## Remote Hubs

In the event of the network connections being too slow, it is possible to select the response time of the Hubs to allow longer *Timeouts* and facilitating their correct operation.

Take into account that the Hubs need a fixed IP address so that they can communicate with the PC.

This selection is made during the configuration by means of the InitHubIP application. The possible settings are the following:

- Low: LAN network connection (default). This is the fastest mode of operation.
- Medium: recommended for WAN networks.
- High: connection through the Internet (remember that the Hub needs a fixed IP address). This is the slowest mode of operation.



Setup HUB IP Address Version 6.04.04

Target HUB :

TCP/IP Address: 10 . 248 . 196 . 210

Local PC :

TCP/IP Address: 10 . 248 . 196 . 101

HUB's settings parameters :

TCP/IP Address: 10 . 248 . 196 . 210

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 246 . 80 . 254

Network Latency: ● Low ○ Medium ○ High

(Low=LAN - High=internet)

Hub Name: Planta alta

Frequency MHz: ● 868 ○ 915

Selected RF Channel : 11

RF MAC Address: 255.0.175.251

OK: Hub's RF is connected

Hub version : 05.01

Hub's RF version : 05.10

□ Do not select the High mode for a LAN connection, since communication with the Hubs would unnecessarily become much slower.

## Firmware update

The V3 wireless system allows updating the firmware in the RF modules and V3 Hubs.

- RF module in door devices (locks and wall readers):

  The new module has to be updated by means of the Portable Programmer or PCToLock. This process will be very similar to the update process for the two relay boards in the wall readers. The two firmware updates will be loaded into the PP or PCToLock (the control module and the RF module).

  Device versions required:

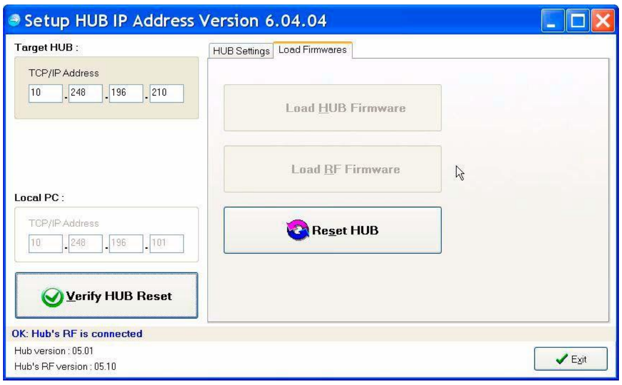
  – PCToLock version 3.10 or higher.

  – PP version 6.70 or higher.

  The new firmware for the RF modules of the door devices will be versions R5RFxx.

- RF module of the V3 HUB:

  The RF modules in the V3 Hubs are similar to the RF modules of the locks, but their firmware version update is carried out by means of the InitHubIP application, version 6.04 or higher, connecting the Hub to the PC through the Ethernet network connection.


Setup HUB IP Address Version 6.04.04

Target HUB :

TCP/IP Address 10 . 248 . 196 . 210

Local PC :

TCP/IP Address 10 . 248 . 196 . 101

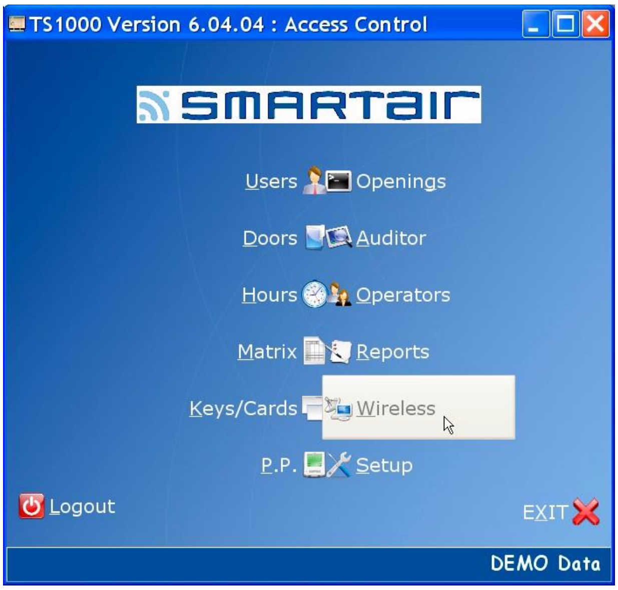
OK: Hub's RF is connected

Hub version : 05.01

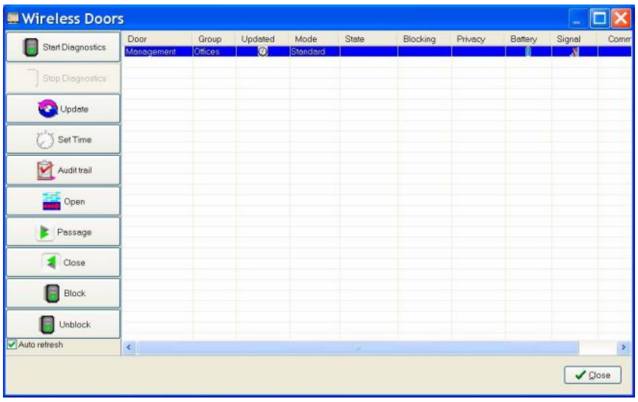
Hub's RF version : 05.10

## J.3 MANAGEMENT OF WIRELESS DEVICES

The management of wireless devices (locks, wall readers, etc.) is carried out by means of the "Wireless" menu of the TS1000 main screen.



In the Wireless menu, the table with the wireless devices controlled by the Hubs connected to that PC is displayed.



| Door | Group | Updated | Mode | State | Blocking | Privacy | Battery | Signal | Comm |
|---|---|---|---|---|---|---|---|---|---|
| Management | Offices |  | Standard |  |  |  |  |  |  |

By selecting a device (in the example, the "Management" lock), it is possible, using the buttons on the left, to carry out the following operations:

- **Start Diagnostic:** a message to test communication between the PC and the locks is sent in order to verify the connection.
- **Stop Diagnostic:** the communication test process can be stopped, in the event that the response is taking too long.
- **Update:** allows updating the locking plan of the wireless lock. This is a manual update, for when the automatic update is taking too long or you wish it to take place immediately for some reason.
- **Set Time:** sets the time in the lock with values from the PC. It is advisable to set the time every time the lock batteries are changed.
- **Auditor:** collects the events which have taken place at the wireless lock. In general, it is not necessary to use this as it is automatically run every time a new event takes place in the door device.
- **Open:** allows opening the wireless lock remotely.
- **Passage:** sets the wireless lock to Open mode.
- **Close:** if the lock is in Open mode, this turns that mode off, setting it to Standard mode.
- **Blocking:** blocks the lock so that it can only be opened by users who have the option "Can open blocked doors" enabled.
- **Unblocking:** unblocks the lock if it is blocked, setting it to Standard mode once again.

# K – Site management

# K – SITE MANAGEMENT

## K.1 INTRODUCTION

After installing the system and starting it up, the users can begin using it. That is to say, they will start opening the doors they have been granted access to, within the corresponding time zone, etc. All these movements will be recorded for consultation and analysis, and the site will be able to evolve based on the interests and needs.

All this management will be performed by the system Operators, who will carry out the operations required, according to their assigned duties (for more information on the Operators, see chapter "G - Operators and Operator Levels").

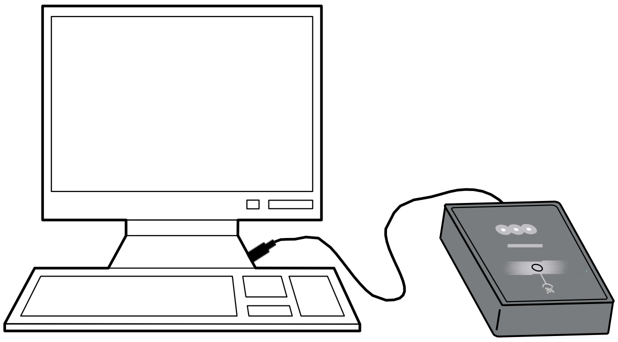
In this chapter, the Management Tools provided by the system are described.

## K.2 READ CARDS/KEYS

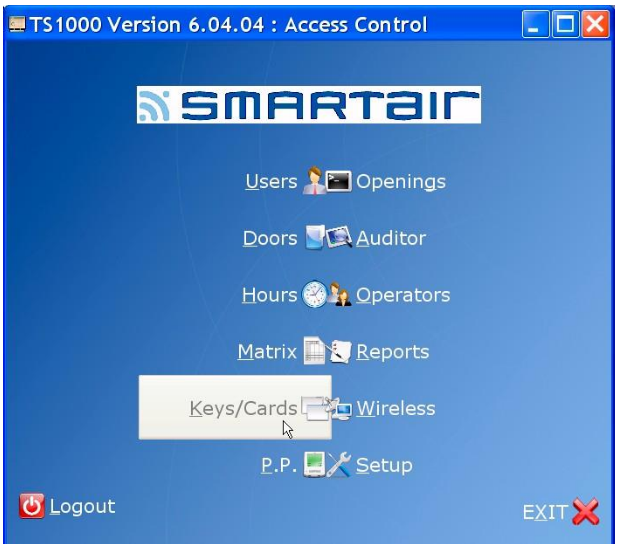
One of the tools provided by the system is reading of credentials.

When encoding a credential, there is no visible physical identification on it about the user it belongs to. Therefore, if an already encoded credential, is found there is no information, beforehand, on who it belongs to.

In order to learn who the credential belongs to, it is possible to read it. For this purpose, the same device employed to encode it is used, that is to say, the Portable Programmer for Keys and the Card Encoder for Cards.

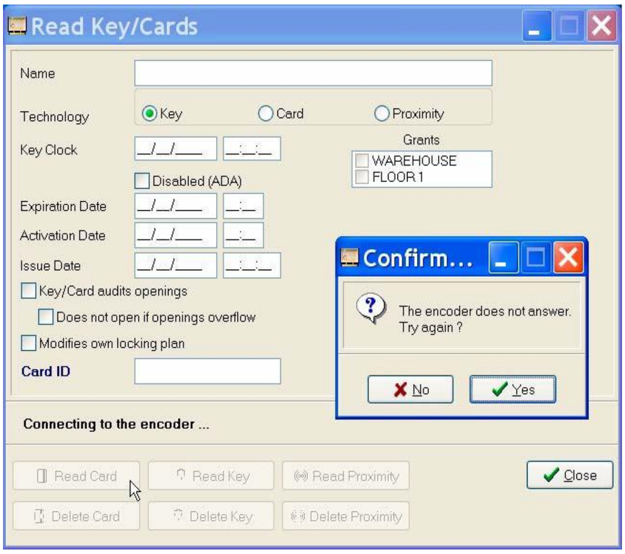


After connecting the Device to the PC, click "Cards" on the TS1000 main screen.



The software will read the credential and display a screen requesting the credential in question be brought closer or inserted.

□ If the system does not manage to communicate with the credential, a window is displayed reporting this, which allows cancelling or retrying the operation. The most frequent cause is not having started the Programmer or Card Encoder (take into account that the Programmer turns off automatically after some minutes of inactivity). It can also be the case that the communication cable does not have a good connection. Verify both possibilities before clicking “Retry”.



Read Key/Cards

Name

Technology ● Key ○ Card ○ Proximity

Key Clock _/_/___ _:_:_

Grants
□ WAREHOUSE
□ FLOOR 1

□ Disabled (ADA)

Expiration Date _/_/___ _:_

Activation Date _/_/___ _:_

Issue Date _/_/___ _:_:_

□ Key/Card audits openings

□ Does not open if openings overflow

□ Modifies own locking plan

Card ID

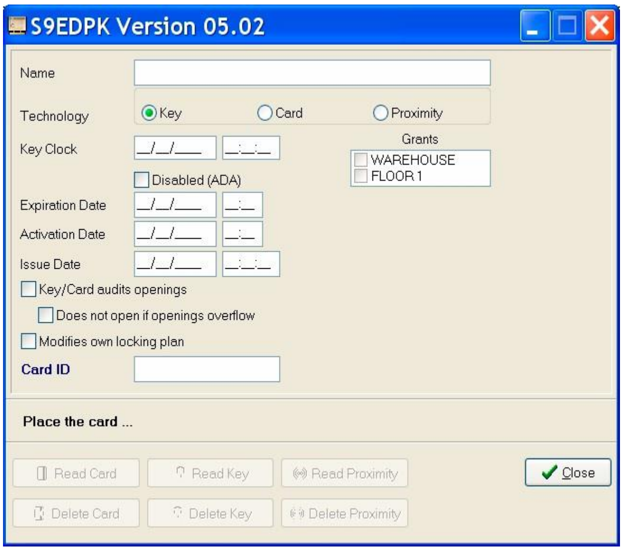
Confirm...

The encoder does not answer.
Try again ?

Connecting to the encoder ...

Once communication has been established, a screen is displayed, with the fields to be read empty, where a message appears requesting the card to be brought closer.

At the top of the window, both the model and version of the Encoder being used to read the card are shown.



S9EDPK Version 05.02

Name

Technology ● Key ○ Card ○ Proximity

Key Clock _/_/___ _:_:_

Grants
□ WAREHOUSE
□ FLOOR 1

□ Disabled (ADA)

Expiration Date _/_/___ _:_

Activation Date _/_/___ _:_

Issue Date _/_/___ _:_:_

□ Key/Card audits openings

□ Does not open if openings overflow

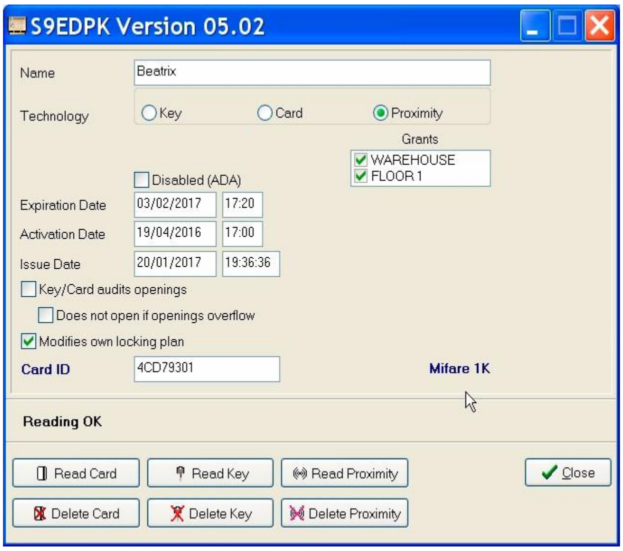
□ Modifies own locking plan

Card ID

Place the card ...

After bringing the card closer, the information related to the User is displayed on the screen, in addition to the message “Reading OK”.

If you want another card to be read, you only need to bring it closer to the Encoder and click the “Read Proximity” button.


S9EDPK Version 05.02

Name: Beatrix

Technology: ○ Key ○ Card ● Proximity

Grants: ☑ WAREHOUSE ☑ FLOOR 1

□ Disabled (ADA)

Expiration Date: 03/02/2017 17:20

Activation Date: 19/04/2016 17:00

Issue Date: 20/01/2017 19:36:36

□ Key/Card audits openings

□ Does not open if openings overflow

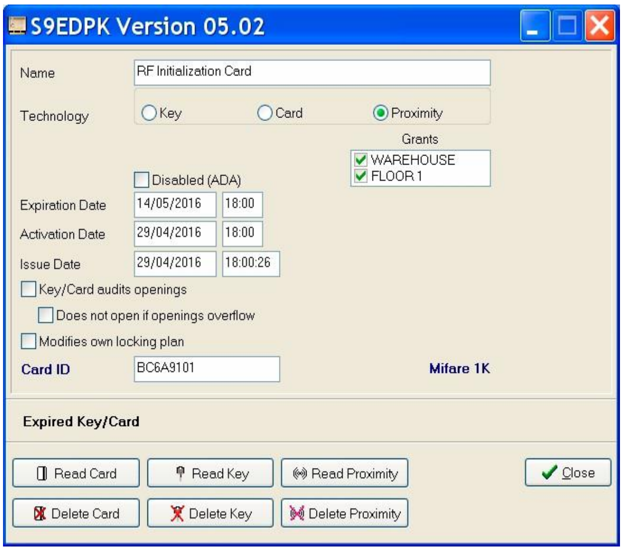
☑ Modifies own locking plan

Card ID: 4CD79301 Mifare 1K

Reading OK

The software also indicates, by means of messages, possible incidents with the cards, such as, for example, “Old Card”, in the event of another one having been subsequently encoded for the same user.

For the Proximity and Electronic Key technologies, provided that the function “Card openings record” is enabled in the credential (see “Settings” in the “Users” menu), after reading the basic data of the credential, the events recorded in it are subsequently collected (see *“Openings read from Credentials by means of the Portable Programmer or Encoder”* on page 158).


S9EDPK Version 05.02

Name: RF Initialization Card

Technology: ○ Key ○ Card ● Proximity

Grants: ☑ WAREHOUSE ☑ FLOOR 1

□ Disabled (ADA)

Expiration Date: 14/05/2016 18:00

Activation Date: 29/04/2016 18:00

Issue Date: 29/04/2016 18:00:26

□ Key/Card audits openings

□ Does not open if openings overflow

□ Modifies own locking plan

Card ID: BC6A9101 Mifare 1K

Expired Key/Card

This screen also allows **deleting the information stored in the credential**. This is carried out by means of the “Delete Key/Card/Proximity” button, depending on the technology. After deleting the credential, it remains empty, but it does not return to its Factory Settings.

## K.3 OPENINGS

The TS1000 Electronic Access Control System allows managing an "Opening Register" or, more precisely, an "Event Register". In their memory, the Door Devices store the Openings which have been carried out, as well as any other event taking place, such as, for example, the communications with the Portable Programmer, attempted openings by unauthorised Users, etc.

The TS1000 system allows checking all these events by means of the Opening Register. In order to be able to check these events by means of the TS1000, it is necessary in the first place to read them from the memory of the Door Devices or Credentials.

In order to read this information and make it available to the TS1000, there are several methods:

- Openings read from Doors by means of the Portable Programmer (valid for any technology).
- Openings read from Credentials by means of the Portable Programmer (valid for Electronic Keys) or Proximity Encoder (valid for Proximity Cards).
- Automatic Opening Register by means of the Updater (valid for Proximity and Electronic Keys).
- Automatic Register by means of Hubs and RF Door Devices (wireless system).

These methods are described below.

### Openings read from Doors by means of the Portable Programmer

This is the traditional system for the collection of data and it is valid for any of the Access Control Technologies available.

The method involves approaching each of the doors intended to be checked with the Portable Programmer and collecting the record stored within it. For this purpose:

1. Connect the Programmer to the door with the corresponding cable.
2. Turn on the Programmer.
3. Access the F4 menu (Openings).
4. Access the "Collect Openings" submenu.
5. Click "OK".

□For more information, refer to the instructions for the Portable Programmer.

After loading all the records into the Portable Programmer, there are two options:

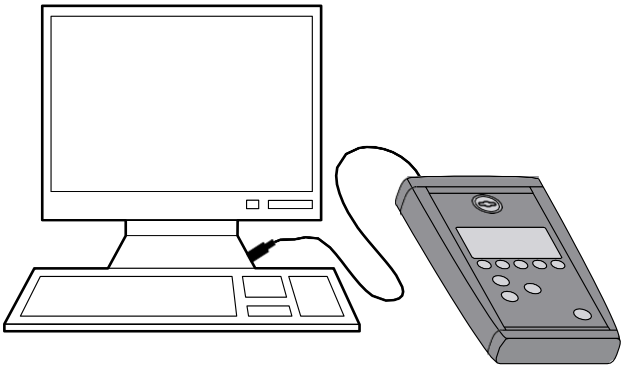
- Viewing the event in the Portable Programmer (in the F4 "Openings" menu, "See Openings" submenu).
- Transmitting the records to the PC and viewing them in the TS1000.

The first option is more appropriate when you wish to quickly view a specific event related to a given door.

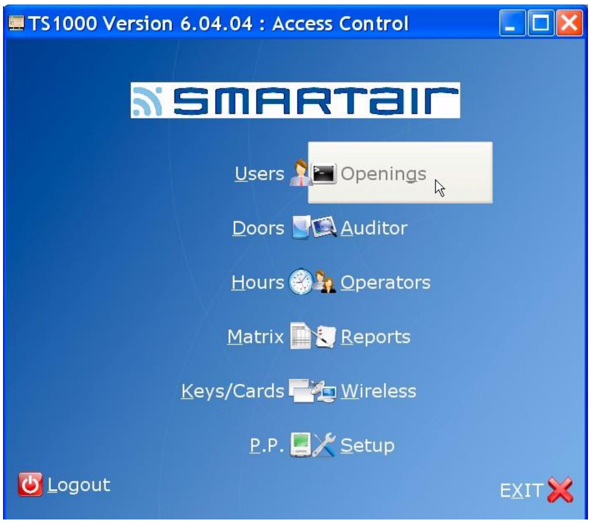
For any other case, the second option is, in principle, more convenient.

The second option is carried out as follows:

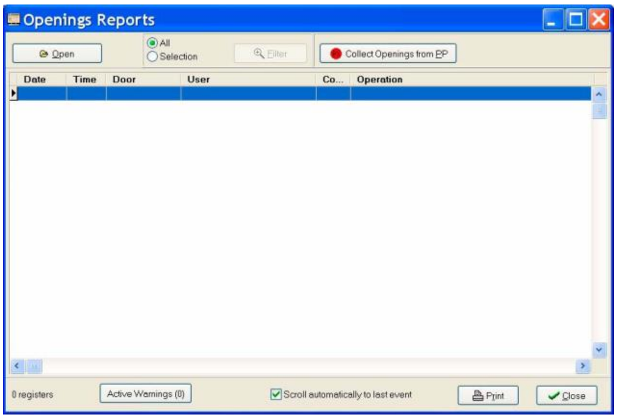
1 Connect the Portable Programmer to the PC with the corresponding serial cable (this can be USB or RS-232, depending on the model).



2 Access the "Openings" menu on the main screen.



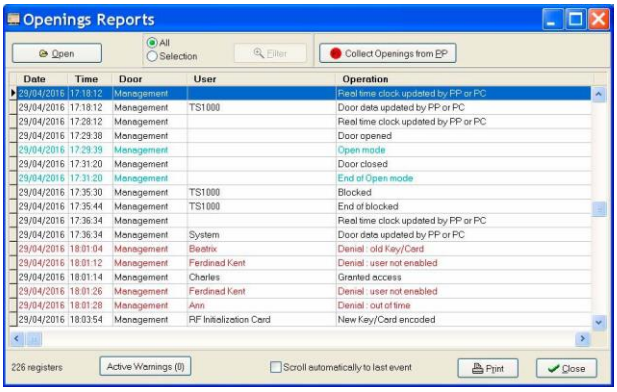
3 The following screen is displayed:



4 Make sure the Programmer is on (it turns off automatically after some minutes of inactivity) and, on the TS1000 screen, click the "Collect Openings from PP" button.

5 When the button is clicked, the PC collects the opening register contained in the Portable Programmer and sorts it in chronological order, as can be seen in the figure.

All the events recorded in the doors are displayed. In addition, next to the "Collect Openings from PP" button, a message is displayed which indicates how many events have been collected in total.



| Date | Time | Door | User | Operation |
|---|---|---|---|---|
| 29/04/2016 | 17:18:12 | Management | | Real time clock updated by PP or PC |
| 29/04/2016 | 17:18:12 | Management | TS1000 | Door data updated by PP or PC |
| 29/04/2016 | 17:28:12 | Management | | Real time clock updated by PP or PC |
| 29/04/2016 | 17:29:38 | Management | | Door opened |
| 29/04/2016 | 17:29:39 | Management | | Open mode |
| 29/04/2016 | 17:31:20 | Management | | Door closed |
| 29/04/2016 | 17:31:20 | Management | | End of Open mode |
| 29/04/2016 | 17:35:30 | Management | TS1000 | Blocked |
| 29/04/2016 | 17:35:44 | Management | TS1000 | End of blocked |
| 29/04/2016 | 17:36:34 | Management | | Real time clock updated by PP or PC |
| 29/04/2016 | 17:36:34 | Management | System | Door data updated by PP or PC |
| 29/04/2016 | 18:01:04 | Management | Beatrix | Denial : old Key/Card |
| 29/04/2016 | 18:01:12 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:14 | Management | Charles | Granted access |
| 29/04/2016 | 18:01:26 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:28 | Management | Ann | Denial : out of time |
| 29/04/2016 | 18:03:54 | Management | RF Initialization Card | New Key/Card encoded |

## Openings read from Credentials by means of the Portable Programmer or Encoder

This option is possible for sites having Electronic Keys and Cylinders, as well as Proximity Credentials and Locks. This option cannot be implemented for sites having Magnetic Stripe Technology due to its nature.

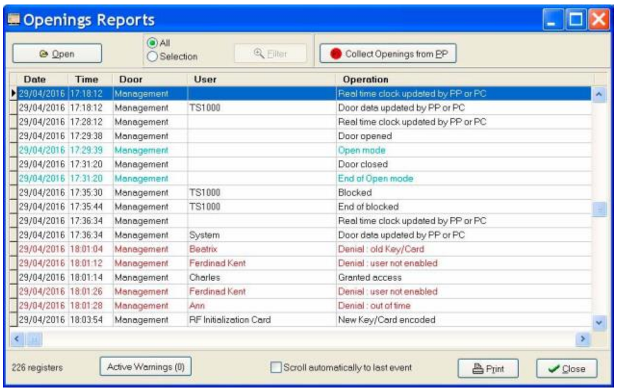
This event collection system is based on the possibility of recording these data not only at the doors, but also in the credentials of each user. This allows finding out the movements of a given credential, without needing to go around the entire site collecting the openings from each door.

The process involves taking the credential of the user and reading it from the "Cards" menu, as has been explained in section *"K.2 Read cards/keys"* on page 153. In addition to finding the form of the credential, the system collects, records and deletes from it all the events stored.

## Analysis of the openings collected

The following information is obtained from each event:

- **Date:** date when the event took place.
- **Time:** time when the event took place.
- **Door:** name of the door where the event took place.
- **User:** name of the user who prompted the event at the door.
- **Operation:** the event itself, that is to say, what happened. For example: "*Denial: user not enabled*".



| Date | Time | Door | User | Operation |
|---|---|---|---|---|
| 29/04/2016 | 17:18:12 | Management | | Real time clock updated by PP or PC |
| 29/04/2016 | 17:18:12 | Management | TS1000 | Door data updated by PP or PC |
| 29/04/2016 | 17:28:12 | Management | | Real time clock updated by PP or PC |
| 29/04/2016 | 17:29:38 | Management | | Door opened |
| 29/04/2016 | 17:29:39 | Management | | Open mode |
| 29/04/2016 | 17:31:20 | Management | | Door closed |
| 29/04/2016 | 17:31:20 | Management | | End of Open mode |
| 29/04/2016 | 17:35:30 | Management | TS1000 | Blocked |
| 29/04/2016 | 17:35:44 | Management | TS1000 | End of blocked |
| 29/04/2016 | 17:36:34 | Management | | Real time clock updated by PP or PC |
| 29/04/2016 | 17:36:34 | Management | System | Door data updated by PP or PC |
| 29/04/2016 | 18:01:04 | Management | Beatrix | Denial : old Key/Card |
| 29/04/2016 | 18:01:12 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:14 | Management | Charles | Granted access |
| 29/04/2016 | 18:01:26 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:28 | Management | Ann | Denial : out of time |
| 29/04/2016 | 18:03:54 | Management | RF Initialization Card | New Key/Card encoded |

226 registers

All the events are sorted in chronological order.

Some events will not make reference to any user, that is to say, the User field will be empty. This is due to the fact that the event is related to an operation of the lock itself, such as initialisation, time setting, etc.

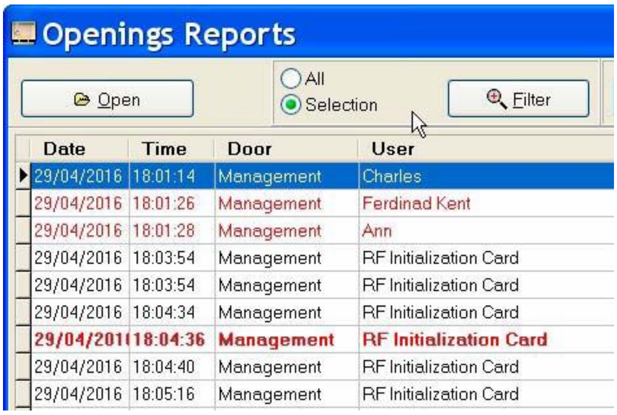
The information presented on this screen can be managed by means of the "Filter" and "Print" tools, which are included on it:

- The "Filter" allows filtering the information, so that only some of the data are shown. For example, it is possible to view only the events related to one user in particular.
- The "Print" button allows the information to be captured either on paper or in an ASCII file, which latter can be imported into another database in use at the site. It is also possible to produce an Excel table, which allows for subsequent processing, if so desired.

## Filter

In the field “Filter”, the option “All” is selected by default, which means that all the events collected and sorted in chronological order are displayed on the screen.

By selecting the option “Selection”, the “Filter” button is enabled.



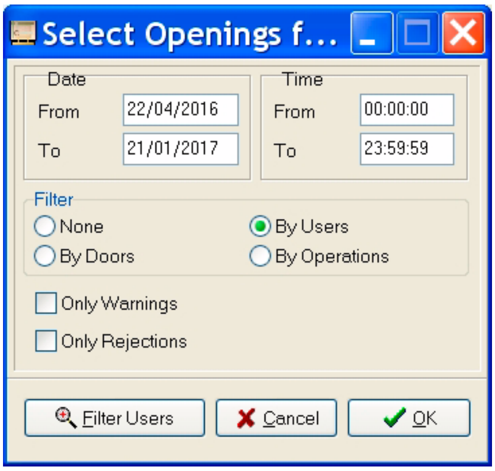
Openings Reports

| | Date | Time | Door | User |
|---|---|---|---|---|
| ▶ | 29/04/2016 | 18:01:14 | Management | Charles |
| | 29/04/2016 | 18:01:26 | Management | Ferdinad Kent |
| | 29/04/2016 | 18:01:28 | Management | Ann |
| | 29/04/2016 | 18:03:54 | Management | RF Initialization Card |
| | 29/04/2016 | 18:03:54 | Management | RF Initialization Card |
| | 29/04/2016 | 18:04:34 | Management | RF Initialization Card |
| | **29/04/201** | **18:04:36** | **Management** | **RF Initialization Card** |
| | 29/04/2016 | 18:04:40 | Management | RF Initialization Card |
| | 29/04/2016 | 18:05:16 | Management | RF Initialization Card |

By clicking the “Filter” button, a screen like the one shown below is displayed:

It offers the possibility to set filters by Date and Time, Doors, Users and Operations.

It is also possible to select the options “Only Warnings” or “Only Rejections”.



Select Openings f...

Date
From 22/04/2016
To 21/01/2017

Time
From 00:00:00
To 23:59:59

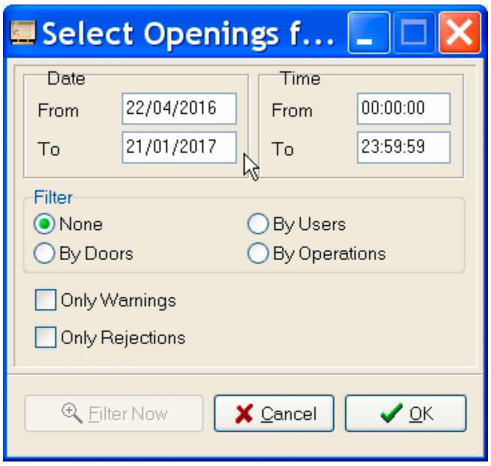
Filter
○ None ● By Users
○ By Doors ○ By Operations

□ Only Warnings
□ Only Rejections

- **Filter by Date and Time:**

  In order to set filters by Date and Time, it is necessary to enter the dates and times in the fields “From” and “To”, and select the option “None” in the field “Filter”.

  Then, you have to click “OK” and the result is displayed.



Select Openings f...

Date
From 22/04/2016
To 21/01/2017

Time
From 00:00:00
To 23:59:59

Filter
● None ○ By Users
○ By Doors ○ By Operations

□ Only Warnings
□ Only Rejections

- **Filter by Doors:**

  In the field “Filter”, the option “By Doors” is selected and the following screen is displayed:

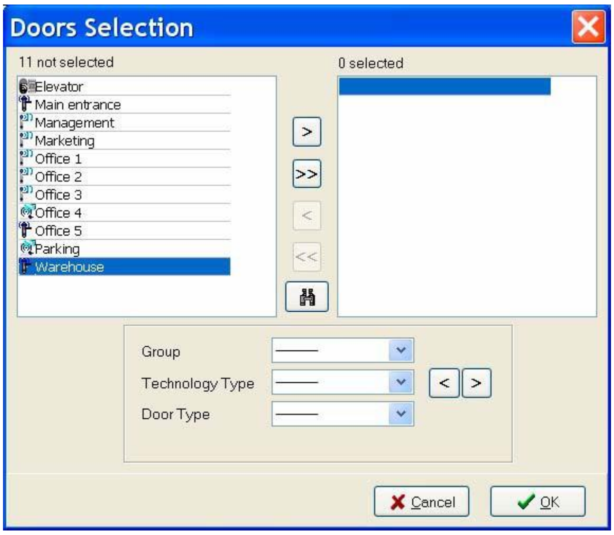
  This screen allows selecting the doors whose events you want to see.

  The doors can be selected individually or by “Groups”.

  They can also be selected by “Technology Type” or “Door Type”.

  It is also possible to conduct searches by means of the 🔍 button.

  After selecting the doors desired, click “OK” and the previous screen will be displayed. Click “OK” again and the events from the doors selected will be displayed.



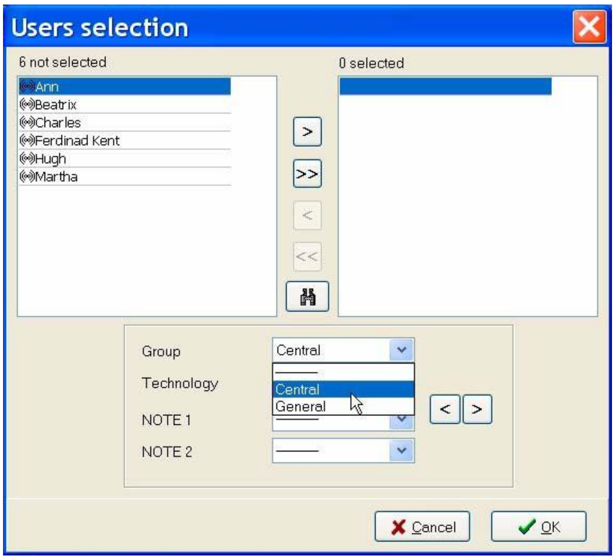
- **Filter by Users:**

  In order to set filters by Users, select the option “By User” in the field “Filter”. The following screen will be displayed:

  In this screen, it is possible to select, individually or by groups, those users whose events you want to see.

  It is also possible to conduct searches by means of the 🔍 button.

  After selecting the users desired, click “OK” and the previous screen will be displayed. Click “OK” again and the events from the users selected will be displayed.

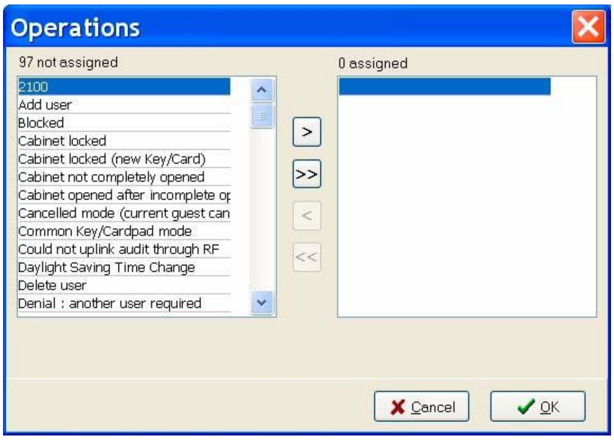


- **Filter by Operations:**

  In order to set filters according to the operations carried out, select the option "By Operations" and the following screen will be displayed:

  This screen allows selecting, from among the different types of possible operations, the ones whose events you want to see.

  After selecting the operations desired, click "OK" and the previous screen will be displayed. Click "OK" again and the events corresponding to the operations selected will be displayed.



Operations

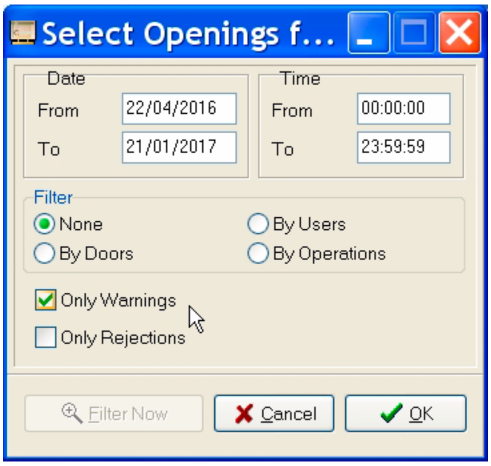
97 not assigned

2100
Add user
Blocked
Cabinet locked
Cabinet locked (new Key/Card)
Cabinet not completely opened
Cabinet opened after incomplete op
Cancelled mode (current guest can
Common Key/Cardpad mode
Could not uplink audit through RF
Daylight Saving Time Change
Delete user
Denial : another user required

0 assigned

- **"Only Warnings" filter:**

  It is possible to apply an additional filtering, so that only the warnings are shown. For this purpose, select the option "Only Warnings" and then click "OK".



Select Openings f...

Date
From 22/04/2016
To 21/01/2017

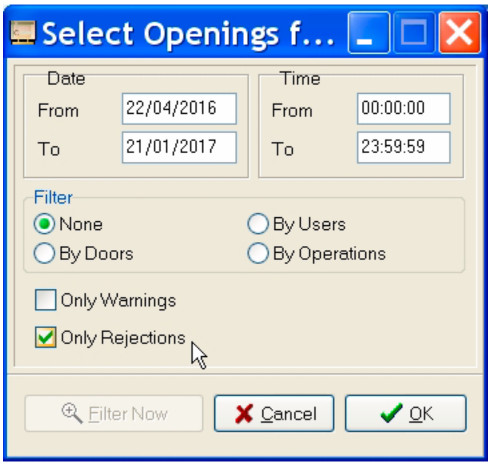
Time
From 00:00:00
To 23:59:59

Filter
● None ○ By Users
○ By Doors ○ By Operations

☑ Only Warnings
□ Only Rejections

- **"Only Rejections" filter:**

  You also have the possibility of filtering to view only the rejections. Select the option "Only Rejections" and, then click "OK".



Select Openings f...

Date
From 22/04/2016
To 21/01/2017

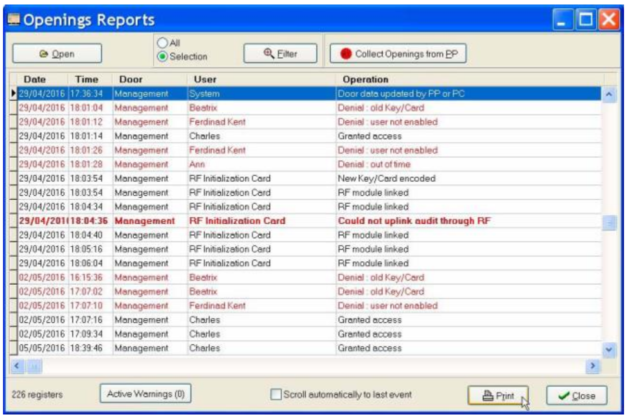
Time
From 00:00:00
To 23:59:59

Filter
● None ○ By Users
○ By Doors ○ By Operations

□ Only Warnings
☑ Only Rejections

## Print

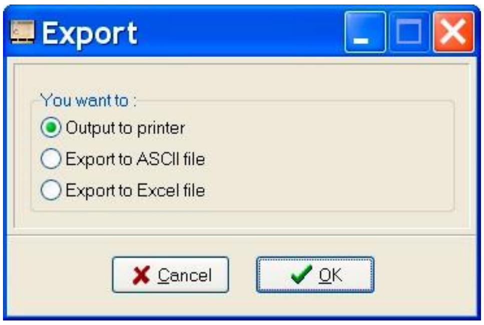
It is possible to print the opening register by clicking the "Print" button located at the bottom right.



| Date | Time | Door | User | Operation |
|---|---|---|---|---|
| 29/04/2016 | 17:36:34 | Management | System | Door data updated by PP or PC |
| 29/04/2016 | 18:01:04 | Management | Beatrix | Denial : old Key/Card |
| 29/04/2016 | 18:01:12 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:14 | Management | Charles | Granted access |
| 29/04/2016 | 18:01:26 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:28 | Management | Ann | Denial : out of time |
| 29/04/2016 | 18:03:54 | Management | RF Initialization Card | New Key/Card encoded |
| 29/04/2016 | 18:03:54 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:04:34 | Management | RF Initialization Card | RF module linked |
| **29/04/201** | **18:04:36** | **Management** | **RF Initialization Card** | **Could not uplink audit through RF** |
| 29/04/2016 | 18:04:40 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:05:16 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:06:04 | Management | RF Initialization Card | RF module linked |
| 02/05/2016 | 16:15:36 | Management | Beatrix | Denial : old Key/Card |
| 02/05/2016 | 17:07:02 | Management | Beatrix | Denial : old Key/Card |
| 02/05/2016 | 17:07:10 | Management | Ferdinad Kent | Denial : user not enabled |
| 02/05/2016 | 17:07:16 | Management | Charles | Granted access |
| 02/05/2016 | 17:09:34 | Management | Charles | Granted access |
| 05/05/2016 | 18:39:46 | Management | Charles | Granted access |

226 registers

After clicking the "Print" button, three possible options are displayed:



You want to :

● Output to printer

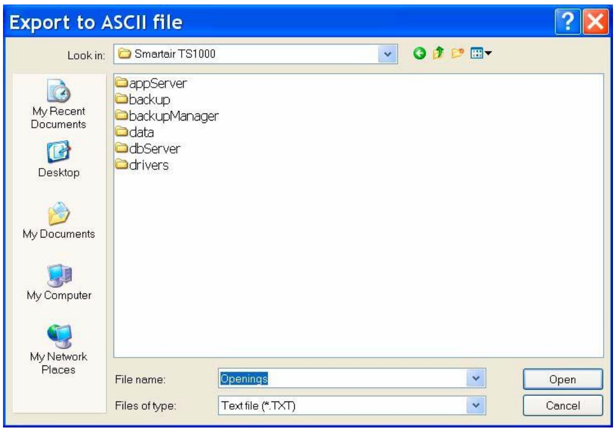
○ Export to ASCII file

○ Export to Excel file

- **Output to printer:**
  allows printing the opening register on the default printer of the computer being used.

- **Export to ASCII file:**
  if you select this option and click "OK", a window will be displayed which allows selecting the location to which you want to export the "Openings.txt" text file, which is created to hold the events.

  It is also possible to modify the name of that file as you wish.



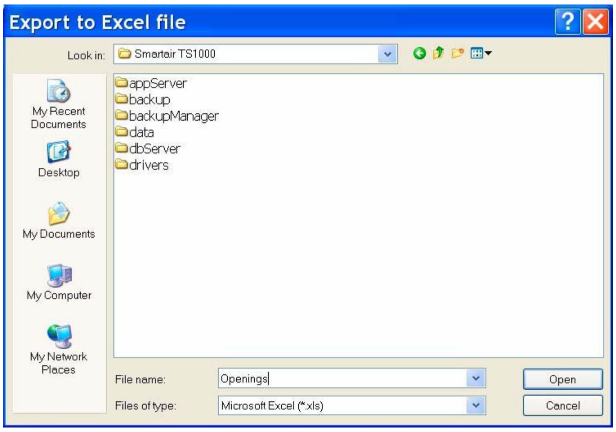
Look in: Smartair TS1000

File name: Openings

Files of type: Text file (*.TXT)

- **Export to Excel file:**
  by selecting this option and, then, clicking "OK", a window will be displayed which allows selecting the location to which you want to export the "Openings.xls" text file, which is created to hold the events.

  It is also possible to modify the name of that file as you wish.



Look in: Smartair TS1000

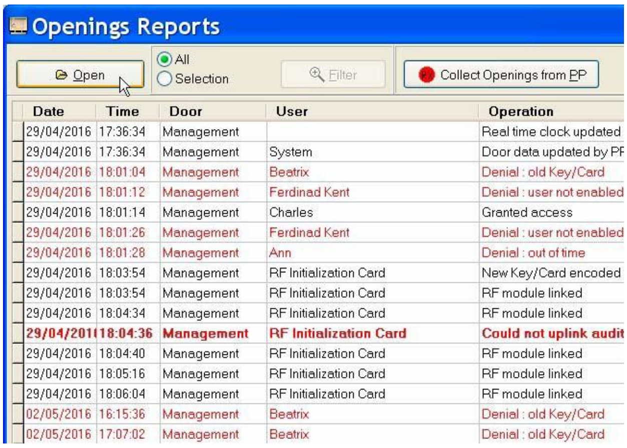
File name: Openings

Files of type: Microsoft Excel (*.xls)

## Open

The “Open” button, located at the top left, allows finding and opening registers which have been previously saved in order to be able to view them when so desired. These are the records which have been saved manually, or automatically during the scheduled purges (see “*Purge auditors periodically”* on page 59).

If you click this button, a window will be displayed allowing you to find these old records.



Openings Reports

Open | ● All ○ Selection | Filter | Collect Openings from PP

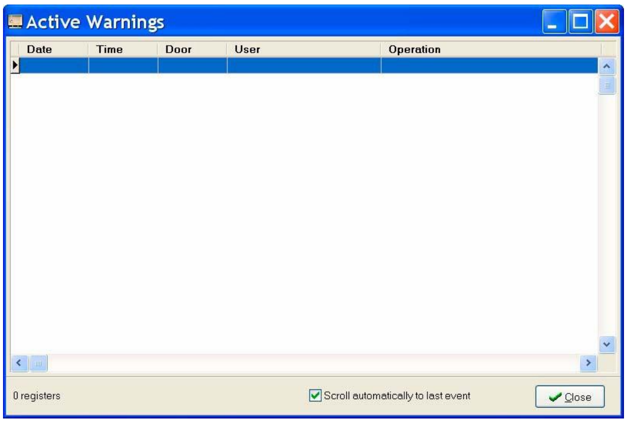
| Date | Time | Door | User | Operation |
|---|---|---|---|---|
| 29/04/2016 | 17:36:34 | Management | | Real time clock updated |
| 29/04/2016 | 17:36:34 | Management | System | Door data updated by PF |
| 29/04/2016 | 18:01:04 | Management | Beatrix | Denial : old Key/Card |
| 29/04/2016 | 18:01:12 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:14 | Management | Charles | Granted access |
| 29/04/2016 | 18:01:26 | Management | Ferdinad Kent | Denial : user not enabled |
| 29/04/2016 | 18:01:28 | Management | Ann | Denial : out of time |
| 29/04/2016 | 18:03:54 | Management | RF Initialization Card | New Key/Card encoded |
| 29/04/2016 | 18:03:54 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:04:34 | Management | RF Initialization Card | RF module linked |
| **29/04/201** | **18:04:36** | **Management** | **RF Initialization Card** | **Could not uplink audit** |
| 29/04/2016 | 18:04:40 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:05:16 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:06:04 | Management | RF Initialization Card | RF module linked |
| 02/05/2016 | 16:15:36 | Management | Beatrix | Denial : old Key/Card |
| 02/05/2016 | 17:07:02 | Management | Beatrix | Denial : old Key/Card |

## Active Alerts

By clicking the “Active Alerts” button, located at the bottom, a new screen will be opened, where the alerts which are active at that moment are shown.

No Active Alert is displayed in the example.

For more information on alerts, see *“Alerts”* on page 175.



Active Warnings

| Date | Time | Door | User | Operation |
|---|---|---|---|---|

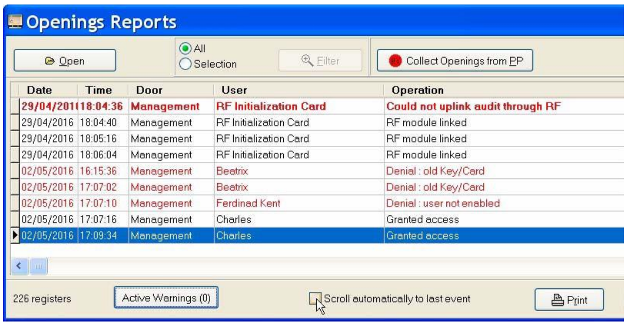
0 registers

☑ Scroll automatically to last event

Close

## Scroll automatically to last event

There is an option, called “Scroll automatically to last event”, which is selected by default, that updates the screen every 2 seconds approximately, adding any new event which has been generated. After each refresh, the cursor is located at the last event recorded. If you want to go through the events earlier than those shown on the screen, you need to disable this check box.



Openings Reports

Open | ● All ○ Selection | Filter | Collect Openings from PP

| Date | Time | Door | User | Operation |
|---|---|---|---|---|
| **29/04/201** | **18:04:36** | **Management** | **RF Initialization Card** | **Could not uplink audit through RF** |
| 29/04/2016 | 18:04:40 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:05:16 | Management | RF Initialization Card | RF module linked |
| 29/04/2016 | 18:06:04 | Management | RF Initialization Card | RF module linked |
| 02/05/2016 | 16:15:36 | Management | Beatrix | Denial : old Key/Card |
| 02/05/2016 | 17:07:02 | Management | Beatrix | Denial : old Key/Card |
| 02/05/2016 | 17:07:10 | Management | Ferdinad Kent | Denial : user not enabled |
| 02/05/2016 | 17:07:16 | Management | Charles | Granted access |
| 02/05/2016 | 17:09:34 | Management | Charles | Granted access |

226 registers

Active Warnings (0)

☐ Scroll automatically to last event

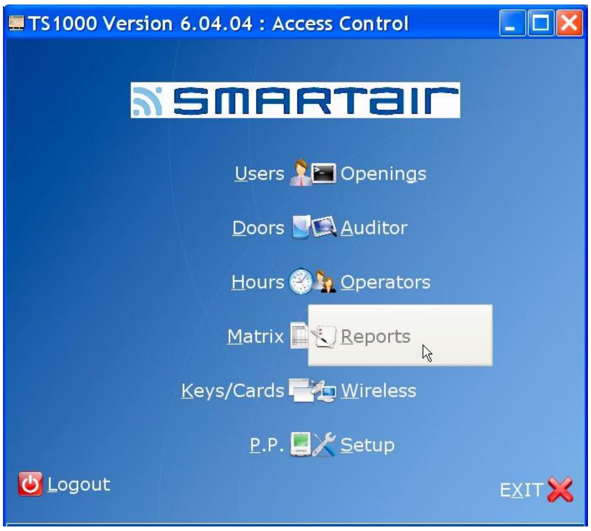
Print

This is useful if the register is very large because, by selecting this check box, the most recent events will be automatically shown.

## K.4 REPORTS

The “Reports” menu allows generating and printing what has been defined in the locking plan, that is to say, users lists, doors lists, locking plans for users, etc.

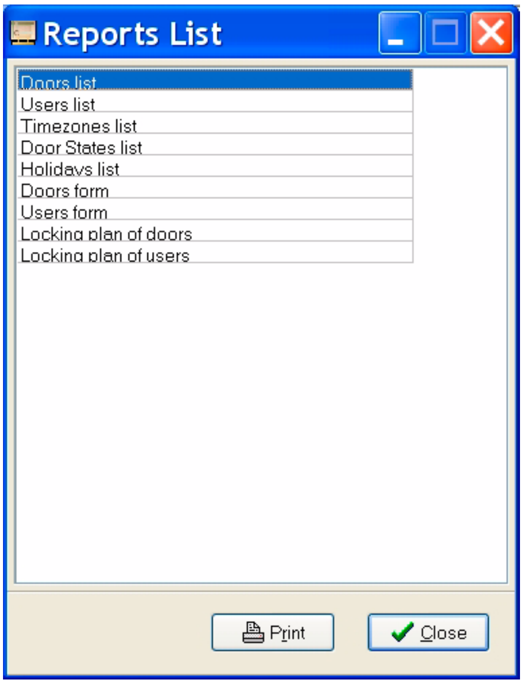
In order to access the “Reports” screen, on the TS1000 main screen, click “Reports”.



The following screen is displayed:

All the types of reports which can be printed are displayed on this screen.

There are three different types of processes to be followed in order to print successfully, depending on the type of report selected. Each of the three types is explained below.

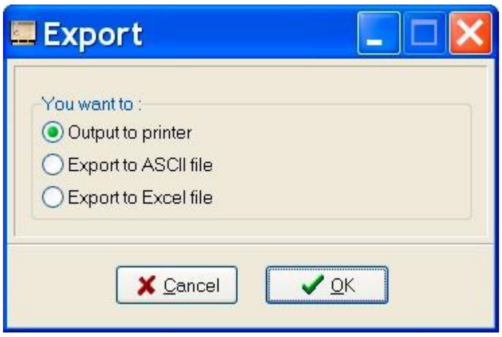

Reports List

- Doors list
- Users list
- Timezones list
- Door States list
- Holidays list
- Doors form
- Users form
- Locking plan of doors
- Locking plan of users

### Doors List, Users List (Type 1)

If the Doors List or Users List is selected and the “Print” button is clicked, a screen is displayed where three options are shown:

- Output to printer
- Export to ASCII file
- Export to Excel file

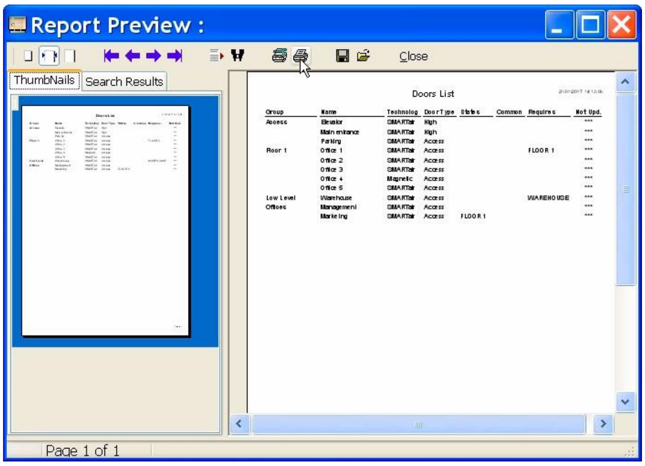

Export

You want to :

● Output to printer
○ Export to ASCII file
○ Export to Excel file

If the option “Output to printer” is selected, a screen is displayed with a preview of what will be sent to the printer.

By clicking the “Print” button, the information is sent to the printer configured for this purpose, which can be modified with the “Printer Setup” button.



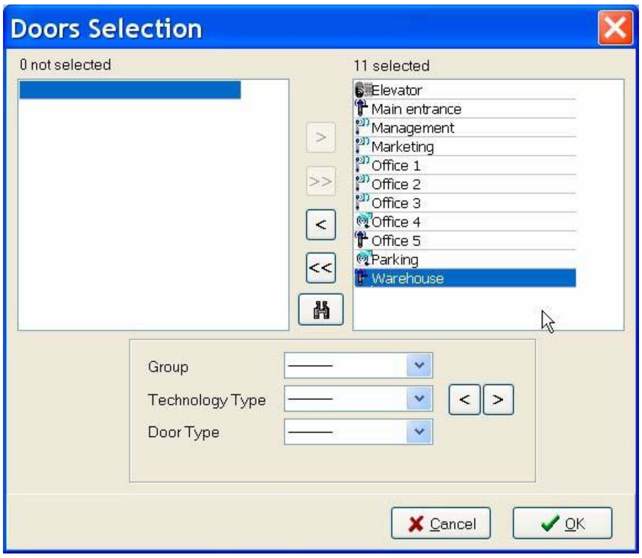
Doors List

21/01/2017 14:13:06

| Group | Name | Technolog | Door Type | States | Common | Requires | Not Upd. |
|---|---|---|---|---|---|---|---|
| Access | Elevator | SMARTair | High | | | | *** |
| | Main entrance | SMARTair | High | | | | *** |
| | Parking | SMARTair | Access | | | | *** |
| Floor 1 | Office 1 | SMARTair | Access | | | FLOOR 1 | *** |
| | Office 2 | SMARTair | Access | | | | *** |
| | Office 3 | SMARTair | Access | | | | *** |
| | Office 4 | Magnetic | Access | | | | *** |
| | Office 5 | SMARTair | Access | | | | *** |
| Low Level | Warehouse | SMARTair | Access | | | WAREHOUSE | *** |
| Offices | Management | SMARTair | Access | | | | *** |
| | Marketing | SMARTair | Access | FLOOR 1 | | | *** |

If the option “Export to ASCII file” is selected and the “OK” is clicked, a window is opened which allows selecting the doors (or users) you want to be displayed on the list. By default, all the doors (or users) selected are displayed.

After selecting the doors (or users) you want, click “OK”.



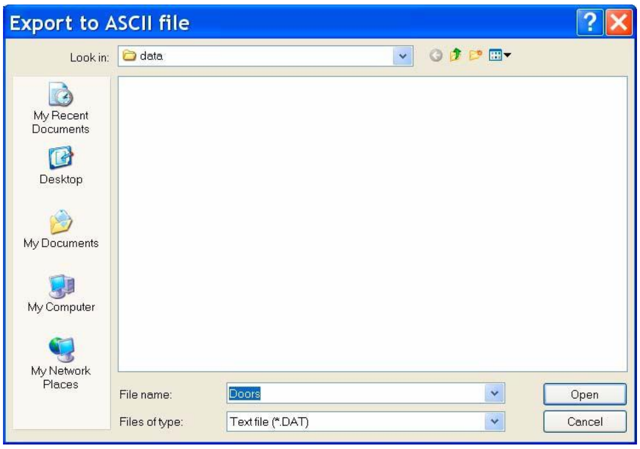
0 not selected

11 selected

- Elevator
- Main entrance
- Management
- Marketing
- Office 1
- Office 2
- Office 3
- Office 4
- Office 5
- Parking
- Warehouse

After clicking “OK”, a window is displayed requesting the location to which to save the “Doors.dat” (or “Users.dat”) file.

If you wish, the name of this file can be changed.

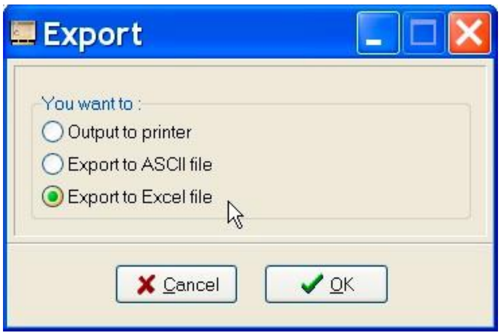


Look in: data

File name: Doors

Files of type: Text file (*.DAT)

If the option “Export to Excel file” is clicked, something similar to the previous case happens, that is to say, a window is displayed for selecting the doors (or users) you want and, after making the selection and clicking “OK”, another window is displayed for selecting the name and location of the file to be saved.



You want to :

○ Output to printer

○ Export to ASCII file

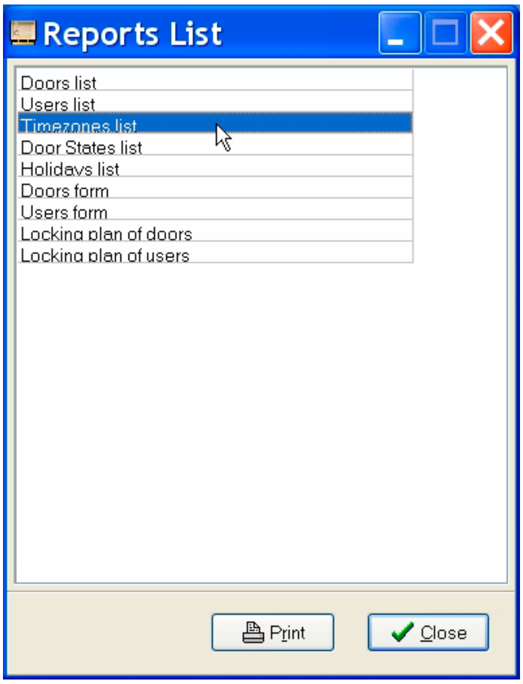
● Export to Excel file

## Timezones List, Door States List, Holidays List (Type 2)

If, in the “Reports” window, any of these reports is selected:

- timezones list,
- door states list,
- holidays list,

and then “Print” is clicked, a window is displayed showing a preview of what will be sent to the printer.



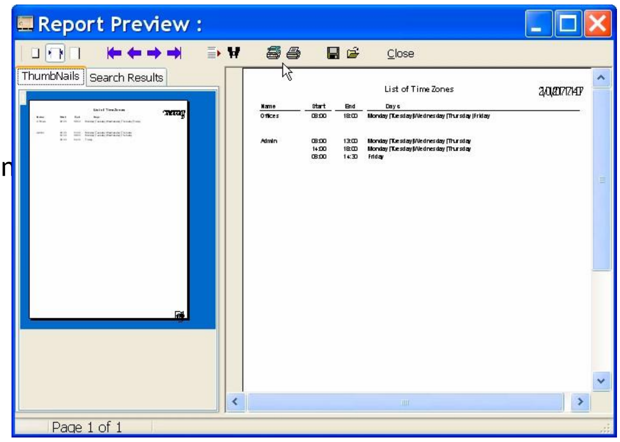
Reports List

Doors list
Users list
Timezones list
Door States list
Holidays list
Doors form
Users form
Locking plan of doors
Locking plan of users

The window showing the preview allows configuring the printer with the “Printer Setup” button.

In order to print, click the “Print” button

By means of the corresponding buttons, it allows conducting searches for specific pages and texts, which allows you to select what you want to print.



Report Preview :

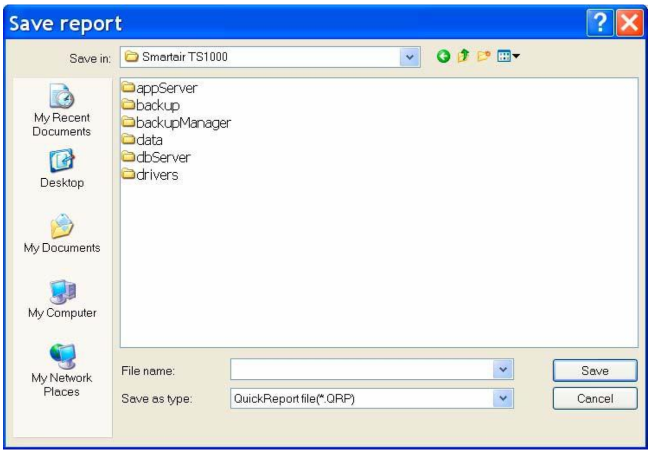
List of Time Zones 2/01/2007 17:14:07

| Name | Start | End | Days |
|---|---|---|---|
| Offices | 08:00 | 18:00 | Monday \|Tuesday\|Wednesday \|Thursday \|Friday |
| Admin | 08:00 | 13:00 | Monday \|Tuesday\|Wednesday \|Thursday |
| | 14:00 | 18:00 | Monday \|Tuesday\|Wednesday \|Thursday |
| | 08:00 | 14:30 | Friday |

Page 1 of 1

It also allows saving reports, in *.QRP format, as well as opening other reports which have been previously saved.

This is done with the “Save Report” and “Load Report” buttons, respectively.



Save report

Save in: Smartair TS1000

appServer
backup
backupManager
data
dbServer
drivers

File name:

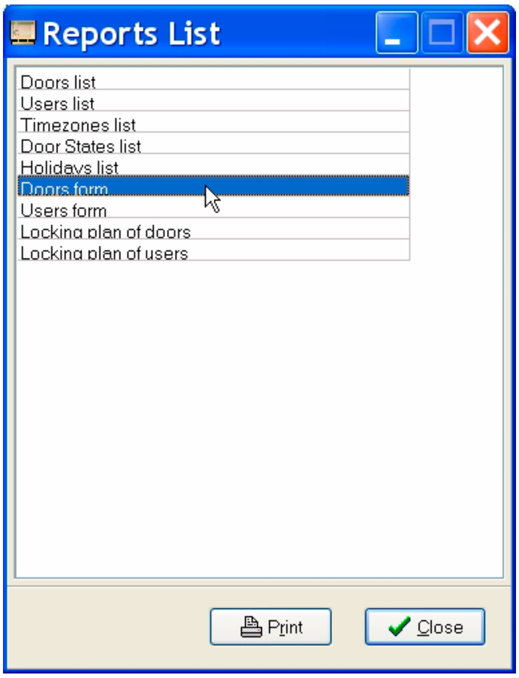
Save as type: QuickReport file(*.QRP)

## Doors Form, Users Form, Locking Plan for a Door, Locking Plan for a User (Type 3)

If, in the “Reports” window, any of these reports is selected:

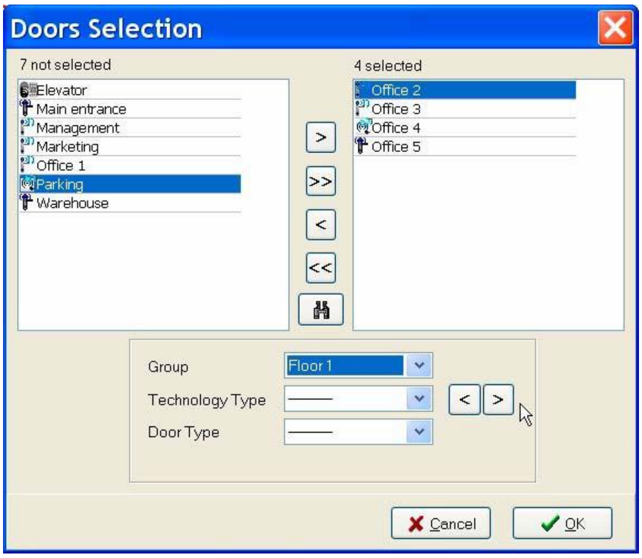
- doors form,
- users form,
- locking plan for a door,
- locking plan for a user,

and then “Print” is clicked, a window is displayed which allows selecting the forms (or plans) you want to be displayed on the report.



On this screen, the doors (or users) whose forms or locking plans you want to see are selected.

After the selection, click “OK”.



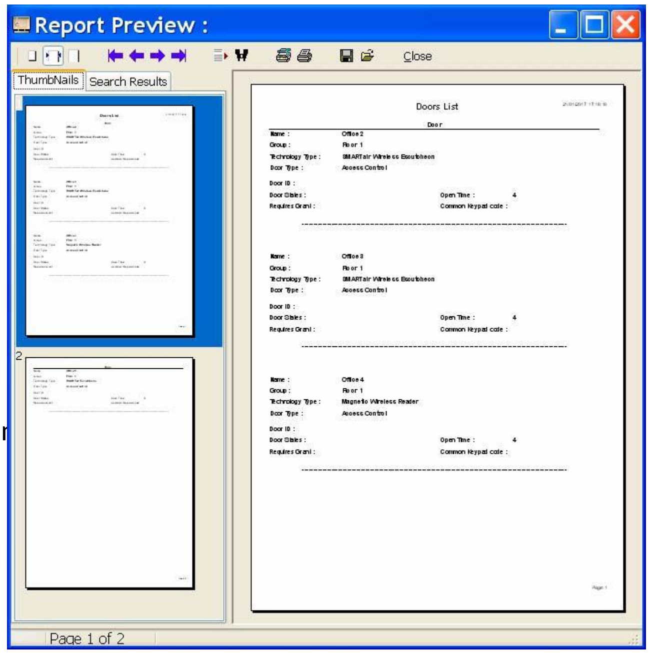
Group: Floor 1
Technology Type: ——
Door Type: ——

After clicking “OK”, a window is displayed where the preview of what will be sent to the printer is shown.

Just like in the previous cases, it is possible to conduct searches, configure the printer, save the report or load another one which has been previously saved.

In order to print the report, click “Pri

In order to exit without printing, click “Close”.



Doors List

Door

Name : Office 2
Group : Floor 1
Technology Type : SMARTair Wireless Escutcheon
Door Type : Access Control
Door ID :
Door States : Open Time : 4
Requires Grant : Common Keypad code :

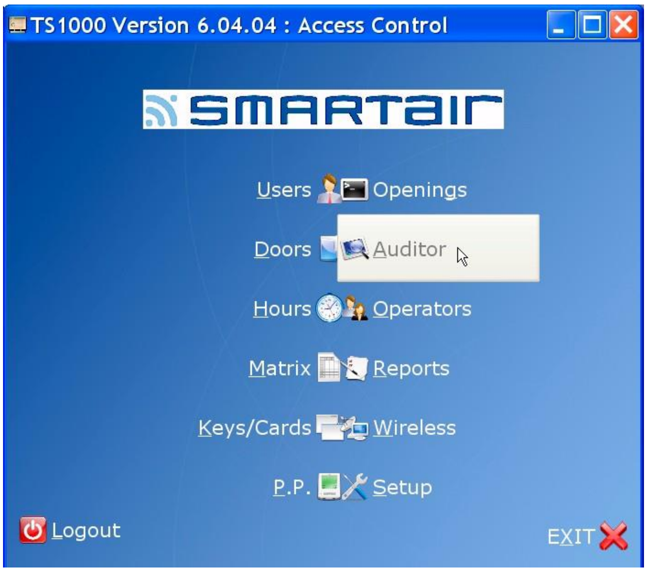
Name : Office 3
Group : Floor 1
Technology Type : SMARTair Wireless Escutcheon
Door Type : Access Control
Door ID :
Door States : Open Time : 4
Requires Grant : Common Keypad code :

Name : Office 4
Group : Floor 1
Technology Type : Magnetic Wireless Reader
Door Type : Access Control
Door ID :
Door States : Open Time : 4
Requires Grant : Common Keypad code :

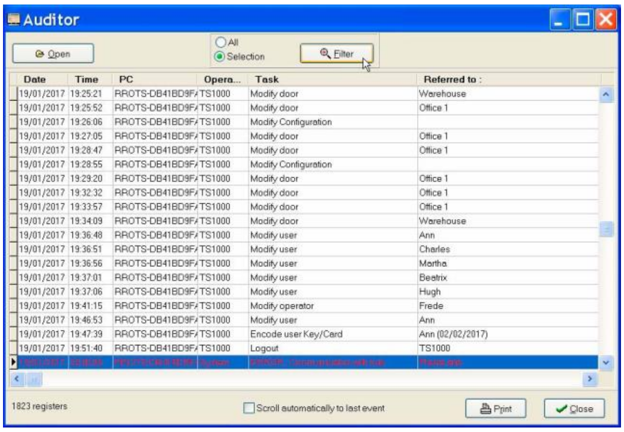
## K.5 AUDITOR

The Auditor is a tool responsible for recording, in the form of a database, absolutely all the actions which the different operators perform in the TS1000 management software, which allows filtering and viewing as desired.

In order to access the Auditor, click “Auditor” on the main screen of the TS1000.



The following screen is displayed:



| | Date | Time | PC | Opera... | Task | Referred to : |
|---|---|---|---|---|---|---|
| | 19/01/2017 | 19:25:21 | RROTS-DB41BD9F/ | TS1000 | Modify door | Warehouse |
| | 19/01/2017 | 19:25:52 | RROTS-DB41BD9F/ | TS1000 | Modify door | Office 1 |
| | 19/01/2017 | 19:26:06 | RROTS-DB41BD9F/ | TS1000 | Modify Configuration | |
| | 19/01/2017 | 19:27:05 | RROTS-DB41BD9F/ | TS1000 | Modify door | Office 1 |
| | 19/01/2017 | 19:28:47 | RROTS-DB41BD9F/ | TS1000 | Modify door | Office 1 |
| | 19/01/2017 | 19:28:55 | RROTS-DB41BD9F/ | TS1000 | Modify Configuration | |
| | 19/01/2017 | 19:29:20 | RROTS-DB41BD9F/ | TS1000 | Modify door | Office 1 |
| | 19/01/2017 | 19:32:32 | RROTS-DB41BD9F/ | TS1000 | Modify door | Office 1 |
| | 19/01/2017 | 19:33:57 | RROTS-DB41BD9F/ | TS1000 | Modify door | Office 1 |
| | 19/01/2017 | 19:34:09 | RROTS-DB41BD9F/ | TS1000 | Modify door | Warehouse |
| | 19/01/2017 | 19:36:48 | RROTS-DB41BD9F/ | TS1000 | Modify user | Ann |
| | 19/01/2017 | 19:36:51 | RROTS-DB41BD9F/ | TS1000 | Modify user | Charles |
| | 19/01/2017 | 19:36:56 | RROTS-DB41BD9F/ | TS1000 | Modify user | Martha |
| | 19/01/2017 | 19:37:01 | RROTS-DB41BD9F/ | TS1000 | Modify user | Beatrix |
| | 19/01/2017 | 19:37:06 | RROTS-DB41BD9F/ | TS1000 | Modify user | Hugh |
| | 19/01/2017 | 19:41:15 | RROTS-DB41BD9F/ | TS1000 | Modify operator | Frede |
| | 19/01/2017 | 19:46:53 | RROTS-DB41BD9F/ | TS1000 | Modify user | Ann |
| | 19/01/2017 | 19:47:39 | RROTS-DB41BD9F/ | TS1000 | Encode user Key/Card | Ann (02/02/2017) |
| | 19/01/2017 | 19:51:40 | RROTS-DB41BD9F/ | TS1000 | Logout | TS1000 |
| ▶ | [illegible] | [illegible] | [illegible] | System | [illegible] | [illegible] |

1823 registers

□ Scroll automatically to last event

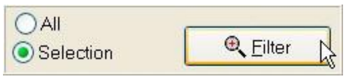
On this screen, all the operations carried out on the TS1000 are displayed in chronological order.

The following information is shown:

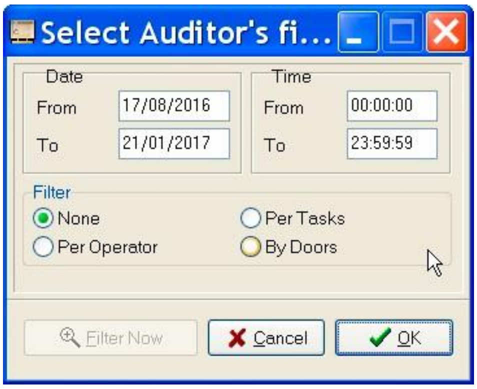
- **Date:** date when the operation was carried out.
- **Time:** time when the operation was carried out.
- **PC:** computer where the operation was carried out. This information is very useful when the site is on a network.
- **Operator:** name of the operator who carried out the operation.
- **Task:** operation carried out.
- **Referred to:** what was actually affected by the operation carried out.

Just as with the Opening Register, filters can be applied to the information in the Auditor file.

By selecting the option "Selection", the "Filter" button is enabled in the field "Filter".



When clicking the "Filter" button, the following screen is displayed:



Date

From 17/08/2016

To 21/01/2017

Time

From 00:00:00

To 23:59:59

Filter

● None ○ Per Tasks

○ Per Operator ○ By Doors

This screen allows applying filters:

- by Date and Time,
- by Operator,
- by Tasks,
- by Doors.

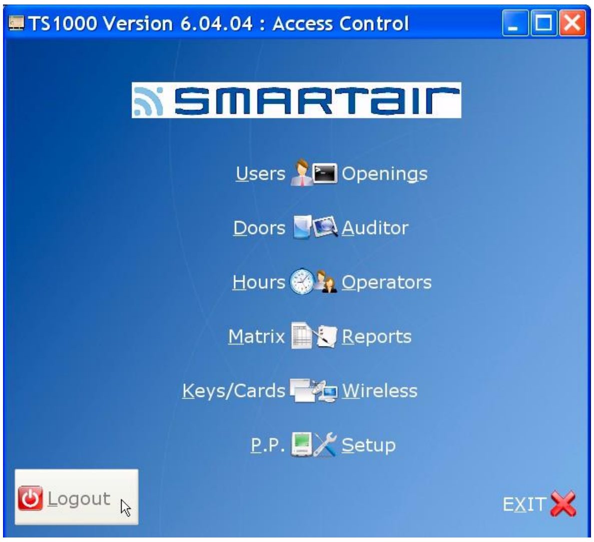
The way to proceed is similar to the one corresponding to the Openings menu, explained in *"Analysis of the openings collected"* on page 158.

## *K.6 LOGIN AND LOGOUT*

Clicking "Logout", on the main screen and finishes the session in progress, but without closing the programme.

All the options from the main screen are disabled and, as a result, it is not possible to access any menu, although the screen remains open.

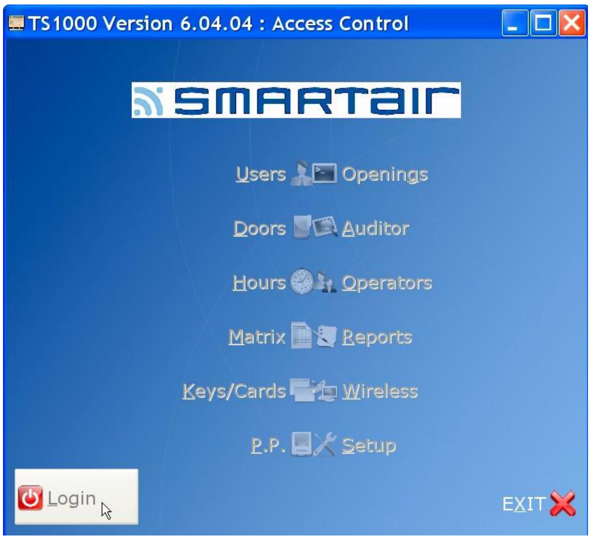
In addition, the "Logout" button turns into "Login".



If you want to use the software again, it is necessary to start a new session, by clicking "Login".

Then, a window is displayed requesting an "Operator Name" and "Password".

By entering the Operator Name and its corresponding Password, the corresponding session will be started, with the access levels corresponding to the Operator whose name and password have been entered.

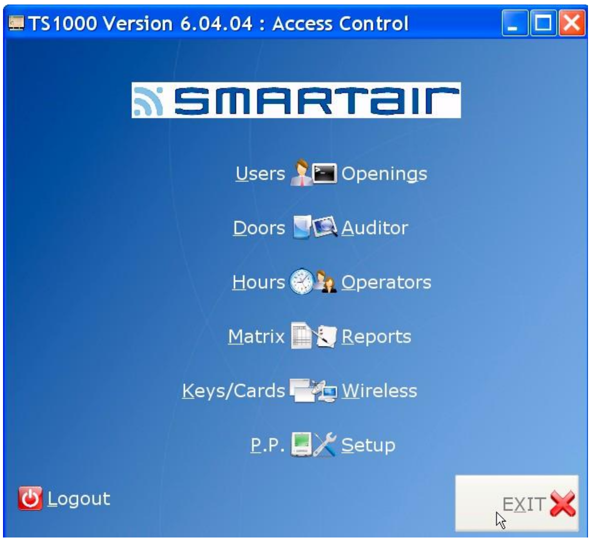


Only the buttons whose options are accessible to the operator identified will be enabled, according to their access levels.

## K.7 LOGOUT

In order to exit the programme, click the “Exit” button, which closes the main window.

This is the correct way to leave the programme.



## K.8 SITE MANAGEMENT THROUGH THE WEB

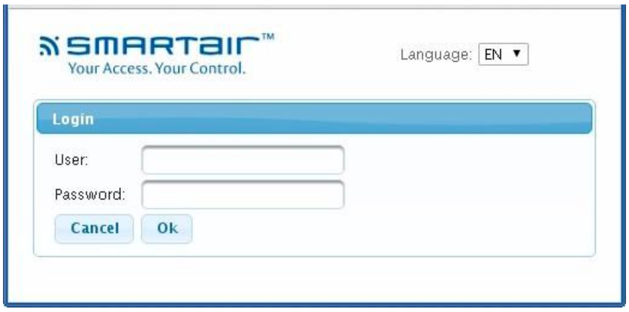
It is also possible to manage the site by means of the Web application, without accessing the TS1000 software. For this purpose, it is necessary to have the GlassFish service installed and running.

The Web application is accessed through the following URL address:

https://host:8181/TesaSmartairPlatform

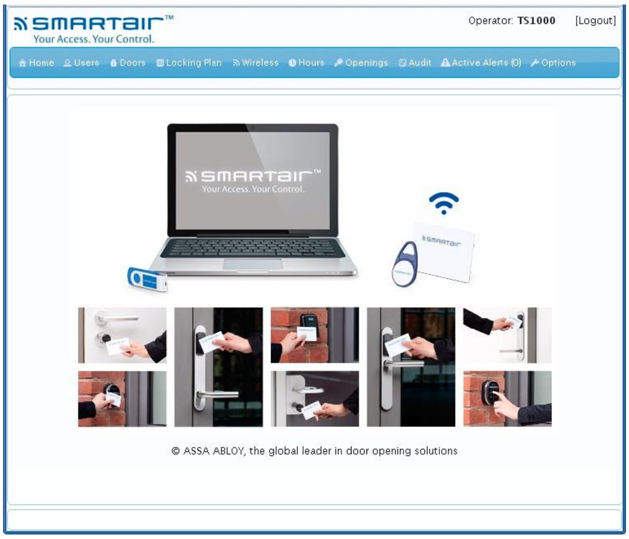
The application is accessed through an operator (User and Password) defined in the TESA - SMARTair TS1000 application.

For more information on the User and Password, see *"E.1 Operator Name and Password"* on page 57.



By means of this application, it is possible to access the system menus, similarly to how this is done in the TS1000 application. The following menus are available:

- Users
- Doors
- Matrix
- Wireless
- Hours
- Openings
- Auditor
- Active Alerts
- Settings

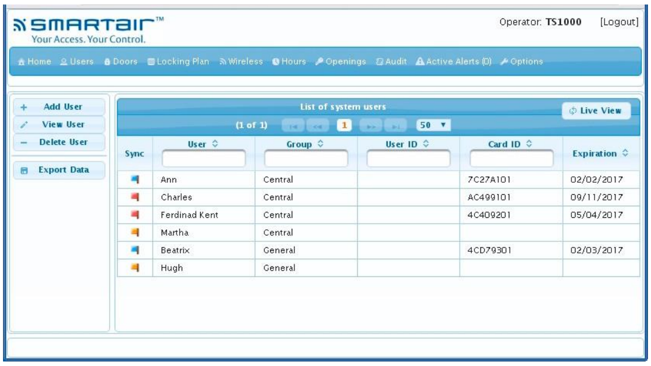


### Users menu

By means of this menu, it is possible to see the forms of the system users and, in addition, you can:

- Add User
- View User
- Delete User
- Export Data

For more information on these functions, see *"F.2 "Users" menu"* on page 69.



List of system users

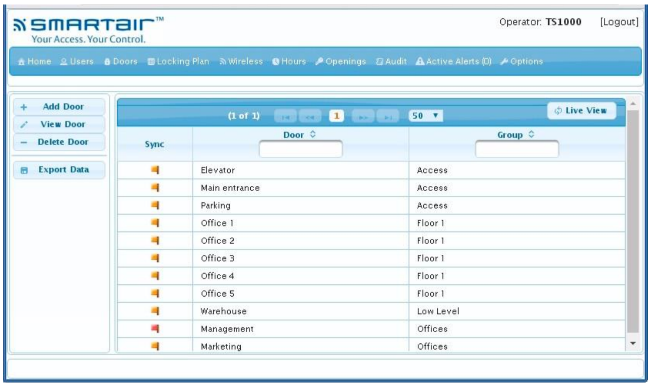
| Sync | User | Group | User ID | Card ID | Expiration |
|---|---|---|---|---|---|
| 🟦 | Ann | Central | | 7C27A101 | 02/02/2017 |
| 🟥 | Charles | Central | | AC499101 | 09/11/2017 |
| 🟥 | Ferdinad Kent | Central | | 4C409201 | 05/04/2017 |
| 🟧 | Martha | Central | | | |
| 🟦 | Beatrix | General | | 4CD79301 | 02/03/2017 |
| 🟧 | Hugh | General | | | |

## Doors menu

This menu allows viewing the doors defined in the system and, addition, you can:

- Add Door
- View Door
- Delete Door
- Export Data

For more information on these functions, see *"F.3 "Doors" menu"* on page 74.

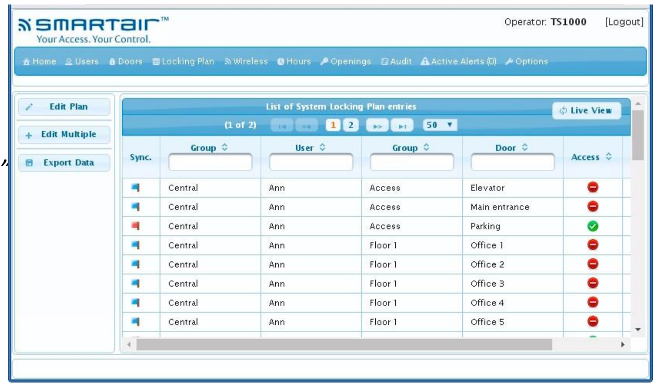


| Sync | Door | Group |
|---|---|---|
| ⚑ | Elevator | Access |
| ⚑ | Main entrance | Access |
| ⚑ | Parking | Access |
| ⚑ | Office 1 | Floor 1 |
| ⚑ | Office 2 | Floor 1 |
| ⚑ | Office 3 | Floor 1 |
| ⚑ | Office 4 | Floor 1 |
| ⚑ | Office 5 | Floor 1 |
| ⚑ | Warehouse | Low Level |
| ⚑ | Management | Offices |
| ⚑ | Marketing | Offices |

## Matrix

By means of the matrix, the users, doors and hours are related, thus configuring the locking plan.

For more information, see *"F.5 Matrix"* on page 86.

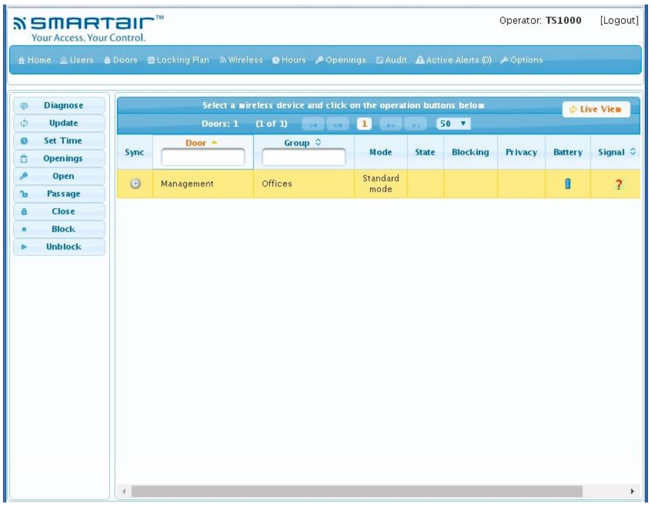


List of System Locking Plan entries

| Sync. | Group | User | Group | Door | Access |
|---|---|---|---|---|---|
| ⚑ | Central | Ann | Access | Elevator | ⛔ |
| ⚑ | Central | Ann | Access | Main entrance | ⛔ |
| ⚑ | Central | Ann | Access | Parking | ✓ |
| ⚑ | Central | Ann | Floor 1 | Office 1 | ⛔ |
| ⚑ | Central | Ann | Floor 1 | Office 2 | ⛔ |
| ⚑ | Central | Ann | Floor 1 | Office 3 | ⛔ |
| ⚑ | Central | Ann | Floor 1 | Office 4 | ⛔ |
| ⚑ | Central | Ann | Floor 1 | Office 5 | ⛔ |

## Wireless Doors

It will be possible to interact with the wireless devices which have been configured, the following operations being available:



Select a wireless device and click on the operation buttons below

| Sync | Door | Group | Mode | State | Blocking | Privacy | Battery | Signal |
|---|---|---|---|---|---|---|---|---|
| ◷ | Management | Offices | Standard mode | | | | ▮ | ? |

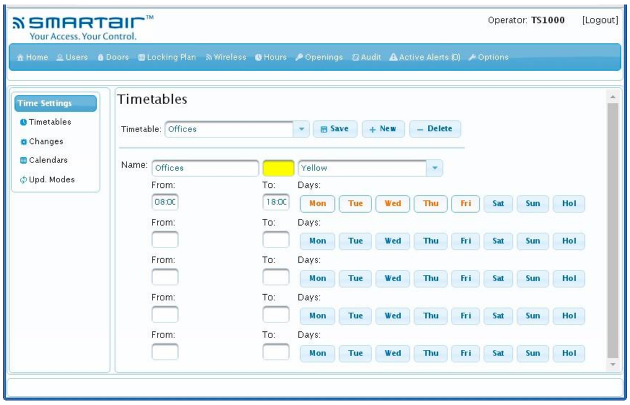
- Diagnostic: verifies the state of the wireless device of the door.
- Update: updates the wireless device of the door.
- Set Time: sets the time in the wireless device of the door.
- Openings: shows the events of the wireless device selected.
- Open: opens the device during the opening time set in the menu of the door.
- Passage: leaves the device open.
- Close: closes a device previously left open.
- Block/Unblock: blocks or unblocks the device, allowing only the authorised users (with the parameter "Can open blocked doors" enabled) to open the door.

For more information on these functions, see *"J.3 Management of wireless devices"* on page 150.

## Hours

The “Hours” menu allows configuring the different timetables which will be used to define the locking plan.

For more information, see *“F.4 “Hours” menu”* on page 81.



Timetables

Timetable: Offices

Name: Offices Yellow

From: 08:0C To: 18:0C Days:

From: To: Days:

From: To: Days:

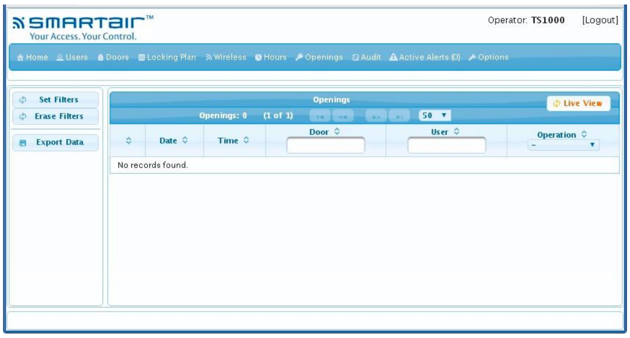
From: To: Days:

From: To: Days:

## Openings

The events of the door devices are shown in this tab, it being possible to apply filters.

For more information, see *“K.3 Openings”* on page 156.



Openings

Openings: 0 (1 of 1) 50

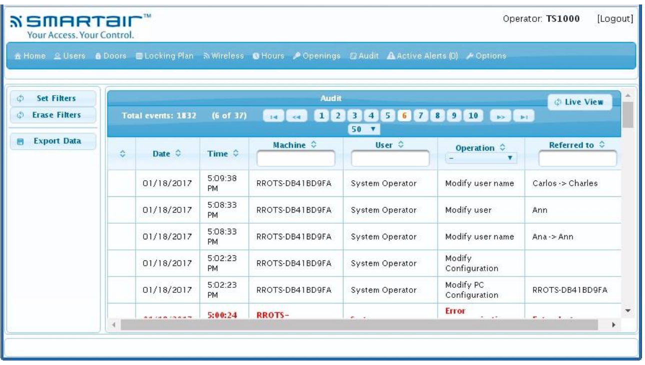
| Date | Time | Door | User | Operation |
|---|---|---|---|---|

No records found.

## Auditor

The Auditor shows all the operations carried out in the system, as well as who has carried them out.

For more information, see *“K.5 Auditor* on page 168.



Audit

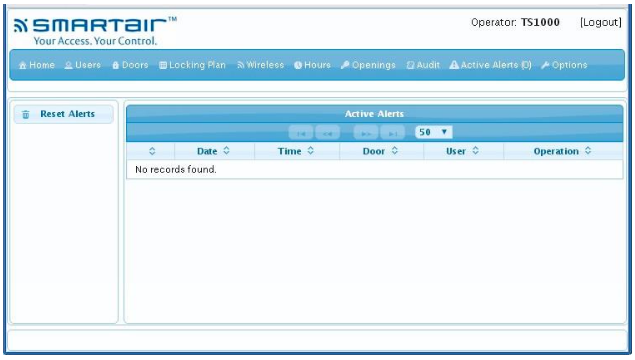
Total events: 1832 (6 of 37) 50

| Date | Time | Machine | User | Operation | Referred to |
|---|---|---|---|---|---|
| 01/18/2017 | 5:09:38 PM | RROTS-DB41BD9FA | System Operator | Modify user name | Carlos -> Charles |
| 01/18/2017 | 5:08:33 PM | RROTS-DB41BD9FA | System Operator | Modify user | Ann |
| 01/18/2017 | 5:08:33 PM | RROTS-DB41BD9FA | System Operator | Modify user name | Ana -> Ann |
| 01/18/2017 | 5:02:23 PM | RROTS-DB41BD9FA | System Operator | Modify Configuration | |
| 01/18/2017 | 5:02:23 PM | RROTS-DB41BD9FA | System Operator | Modify PC Configuration | RROTS-DB41BD9FA |
| | 5:00:24 | RROTS- | | Error | |

## Alerts

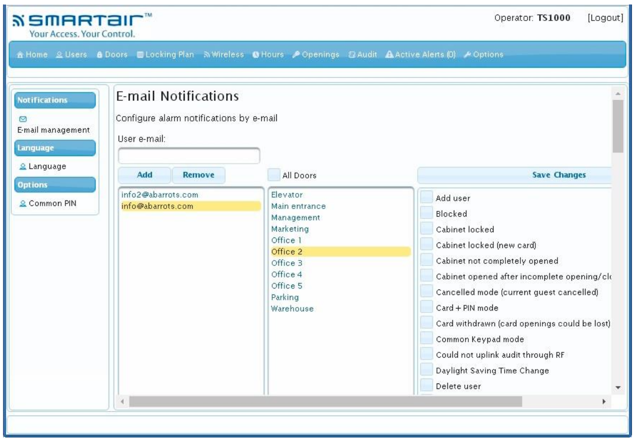
All the alerts which are active are shown on this screen.
The possible alerts are the following:

- Very low batteries
- RF module in Always Awake mode
- Real time clock unsettled
- Low batteries
- Intrusion
- Door left open
- Duress opening
- Power on reset
- Watchdog reset
- Reset



| | Date | Time | Door | User | Operation |
|---|---|---|---|---|---|
| No records found. | | | | | |

## Settings



E-mail Notifications

Configure alarm notifications by e-mail

User e-mail:

info2@abarrots.com
info@abarrots.com

□ All Doors

Elevator
Main entrance
Management
Marketing
Office 1
Office 2
Office 3
Office 4
Office 5
Parking
Warehouse

□ Add user
□ Blocked
□ Cabinet locked
□ Cabinet locked (new card)
□ Cabinet not completely opened
□ Cabinet opened after incomplete opening/cl
□ Cancelled mode (current guest cancelled)
□ Card + PIN mode
□ Card withdrawn (card openings could be lost)
□ Common Keypad mode
□ Could not uplink audit through RF
□ Daylight Saving Time Change
□ Delete user

- **E-mail notifications:**

  This allows defining one or more e-mail addresses for receipt of notifications when certain events take place at given doors.

  For this purpose, first of all, write the e-mail address where you want to receive the notifications in the field "User e-mail" and click Add. The e-mail address will be displayed in the column on the left.
  If you wish, you can repeat the process to add more e-mail addresses.

  Then, in the column on the left, select the e-mail address, in the central column, select the door and, in the column on the right, select the events desired. The notifications will be received at the address selected when the events selected take place at the door selected.

  Finally, click the "Save Changes" button.

  If you wish, repeat the process with another e-mail address.

  **NOTE:** for this setting to be available, the option "Enable applications for mobiles" in the "Licence" tab of the "Setup" menu of the TS1000 must be selected (for more information, see section *"Licence" tab* on page 59).

- **Language:** allows selecting the display language.

- **Common PINs:** allows defining a maximum of 7 common PINs. For more information, see *"Common PINs" tab* on page 65.

# L – Other Functions

# L – OTHER FUNCTIONS

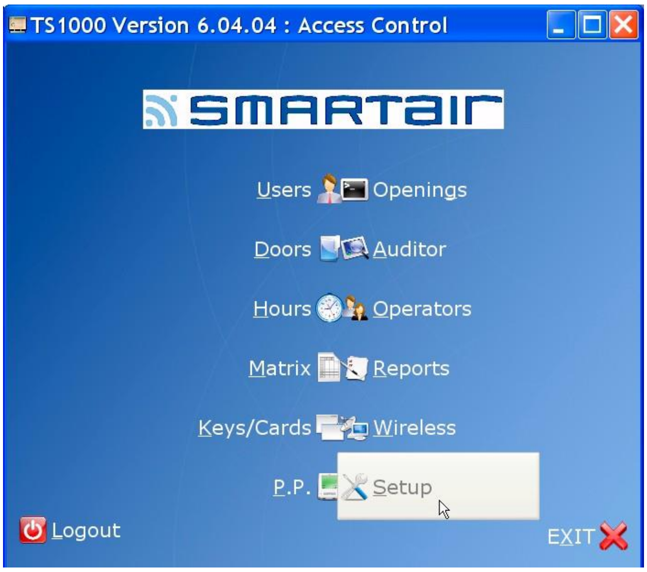
## L.1 INTRODUCTION

The TS1000 Access Control Software has several functions which are not used frequently, but are of great interest on many occasions.

Some of them are characteristic of certain sites and, where needed, they become essential throughout the lifespan of the site. As a result, they are generally configured during start-up.

Other functions may be necessary only on certain occasions, or for given users of the system, and, thus, remain available for use at any time.

This chapter describes what all these functions mean and how they work.

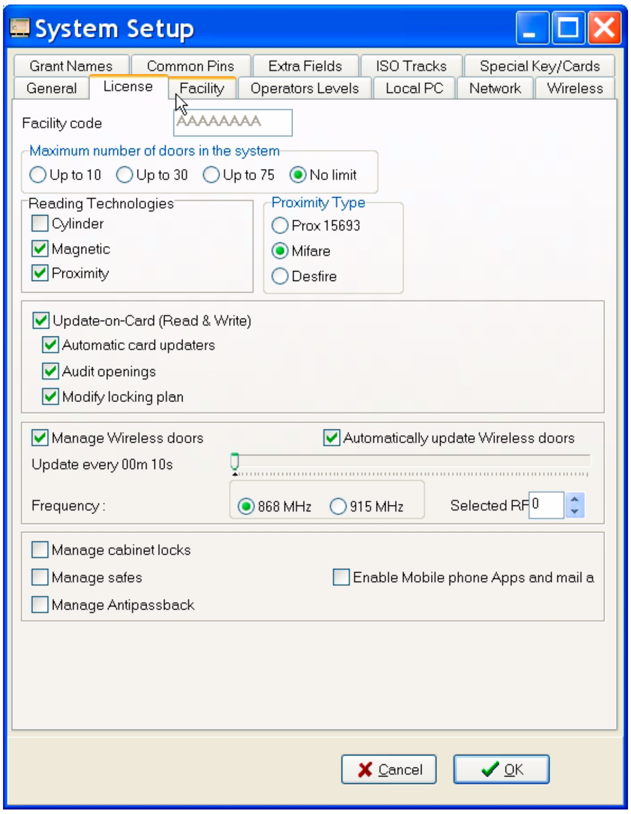


## L.2 SPECIAL FUNCTIONS (SETUP MENU)

If the TS1000 is accessed with the Operator Name and Password related to setup and maintenance (provided by the Technical Service of TESA), two more tabs are displayed in the Setup menu: “Licence” and “Facility”.

These two tabs are normally hidden, since the functions defined here do not tend to be modified once the system has been set up.

Basically, the “Licence” tab allows defining the technology which is to be used in the site. In general, it is only necessary to configure it once, during start-up. This tab is described in *“Licence” tab* on page 59.



Facility code AAAAAAAA

Maximum number of doors in the system
○ Up to 10 ○ Up to 30 ○ Up to 75 ● No limit

Reading Technologies
□ Cylinder
☑ Magnetic
☑ Proximity

Proximity Type
○ Prox 15693
● Mifare
○ Desfire

☑ Update-on-Card (Read & Write)
☑ Automatic card updaters
☑ Audit openings
☑ Modify locking plan

☑ Manage Wireless doors ☑ Automatically update Wireless doors
Update every 00m 10s
Frequency : ● 868 MHz ○ 915 MHz Selected RF 0

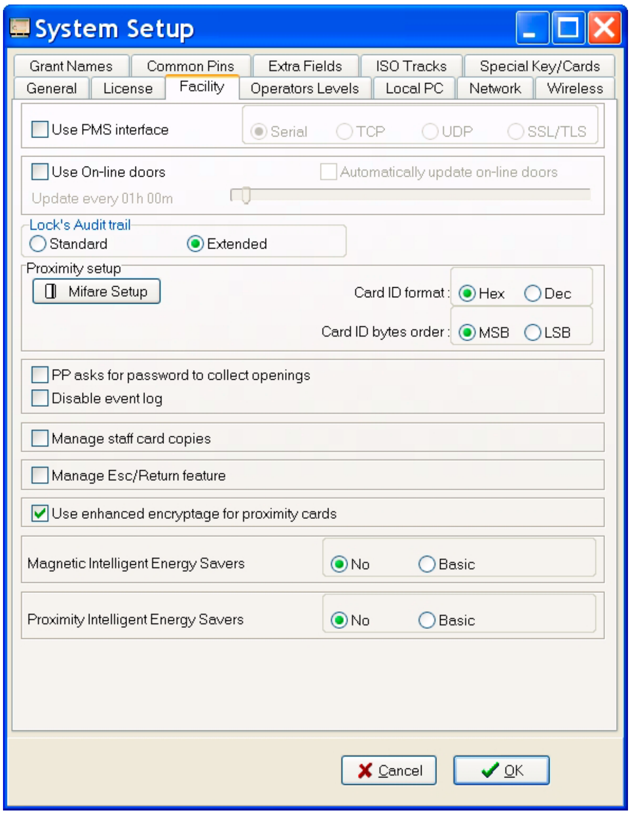
□ Manage cabinet locks
□ Manage safes □ Enable Mobile phone Apps and mail a
□ Manage Antipassback

The “Facility” tab allows defining a series of special functions which will only be used in certain specific cases.

These functions are the following:

- Use PMS interface
- Lock’s Audit trail
- Proximity setup
- PP asks for password to collect openings
- Disable event register
- Manage staff card copies
- Manage Esc/Return feature
- Use enhanced encryption for proximity cards
- Proximity Intelligent Energy Savers

These functions are described below.



☐ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

☐ Use On-line doors ☐ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup: Card ID format : ● Hex ○ Dec

Card ID bytes order : ● MSB ○ LSB

☐ PP asks for password to collect openings

☐ Disable event log

☐ Manage staff card copies

☐ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

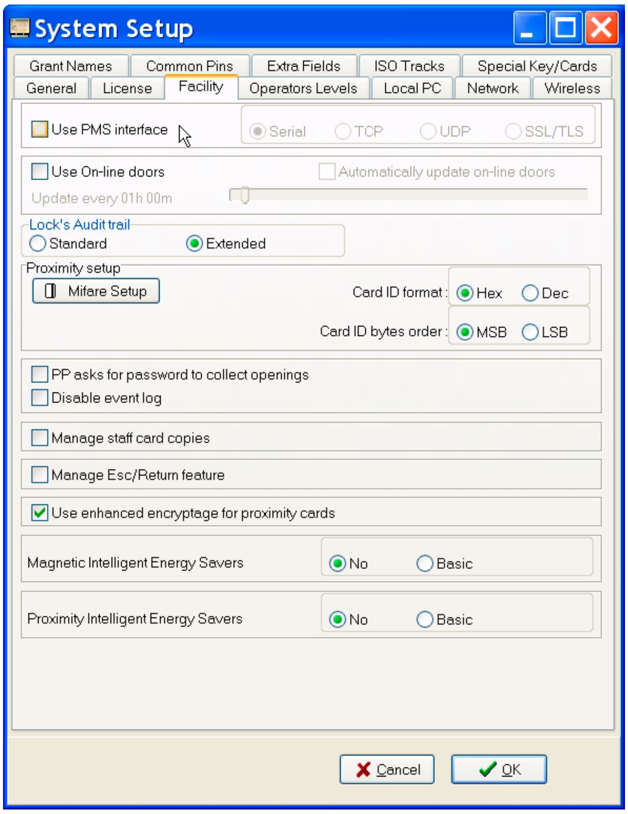
## Use PMS interface

On the market, there are systems for the management of buildings depending on their use. That is to say, there are systems to manage hospitals, schools, hotels, etc. These systems are called PMS (Property Management Systems).

It may be the case that, in the building where the TESA Access Control system is intended to be installed, there is a PMS or there are plans to install one, so that the end user does not want to manage the access control system from the TS1000 software, but rather prefers to manage it from the PMS management system itself.

TESA Access Control offers the possibility of integrating the TS1000 system with any management system on the market. For this purpose, a communication protocol is provided which describes how to integrate certain actions.

For more information, contact your distributor.



☐ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

☐ Use On-line doors ☐ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup: Card ID format : ● Hex ○ Dec

Card ID bytes order : ● MSB ○ LSB

☐ PP asks for password to collect openings

☐ Disable event log

☐ Manage staff card copies

☐ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

## Lock’s Audit trail

The field “Lock’s Audit trail” allows choosing between two settings: Standard and Extended:

- Standard Lock’s Audit trail: the doors can store a maximum of 1,500 users and 600 events.
- Extended Lock’s Audit trail: the doors are capable of storing a maximum of 1,000 users and 1,000 events.

## Proximity setup

This field allows configuring the cards (Mifare or Desfire) to calculate how many events and locking plan crosses are stored, as well as for multiple application with other systems.

## PP asks for password to collect openings

With the Portable Programmer, it is possible to collect the event register stored in the electronic cylinders, locks and/or wall readers.

After collecting the information, there are two possibilities:

- Viewing the event register in the Portable Programmer.
- Transmitting the information to the PC to view it from the TS1000.

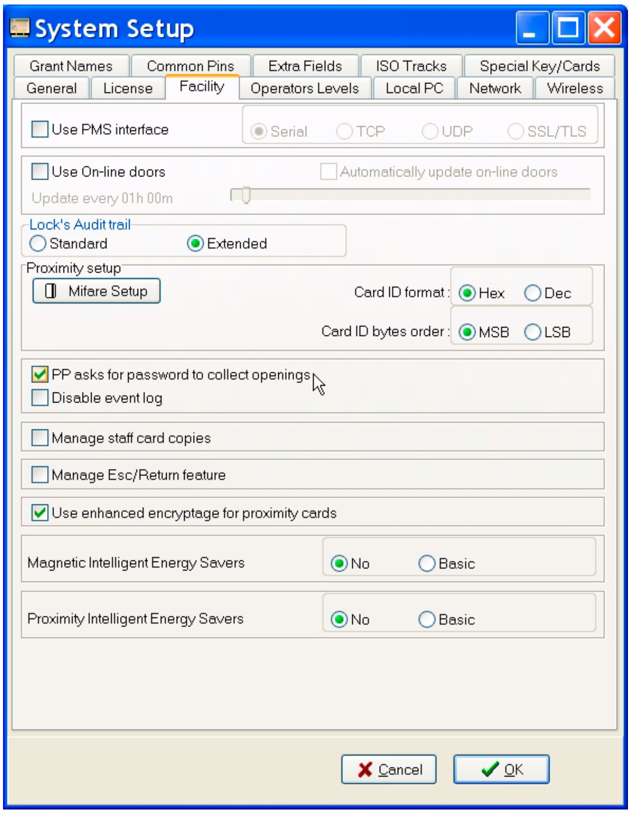
When the event register of a lock is read, it remains unchanged, that is to say, it is read, but not deleted. For this reason, the reading of events from the lock by means of the Portable Programmer does not require, in principle, any additional security measure, that is to say, it does not require the use of the Authorisation Key.

However, it is possible to introduce a security measure for this collection of events from the locks, which involves using a password. This password matches that used for Emergency Openings with the Portable Programmer, which is assigned in the “PP” menu of the TS1000.

In order to establish this password requirement, carry out the following steps:

1 In the "Setup" menu, "Facility" tab, tick the option "PP asks for password to collect openings".

2 Click "OK" to accept it.



System Setup

□ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

□ Use On-line doors □ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup: Mifare Setup

Card ID format: ● Hex ○ Dec

Card ID bytes order: ● MSB ○ LSB

☑ PP asks for password to collect openings

□ Disable event log

□ Manage staff card copies

□ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

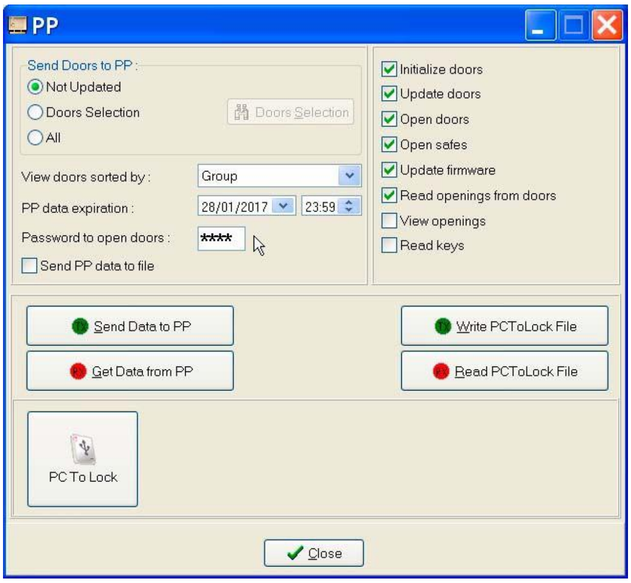
Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

3 In the "PP" menu of the TS1000, "Password to open doors" field, type the password.

4 In that "PP" menu, click the "Send Data to PP" button. Before this, connect the PP to the PC and turn it on.

□WARNING: the password, just like the other parameters in this window, is not stored in the system. It is only used for it to be sent to the PP, where it actually is stored. The next time this window is opened, the default values will be shown again.



PP

Send Doors to PP: ● Not Updated ○ Doors Selection ○ All

View doors sorted by: Group

PP data expiration: 28/01/2017 23:59

Password to open doors: ****

□ Send PP data to file

☑ Initialize doors

☑ Update doors

☑ Open doors

☑ Open safes

☑ Update firmware

☑ Read openings from doors

□ View openings

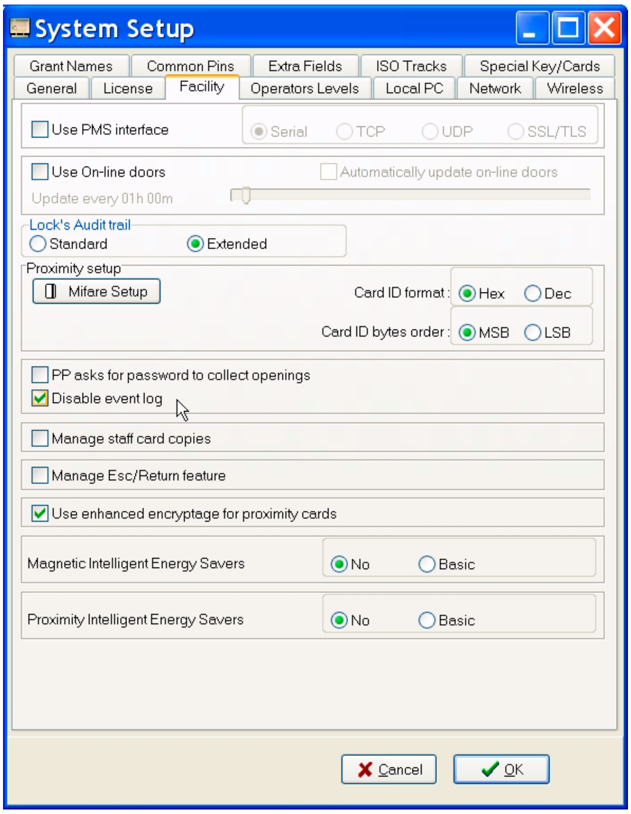
□ Read keys

## Disable event register

In some countries, regulations forbid recording any permitted access, except when it is carried out by means of a PIN (Personal Identification Number) code. That is to say, except when the opening of the door is carried out with the combination of card and keypad.

For this reason, the TESA Access Control programme offers the possibility of "Disabling the event register".

In order to disable this register, tick the option "Disable event register" and, then, click "OK" to accept it.



System Setup
Grant Names | Common Pins | Extra Fields | ISO Tracks | Special Key/Cards
General | License | Facility | Operators Levels | Local PC | Network | Wireless

□ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

□ Use On-line doors □ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup

Card ID format : ● Hex ○ Dec

Card ID bytes order : ● MSB ○ LSB

□ PP asks for password to collect openings

☑ Disable event log

□ Manage staff card copies

□ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

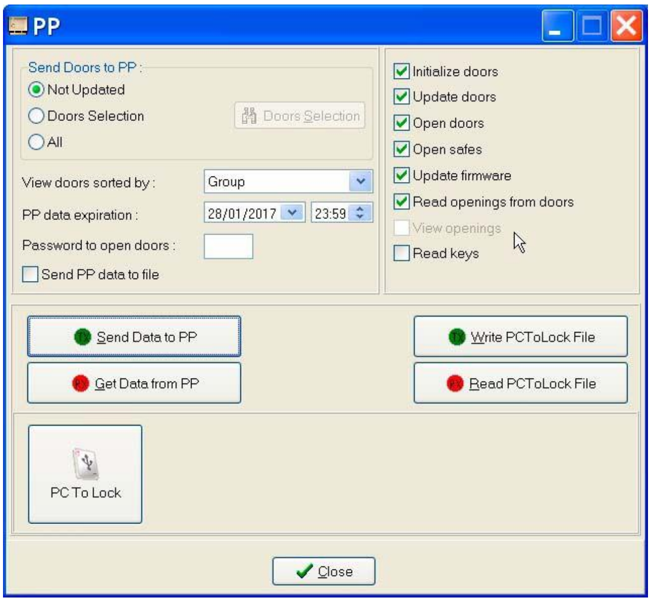
Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

When this option is selected, two things happen:

- The option "View openings" is disabled in the Portable Programmer (this option is selected in the "PP" menu of the TS1000).

- In the event register of the TS1000 software ("Openings" menu), the permitted accesses of the users are not recorded.



Send Doors to PP :
● Not Updated
○ Doors Selection
○ All

View doors sorted by : Group

PP data expiration : 28/01/2017 23:59

Password to open doors :

□ Send PP data to file

☑ Initialize doors
☑ Update doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
□ View openings
□ Read keys

## Manage staff card copies

By default, in the TESA Access Control system, it is not possible to make copies of credentials, that is to say, each user is unique and exclusive.

This means that it is necessary to define each and every one of the system users, regardless of whether or not they have the same locking plan (even if they will enter through the same doors).

Therefore, for each user defined in the system, there is a unique credential:

- User 1 -> Credential 1
- User 2 -> Credential 2
- User 3 -> Credential 3
- Etc.

This way of managing the site allows adding the possibility for the locks to cancel a lost and/or stolen credential automatically to the system.

Should a user lose their credential, in order to cancel that credential and assign a new one, you only need to encode a new credential for that user (the old one becomes invalid automatically). This operation does not affect any other user in the site.

However, the obligation of having to define each and every one of the users of the site may be somewhat inconvenient for some sites.

Consequently, the system allows making copies of credentials, that is to say:

- User 1 -> Credential 1
- User 2 -> Copy 1 Credential 1
- User 3 -> Copy 2 Credential 1
- User 4 -> Copy 3 Credential 1
- Etc.

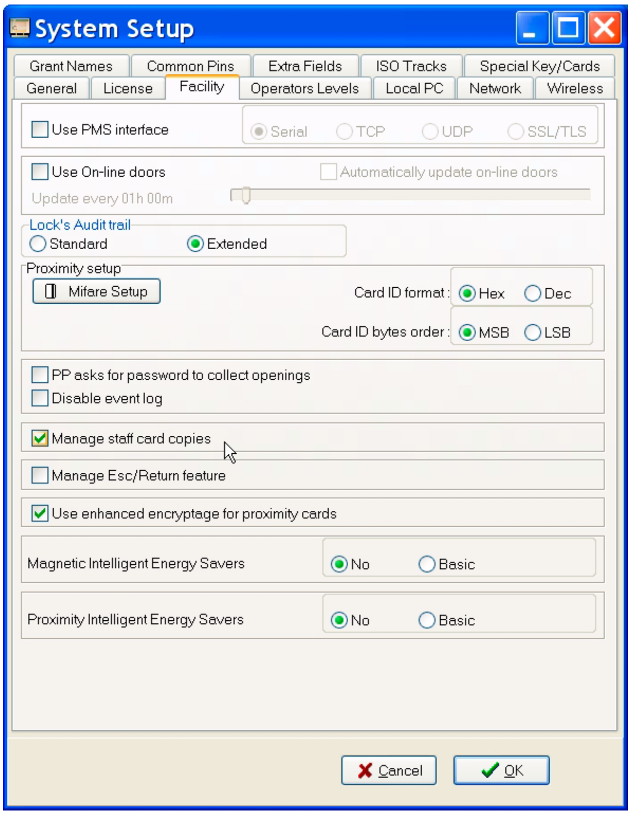
In order to be able to make copies of credentials, tick the option “Manage staff card copies” in the “Facility” tab of the “Setup” menu.

□ WARNING: take into account that, when working with copies of credentials, if a new credential is encoded, the previous credential is cancelled, as well as all its copies. That is to say:

New Credential 1:

- Cancels Credential 1
- Cancels Copy 1 Credential 1
- Cancels Copy 2 Credential 1
- Cancels Copy 3 Credential 1
- Etc.

□ When working with copies of credentials, the copy number is reflected in the event register.



□ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

□ Use On-line doors □ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup: Mifare Setup

Card ID format : ● Hex ○ Dec

Card ID bytes order : ● MSB ○ LSB

□ PP asks for password to collect openings

□ Disable event log

☑ Manage staff card copies

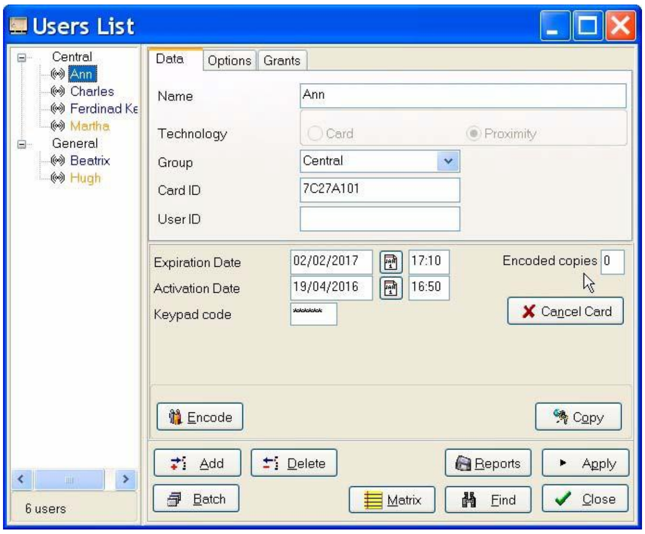
□ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

When the option “Manage staff card copies” in the “Facility” tab of the “Setup” menu is enabled, the button “Copy” is displayed in the “Users” menu of the TS1000, which allows making copies of the credential of that user, as well as the field “Encoded copies”, where the number of copies encoded from that credential is displayed.



Name: Ann

Technology: ○ Card ● Proximity

Group: Central

Card ID: 7C27A101

User ID:

Expiration Date: 02/02/2017 17:10

Activation Date: 19/04/2016 16:50

Keypad code: ******

Encoded copies: 0

## Manage Esc/Return feature (only available in the SMARTair series)

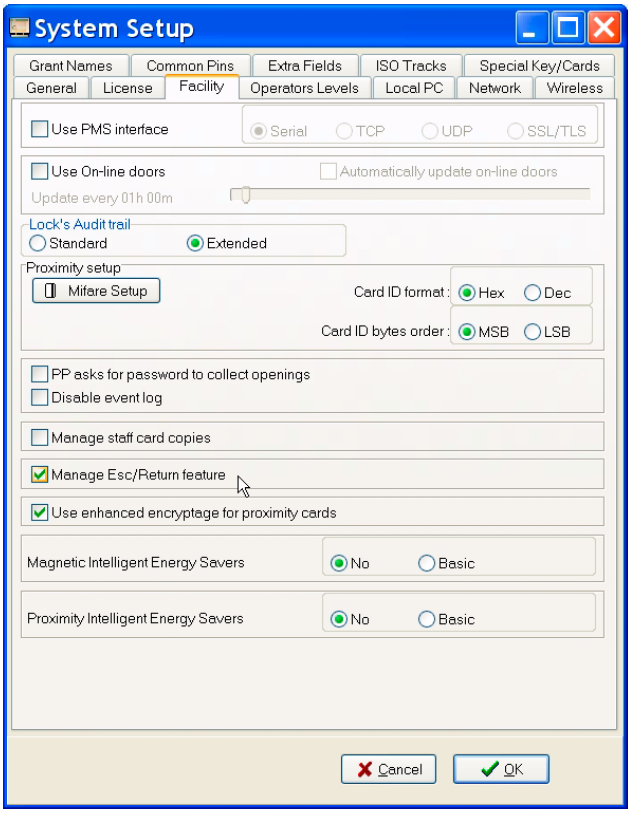
In some European countries, regulations demand that when a user opens a door from the inside, it must remain in a state which allows it to be opened from the outside.

The door must remain in this state during the time the user needs to get out of the room, reach the nearest emergency door and get back into the room.

This function is called “Esc/Return”.

In order to enable this function, tick the option “Manage Esc/Return feature” in the “Facility” tab of the “Setup” menu.

Click “OK” to accept it.



□ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

□ Use On-line doors □ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup

Card ID format : ● Hex ○ Dec

Card ID bytes order : ● MSB ○ LSB

□ PP asks for password to collect openings

□ Disable event log

□ Manage staff card copies

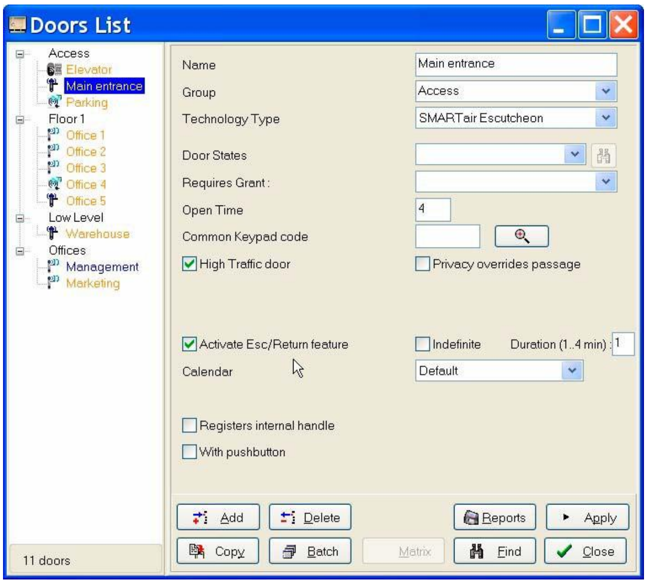
☑ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

When the function “Esc/Return” is enabled, the field “Activate Esc/Return” is displayed in the “Doors” menu, which allows enabling the function for that door, as well as the field “Indefinite”, which allows leaving the door open indefinitely and the field “Duration (1...4 min)”, which allows selecting the time it will remain open.



Name: Main entrance

Group: Access

Technology Type: SMARTair Escutcheon

Door States:

Requires Grant :

Open Time: 4

Common Keypad code:

☑ High Traffic door □ Privacy overrides passage

☑ Activate Esc/Return feature □ Indefinite Duration (1..4 min) : 1

Calendar: Default

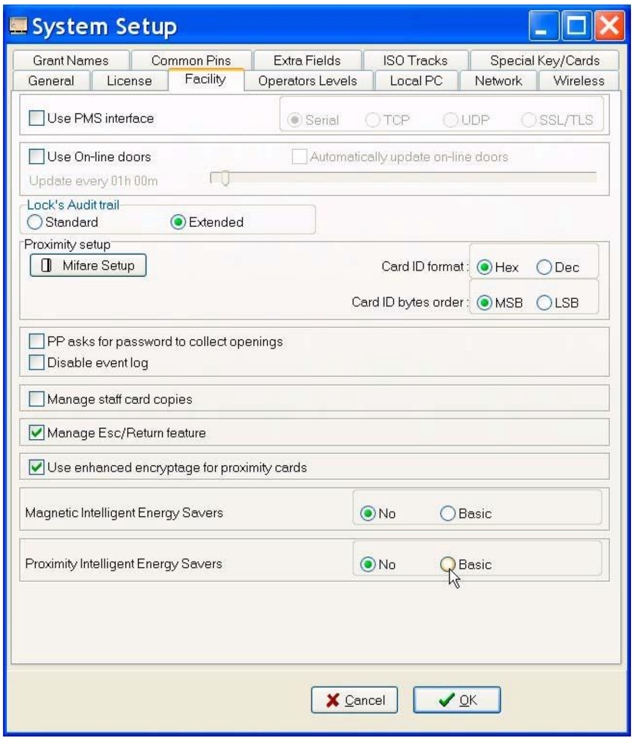
□ Registers internal handle

□ With pushbutton

## Proximity Intelligent Energy Savers

If the option “Basic” is selected, the information necessary to use the energy savers, if they are present in the site, will be encoded in the user cards.

For more information, refer to the corresponding instruction manual of the Proximity Intelligent Energy Saver.



☐ Use PMS interface ● Serial ○ TCP ○ UDP ○ SSL/TLS

☐ Use On-line doors ☐ Automatically update on-line doors

Update every 01h 00m

Lock's Audit trail: ○ Standard ● Extended

Proximity setup

Card ID format : ● Hex ○ Dec

Card ID bytes order : ● MSB ○ LSB

☐ PP asks for password to collect openings

☐ Disable event log

☐ Manage staff card copies

☑ Manage Esc/Return feature

☑ Use enhanced encryptage for proximity cards

Magnetic Intelligent Energy Savers ● No ○ Basic

Proximity Intelligent Energy Savers ● No ○ Basic

## L.3 DEACTIVATION OF THE AUTHORISATION KEY

### Use of the Authorisation Key

**In the first place, it is worth highlighting the importance of the use of the Authorisation Key as a security measure.**

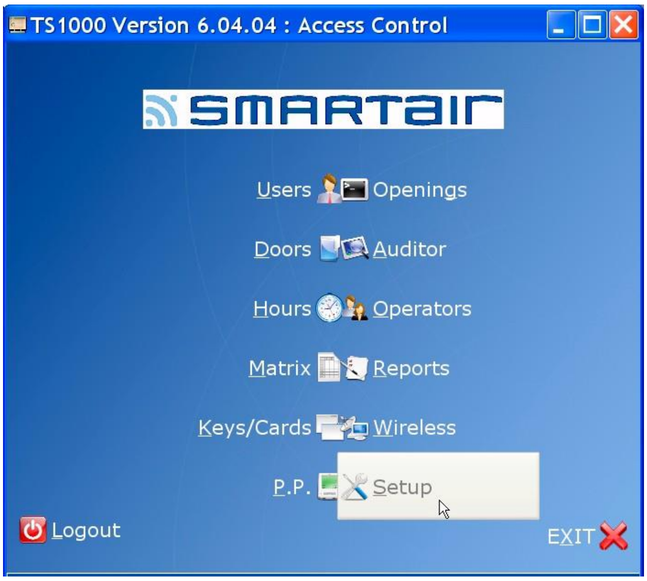
However, it is understandable that, for certain sites, its use may be inconvenient or unnecessary as a security measure.

Therefore, the use of the Authorisation Key may be deactivated in the system, for one or more operators levels. In this way, there may be operators in the system requiring the use of the Authorisation Key and, in turn, others who do not.

As a security measure, in order to deactivate the Authorisation Key, it is necessary to insert it into the Portable Programmer, thus ensuring that only the individual who has this key can decide on its deactivation.

### Deactivating the use of the Authorisation Key to use the PP

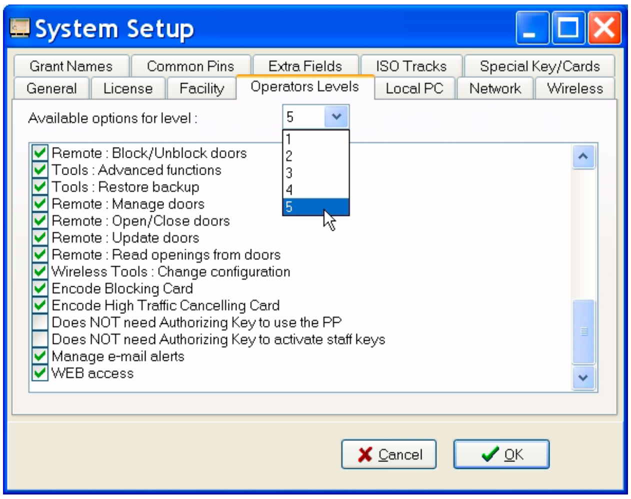
**1** On the TS1000 main screen, access the “Setup” menu.



**2** In the “Setup” menu, access the “Operators Levels” tab.

**3** Select the level you want to deactivate the Authorisation Key for (5 in the example).

As you can see, the options making reference to the Authorisation Key are not ticked.

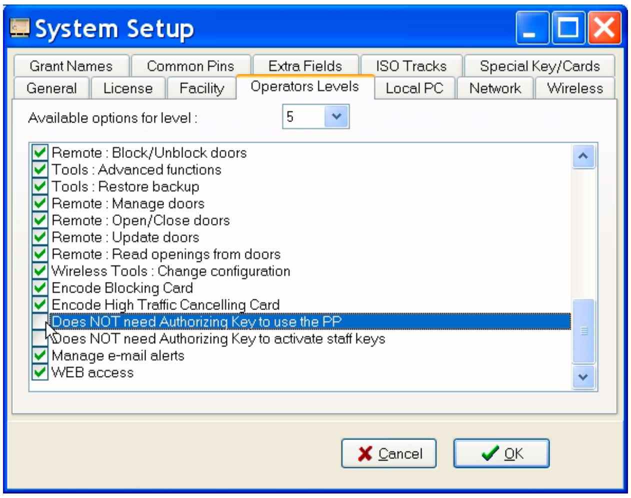


Available options for level : 5

☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
□ Does NOT need Authorizing Key to use the PP
□ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

4 Select the option “Does NOT need Authorisation Key to use the PP”.

If the Portable Programmer was not connected and powered on, a message will be displayed requesting you to do this.

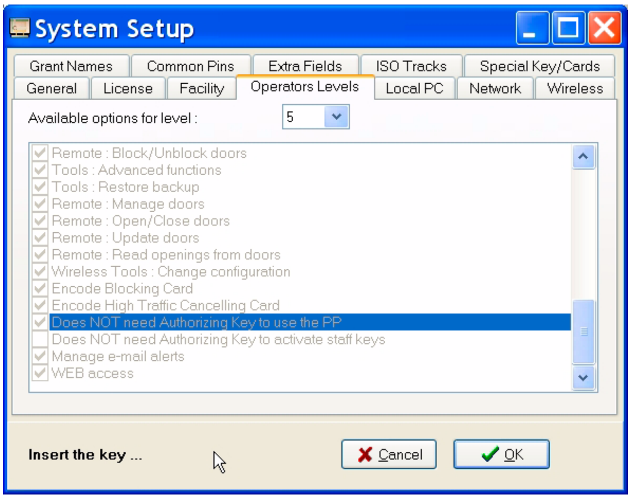


Available options for level : 5

☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
□ Does NOT need Authorizing Key to use the PP
□ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

5 A message is displayed asking you to insert the Authorisation Key.

Once it is inserted and recognised, the option will become “active” and, therefore, the operators from that level will not need the Authorisation Key any more to Initialise, Update and/or Open doors with the Portable Programmer.



Available options for level : 5

☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
☑ Does NOT need Authorizing Key to use the PP
□ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

Insert the key ...

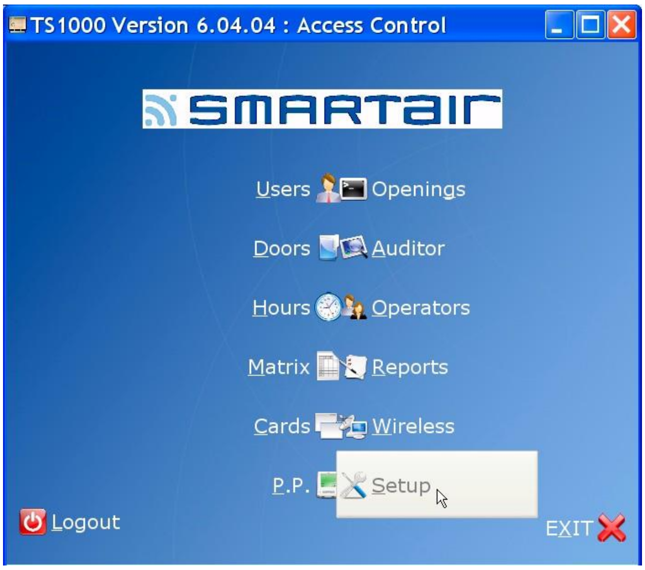
□ When desired, you can activate the use of the Authorisation Key again. The process is similar, differing in that it is not necessary to insert the Authorisation Key into the Portable Programmer.

**NOTE:** every time you access the TS1000 software with the *administrator* operator, the TS1000 will request the Authorisation Key, except in “Demo” mode. Deactivating the use of the Authorisation Key is only used for operators, who will have to enter the software with the password of the operator created.

## “Does NOT need Authorisation Key to activate staff keys” option

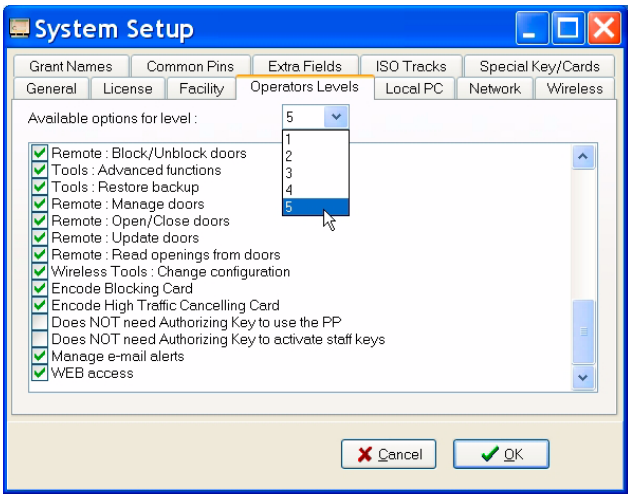
This option allows deactivating the Authorisation Key for the activation of staff keys. It only makes sense for sites with electronic cylinders and keys.

**1** On the TS1000 main screen, access the “Setup” menu.



**2** In the “Setup” menu, access the “Operators Levels” tab.

**3** Select the level you want to deactivate the Authorisation Key for (5 in the example).

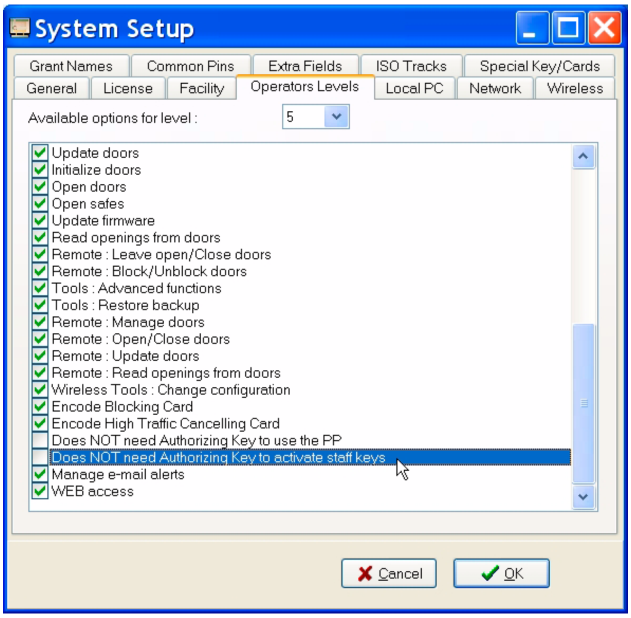


Available options for level : 5

☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
□ Does NOT need Authorizing Key to use the PP
□ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

4 Select the option “Does NOT need Authorisation Key to use the PP”.

If the Portable Programmer was not connected and powered on, a message will be displayed requesting you to do this.

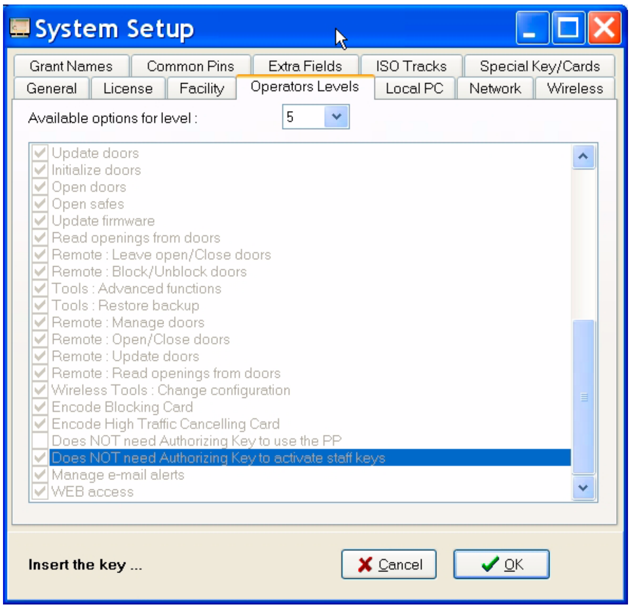


Available options for level : 5

☑ Update doors
☑ Initialize doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
☑ Remote : Leave open/Close doors
☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
☐ Does NOT need Authorizing Key to use the PP
☐ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

5 A message is displayed asking you to insert the Authorisation Key.

Once it is inserted and recognised, the option will become “active” and, therefore, the operators from that level will not need to activate the user keys after encoding them, since they will be encoded active.



Available options for level : 5

☑ Update doors
☑ Initialize doors
☑ Open doors
☑ Open safes
☑ Update firmware
☑ Read openings from doors
☑ Remote : Leave open/Close doors
☑ Remote : Block/Unblock doors
☑ Tools : Advanced functions
☑ Tools : Restore backup
☑ Remote : Manage doors
☑ Remote : Open/Close doors
☑ Remote : Update doors
☑ Remote : Read openings from doors
☑ Wireless Tools : Change configuration
☑ Encode Blocking Card
☑ Encode High Traffic Cancelling Card
☐ Does NOT need Authorizing Key to use the PP
☑ Does NOT need Authorizing Key to activate staff keys
☑ Manage e-mail alerts
☑ WEB access

**Insert the key ...**

□ When desired, just as in the previous case, you can activate the use of the Authorisation Key again. The process is similar, differing in that it is not necessary to insert the Authorisation Key into the Portable Programmer.

## L.4 OTHER CREDENTIALS

### Blocking key or Card

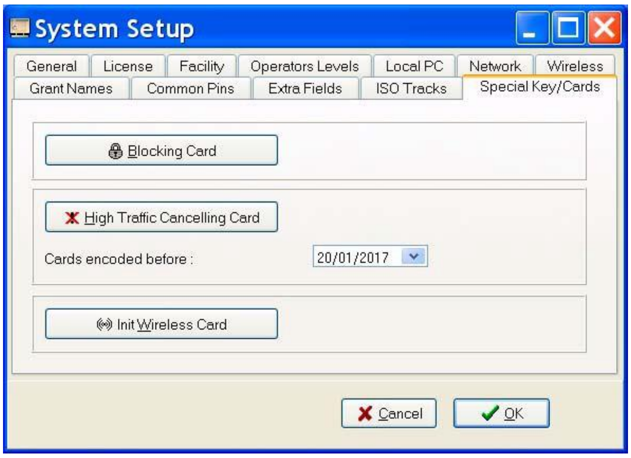
The TS1000 system has one special credential: the Blocking Key or Card.

The blocking credential allows “blocking” cylinders, locks and/or wall readers. A “blocked” door will not allow access to anybody, even if they normally have permitted access.

The doors in this blocked state will only allow access to those individuals who normally have permitted access and, in addition, have the option “Can open blocked doors” enabled. This option is defined for each user in the “Options” tab of the “Users” menu.

In order to encode the blocking card, proceed as follows:

1 Access the “Special Cards” tab of the “Setup” menu.



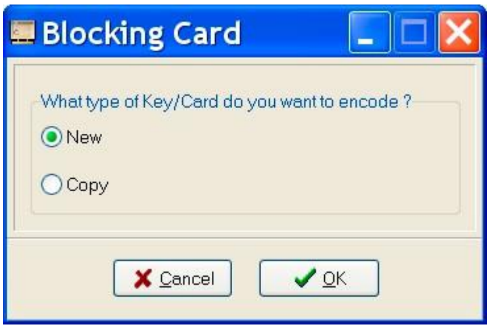
Cards encoded before : 20/01/2017

2 Click the “Blocking Card” button.

If there is more than one technology in the site, the system will ask what type of Blocking Card you want to create: Key (for cylinders), Card (for Magnetic Stripe readers and locks) or Proximity (for Proximity readers and locks).

3 A screen is displayed asking whether you want a “New” card (cancels the previous blocking card) or a “Copy” (which does not cancel it).

In this case, we choose “New” and click “OK”.

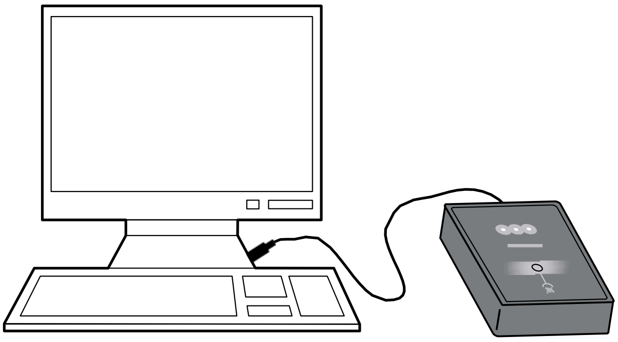


What type of Key/Card do you want to encode ?

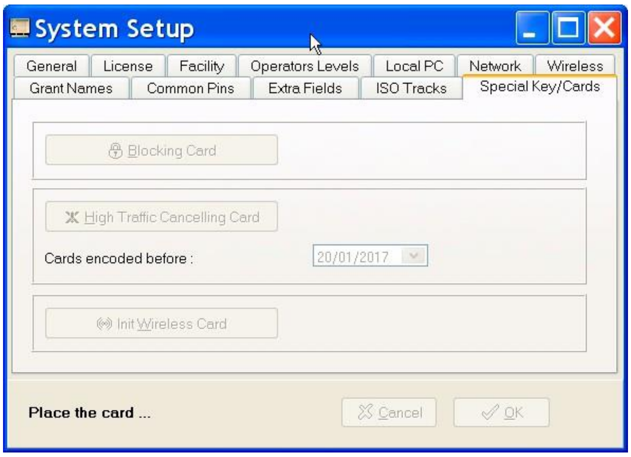
● New

○ Copy

4 If the Card Encoder (or the Portable Programmer, depending on the case) is not connected, a message will be displayed requesting you to do this.



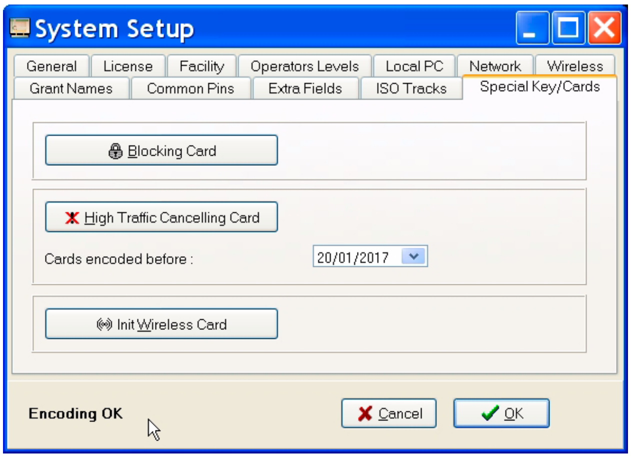
5 A message is displayed indicating you to bring the card close.



Cards encoded before : 20/01/2017

Place the card ...

6 Once the encoding has been finished, the corresponding confirmation message is displayed.



Cards encoded before : 20/01/2017

Encoding OK

## Blocking a door with the Blocking Credential

In order to block a door, you only need to use the Blocking Credential in it. Each technology responds this event differently:

- Electronic key: after inserting the blocking key into the cylinder, it flickers in the same way as for the Authorisation Key.
- Card (Magnetic Stripe or Proximity): after presenting the blocking card, the lock or reader responds with a quick flickering of the red LED for a few seconds.

□While a door remains blocked, any user who is normally authorised to access it will get an access denial signal, except they have the special option to open blocked doors enabled, in which case they can access without problems.

The denial message is also different depending on the technology:

- Electronic key: the user gets a normal red light, just like the one received for a standard non-authorised access.
- Card (Magnetic Stripe or Proximity): the user gets, in the lock or reader, a quick flickering of the green light in conjunction with the red light for a few seconds.

Both in the door and the credential (in the event of R/W Electronic Keys and Mifare Proximity Cards, provided that the openings read from door are enabled in the credential), the event “Denial: can not open blocked doors” will be recorded.

### Unblocking a blocked door

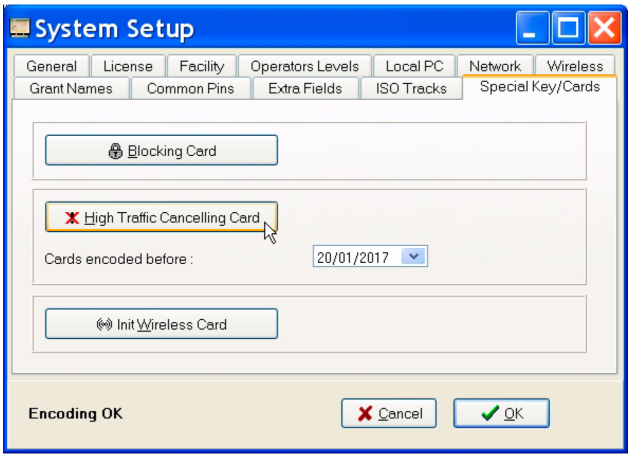
In order to unblock the blocked door, use the Blocking Credential in it once again. Depending on the technology, the response from the system will be different:

- Electronic key: after inserting the blocking key in the cylinder, the key light will come on in red for a few seconds (just like in an access denial).
- Card (Magnetic Stripe or Proximity): after presenting the blocking card, the lock or reader will respond with a quick flickering of the red LED for a few seconds, followed by a brief lighting up of the green LED.

After this step, the door will behave normally once again according to the locking plan programmed.

## High Traffic Cancelling Card

A High Traffic Door can be opened with any credential which belongs to the system, whose dates are correct and which hold the necessary permissions. That is to say, a user with a credential belonging to the site, but without an expiry date, will always have access to the high traffic doors and, in principle, there is no way to cancel such a credential. In order to solve this problem, there exists a "High Traffic Cancelling Card" credential.



Cards encoded before : 20/01/2017

Encoding OK

For more information on high traffic doors, see *High Traffic Door* on page 77.

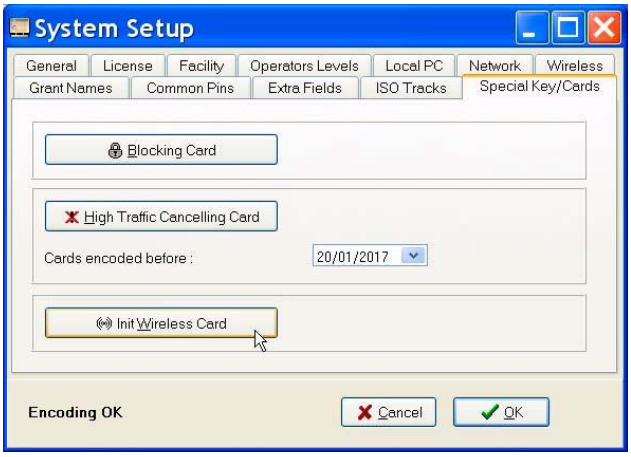
The High Traffic Cancelling Card allows cancelling the credentials which have been encoded before the date selected in the field "Cards encoded before".

Select the date desired, connect the card encoder, click the "High Traffic Cancelling Card" button and place the card on the encoder.

Once the card has been encoded, place it in the corresponding High Traffic Door and, as from that moment, the credentials encoded before the date selected will no longer have access permitted.

## Init Wireless Card

The “Init Wireless” Card is used in V3 wireless systems to automatically link the doors to the Hub having the strongest coverage available.

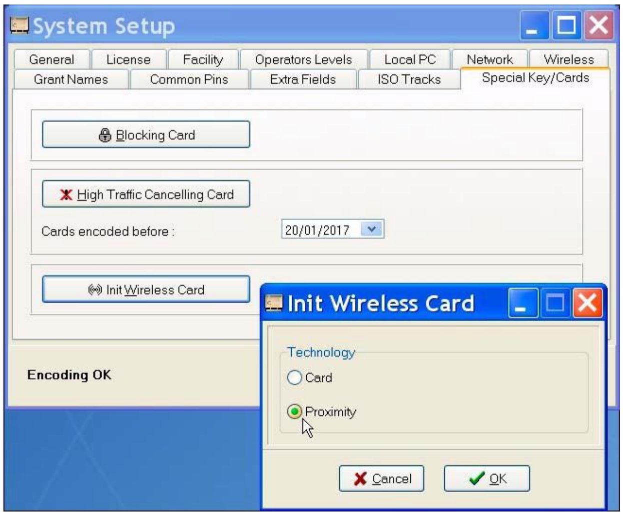


Cards encoded before : 20/01/2017

Encoding OK

In order to encode the card, connect the card encoder and click the “Init Wireless Card” button; a window is displayed asking you to choose the technology of the card.

Select the technology applicable to your card and click “OK”.

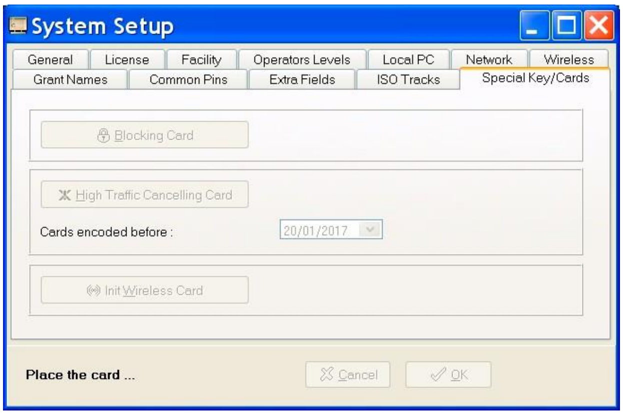


Cards encoded before : 20/01/2017

Encoding OK

Technology
○ Card
● Proximity

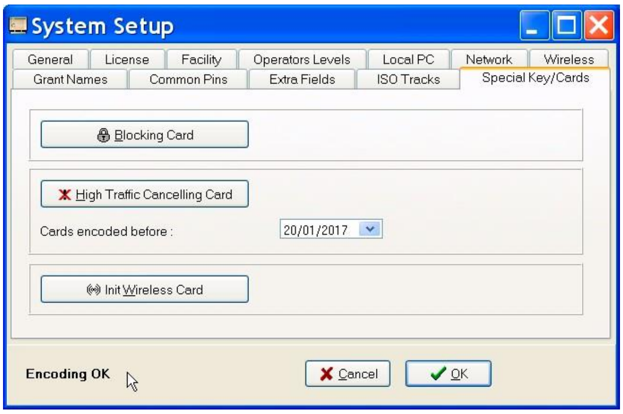
A message is displayed indicating you to bring the card close.



Cards encoded before : 20/01/2017

Place the card ...

Place the card on the encoder. After a brief moment, the card will be encoded and a confirmation message will be displayed.

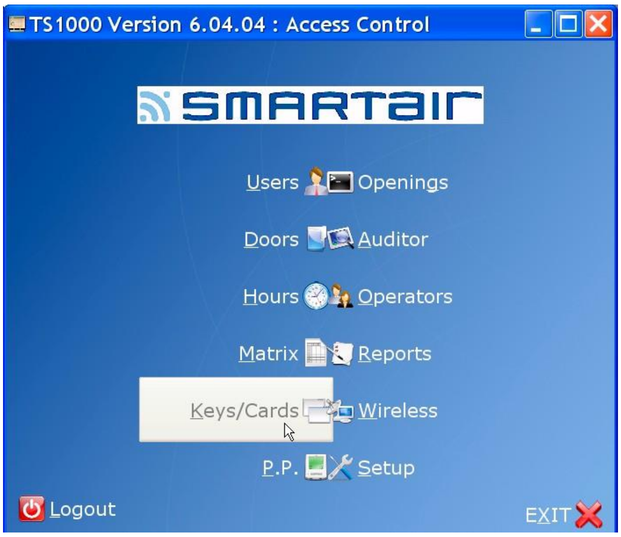


Cards encoded before : 20/01/2017

Encoding OK

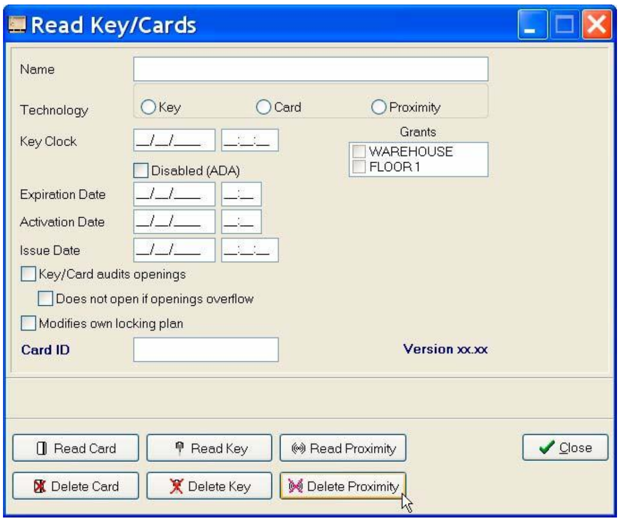
**Once the initialisation process has been carried out, it is advisable to delete the card so as to avoid activating the RF modules accidentally.**

In order to delete it, access the “Cards” menu.



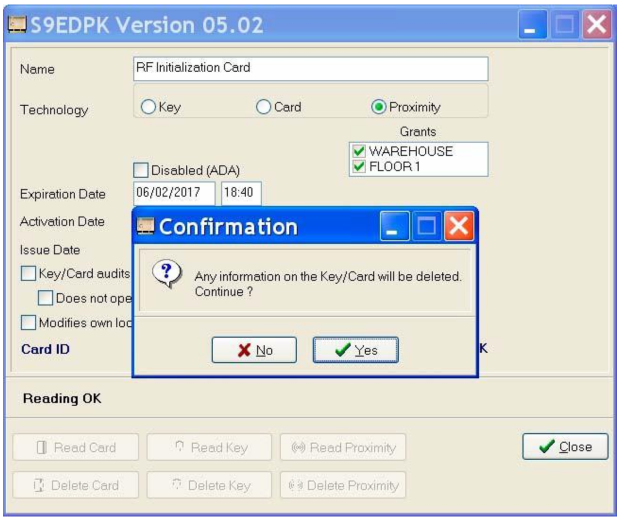
The window “Read Cards/Keys” is displayed; click the “Delete Proximity” or “Delete Card” button, as appropriate.

With the card encoder previously connected, click the corresponding deletion button and place the card on the encoder.



A message is displayed asking you to confirm the deletion of the card.

Click “OK” to confirm.



S9EDPK Version 05.02

Name: RF Initialization Card

Technology: ○ Key ○ Card ● Proximity

Grants: ☑ WAREHOUSE ☑ FLOOR 1

□ Disabled (ADA)

Expiration Date: 06/02/2017 18:40

Activation Date

Issue Date

□ Key/Card audits

□ Does not ope

□ Modifies own loc

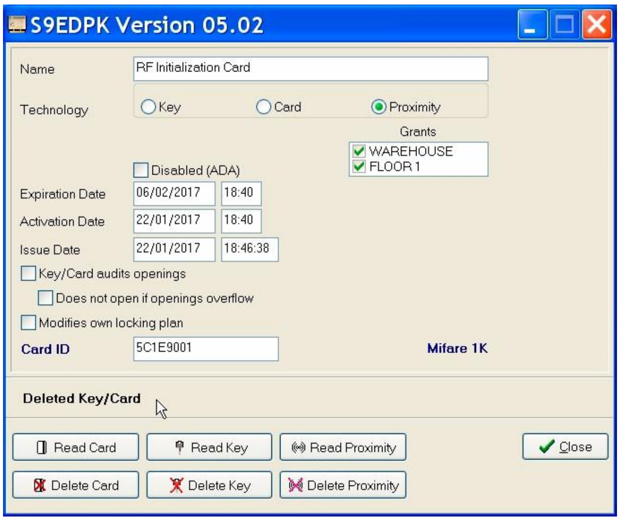
Card ID

Confirmation

Any information on the Key/Card will be deleted. Continue ?

Reading OK

The deletion takes place and a confirmation message is displayed.



S9EDPK Version 05.02

Name: RF Initialization Card

Technology: ○ Key ○ Card ● Proximity

Grants: ☑ WAREHOUSE ☑ FLOOR 1

□ Disabled (ADA)

Expiration Date: 06/02/2017 18:40

Activation Date: 22/01/2017 18:40

Issue Date: 22/01/2017 18:46:38

□ Key/Card audits openings

□ Does not open if openings overflow

□ Modifies own locking plan

Card ID: 5C1E9001 Mifare 1K

Deleted Key/Card

ASSA ABLOY is the global
leader in door opening
solutions, dedicated to
satisfying
end-user needs for security,
safety and convenience.

www.assaabloy.com

TESA is the leading Spanish manufacturer and supplier of locking solutions and access control technology for the residential and institutional markets. TESA has a wide and complete range of products including panic exit devices, cylinders, security locks, knobs and handles, door closers, access control solutions with electronic cylinders, electromechanical and electromagnetic solutions and armoured doors. TESA exports to markets such as Latin America, Middle East, Europe, Asia Pacific and the North African countries.

Your Access. Your Contro

SMARTair™ is a powerful access control system that offers an intelligent, yet simple, step up from keys. SMARTair™ is the cost-effective alternative to a full high-security system.
SMARTair™ contactless, smart card technology is easily incorporated into existing systems, with multiple management solutions. No bells, whistles, or wires, just sleek, reliable security.

ASSA ABLOY NEW ZEALAND LTD
6 Armstrong Road, Albany,
Auckland, New Zealand
nzsales@assaabloy.com

We reserve the right to make technical modifications: SMARTair™ user guide 09 2016 ENG