



TESA Hotel software User manual



ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions

Contents

A – Introduction to the TESA Hotel manual

A

B – System description

B

C – License

C

D – Setup

D

E – Running the programme for the first time

E

F – Creating the Locking Plan

F

G – Operators and Operator Levels

G

H – Grants

H

I – Encoding keys and programming doors

I

J – Wireless System

J

K – Site management

K

L – Other Functions

L

A – Introduction to the TESA Hotel manual

Chapters of the TESA Hotel manual	5
TESA Hotel main screen	7
Setup Menu	8
Reception Menu	8

A – INTRODUCTION TO THE TESA HOTEL MANUAL

A.1 CHAPTERS OF THE TESA HOTEL MANUAL

This manual describes how to install and use the TESA Hotel 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 TESA Hotel manual

This chapter.

B System description

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

C License

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

D Setup

Step-by-step description of the setup procedure for the TESA Hotel 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 TESA Hotel:

- “Users” menu, to define *Who* can enter. This menu defines the hotel staff (master cards), but not the guests.
- “Doors” menu, to define *Where* the users (hotel staff) can enter, as well as the guests.
- “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 TESA Hotel 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 Operator 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, with no need to modify the locking plan or reprogramme the doors with 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 (hotel staff). The grants for guests are assigned on the “Doors” menu and the “Check in” menu.

I Encoding keys and programming 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 (locks, cylinders, wall readers, etc.).

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

- The programming of the users’ credentials (hotel staff) is carried out by means of the “Users” menu, using the corresponding device connected to the computer (Magnetic Stripe Encoder, Proximity Encoder, Portable Programmer for the electronic keys).
- The credentials of the guests are encoded in the “Check in” menu, and in the “Copy Guest” menu.
- 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 transfer the locking plan to it by means of the “PP” menu (Portable Programmer).

J Wireless System

The wireless system allows the wireless devices (locks, wall readers or cylinders) of the doors to communicate with the computer by radio, through hubs connected to it. This allows carrying out many operations without having to go physically to the doors with the Portable Programmer

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

- Configure the hubs one by one by means of the “InitHubIP” software.
- Connect the hubs to the TESA Hotel server computer network.
- Incorporate the hubs and wireless devices of the doors into the system by means of the TESA Hotel “Setup” menu.
- Manage the wireless devices of the doors by means of the TESA Hotel “Wireless” menu.

K Site management

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

- Registering and de-registering the guests who arrive in and leave the hotel by means of the “Check In”, “Copy Guest” and “Check Out” menus.
- Encoding cards to be used in special and emergency situations, by means of the “Special Key/Cards” menu.
- Reading and/or deleting credentials of staff and guests by means of the “Read Keys/Cards” menu.
- Managing the wireless devices of the doors by means of the “Wireless” menu.
- Reading the record of openings or events of the doors by means of the “Openings” menu.
- Updating the locks and reading their events by means of the portable programmer and the “PP” menu.
- Managing the record of the operations carried out by the Operators in the system by means of the “Auditor” menu.
- Generating and printing different reports by means of the “Reports” menu. These can be, for example, users lists, doors lists, hours, locking plan, etc.

L Other Functions

There are also less common configuration functions which in certain cases can be very useful. They can be found in the “Setup” menu.

A.2 TESA HOTEL MAIN SCREEN

The TESA Hotel main screen, which displays after installing and running the programme, is shown below. This screen allows accessing all the menus which have been mentioned above.

The box at the top left displays the name of the operator who has accessed the application, in this case, “TESA”.



Fig. 1 TESA Hotel main screen

This screen has two different zones or menus:

- The *Setup* menu
- The *Reception* menu

These two menus are described below

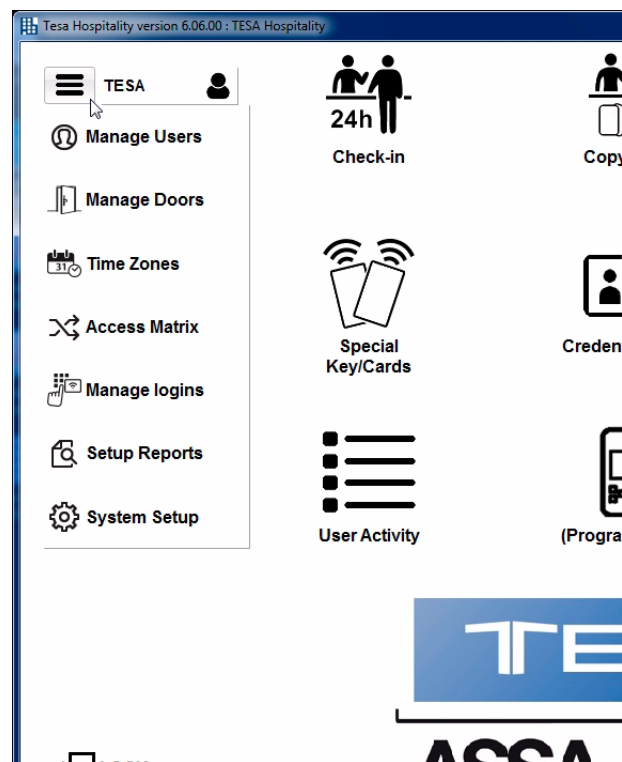
Setup Menu

The *Setup menu* is displayed by clicking on the corresponding drop-down button at the top left of the main screen.

It has the following sub-menus:

- Users
- Doors
- Hours
- Matrix
- Operators
- Reports
- Setup

This menu is used in the start-up, for configuration of the system and creating the different users (hotel staff), hotel doors, times, locking plan, etc.

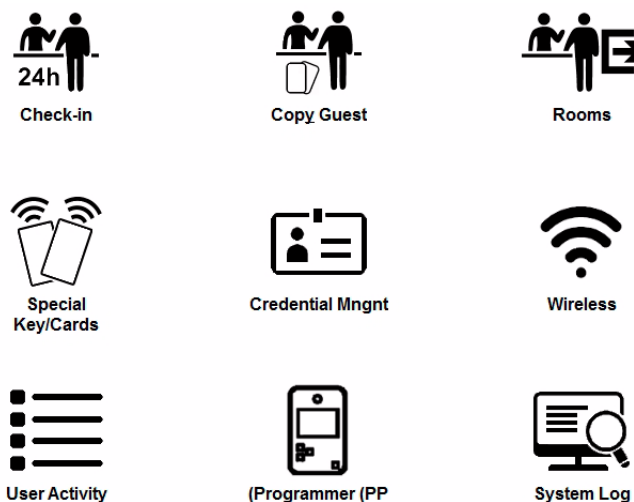


Reception Menu

The *Reception menu* occupies the central part of the main screen, and is used for the day-to-day management of the hotel (Check In and Check Out of guests, reading and encoding of cards, monitoring of openings, etc.).

It is comprised of the following sub-menus.

- Check In
- Copy Guest
- Check Out
- Special Key/Cards
- Read Keys/Cards
- Wireless
- Openings
- P.P. (portable programmer)
- Auditor



B – System description

TESA Hotel Platform11

B – SYSTEM DESCRIPTION

B.1 TESA HOTEL PLATFORM

The TESA Hotel platform is made up of a server and one or more clients that access it.

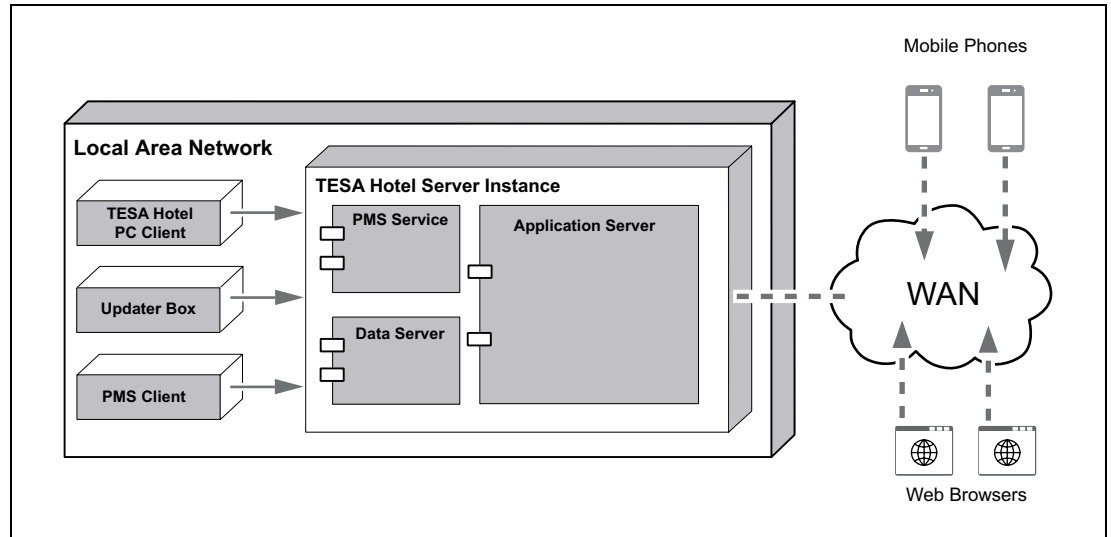


Fig. 2 System overview

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

- **PMS Service:** this is the PMS Service which is run in the server. By default, it uses the TCP Port 7779.
- **Data Server:** this is the database server in charge of providing data to the clients 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.
- **Time Service:** 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 – License

Introduction	15
TESA Hotel management software	16
Customised DATA folder	16
License types	16
License expansion	17
Export the “license.zip” file using the application “Tools.exe”	17
Import the new “license.zip” file using the application “Tools.exe”	18

C – LICENSE

C.1 INTRODUCTION

The *license* folder of the TESA Hotel system is made up of the following elements:

- Pen drive with the TESA Hotel management software customised with initial DATA file, manuals and tools.
- Setup identification system code.

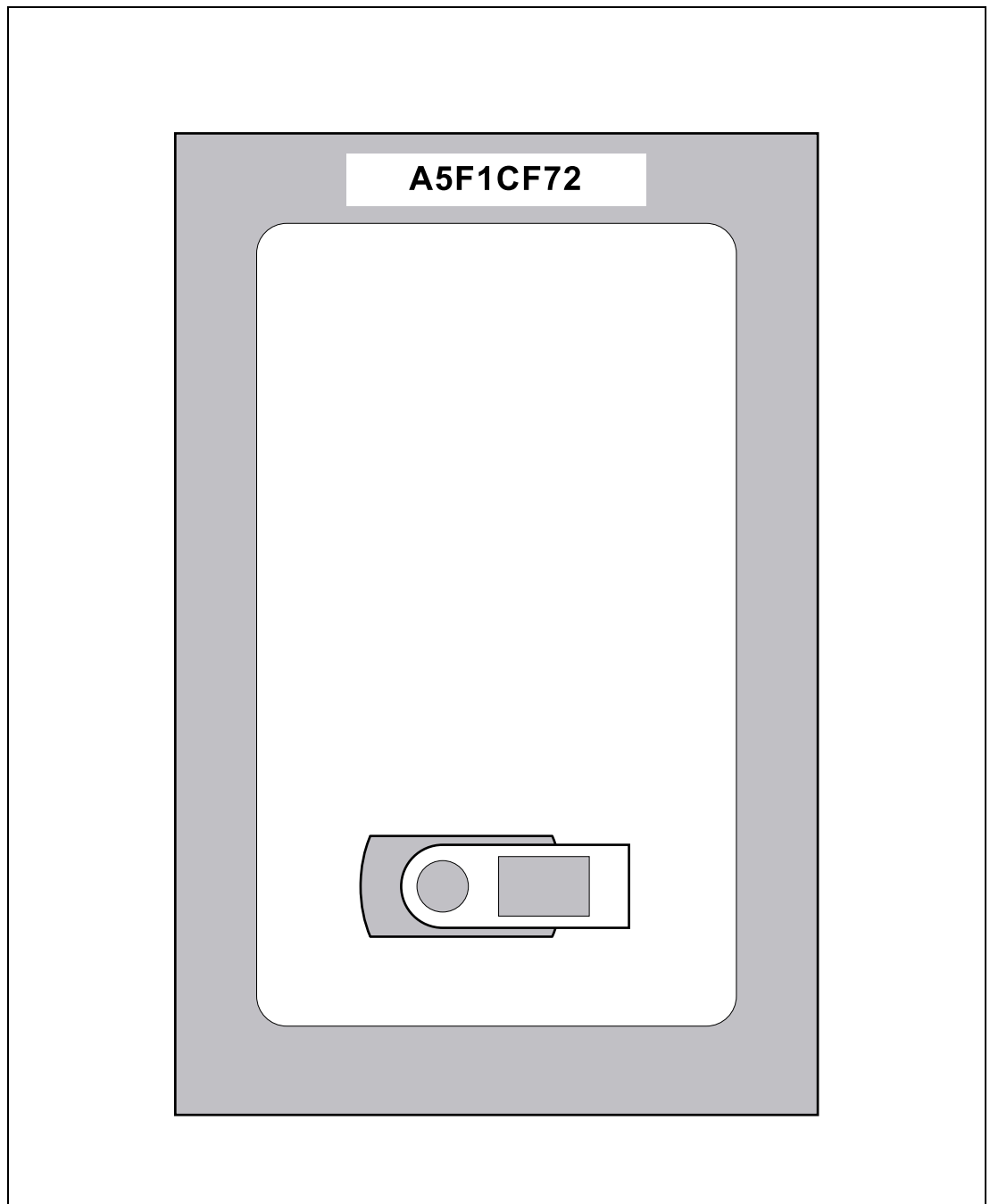


Fig. 3 Pen drive with license in the file supplied

C.2 TESA HOTEL MANAGEMENT SOFTWARE

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

The main features of the TESA Hotel V6.xx software are:

- Easy to use.
- It allows managing all the access control products: electronic locks, electronic cylinders and wall readers (on/off-line).
- It can be run on any PC with 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 are stored in a file called *Data.fdb* which is saved in a folder called "Data". These are the data referring to the users, doors, time zones, etc., and they are customised and exclusive for each site, with its own, unique system code.

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 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 LICENSE TYPES

The TESA Hotel system, to better fit the real needs of each site, offers several license types, based on the following features:

- number of doors: 30, 75, 150 and unlimited
- system type: Read / Write or Wireless
- "mobile app" license, which includes the *remote opening by mobile functionality*

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

C.5 LICENSE EXPANSION

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

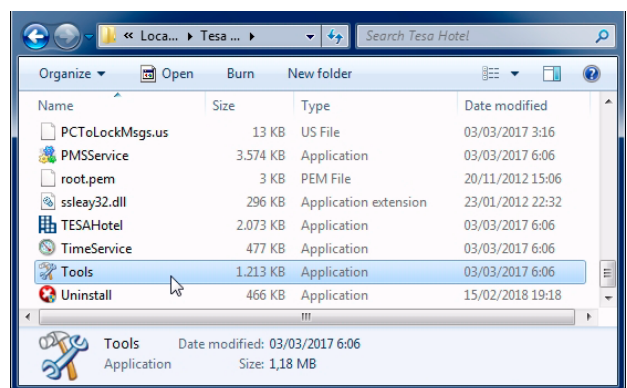
The license expansions that require an order are: opening by mobile App, NFC management, mobile BLE app, System change and Expansion of the number of doors. Contact your distributor if you wish to acquire any of these upgrades.

- The order must be accompanied by a copy of the “license.zip” file, which is imported and exported using the “Tools” application.
This file can either be sent by e-mail or in any other digital format.
- Once the order has been placed, a new “license.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 be possible to run the management software as you did before.

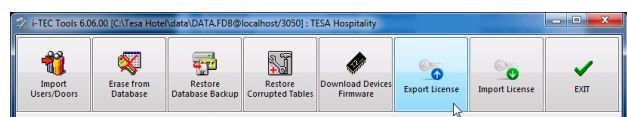
Export the “license.zip” file using the application “Tools.exe”

1 Ensure the TESA Hotel application is closed.

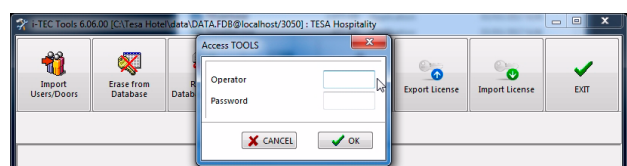
2 Run the Tools.exe application, which is in the same directory as the TESA Hotel application (by default, C:\Tesa Hotel).



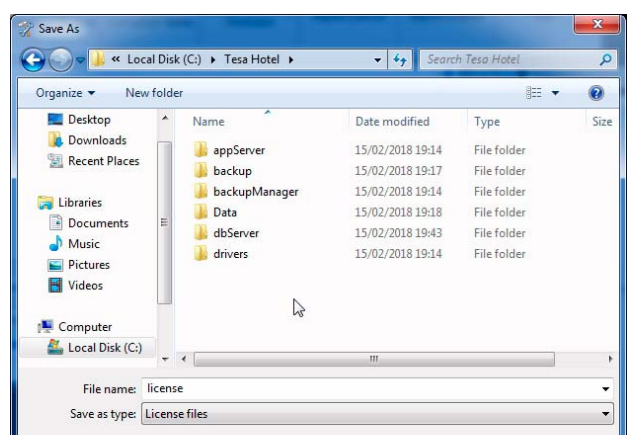
3 Click on the “Export License” button.



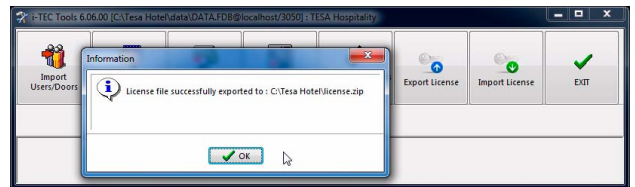
4 Enter an “Operator” name and “Password” that are valid in the TESA Hotel application.



5 Save the license file in your preferred folder in order to send this file to Talleres de Escoriaza, S.A.



- If the file is exported correctly, the corresponding confirmation notice will appear.

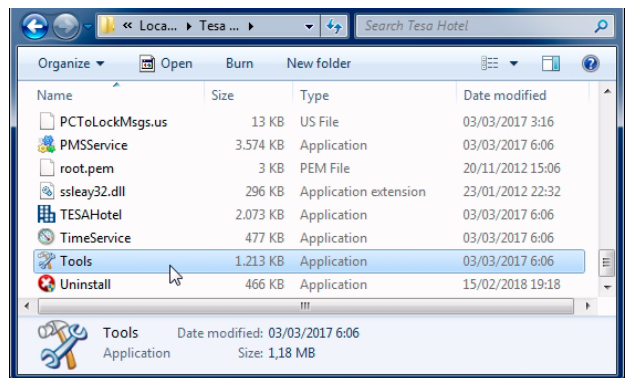


Import the new “license.zip” file using the application “Tools.exe”

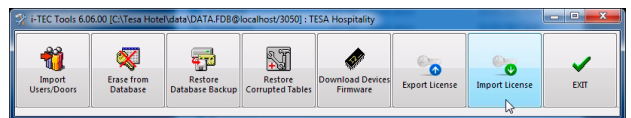
When Talleres de Escoriaza, S. A. sends you the new updated license, it must be imported using Tools.exe, as follows:

- Ensure the TESA Hotel application is closed.

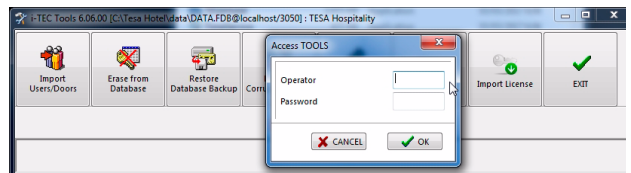
- Run the Tools.exe application, which is in the same folder as the TESA Hotel application (by default, C:\Tesa Hotel).



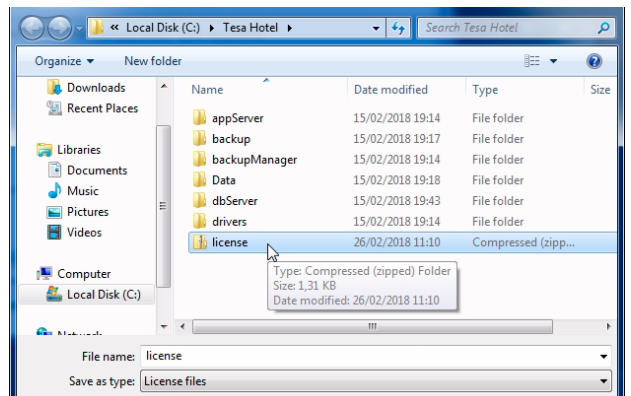
- Click on the “Import License” button.



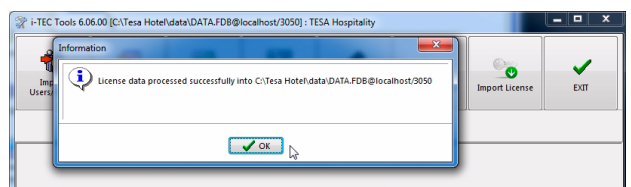
- Enter an “Operator” name and “Password” that are valid in the TESA Hotel application.



- Import the license file from the folder you saved it in after receiving it from Talleres de Escoriaza, S.A.



- If the file is imported correctly, the corresponding confirmation notice will appear.



D – Setup

Executable file	21
System requirements	21
Setup preparation	22
Uninstalling older versions of the TESA Hotel application	22
Setup process	23
Complete Setup	24
Setup of the Client Only, with Wireless mode	31
Summary and end of the application setup	33
Windows services installed	34
Configuration of the client PC	35
Configuration of the server PC	36
Configuration of the datasource	36
Configuration of the PMS Service	37
Configuration of the E-mail Server	38
Configuration example: typical SMTP configuration for GMAIL	38
Server mode	40
Advanced settings	41
Expiry of the HTTP sessions	41
Administrator Password	41
Configuration of the Server Logs	42
Notes to be considered in relation to the Windows antivirus or firewall	42
Setup and validation of the Server Certificate	43
Setup of the TESA CA certificate with Internet Explorer	44
Setup of the TESA CA certificate with Mozilla Firefox	46
Setup of the TESA CA certificate with Google Chrome	47

- Import of a database from an older version of the TESA Hotel application50**
 - Import of a database from a 4.x version50
 - Import of a database from a 5.x version51
- Troubleshooting52**
 - Errors or alerts from the security certificate52
 - TESA Hotel Client Message:
 - “The Web Server is not running or it is not available”52
 - TESA Hotel Client Message:
 - “The TESA Hotel database and the location of the database do not match”52
 - The TESA HotelPlatform web application is not running53
 - The ServerConfig application displays the “Deployment Error” message when setting the location of the database53

D – SETUP

D.1 EXECUTABLE FILE

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

If the Client is going to manage wireless devices, the Server will be installed with the GlassFish service. Otherwise (Client 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 159).

If GlassFish is installed on a Read / Write system, the system works in the same way, but with a Java service added to it (the Read / Write system is explained on page 62).

In the event of having only one PC for the setup of the system, the Server and the Client will be installed together on the same machine. In a multiuser setup, there will be one complete setup (Server + Client on a server machine) and several Client 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 client and server) are the following:

- PC with Dual Core or higher.
- 4 GB of free RAM.
- 4 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, Windows Me and Windows XP 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 antivirus/firewall. It also uses the UDP 7790, TCP 7890 and TCP 7881 ports for other internal functions.
- 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 antivirus/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 antivirus/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 4GB of free RAM memory for the server.

D.3 SETUP PREPARATION

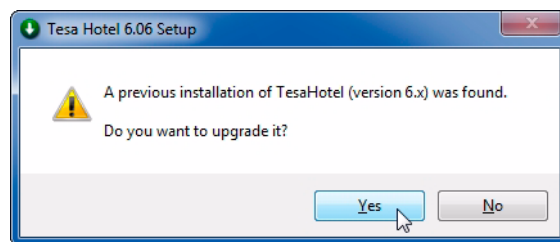
Before starting with the setup, a series of points have to be considered. One of the most important points is the selection of the PC where the Server is to be installed. Consider the following:

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

D.4 UNINSTALLING OLDER VERSIONS OF THE TESA HOTEL APPLICATION

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.



- 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 (less recommendable option).

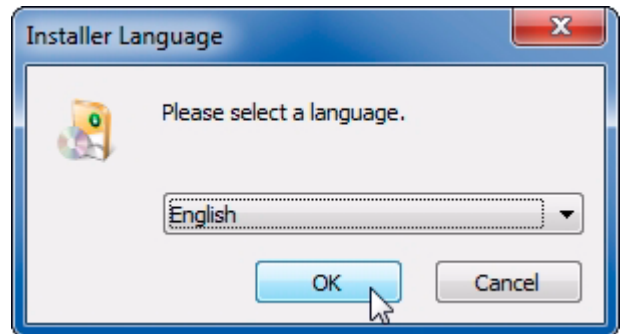
When versions 5.x and 6.x are installed on the same PC, take into account that the same ports will be shared by both versions (for example, the ports of the system of wireless communications or the ports of PMS communications). It will not be possible to run both versions simultaneously.

In order to be able to run version 6.x of the TESA Hotel 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 TESA Hotel version 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.

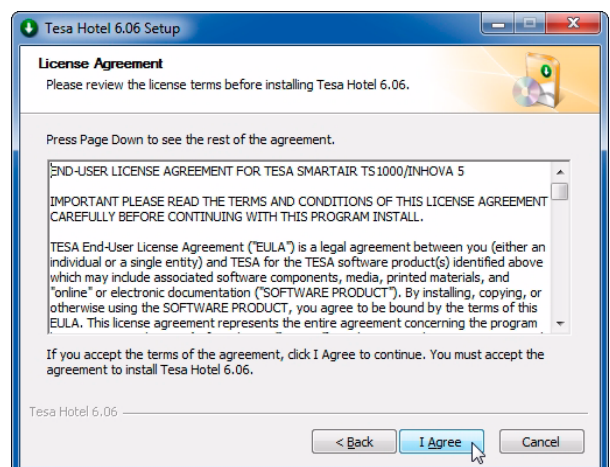
- 1 Insert the Pen-Drive. It is advisable to copy the “TESA Hotel 6.x Setup.exe” file to the PC which will work as a Server, to run it from there.
- 2 Run the “TESA Hotel 6.x Setup.exe” programme (the one you have copied to the PC which will work as a Server).
- 3 Select the language to be used during the setup.
Click “OK” to continue.



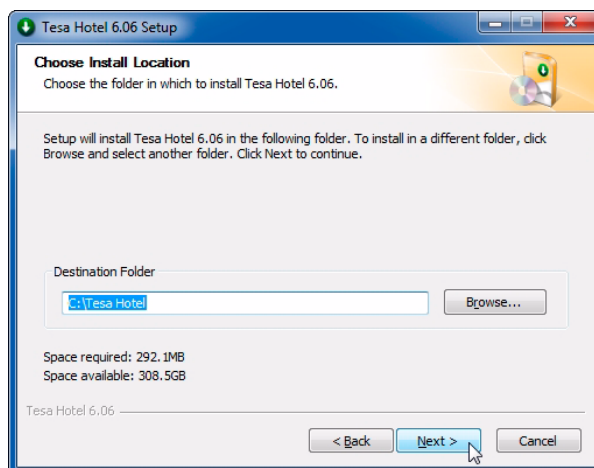
- 4 A welcome message is displayed.
Click “Next” to continue with the setup.



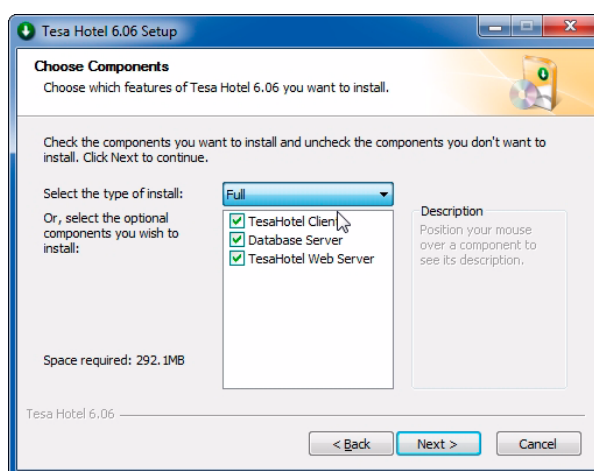
- 5 Read and accept the license terms.



- Specify the path for the setup of the application.



- Select the setup type:
 - “Complete” (Server+Client) includes Web Server and Wireless system
 - “Client Only, with Wireless”,
 and click on “Next”.



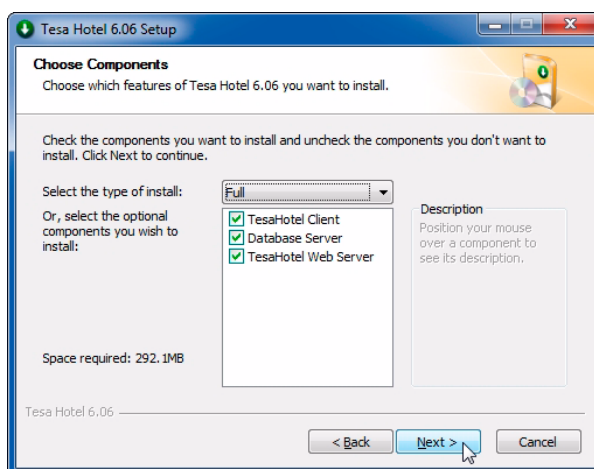
Complete Setup

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

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

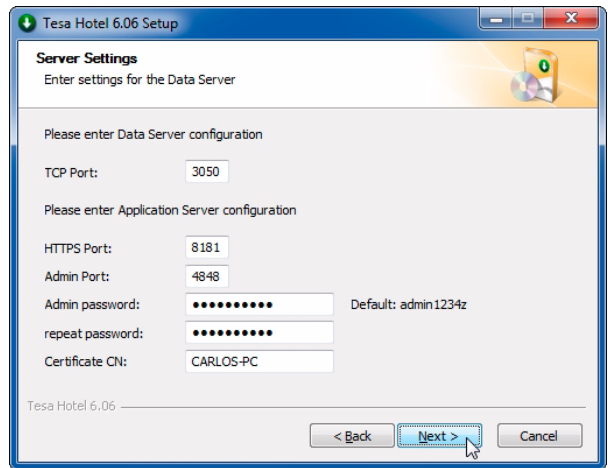
If the hotel only has one PC where the application is going to be installed, we will always select this option (Complete).

If the application is going to be installed in several computers, one of them must be chosen as the Server, where the *Complete* application will be installed, and in the rest the *Client Only* version will be installed



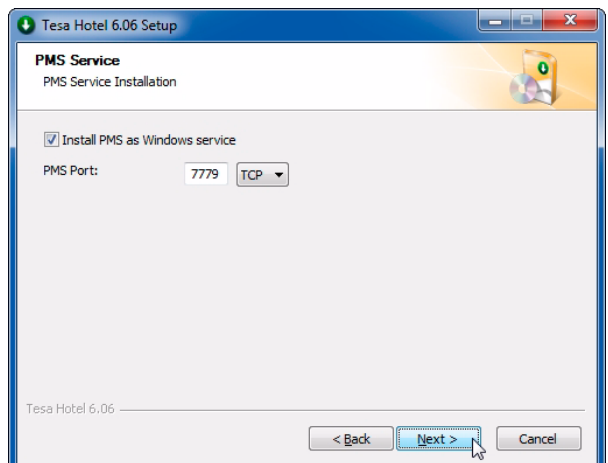
- The “Server Settings” screen is displayed, which allows you to configure the parameters of the server. Configure the parameters (see the table below) and click “Next” to continue.

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.



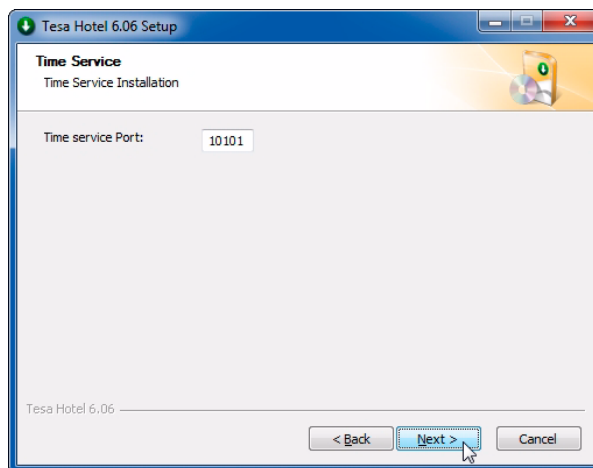
Server settings	Default value	Description
TCP port of the data server	3050	TCP communication port of the application with the data server
HTTPS port	8181	HTTPS communication port with the application server
Admin Port	4848	Administrator communication port with the application server
Admin Password	admin1234z	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 match the IP or machine name used in the browser for web access.

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



Server settings	Default value	Description
Communication port for the PMS protocol service	7779/TCP	Port by which the PMS communicates with the PMS service

- 4 Configure the port for the Time service and click “Next” to continue. The Time service is used to synchronize the dates / times of the devices.

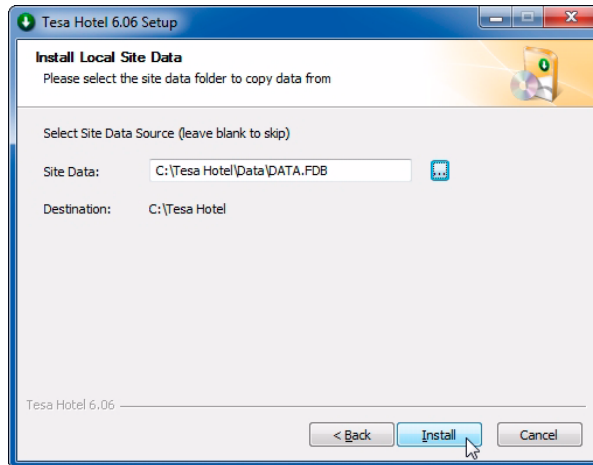


Server settings	Default value	Description
Time service Port	10101	

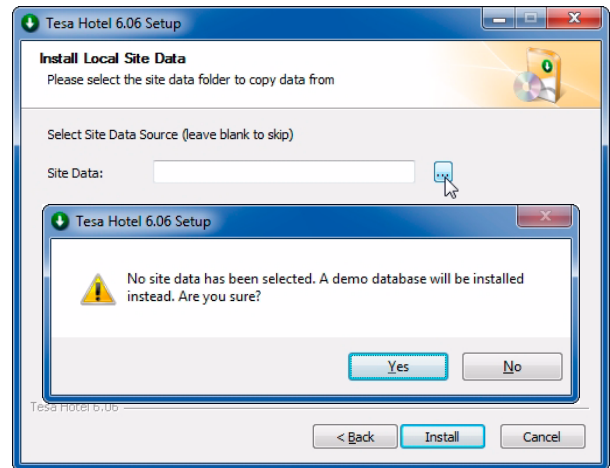
- 5 Data folder: source (physical unit and path) where the database (Data.fdb) to be used is hosted.

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

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



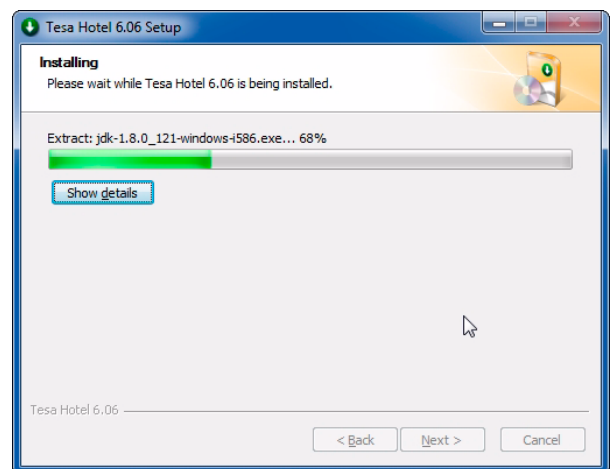
- ☞ If you have not selected the source of the database, a “demo” database is installed by default. **THE “demo” OPTION MUST NOT BE USED ON A REAL SITE**, as its features are limited, and it is not customised according to your order. The “demo” option is appropriate only for tests and demonstrations.



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

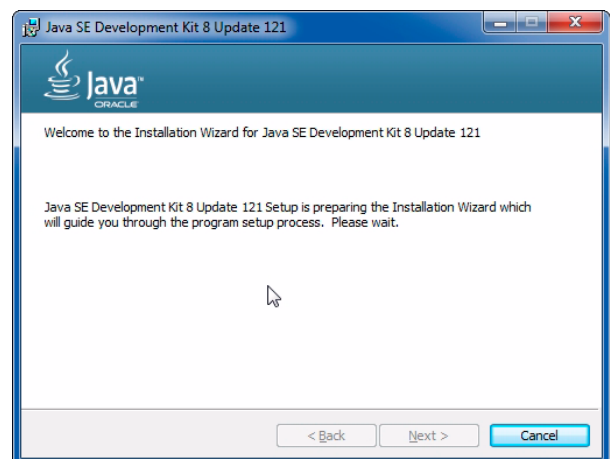
The setup files will be copied to the PC in the following step. Click “See Details” if you wish to view the setup process.

The setup of the application may take several minutes.

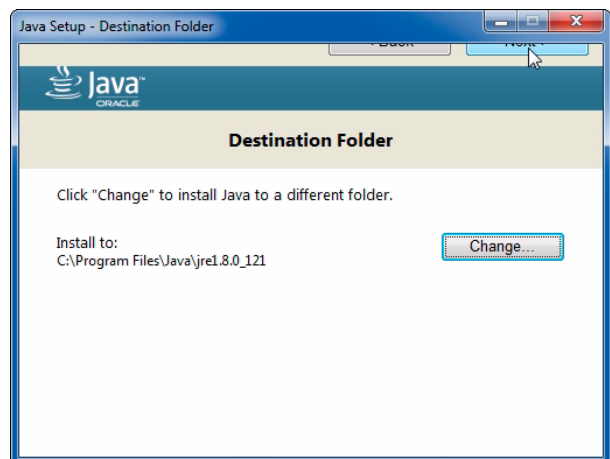
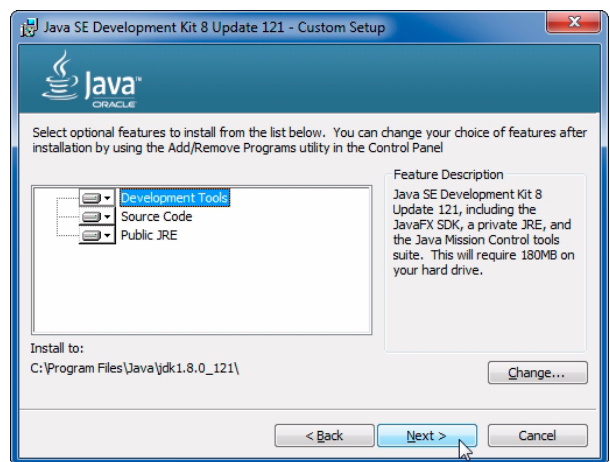
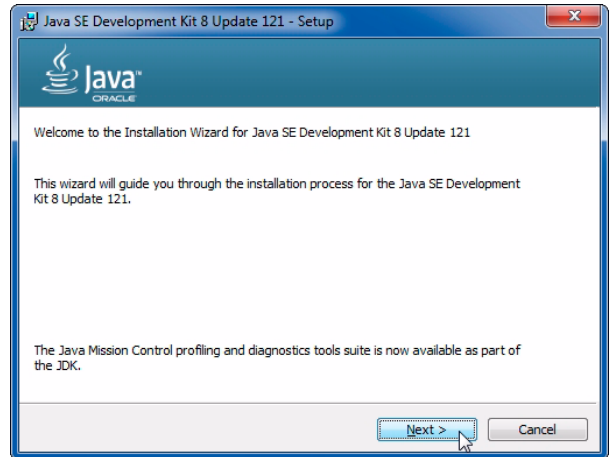


- 7 The setup begins.

If the PC used does not have Java, or it does not have the required version, the installation of Java will be carried out. In such a case, a message pointing this out is displayed. Follow the instructions:

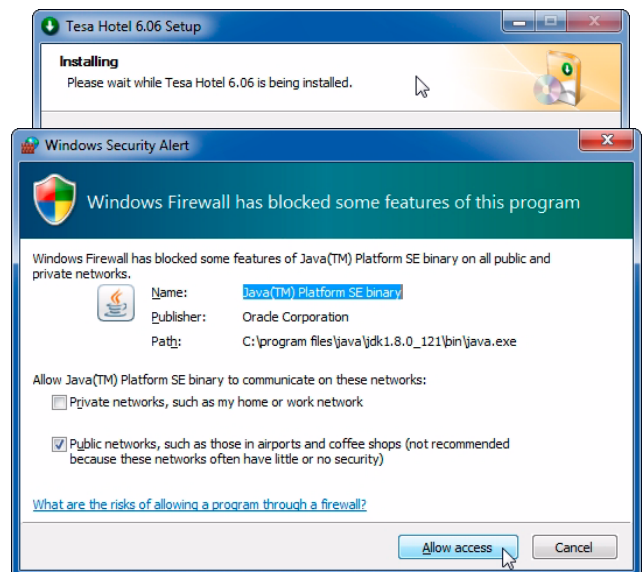


- Click on "Next", and the Java installation will start.

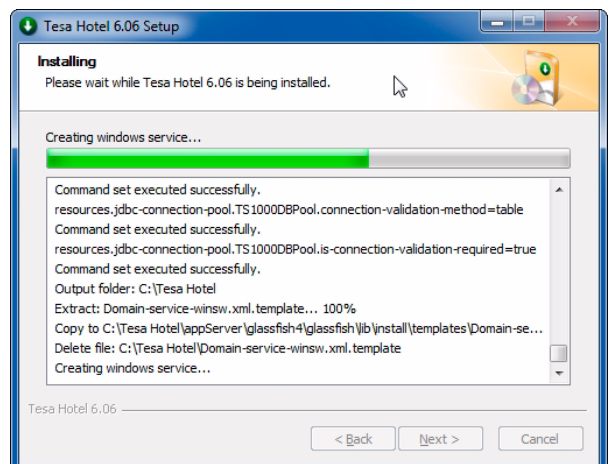




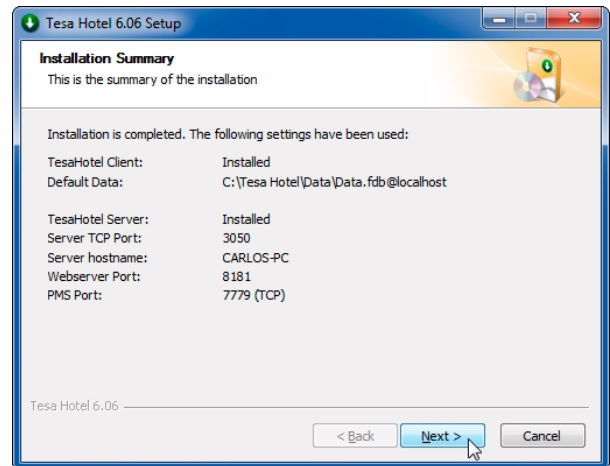
- 9 A warning is displayed indicating that the port which was previously configured in the Windows firewall will be opened. Click “Unblock”.



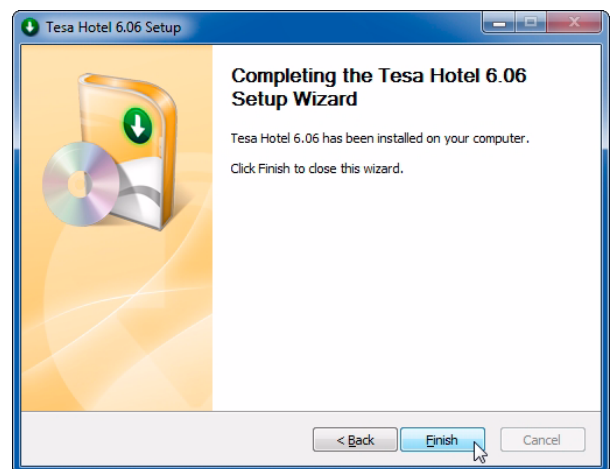
- 10 The setup continues.



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



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



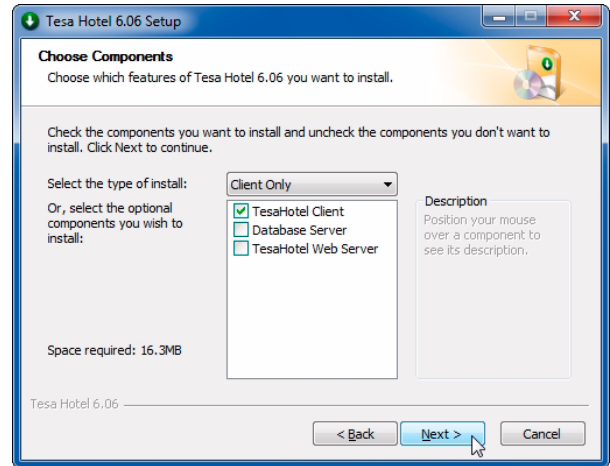
- 13 If the firewall warning shown is displayed, click on “Grant access”.



Setup of the Client Only, with Wireless mode

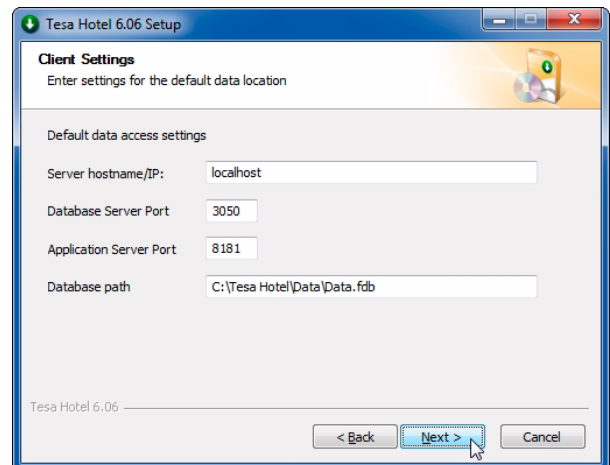
A setup of type Client Only with Wireless installs the application in the Client Only mode on the PC, for example a reception PC, which allows managing wireless devices. A PC with the TESA Hotel application in the Client Only mode communicates with the application server through TCP/IP to access the database and services.

- 1 Select the setup type “Client Only” and click “Next”.



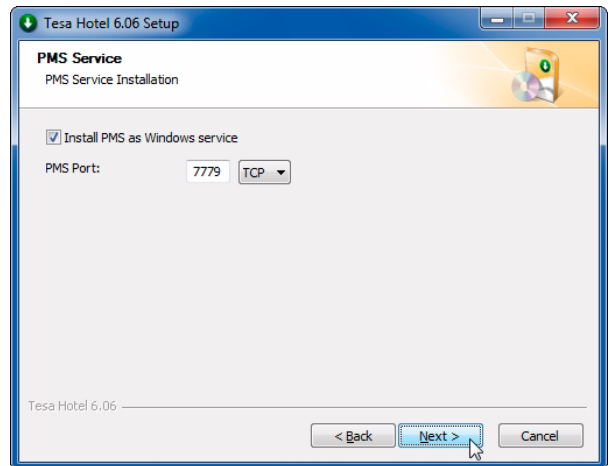
- 2 Apply the Client Settings, which involves configuring the parameters of the Server for the Client PCs.

Once you have finished, click “Next” to continue.

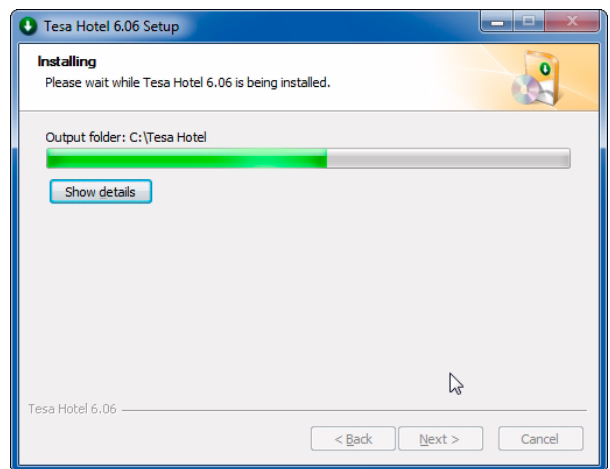


Server settings	Description
Name of the Server PC on the network/IP	Name of the Server PC on the network itself or, otherwise, the IP address on the network
Port of the Database Server	TCP port through which communication is established with the Server which contains the Database
Port of the application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

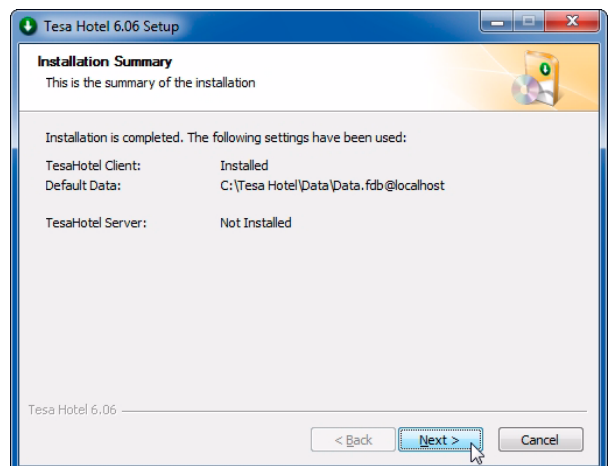
- 3 Configure the PMS service (in the event of being necessary in your site).
By default, the PMS service is on.



- 4 The setup is carried out.



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



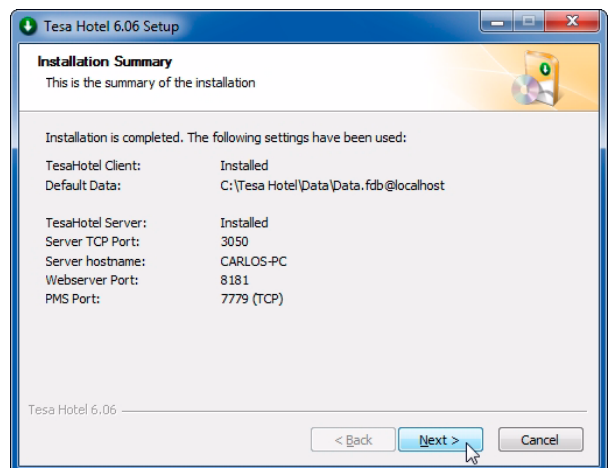
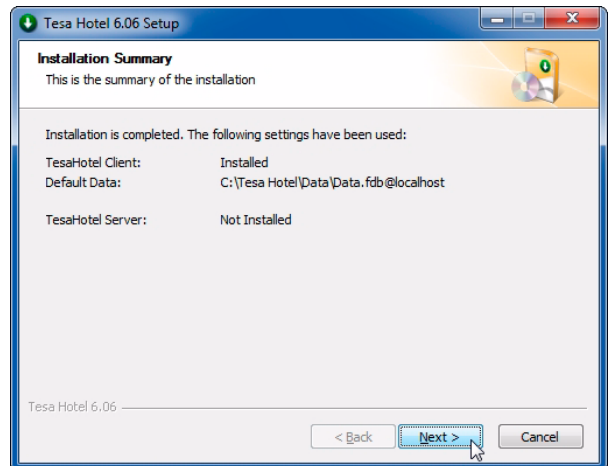
Summary and end of the application setup

In order to finish the setup process (either Server+Client or Client 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+Client. 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 information for Technical Service, for example, in order to solve possible issues during the setup.

Click the “Next” button to continue.



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



If the *Complete Setup* has finished, the Server generates two web applications which can be accessed through the web browser:

Application	URL
TESA Hotel Web Application	https://localhost:8181/TesaHotelPlatform
Server Settings Web Application	https://localhost:8181/TesaServerConfig

replace *host* with the IP address of the server, or in its absence, by the name of the machine in the network

Windows services installed

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

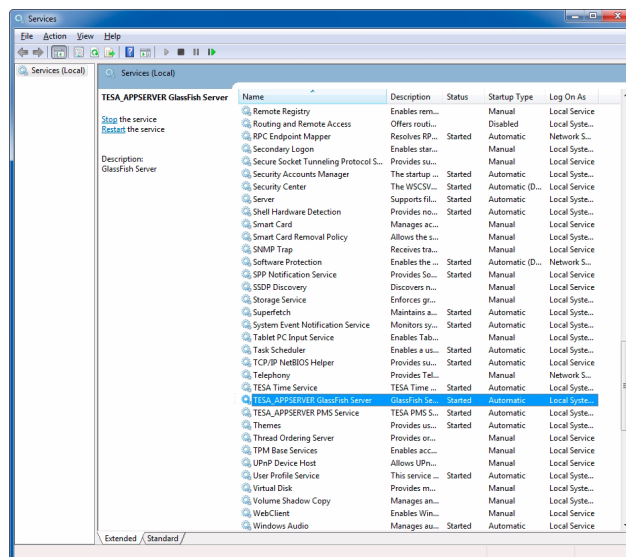
All the possible services are shown below, although only the ones selected are installed:

Name of the Windows service	Description
Firebird Server TESA_DATASERVER_6	Database server This is always installed
TESA Time Service	Service for synchronising the Date and Time with updaters
TESA_APPSERVER GlassFish Server	Application server The <i>Client Only</i> option is not installed
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).



D.6 CONFIGURATION OF THE GUEST PC

Configuration to connect the Client 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 on the Client PC. By default, the folder is "C:\TESA Hotel".

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, where the file of the database (data*.fdb) is located. By default: "C:\TESA Hotel\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:

- ☞ If there is a firewall on the Client 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 clients installed.

```
[SERVERS]
DataServer=210.110.20.28
DataServerPort=3050
DatabasePath=C:\Tesa Hotel\Data\DATA.FDB
WebServer=210.110.20.28
WebServerPort=8181
```

D.7 CONFIGURATION OF THE SERVER PC

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

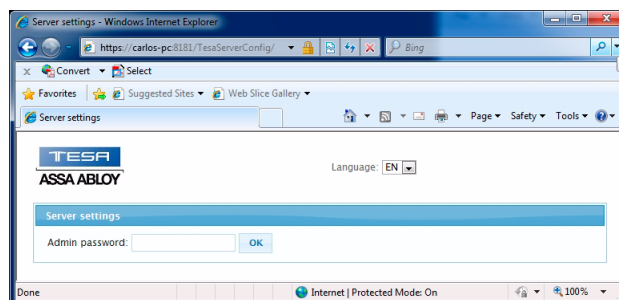
In the event of selecting a local database during the setup process, the Server is configured automatically; therefore, this step is not necessary.

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

<https://localhost:8181/TesaServerConfig>

*replace localhost with the IP address of the server or the name of the machine in the network.

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



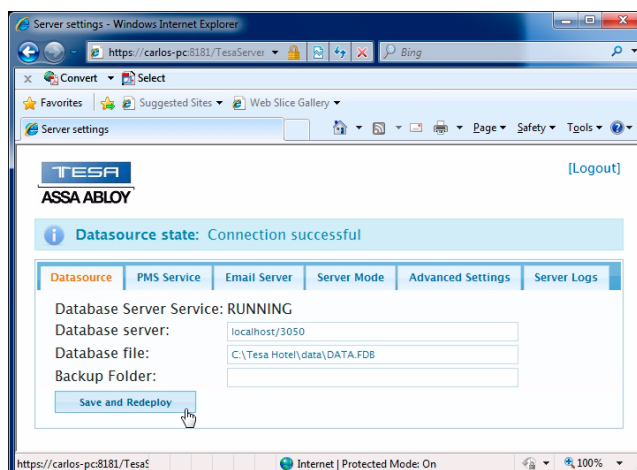
Configuration of the datasource

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:

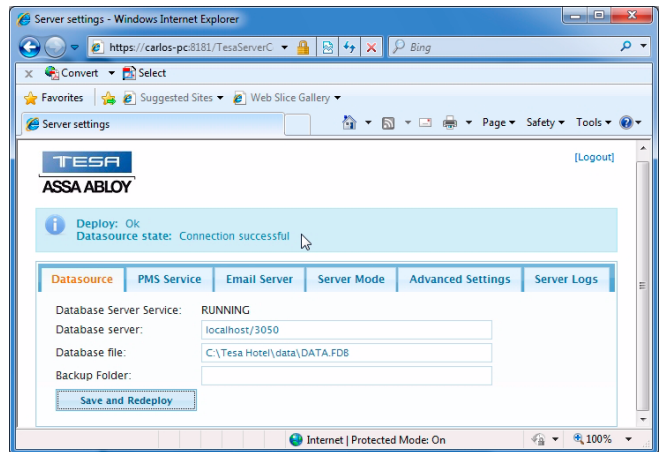
Parameter	Description	Example
Database server	Name of the PC which contains the DATA and its Communication port. Format: Server name/port or IP/port This must always match the path written in the config.ini file of the guests and the server.	localhost/3050
Database file	Path to the FDB Database file	C:\TESA Hotel\Data\Data.fdb

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



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, using the Task Manager of Windows.



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

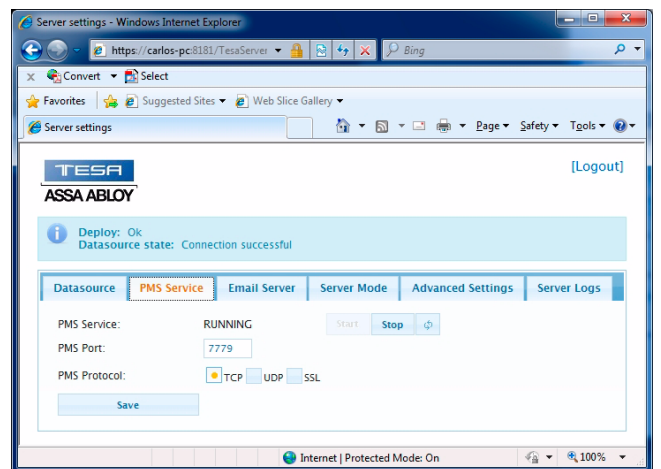
In order to configure the PMS Service, access the “PMS Service” tab and configure the following settings (this tab only appears if, during the setup, the option “Install as a Windows service” has been selected, on the screen “PMS service setup”):

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 client is compatible.

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



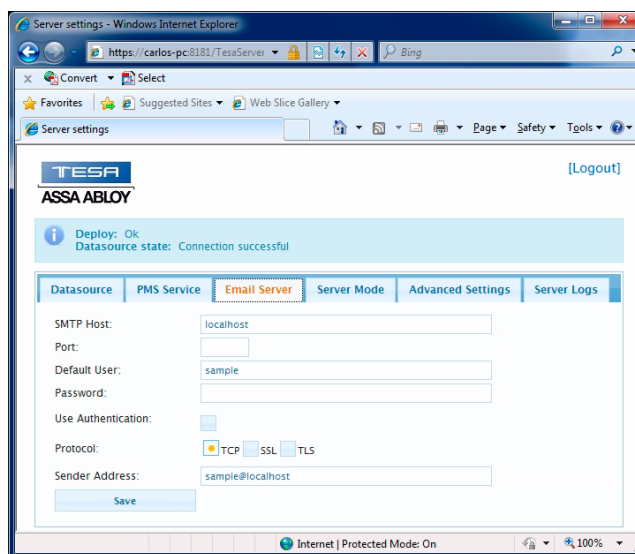
Configuration of the E-mail Server

The Server can be configured to connect to an Internet SMTP server and send warning/alarm e-mails. This e-mail server is also necessary if we wish to use the *Check In PIN* or automatic *App Wireless* functionalities. 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 (e-mail address)
Password	Password for SMTP authentication
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@TesaHotel_warning)

Click “Save” to save the changes. If a new E-mail Server is configured, it is necessary to restart the GlassFish 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).



Configuration example: typical SMTP configuration for 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.

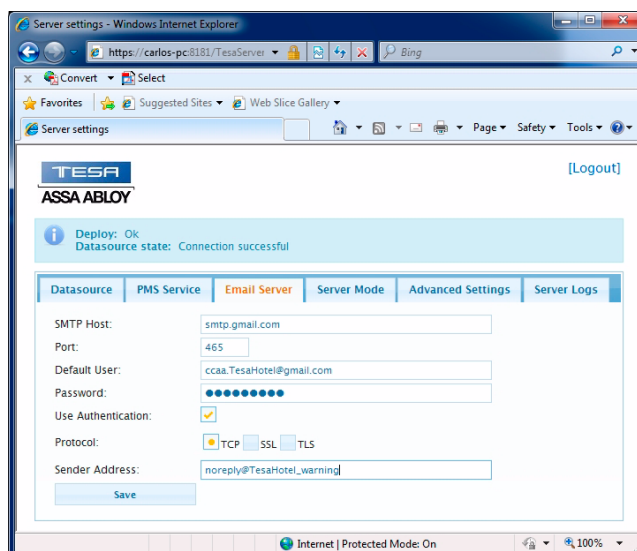
Both protocols use a secure connection for their encrypted communications.

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@TesaHotel_warning

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@TesaHotel_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 more restricted access.

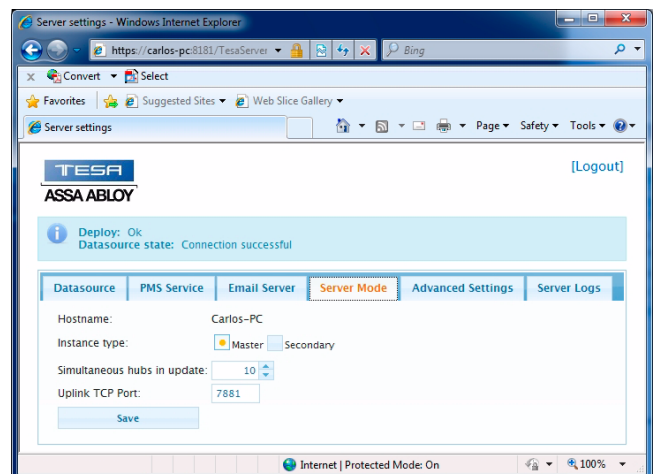
When there are several servers for the site, one of them must be configured as Master and the rest as Secondary.

- 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/connected 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 (**VERY IMPORTANT**).

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.

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 175.

Advanced settings

The expiry of the HTTP sessions (*auto-logout*) and the administrator password are configured in this tab.

Expiry of the HTTP sessions

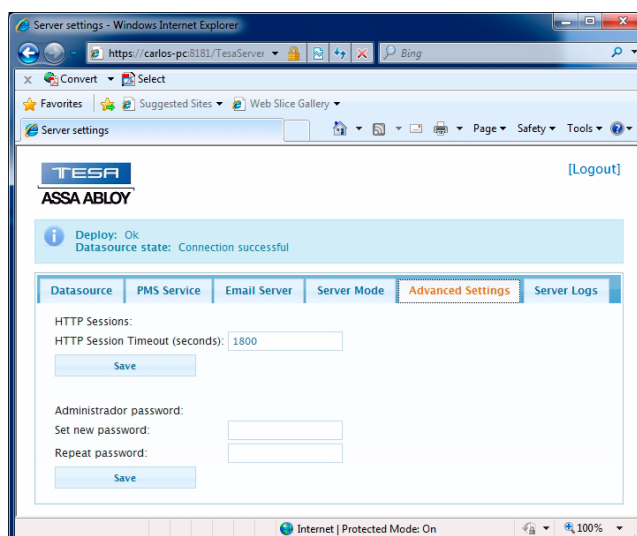
The value in seconds of the expiry of the HTTP session defines after how many seconds of inactivity the system automatically ends the session of the web application. The default timeout is 1,800 seconds (30 minutes), but it can be customised to the desired value. After configuring the value in seconds, 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.

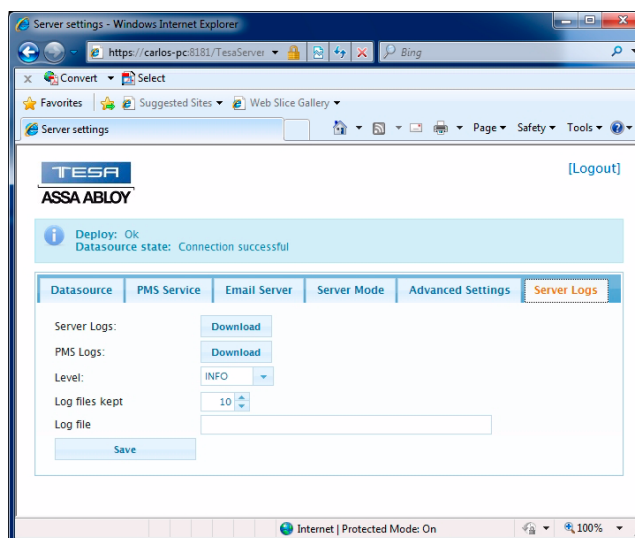


Configuration of the Server Logs

It is possible to download the information from 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 (no 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	No 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 Information for Technical Service in the event that any problem arises 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.



Notes to be considered in relation to the Windows antivirus or 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 clients 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:

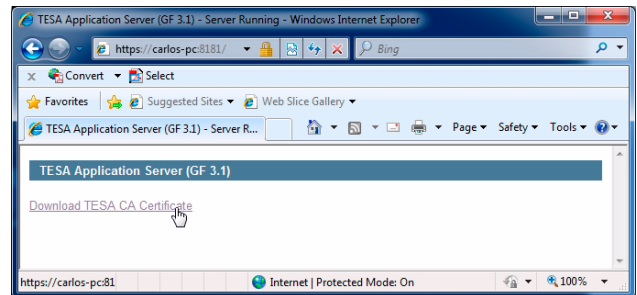
TESA CA Certificate property	Value
Serial number	00 f3 74 bc 60 6a ee 0e f8
SHA-1 hash	e1 13 16 37 c8 fe f6 ba 5a 87 dd 9a 7a 70 1d f5 61 5f60 c2

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:\Tesa Hotel).

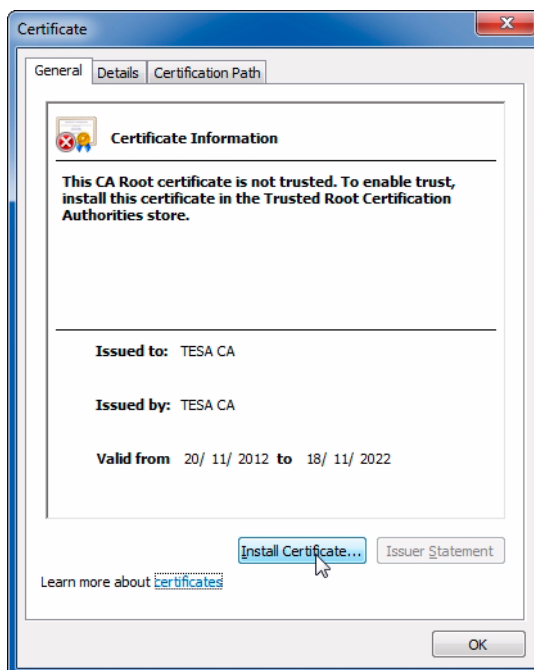
In addition, it can be downloaded through the browser, from the URL address of the Server location (for example, <https://host:8181/>) by clicking the link [Download TESA CA Certificate](#).

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



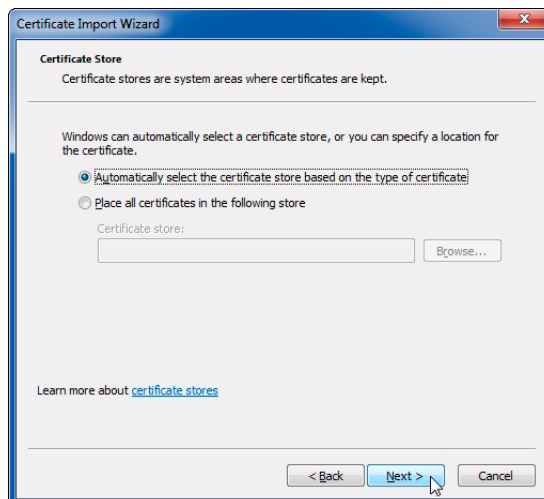
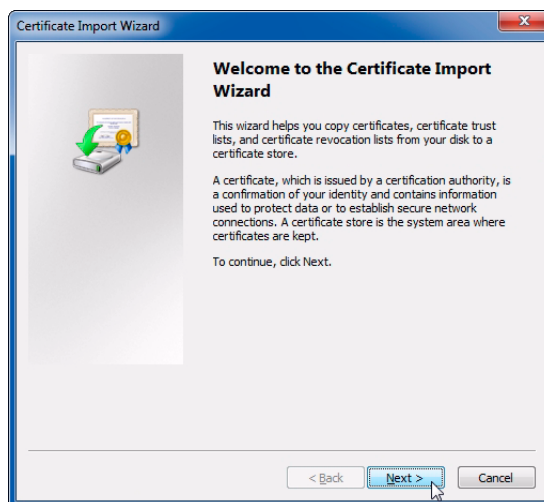
Setup of the TESA CA certificate with Internet Explorer

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

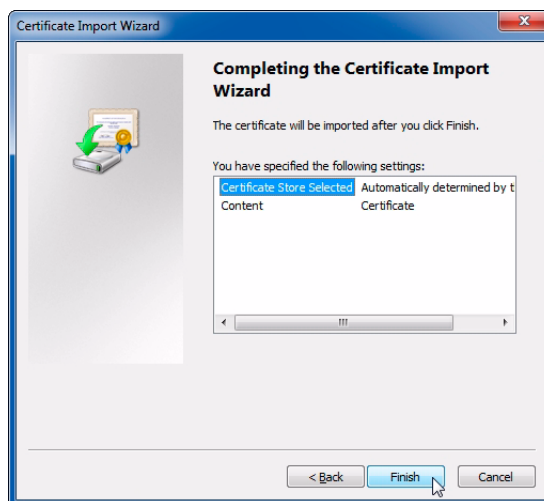


Click the “Install Certificate” button. A setup wizard is run.

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



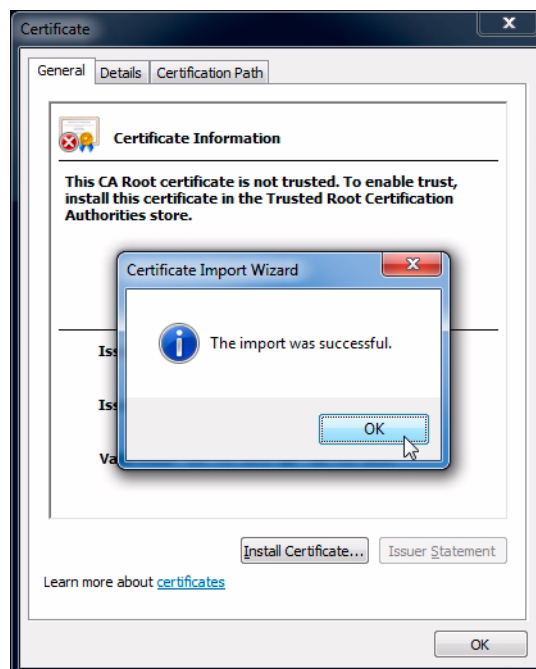
In the last step, click “Finish”.



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

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

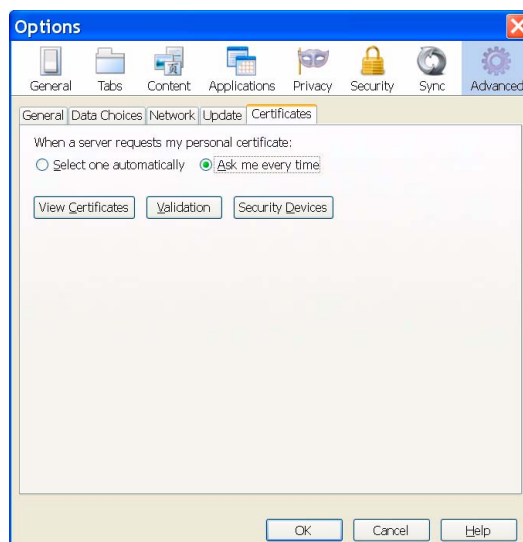
Finally, a message confirming that this has been done correctly is displayed.



Setup of the TESA CA certificate with Mozilla Firefox

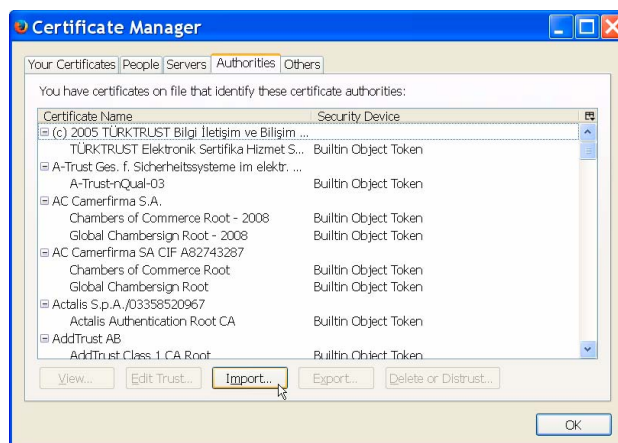
Open the Options menu (Tools -> Options) of the browser.

Click the "Advanced" menu in the "Certificates" tab.



Click the "See certificates" button and select the "Authorities" tab.

View Certificates

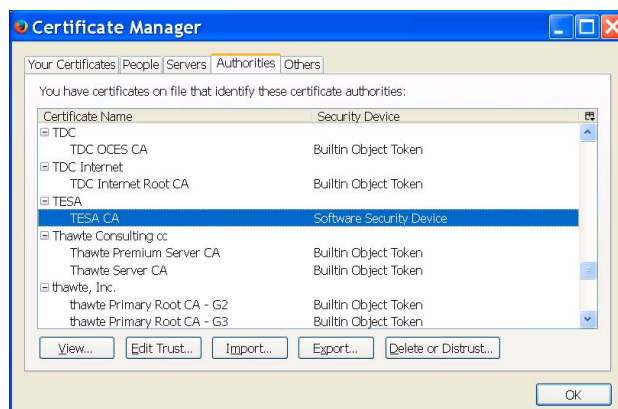


Click the "Import" button and select the ca.crt file from its location in the system.

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



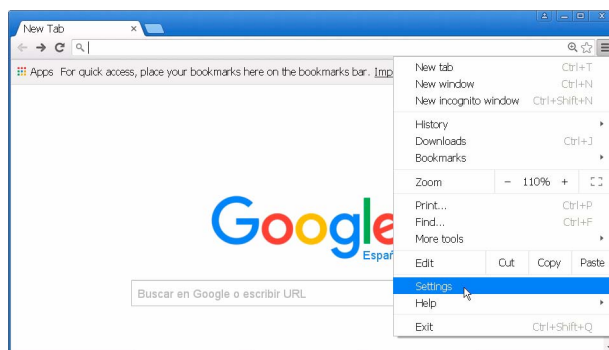
The authorisation of the TESA CA certificate will be added to the list of authorised certificates.



Setup of the TESA CA certificate with Google Chrome

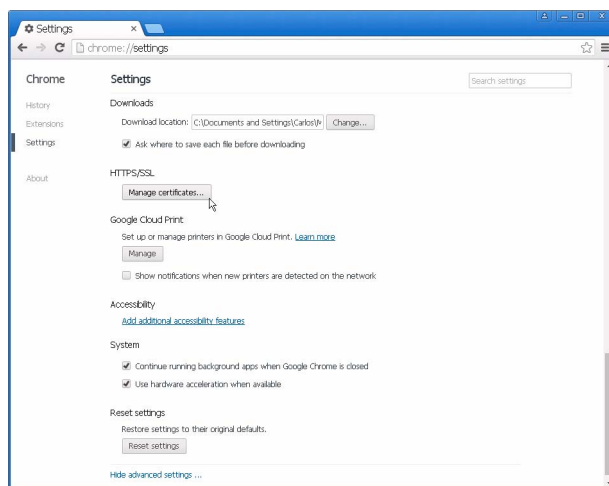
Open the Google Chrome browser and proceed as follows:

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

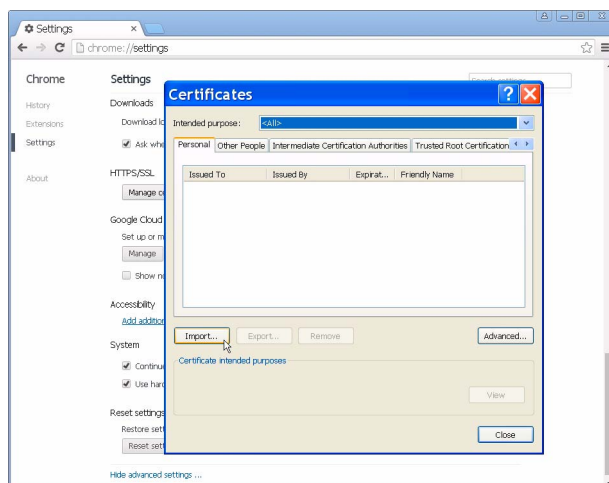


- 2 Scroll down, through the Advanced Settings, until you reach HTTPS/SSL.

Click the “Manage certificates” button.



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



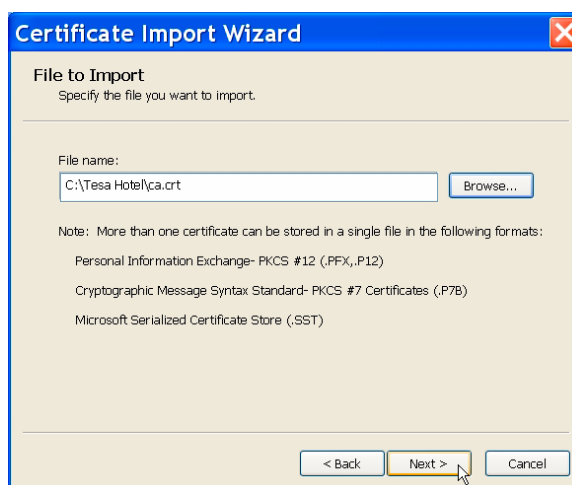
- 4 The “Certificate import wizard” is displayed.

Click the “Next” button.



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

Click the “Next” button.



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

Leave the default option and click “Next”.

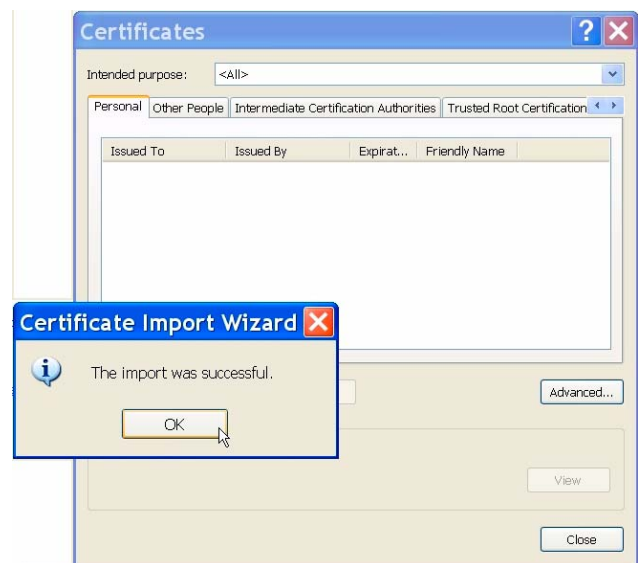


- 7 A window is displayed showing a box with the properties of the certificate imported.

Click "OK".



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



D

D.9 IMPORT OF A DATABASE FROM AN OLDER VERSION OF THE TESA Hotel APPLICATION

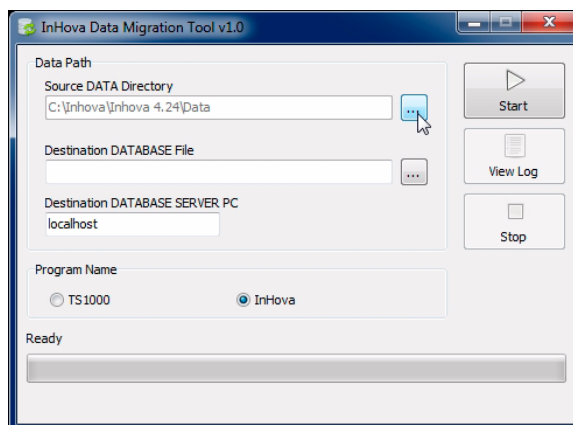
Import of a database from a 4.x version

This process can only be carried out if the both database engines are installed, Paradox (for 4.x databases) and Firebird (for 5.x databases and higher); both versions installed in the PC.

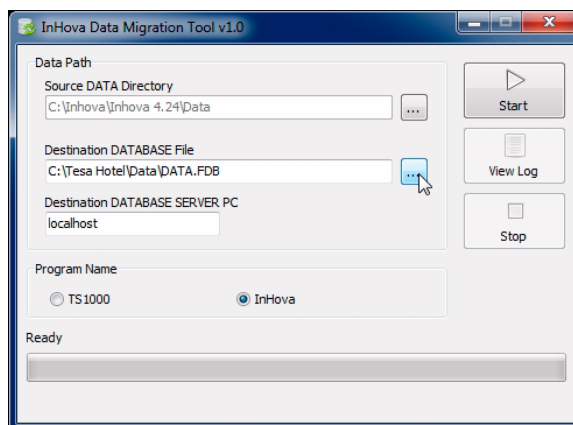
The resulting file is directly compatible with the 5.x versions, but not with the 6.x. It is necessary to open it with a 5.6 so that it can then be opened with a 6.x. If the client has a 6.x version, it will not be able to open the database even if it manages to import it.

In order to import a *data* from a TESA Hotel 4.x version, into a TESA Hotel 5.x 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.



- 2 Select the name of the target database (for example, DATA.FDB) in the server. If the database does not exist, type a new name.

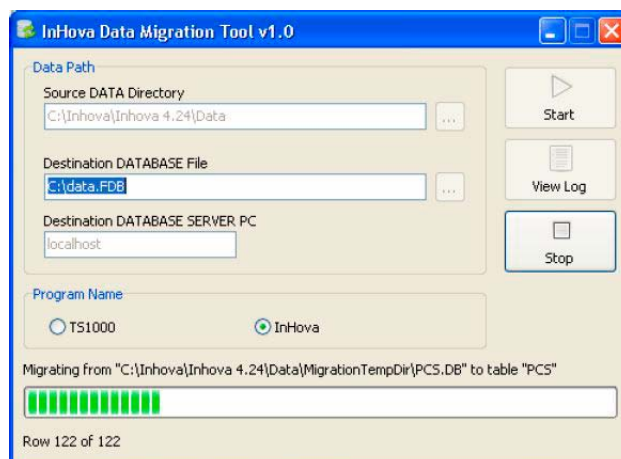


- 3 Choose the name of the database type “Inhova”.

- 4 Click the “Start” button.



- 5 Wait while the process is carried out.



- 6 When the process ends, a message similar to this one will be displayed:



- 7 Open the database converted by means of the TESA Hotel 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 TESA Hotel is too old, so that, before using the migration tool, you would have to update the database to a higher version of TESA Hotel, 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 of the 6.x version itself.

When a 5.x version is updated to a 6.x version, the TESA Hotel application is run during the update process and a dialogue box is displayed asking for permission to update the database to v6.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 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.

A converted database and a 6.x version can no longer be opened / used by a 5.x version.

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 match 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.

TESA Hotel Client Message:**“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.

TESA Hotel Client Message:**“The TESA Hotel database and the location of the database do not match”****Possible cause:**

The TESA Hotel Client PC and the Server PC are accessing different databases, or the Server is using the *localhost* name rather than the real name of the machine in the network, or the redirection 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 client 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” in the file *config.ini* and the field “Database server” do not match. 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 client and server at the same time.

The TESA HotelPlatform web application is not running

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 HotelPlatform application is only available at the URL address

<https://host:8181/TesaHotelPlatform/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

Operator Name and Password	57
“Setup” menu	58
“General” tab	58
“License” tab	61
“Antipassback” tab	63
“Network” tab	65
“Local PC” tab	65
“Common PINs” tab	67
“Extra Fields” tab	67
Other tabs and functions	67

E

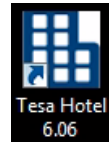
E – RUNNING THE PROGRAMME FOR THE FIRST TIME

E.1 OPERATOR NAME AND PASSWORD

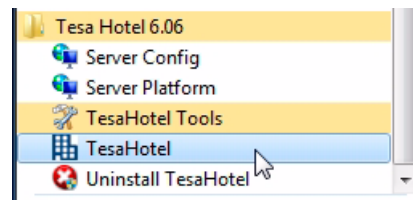
After installing the software as described in the corresponding chapter, the programme is now ready to be run.

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

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

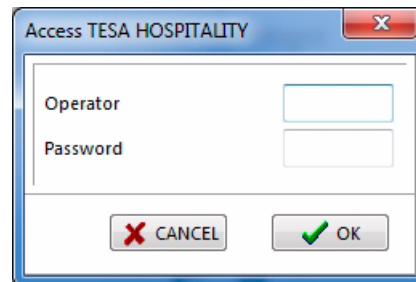


- In the event of a local setup, running it from the TESA Hotel entry of the “Programmes” menu of Windows.



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 TESA Technical Service, indicating the 8-digit alphanumeric code which is labelled in the license.



- ☞ 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 123.

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

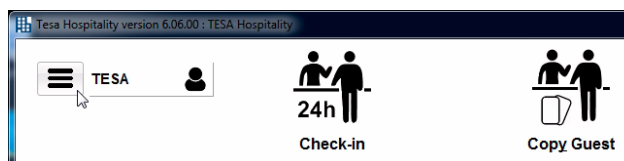
The main screen of the TESA Hotel programme is displayed and, as a result, it is possible to start configuring the locking plan.



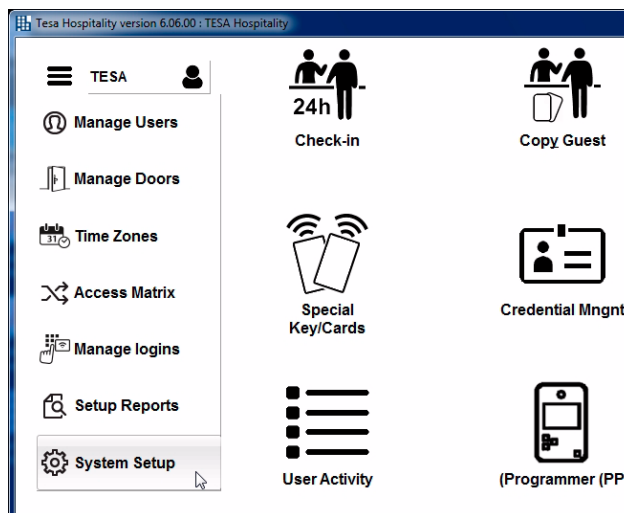
E.2 “SETUP” MENU

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.

Unfold the setup menu by clicking on the corresponding button, located at the top left of the main screen.



Access the “Setup” menu by clicking on the corresponding button on the main screen.



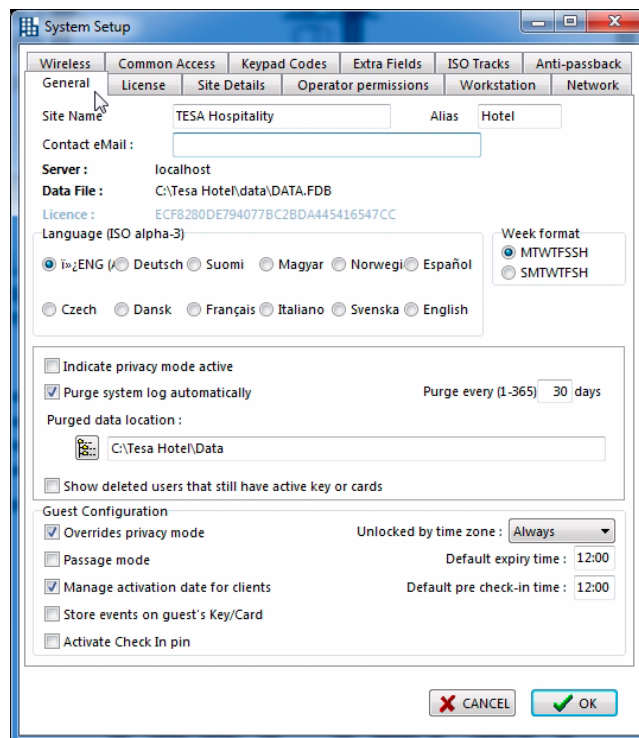
“General” tab

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

- Site name
- Short
- Contact e-mail
- Language
- Week type
- Signal privacy to staff
- Purge auditors periodically
- Show deleted users with non-expired card/key

Options for guests:

- Overrides privacy
- Can leave door open
- Manage activation date for guests
- Audit openings on guest's Card/Key
- Activate Check In PIN
- Open with timezone
- Default expiration time
- Default Pre-Check In time



Each of the fields is described below.

Site name: this is the name which will be displayed on the main screen of the TESA Hotel programme, 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 site name from being seen if it is too long.

Contact e-mail: during setup and registration of the application, this field will serve as a contact for future communications with your distributor or official TESA technical service.

Language: this is the language used in the TESA Hotel 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).

Signal privacy to staff: this option enables staff to know whether a room is occupied (with privacy activated) without having to open the door. If the "Signal privacy to staff" option is activated, when the staff card is inserted in a lock that has privacy activated on the inside, the LEDs of the lock flash red and green, informing us that the lock has the privacy lever deployed (and therefore the room is occupied). Afterwards, if the user has a grant to open the door, it will open or not, depending on whether the user overrides privacy or not, as configured in their matrix.

Purge auditors periodically: the Auditor is a file where all the operations carried out in the TESA Hotel programme are recorded. Each record provides information on 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 system 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. Every certain number of days this function automatically saves the registers of the audit file in an ASCII file, which can subsequently be audited at any time.

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.8 Openings" on page 216 and "K.10 Auditor" on page 226).

Show deleted users with non-expired card/key: If this action is activated, 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.

OPTIONS FOR DEFAULT GUEST CONFIGURATION:

Overrides privacy: selecting this option allows all the guests to “override” the privacy lever of the lock of their own room. This means that if someone inside the room has activated privacy using the corresponding lever, it is possible to enter from the outside by swiping the card and pushing the handle, which will withdraw both the latch from the lock and the privacy lever.

If the “overrides privacy” option were not activated and the privacy lever of the lock were not deployed, the door could not be opened from the outside with the guest's card or the copy thereof, and the lock would indicate this by the flashing of both warning LEDs.

In hotels the most common practice is to select this field.

Can leave door open: if this option is selected, the guests can leave the door of their room in Open Mode if they so wish. It is possible to change from Open Mode to Standard Mode or vice versa, by swiping the card through the lock twice in a row. If the door is in Open Mode, anybody can enter the room with no need for any card whatsoever, simply by pushing the handle down.

In hotels it is NEVER advisable to activate the “can leave door open” option as it is highly likely that some guests may leave their door in Open Mode without realising it, with the consequent risk that anybody could access that room.

Manage activation date for guests: if this option is activated, it is possible to encode the guests' cards before their arrival, indicating the date and time at which they will be operational in them. In this way, the cards can be encoded days before the guest arrives, but they will not work until the activation date indicated.

This option is very useful when arrival of a large group of guests is expected on an upcoming date. In this case, it is possible to encode the cards in advance and have them ready for their arrival.

Audit openings on guest's Card/Key: if this option is activated, the guest's card or key will audit all the openings they perform in all of the doors of the facility using said card or key, as long as they incorporate proximity locks or electronic cylinders with the Read and Write system and the credential is Mifare 1K or 4K.

Activate Check In PIN: select this option to activate the *Check In PIN* functionality for the guests. When Wireless locks with keypad are used, this functionality enables us to send an e-mail to the guest, indicating their PIN code to access the room without the need for any credential whatsoever. For more information, see “L.4 *Check-in PIN*” on page 251.

Opened with timezone: activating this option restricts guests' access to their rooms in accordance with a timezone. All of the guests will have the same timetable restriction. There are two predefined options - Always and Never. To make more timezones available to choose from, they must first be defined in the “Hours” menu (see F.4 “Hours” menu on page 108).

Default expiry time: this option indicates the default time at which the guest's card expires, on the day they perform the *Check Out*. This time, which is predefined for all the guests, may be customised for any guest when their card is encoded during *Check In*.

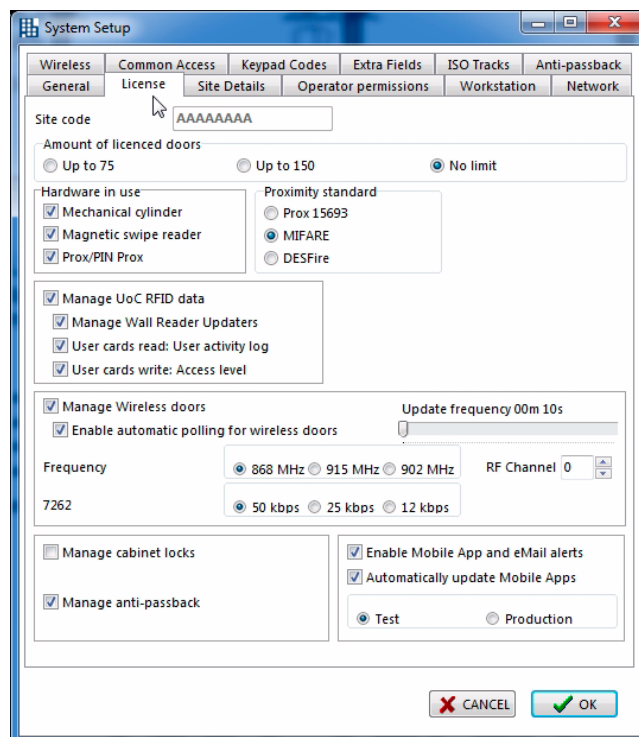
Default Pre-Check In time: this option indicates the default time at which the cards are activated, when the encoding mode *Pre-Check In* is used. This time, which is predefined for all the guests, may be customised for any guest when their card is encoded during Pre-Check In, in the “Check In” menu.

“License” tab

Only the “Reading technologies” parameters and the parameters of the wireless management can be modified in this tab (the latter if a wireless license 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 setup 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.



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

- Facility code (unique and exclusive to each site)
- Maximum number of doors of the site
- Update on Card and its parameters (Read and Write functions)
- Manage wireless doors
- Manage Emotion cabinet locks
- Manage Antipassback
- Allow applications for mobiles and sending of e-mails (by default for wireless setups)
- Automatically update Mobile Apps
- Test / Production

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 on the identification labels of the license folder (see “Licence” on page 15).

Reading technologies: the TESA Hotel 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 determined 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:**
Proximity read-write chips according to the ISO 15693 standard.
- **Mifare:** Proximity 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. To do so, we must access the “Facility” tab (contact your distributor or the official TESA technical service).
- **Desfire:** Compatible with Desfire EV1.

Update on Card (Read & Write): this allows defining whether updaters will be installed, in addition to readers and/or read and write 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 locking plan of the doors without having to go to them. For this purpose, Updaters are available, which are connected to the PC over Ethernet. In this way, when any modification is made in the matrix of the TESA Hotel software, the information is transmitted to the Updater over Ethernet, which updates the user’s card when it is held within range of the Updater. Afterwards, when the user holds the card by the door, that door will be updated with the new information contained in the card.

The menu allows for activation of communications with the Updaters, auditing of openings in the credentials and modifications in the locking plan entries in the same credential.

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 159.

Manage cabinet locks: it is also possible to manage *Emotion* cabinets. In order to manage this type of device, it is necessary for this box 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 import 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 license acquired. Management of the *app* for both users and guests is handled manually by the hotel.

Automatically update Mobile Apps: in the wireless licenses, this allows the IP changes to be sent to the wireless Apps of the site automatically, so we may dispense with fixed IP addresses in the site. For more information, see “L.5 Wireless APP” on page 258.

Test / Production: this field indicates whether the management of “Automatically update Mobile Apps” is conducted in a “Test” environment, that is, demo-tests, or in a standard “Production” environment.

“Antipassback” tab

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

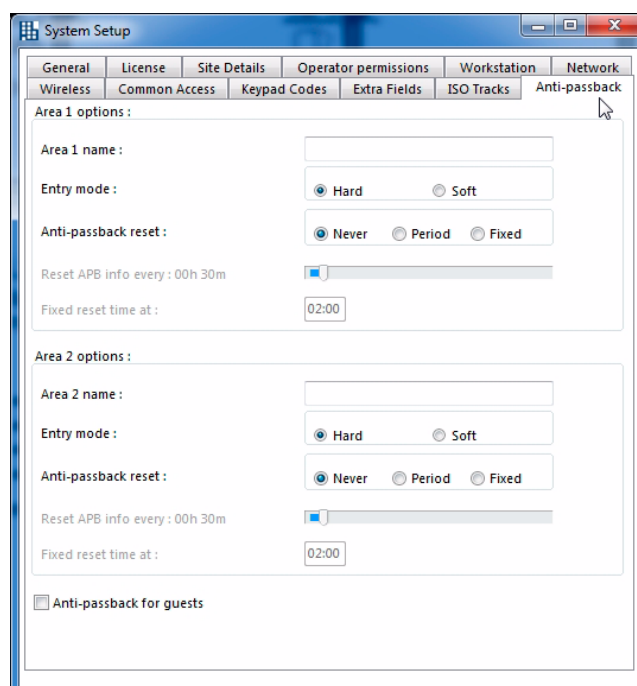
The Antipassback system serves to prevent multiple accesses with the same credential, preventing for example two people going through the same door one after the other using the same credential, having passed it from one to the other. It functions as follows:

- 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 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* and then deletes it
 - 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 every...* to be defined).

After having defined at least one antipassback area, in the “Doors” menu, for each door, a field is displayed which allows us to define 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.

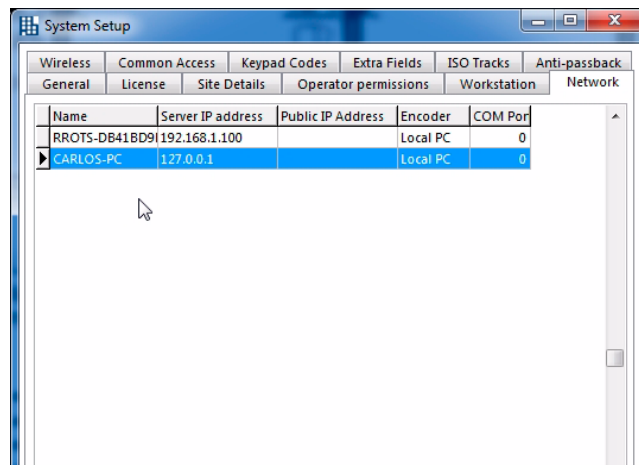
- **Antipassback for guests:** this operates in the same way as the user's credentials, applied to guests.

“Network” tab

The TESA Hotel system can be installed on a network of PCs.

In the “Network” tab of the “Setup” menu of the TESA Hotel 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 it.

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.



“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 TESA Hotel programme is being run.

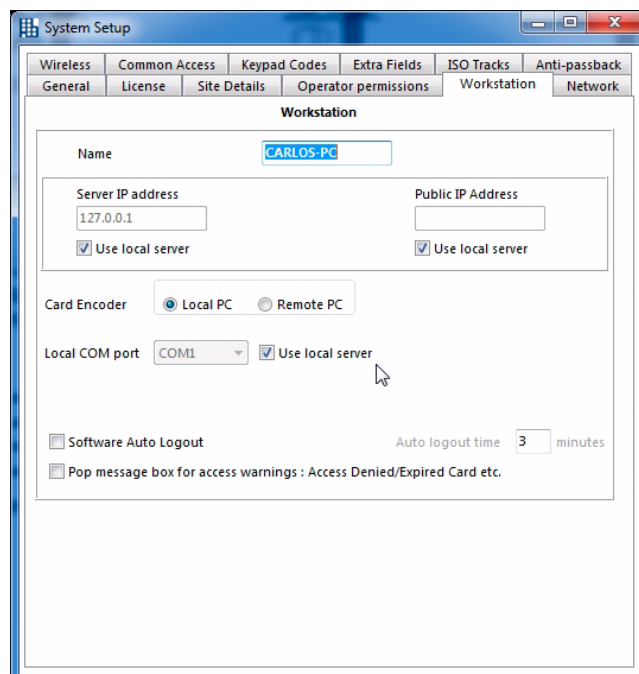
The following data are shown:

- Name of the PC in the network
- IP Address
- Public IP address on Internet
- Card Encoder
- Local COM
- Use timed auto logout
- Pop up openings rejections and warnings

Each of the fields is described below.

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’s “Control Panel” in Windows.

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 encoder and, therefore, it is necessary to enter an identification name, clicking the “Change” button. Contact your distributor if you need assistance.



IP address (private or public): these IP addresses can be configured to remain fixed or be automatically updated. You simply have to set the public IP to automatically update when the server is accessible from the Internet and has not engaged a fixed IP address.

Card Encoder: if the TESA Hotel system is installed on a single PC, the card encoder will always have to be connected to that computer 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 may be connected via RS-232 or USB to one of the PCs and the rest will be able to use it remotely (for example, by sharing an encoder in a reception area with several PCs with the TESA Hotel application). This is valid for:

- Encoder of magnetic stripe cards
- Proximity card 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 or USB, 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 TESA Hotel 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 TESA Hotel 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 virtual 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 on the PC that has the TESA Hotel software installed in it, “Pop ups” will be displayed showing the denials and warnings of the doors automatically.

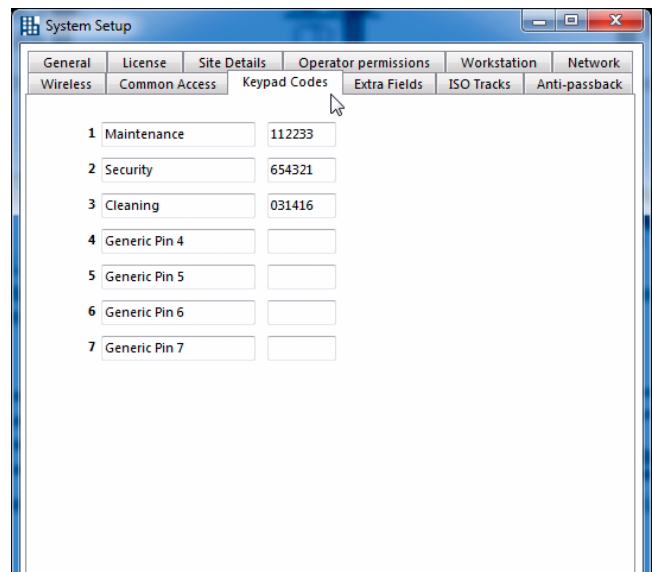
A “Pop up” is a pop-up window located in the lower right-hand area of the screen, which is only displayed when a new alert is generated.

“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, as a staff PIN.

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

It is necessary to assign the Common PINs to the doors where they will be used (see F.3 “Doors” menu on page 82).



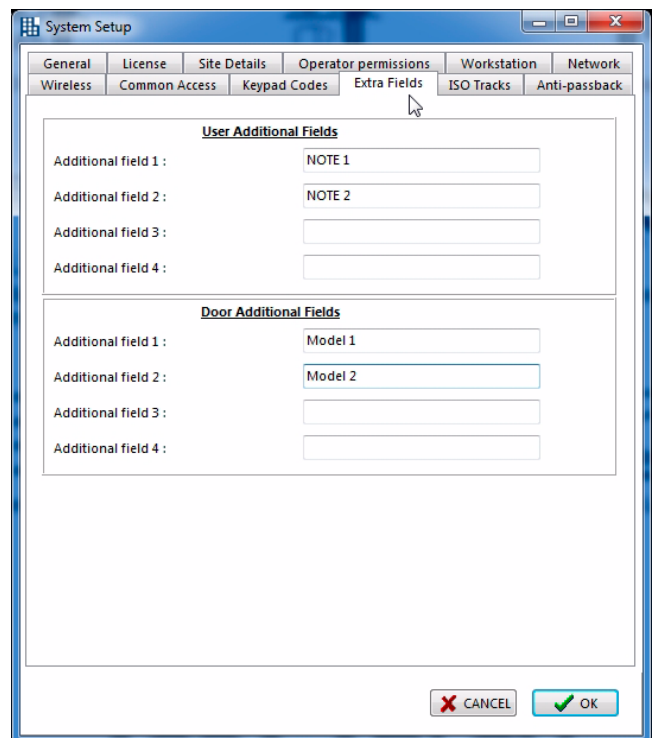
“Extra Fields” tab

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.

Extra Fields are applicable both to staff card users and guests.

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 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.



Other tabs and functions

The other tabs and functions are explained in chapter “L – Other Functions” on page 237.

F –Creating the Locking Plan

Introduction	71
“Users” menu (master)	72
Staff card copies	80
“Doors” menu	82
Doors list	82
Create the doors list of a hotel	88
Reports	105
Multi	105
Find	107
Matrix	107
“Hours” menu	108
“Hours” tab (timezones)	108
State table	109
“Updating Mode” tab	111
Calendar	112
“Daylight Saving Time” tab	113
Matrix	114
Saving and transferring the locking plan	117

F – CREATING THE LOCKING PLAN

F.1 INTRODUCTION

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

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

- 1 Creating the users list, by means of the “Users” menu.
- 2 Creating the doors 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 the plan into the Portable Programmer to initialize the locks, readers and/or cylinders, as will be seen in the corresponding chapters.

- ☞ 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 *Read and Write* systems, **it is VERY IMPORTANT to previously configure the distribution of data on the cards** (see “Proximity setup” on page 239).

F.2 “USERS” MENU (STAFF CARDS)

The first step in creating a locking plan is creating the users list in the “Users” menu (staff cards). In this menu we define the system users who form part of the hotel staff (not the guests). The guests are defined in the “Doors” menu, when the doors or locks of all of the hotel rooms and suites are created.

Therefore, in this menu we define all of the users who are not guests and who have a credential to open locks, or those who will be system operators, or both.

The system is capable of managing up to 65,000 users and every lock is able to recognise up to 1,500 different users.

We could give the example of a hotel with the following staff structure:

- MANAGERS
 - Manager
 - Head Receptionist

- CLEANING
 - Cleaning 1
 - Cleaning 2

- MAINTENANCE
 - Maintenance 1
 - Maintenance 2

The system allows for identification of staff by their name, by their post, by an identification number, etc. In the example, we will use generic names (Cleaning 1, Maintenance 1, etc.).

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

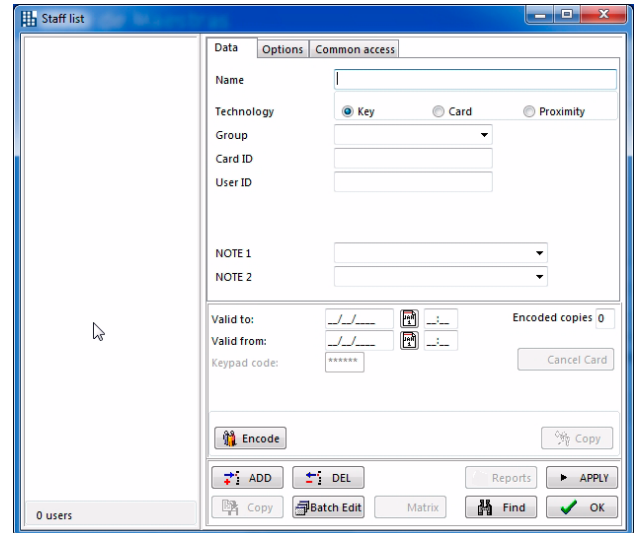


Creating the Locking Plan

The “Staff List” window will open.

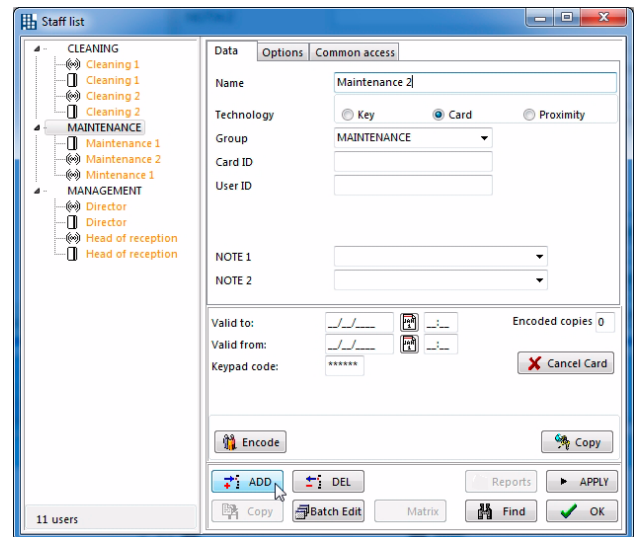
Click on “Add” to start adding users.

Fill out the fields, and when you finish, click on “Add” and accept the confirmation message that appears next.



Proceed similarly to add more users.

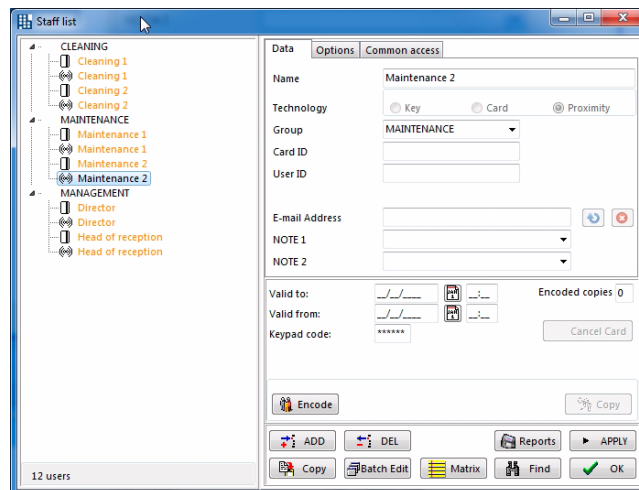
If you want the same user to be able to have two different opening technologies available (for example, magnetic card and proximity card), the user has to be created twice, with the same name, changing only the technology type.



F

In the “Staff List”, in the “Data” tab, the following fields and buttons are displayed:

- **Name:** user name.
- **Technology:** technology of the credential that will be delivered to the user. There are three types: key, magnetic stripe card and proximity card.
- **Group:** name of the group the user belongs to. In the example, the users have been organised into three groups: “Cleaning”, “Management” and “Maintenance”.
- **Card ID:** unique identification number incorporated into all the source credentials, which is read and recorded when the user card is encoded (UID).

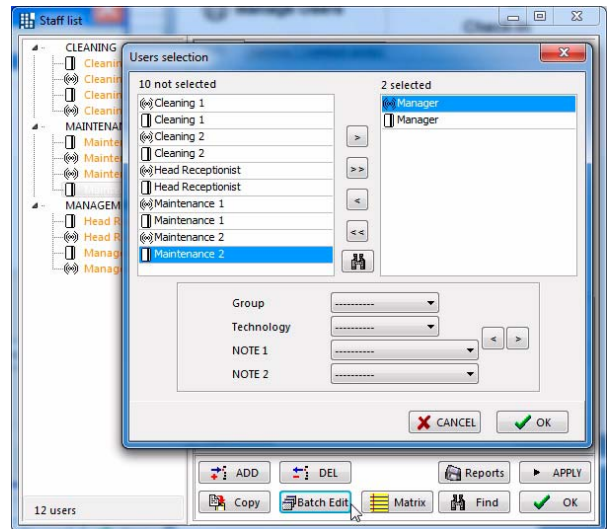


It is also possible to carry out the process the other way around: writing the ID manually if this is known, distributing the credentials which are not encoded, and delegating the encoding to an automatic updater which is connected to the database and made available to the users.

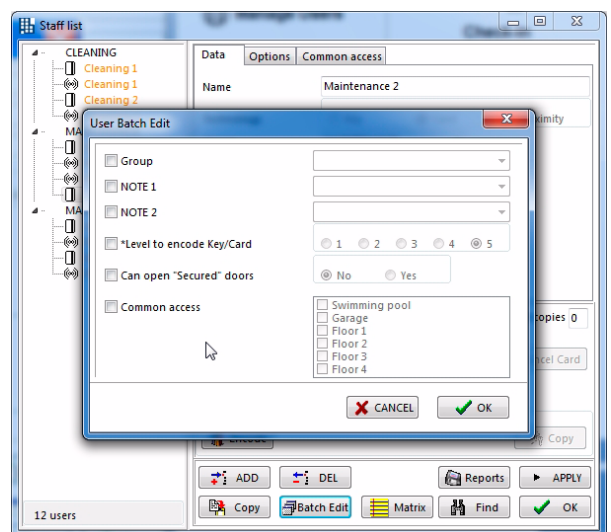
- **User ID:** additional information you wish to add in relation to the user (ID card, identification number, etc.).
- **E-mail address:** e-mail address for users of the V3 mobile APP application.
- **NOTE 1, NOTE 2:** customised fields. It is possible to define a maximum of 4 customised fields, which can be configured in the “Extra Fields” tab of the “Setup” menu, as shown in section “Extra Fields” tab on page 67.
- **Expiration 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 can 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 109.
- **encoded copies:** indicates the number of times the user's credential has been copied. Cards encoded as copies do not cancel each other.
- **“Cancel card” button:** this allows cancellation of a credential and all of its copies.
- **“Encode” button:** this allows encoding the credential of the user (see chapter “I – Encoding keys and programming doors”).
- **“Copy” button:** this allows a copy to be made of staff cards, after the original card has been encoded first. For more information, see “Staff card copies” on page 80.
- **“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 us to delete the user from the locking plan, after having selected them from the list in the column on the left.
- **“Copy” button:** makes a copy of this user, with the aim of facilitating creation of another user with identical characteristics, instead of using “Add” and filling out all the fields individually. In this way, one can quickly create a series of users (for example, “Maintenance 2”, ... “Maintenance 10”) from “Maintenance 1”.

Creating the Locking Plan

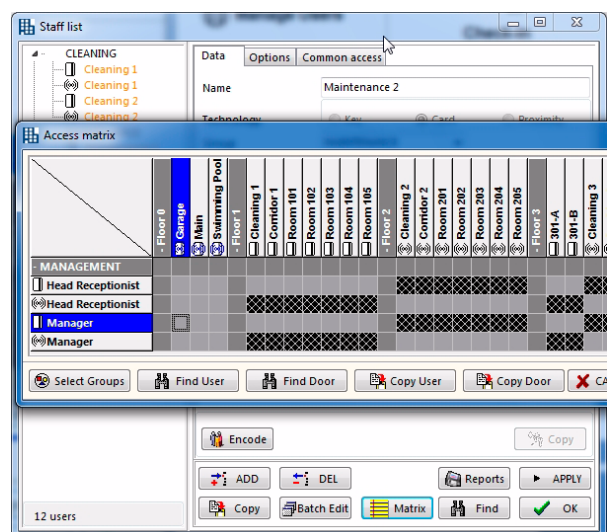
- **“Batch” button:** allows modification of properties common to different users at the same time, by selecting them and clicking “OK”, for example to change the group to which they belong, the grants, etc.



Finally, the options to be modified are selected and you click “OK” to save the changes.



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



F

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

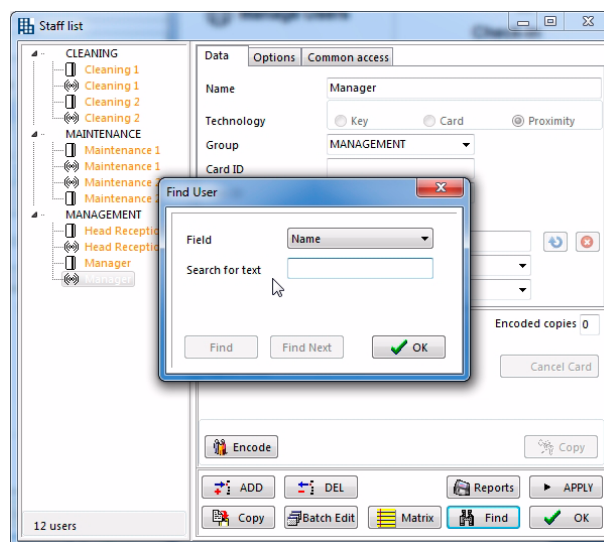
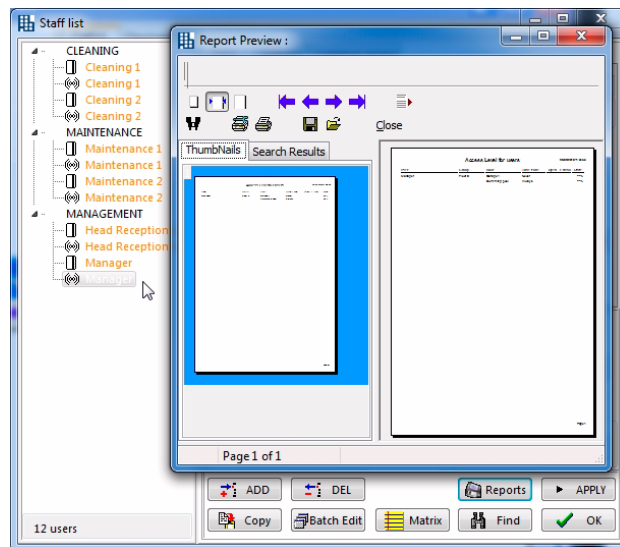
The information shown by the reports is the following:

- *User:* user name.
- *Group:* name of the group the user belongs to.
- *Door:* names of the doors they have access to.
- *Timezone:* hours when the user has access to the door in question.
- *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 114.
- *Privacy:* if the “@” symbol is displayed, then the user overrides privacy. For more information on the “Overrides privacy” concept, see “F.5 Matrix” on page 114.
- *State:* this indicates the situation which the encoding process of a user is in. An arrow pointing to the right, (\Rightarrow), indicates that the changes made to the locking plan of a user have NOT yet been transferred to the user’s credential or the Portable Programmer, with the subsequent updating of the door and return of the data to the PC. An arrow pointing to the left (\Leftarrow) indicates that the changes made in the locking plan of a user have already been transferred to the credential, but there is no guarantee that they have been transferred to the door. 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 TESA Hotel software.

❗ **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 initialization/update of the locks 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.

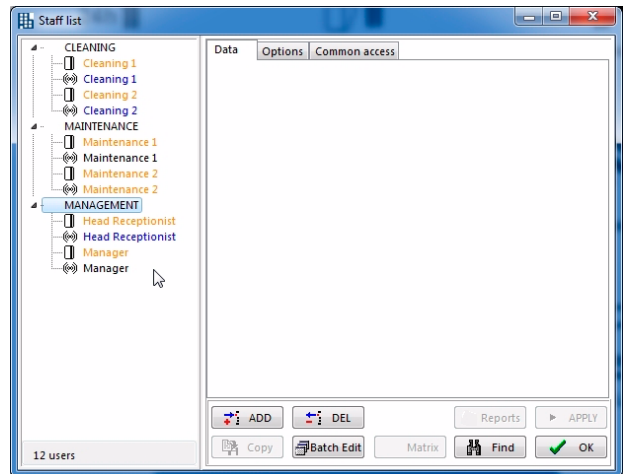


- **“Apply” button:** this saves the latest changes made.
- **“Close” button:** this closes the users window and saves the changes made.

On the column in 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:

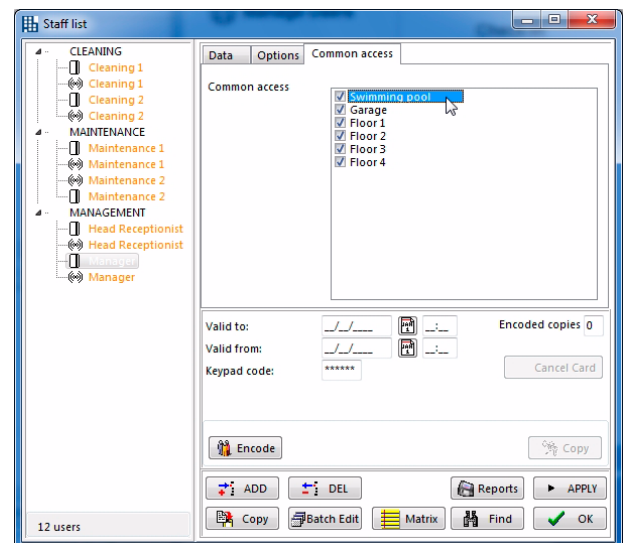
- **ORANGE** indicates that the credential of the user has not been encoded yet.
- **BLUE** indicates that there are pending modifications and, therefore, the card has to be encoded again.
- **BLACK** indicates that the credentials of the user have already been encoded or the pending modifications have already been transferred to the locks/cylinders. The system is synchronized.



“Grants” tab

This tab provides access to a window that allows the selected user (highlighted in blue) to be assigned one or several of the grants we have defined in the “Setup” menu.

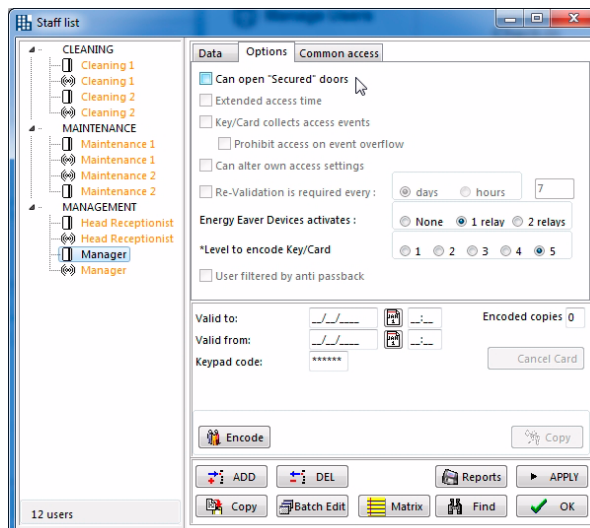
In the example, the user “Manager” has been assigned all the grants available, so that he or she can access any of the hotel's doors.



“Options” tab

This menu allows us to customise some characteristics inherent in each user:

- **“Can open blocked doors” option:** if this field is selected, the user will be able to open the doors they have authorised access for, even if they are blocked with the blocking card or by means of real-time control of the wireless devices.
For more information, see “Blocking Card” on page 193.
- **“Disabled (ADA)” option:** if we select this option, the opening time configured in the “Doors” menu will be doubled to facilitate this person's access.
This option is not available for electronic cylinders or magnetic stripe devices.

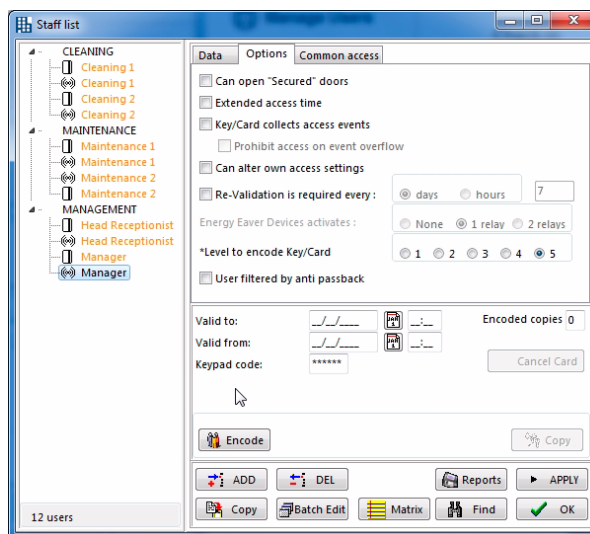


If the “Update-on-card (read & write)” option is selected in the “License” tab of the “Setup” menu, configuration of the following options is allowed, which are typical of the cards of a Read and Write system:

- **“Card/Key audits openings” option:** if this option is selected, the user's card will record all of the events that it performs in the locks, cylinders or readers with read and write technology, including warnings of devices with low battery level signals.
The amount of memory for recording the user's openings is limited by the type of card used. The cards used in a read and write system will be *Mifare Classic* and, depending on the capacity of the sectors of the card, they may be 1K or 4K. A 1K card has 15 sectors and a 4K card has 39 sectors.

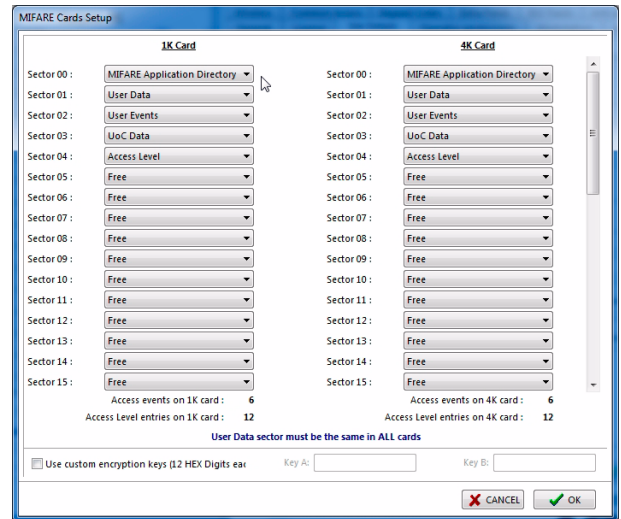
If all of the sectors of each of the cards were used to record events, the capacity would be as follows:
1K card = 72 events registered; 4K card = 414 events registered.

For more information, consult the TESA “Read and Write System” manual.



- **“Modifies own locking plan” option:** allows alteration of the locking plan of the card (encoding on the card's memory), modifications to its accesses in the setup according to the matrix. The card itself will then update the memory of the locks when it is used in them.

The number of modifications that can be encoded on the *Mifare* card depends on its memory capacity. A locking plan entry is the granting or removing of a user's access to a door in the matrix. If all the free sectors of a 1K Mifare card are used to store openings, a maximum of 144 locking plan entries can be stored; in the case of a 4K Mifare card, a maximum of 828 locking plan entries can be stored. See the “Setup” tab on the main menu.



- **“Update Key/Cards every” option:** enables revalidation of cards every certain amount of time, otherwise they will be temporarily invalidated.

In this case the card must be passed through an updater or read in the reception encoder every certain amount of time. In this way, the card is revalidated so that it continues to work in the locks for the next period, and the openings contained in it are collected. Moreover, any possible crosses of its locking plan carried out from the reception PCs will be encoded again. When this field is selected, the option of choosing how often we wish to revalidate the credential is displayed.

- **“Level to encode key/card” field:** Indicates the level the operator who is managing the system needs to have in order to encode or copy a staff card of the corresponding user (in this case, the Manager).

Every operator can encode cards of a level that is the same as or lower than their own access level. This means that a receptionist who is a system operator with operator level 3 will not be able to encode a Manager's card, as level 5 is required to encode the latter's card. Only system operators who have operator level 5 will be able to encode the manager's card.

The operations allowed at each operator level are defined in the “Operator Levels” tab of the “Setup” menu. System users who will also be system operators are identified in the “Operators” menu.

- **“User filtered by antipassback” option** a user who has this option selected is controlled by the *antipassback* system just as it was configured. If it is not selected, this allows the user to use their credential to enter the same door twice consecutively using this credential. Therefore, this user's credential allows two people to go through the same door consecutively, using the credential.

Staff card copies

In the TESA Hotel system, every 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.

The copies of credentials cannot be customised with names that are different to the original credential. They can only be distinguished by the copy number.

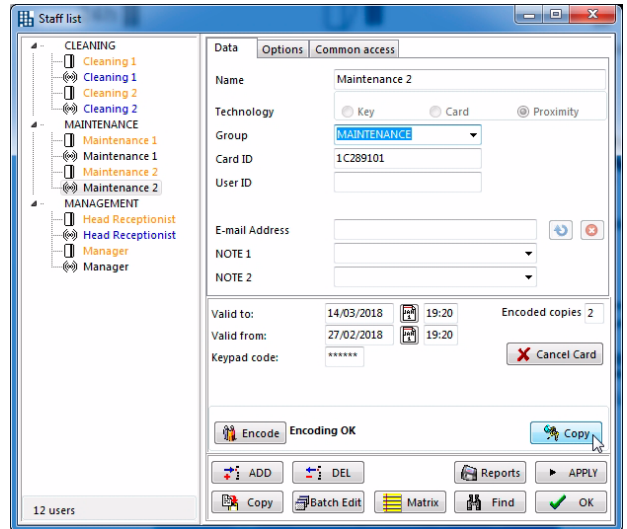
⚠ **WARNING:** take into account that, when working with copies of credentials, if a new credential is encoded, the previous credential is cancelled, as well as all its copies. That is to say:

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.

The “Users” menu of TESA Hotel displays the button “Copy”, which allows making copies of the credential of that user, as well as the field “No. of encoded copies”, where the number of copies encoded from that credential is displayed.



F.3 “DOORS” MENU

Doors list

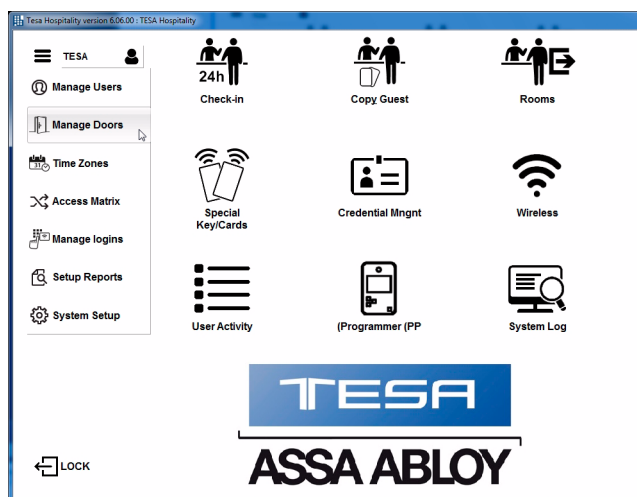
After creating the users list, the next step involves creating the doors list, by means of the “Doors” menu.

Prior to this, it is advisable to create the state tables (see “States” on page 109) and define the necessary grants (see “Defining the Grants” on page 133).

The system classifies the doors depending on their usage, and the following cases exist:

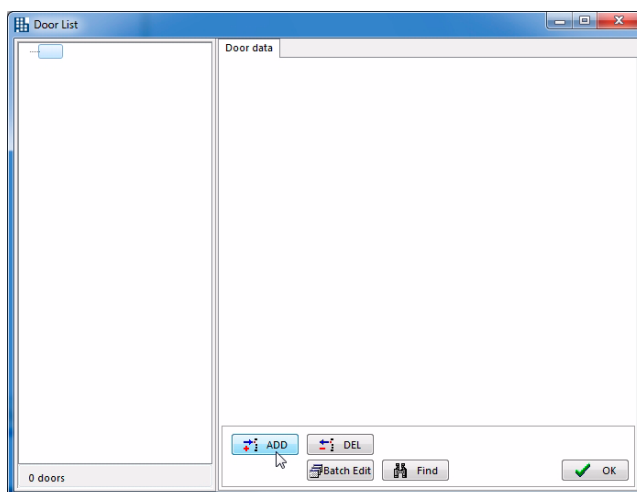
- Rooms (for guests)
- Suites (for guests)
- Common access doors (for hotel staff and guests)
- Doors with access control (exclusively for hotel staff)
- High traffic (doors where the number of people accessing them is higher than 1,500)

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



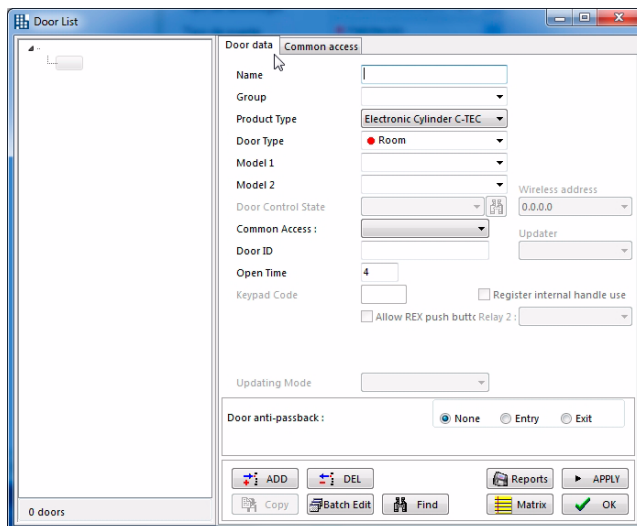
As no doors have been created yet, the doors list is displayed empty.

Click on the “Add” button to add doors to the list.



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):

- **Name:** name assigned to the door.
- **Group:** name of the group the door belongs to. Doors can be ordered in groups as desired, for example, by floors, buildings, zones, etc.
- **Technology type:** type of lock, cylinder or reader in the door.



Technology type	Description
Lock Mag. Donna	Lock model Donna, exclusively magnetic stripe model
Lock Mag. SpyDesign	Lock model SpyDesign, Dual reader, only magnetic stripe technology
Lock Prox. Spy / Donna	Lock models Spy (with or without keypad) / SpyDesign or Donna, only proximity technology
Lock DualSpyDesign / Donna	Lock models SpyDesign Dual or Donna Dual proximity and magnetic stripe technologies
Lock Wireless Mag. SpyDesign	Lock model SpyDesign Dual Wireless only magnetic stripe technology
Lock Wireless Prox. Spy / Design	Lock model Spy (with or without keypad) / SpyDesign Wireless
Lock Wireless DualSpyDesign	Lock model SpyDesign model Dual Wireless
Electronic Cylinder C-TEC	Electronic Cylinder with C-TEC contact chip
Knob Cylinder Prox.	Knob Cylinder Prox.
Knob Cylinder Prox. Wireless	Proximity Wireless Knob Cylinder
WR Mag. Spy / Donna	Wall Reader Donna / SpyDesign dual reader only magnetic stripe technology
WR Prox. Spy / Donna	Wall Reader Spy (with or without keypad) / SPYDesign / Donna only proximity technology
WR DualSpy / Donna	Wall Reader Donna Dual / SpyDesignDual, magnetic stripe + proximity technologies
WR Wireless Mag. Spy	Wall Reader SpyDesign dual reader only wireless magnetic stripe technology

F

Technology type	Description
WR Wireless Prox. Spy	Wall Reader Spy (with or without keypad) / SpyDesign / SpyDesignDual only wireless proximity technology
WR Wireless DualSpy	Wall Reader SpyDual magnetic stripe + Wireless proximity technologies
WR Elevators Mag.Spy / Donna	Wall Reader Donna or Spy model Dual only magnetic stripe technology with 8-relay panel
WR Elevators Prox.Spy / Donna	Wall Reader Donna / Spy (with or without keypad) only proximity technology with 8-relay panel
WR Elevators DualSpy / Donna	Wall Reader Donna / Spy Dual technology with 8-relay panel
WR Elevators Wireless Mag. Spy	Wall Reader SpyDual only Wireless magnetic stripe technology with 8-relay panel
WR Elevators Wireless Prox. Spy	Wall Reader Spy Wireless proximity technology (with or without keypad) with 8-relay panel
WR Elevators Wireless DualSpy	Wall Reader Spy Dual Wireless with 8-relay panel
WR Energy Saver Mag. Spy	Wall Reader SpyDual function energy saver only magnetic stripe technology
WR Energy Saver Prox. Spy	Wall Reader SpyDual only proximity technology energy saver function
WR Energy Saver DualSpy	Wall Reader Spy Dual, Dual technology (magnetic stripe + proximity), energy saver function
Safe Mag. + PIN	Safe technology Magnetic Stripe Card + PIN (Card + PIN function, PIN only or card only)
Safe Prox. + PIN	Safe technology proximity Card + PIN (Card + PIN function, PIN only or card only)
Safe only PIN	Safe technology PIN only (sites with magnetic stripe or proximity locks, without distinction). If a safe, either card + PIN model, or a PIN Only model, is initialized as "Safe PIN Only", it will function in PIN Only mode, without having to apply any additional change of state.
Updater Reader	Updater Reader with mini PC (with door control, one or two readers)
E-motion cabinet lock	Proximity cabinet lock model EMOTION
E-motion Cabinet Lock Visualizer	"Cabinet no. assigned" visualizer for EMOTION cabinet locks.

- **Door type:** TESA Hotel allows doors to be classified into the following types: Room, Suite, Access Control, Common Access, High Traffic.
- **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 67.

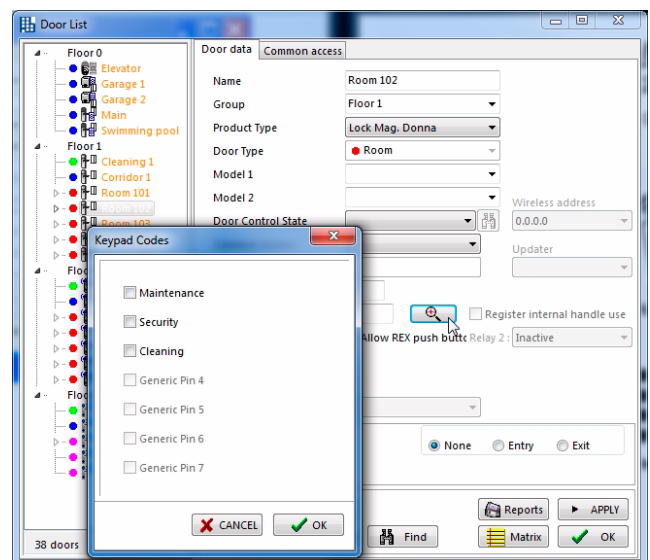
Creating the Locking Plan

- **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 109.
- **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 users who hold this grant. For more information, see “Grants” on page 131.
- **Door ID:** identification number assigned to the door (optional customised field, like Model 1 and Model 2).
- **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, and may vary from 1 to 15 seconds.
- **Common Keypad code:** code ranging from 4 to 6 digits for opening the door if it is in the state “Common Keypad”: refer to “States” on page 109.

- **Common PINs:** the Common PINs are identification PIN codes 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.

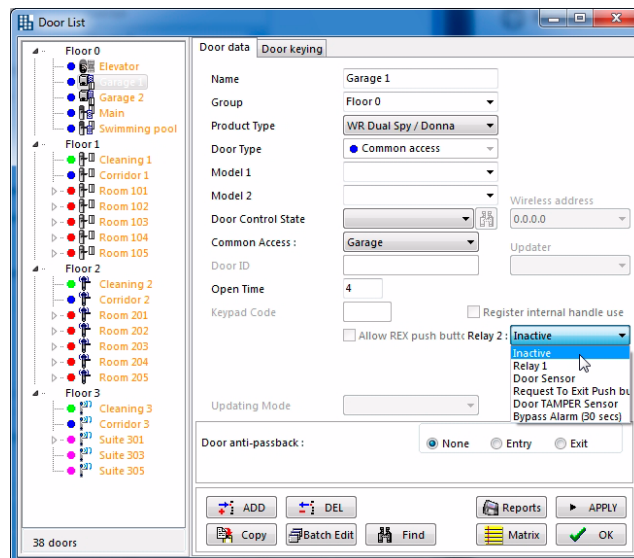
The Common PINs are defined in the “Setup” menu, “Common PINs” tab, by means of their identification name, followed by the “PIN” number, as shown in section “Common PINs” tab on page 67.

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.



- **High Traffic Door:** see section “High Traffic Door” on page 103.
- **Wireless Address:** this is automatically filled in when the wireless doors are initialized.
- **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.
- **Registers internal handle:** saves the record every time the inside handle of the lock is pushed down.
- **With pushbutton:** this allows opening by means of external on-line 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.

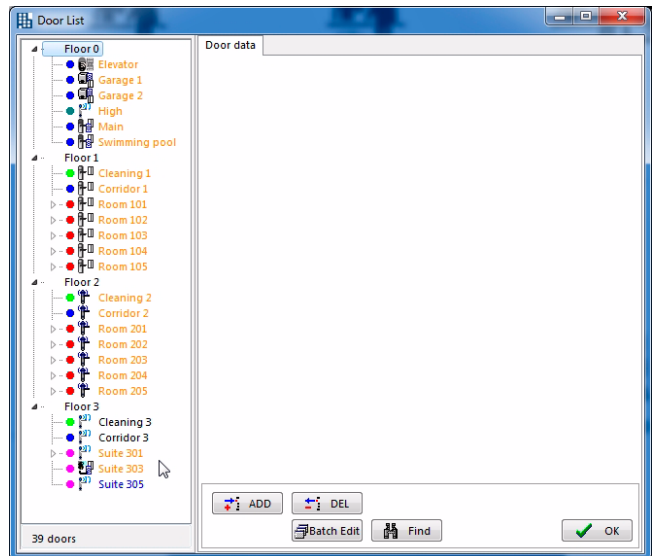


- Privacy overrides passage:** If this option is activated and the privacy lever is activated from the inside of the door, a user with authorised access cannot enter, even though they have the “Overrides privacy” option activates. This option is only available in some door types. When the privacy lever or the electronic privacy is off, the lock is automatically left in Free Passage mode.
- Updating mode (option available only for doors with Updater Readers):** in this drop-down menu, the updating modes that we have defined in the “Hours” menu, “Updating modes” tab are displayed. It allows us to select the updating mode we desire for the door in question, fitted with an Updater Reader. Therefore this option is only available for doors with an Updater Reader.
- Door antipassback:** this allows us to select the “Antipassback” mode in this door for entry, exit, or not select it. Antipassback mode prevents two users from being able to go through the same door one after another, using the same credential. That is to say, it prevents two consecutive entries through the same door using the same credential.
- “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 selected from the list.
- “Multi” button:** this modifies the properties of several doors at the same time: see section “Batch” on page 105.
- “Matrix” button:** see section “Matrix” on page 107.
- “Reports” button:** see section “Reports” on page 105.
- “Find” button:** see section “Find” on page 107.
- “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 initialized yet; it is necessary to initialize it.
- **BLUE** indicates that the door is initialized, 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 initialized and there is no information which has to be transmitted to it.



Create the doors list of a hotel

This section shows how to create the doors list of a hotel, the doors structure of which is shown below as an example:

- Main floor:
 - Garage door (common access type)
 - Main door (common access type)
 - Swimming pool (common access type)
 - Staff room (access control type)
 - Office (access control type)
 - Reception (access control type)
- 1st floor:
 - Corridor 1 (common access type)
 - Cleaning room 1 (access control type)
 - Rooms 101 to 105 (room type) with safe
- 2nd floor:
 - Corridor 2 (common access type)
 - Cleaning room 2 (access control type)
 - Rooms 201 to 205 (room type) with safe
- 3rd floor:
 - Corridor 3 (common access type)
 - Cleaning room 3 (access control type)
 - Suites 301 and 302 (suite type)
 - Rooms 301-A and 301-B (suite type), with safe, inside suite 301
 - Rooms 302-A and 302-B (suite type), with safe, inside suite 302

As can be seen, four types of doors of the five that exist in TESA Hotel are represented:

- Room (for guests)
- Suite (rooms with two or more rooms inside them)
- Common access (doors for both hotel staff and guests)
- Access control (doors exclusively for the use of the hotel staff)
- High traffic (doors where the number of people accessing them is higher than 1,500)

To create the doors list in TESA Hotel, proceed as follows:

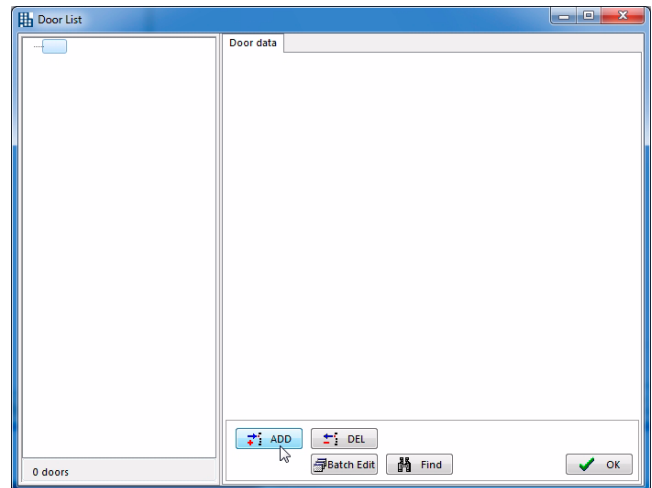
- 1 Access the “Doors” menu by clicking this option on the main screen.



Creating the Locking Plan

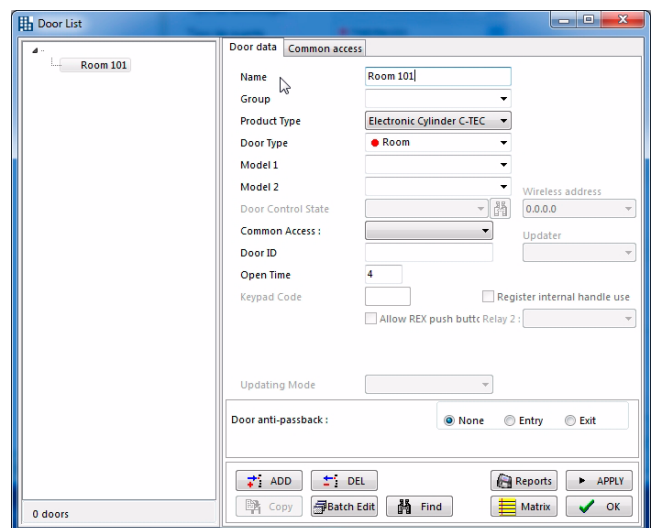
- 2 As no doors have been created yet, the doors list is displayed empty.

Click on the “Add” button to add doors to the list.

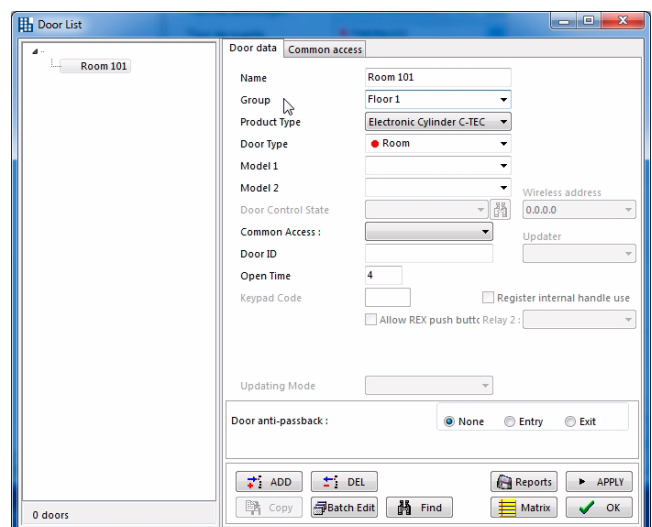


“Room” doors

- 3 Enter the name of the first door. In the example, “Room 101”.



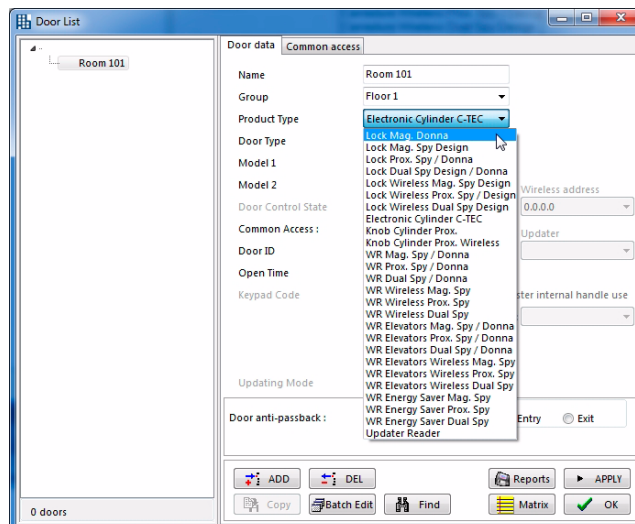
- 4 Enter the name of the group the door will belong to. This is not mandatory, but it is advisable in order to keep the doors well-organised. In the example, we will organise the doors according to the floor they belong to. Therefore, write “Floor 1” in the “Group” field, as no group has been created yet.



5 Select the type of lock of the door.

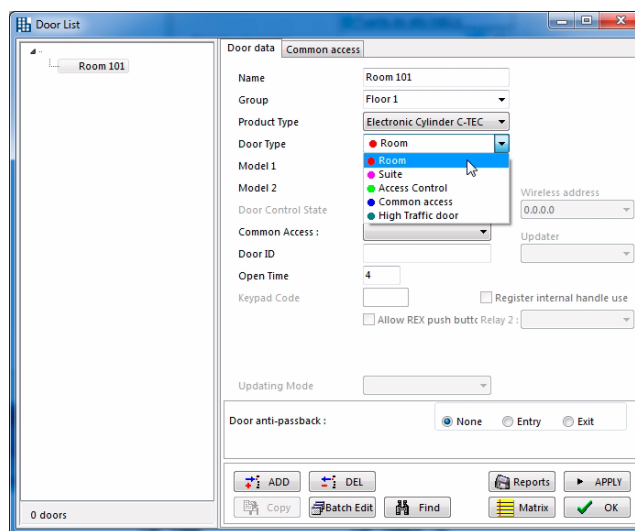
In the example, "Lock Mag. Donna".

The "Safe" option is not displayed as available until the room to which the safe is assigned has been created, because safes will always be associated to their corresponding room and will be opened using the same card as the room door.

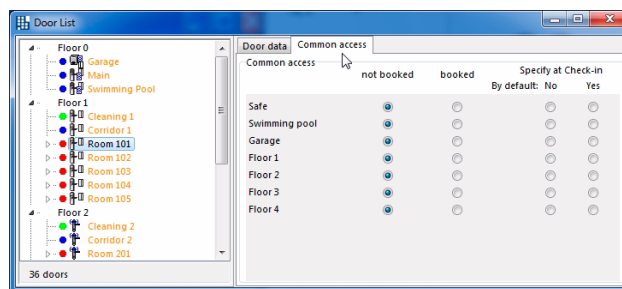


6 Select the door type.

In the example, "Room".



Since this is a room, the "Grants" tab is displayed, indicating the grants available which were defined previously (see "Defining the Grants" on page 133). By default, the grants are not assigned to the guest of this room 101, so they will not be able to access the safe of their room, or the swimming pool, or the garage.



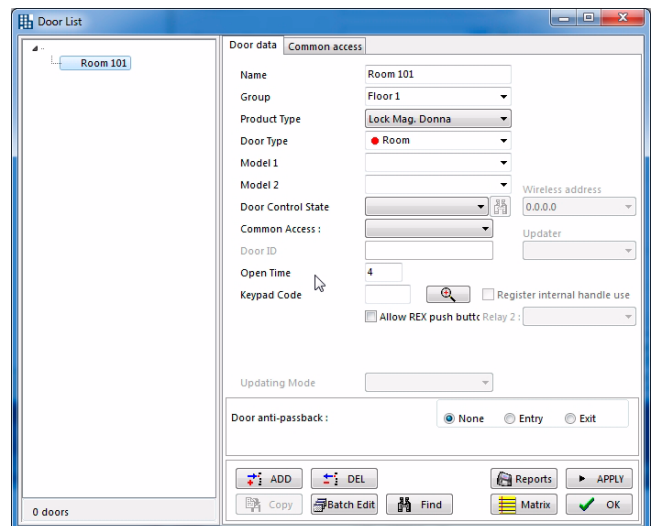
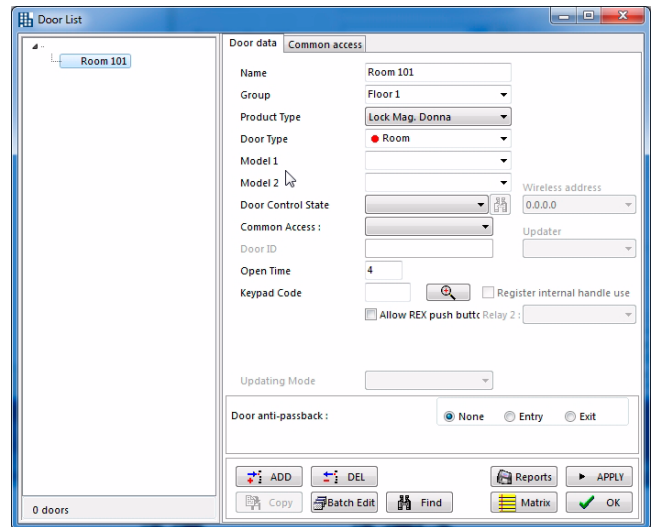
7 The fields “Model 1” and “Model 2” are optional, and are displayed because we defined them previously in the “Setup” menu, so we can use them as we prefer.

8 We leave the “Door states” field blank, as we have only defined states for the Main Door and the Corridors.

9 We also leave the “Requires grant” field blank as we have only defined the “Safe”, “Pool” and “Garage” grants.

10 The “Open time” field allows us to set the time available for opening the door once the access is granted (green LED). You can select a time of between 1 and 16 seconds. For electronic locks, the recommended default value is 4 seconds.

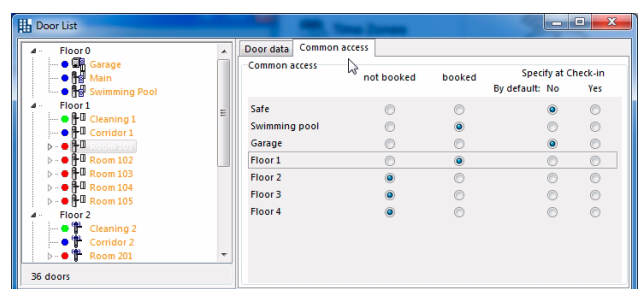
11 In the “PIN code” field, we enter the 4 to 6 digit code which must be keyed in for opening the door, if there is a keypad.



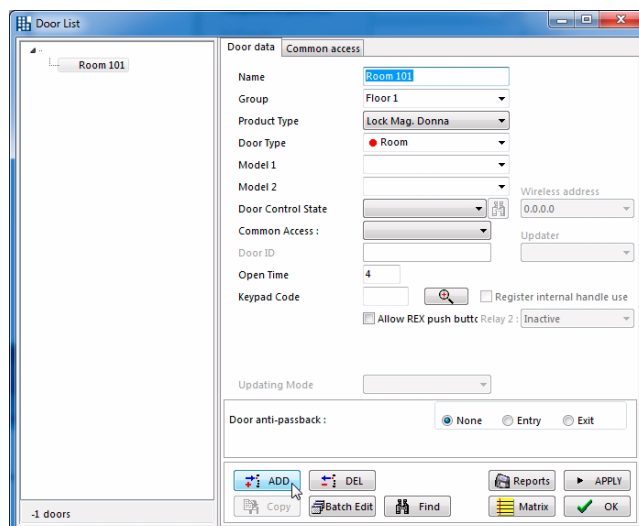
12 The grants that are assigned to a guest are determined on the “Guest's Grants” tab. There are four possibilities for each grant:

- Not assigned: the guest will never have access to the doors that require this grant.
- Assigned: the guest always has access, because the grant is encoded on his/her credential.
- Specify at Check-In, by default Yes: the guest has access to these doors by default, although the grant can be denied during Check-in.
- Specify at Check-In, by default No: the guest does not have access to these doors by default, although the grant can be assigned during Check-in. This is the most frequently used way of managing the grants for services requiring rental.

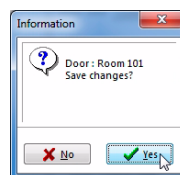
The example shows that the guest of room 101 has unrestricted access to the swimming pool and to go up to their floor (floor 1), but access to the garage and the safe of his/her room can be assigned when his or her card is encoded.



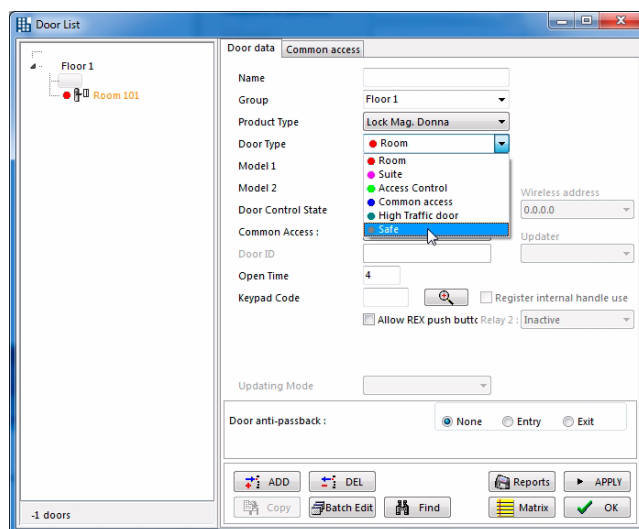
13 When you finish, click on the “Add” button.



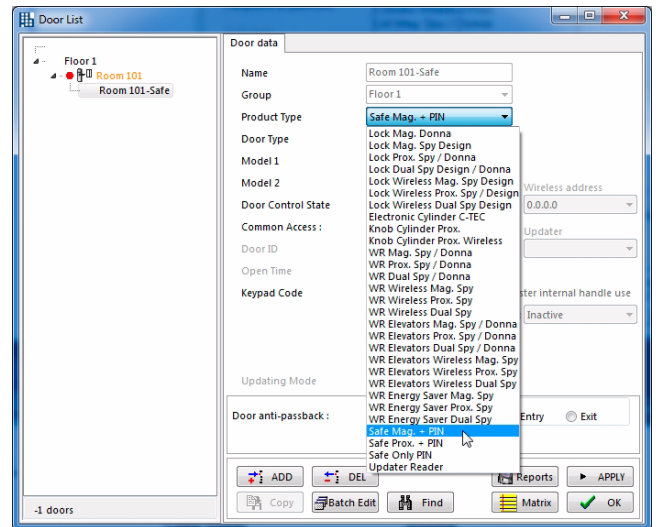
14 A confirmation message is displayed. Click “Yes” to accept it.



15 After creating room 101, the system allows us to add a safe associated to that room: the safe option is displayed in the “Door type” field. Select this option.

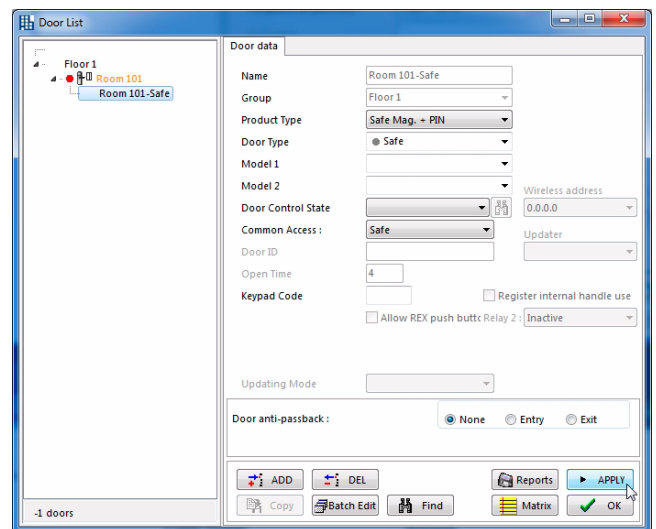


16 After selecting the safe, in the “Technology type” field, the system allows different safes to be chosen. We select “Magnetic Stripe Safe”, as we are assigning it to a lock with magnetic stripe technology.



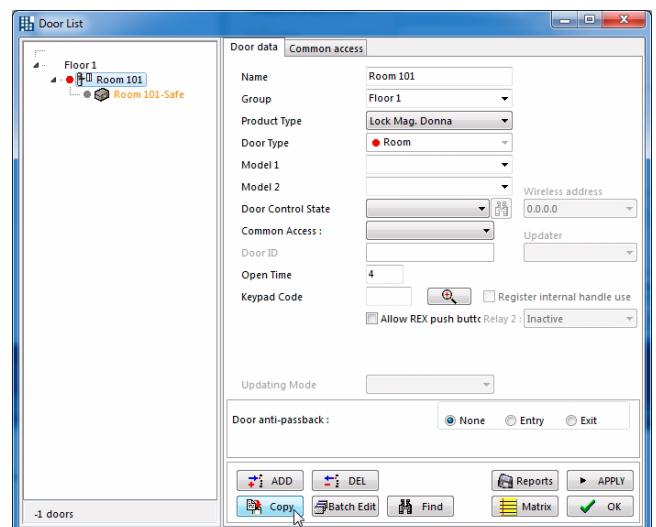
17 Click “Apply”; the list of doors updates, and the safe associated to room 101 also appears.

The definition of room 101 is now completed.

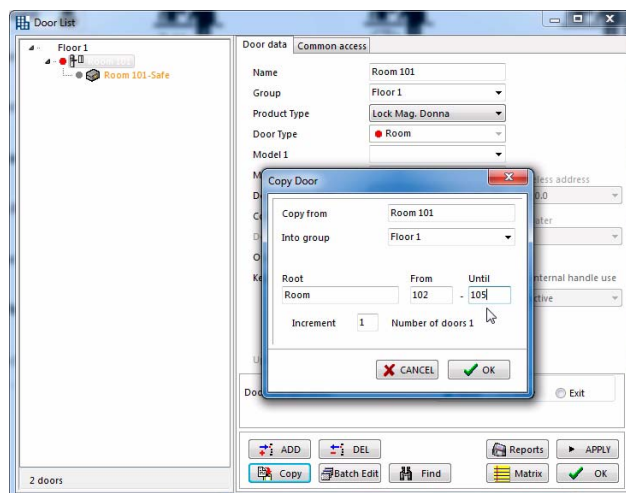


18 Since all the rooms on Floor 1 are the same, we create the other rooms by copying them from 101, already created.

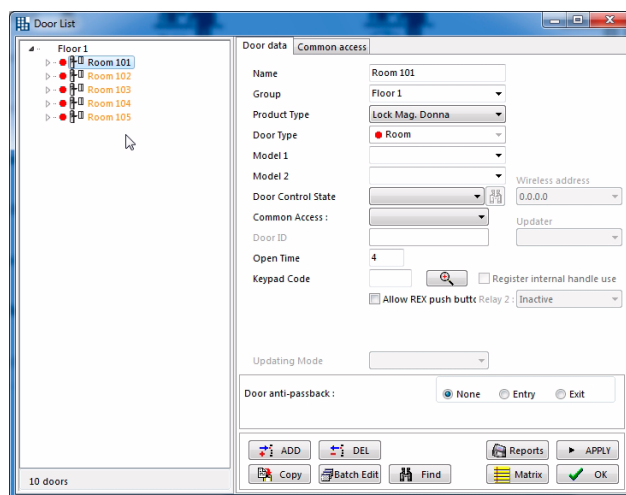
To do so, select room 101 from the doors list (highlighted in blue) and click on “Copy”.



19 The “Copy Door” window is displayed which allows us to create a series of doors the same, selecting the root of the name (in our case, “Room”), the initial room (102 in our case), the final one (105) and the increment in numbering (1, one by one in our example). Fill in the details and click “OK”.

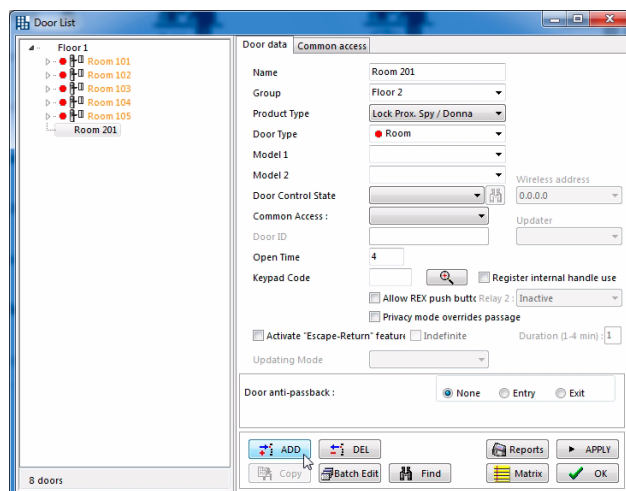


20 As you can see, the system has automatically created rooms 102 to 105 exactly the same as 101, including the safe.

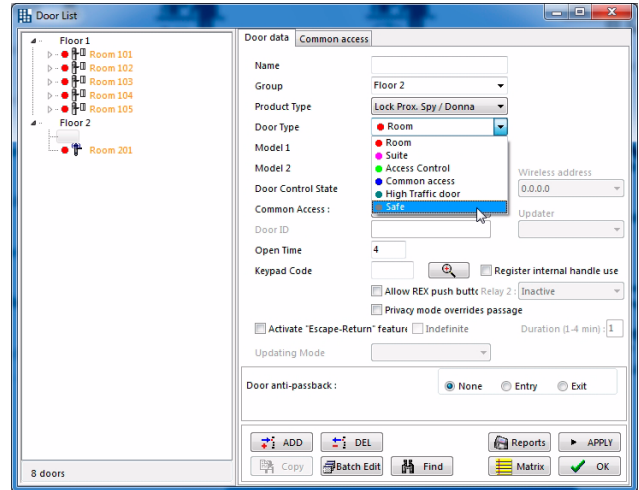


21 Now that the first floor is completed, we create the first room on the 2nd floor, number 201, which is similar to 101 but with SPY proximity locks.

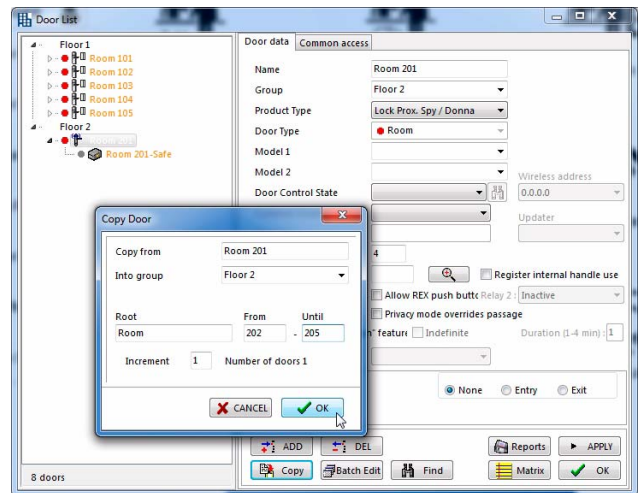
After filling out the fields, click on “Apply” and accept the confirmation message that appears next.



22 If you wish to, associate the corresponding safe to room 201, in the same way as you did with room 101.

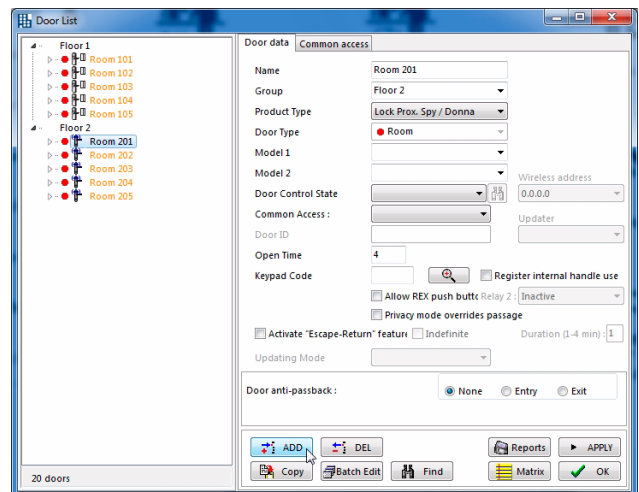


23 After finishing the definition of room 201, proceed to create numbers 202, 203, 204 and 205 using the “Copy” button in the same way as you did on Floor 1.



24 In this way Floor 2 is completed.

We will now proceed to create the Suites on floor 3, for which we click on the “Add” button.

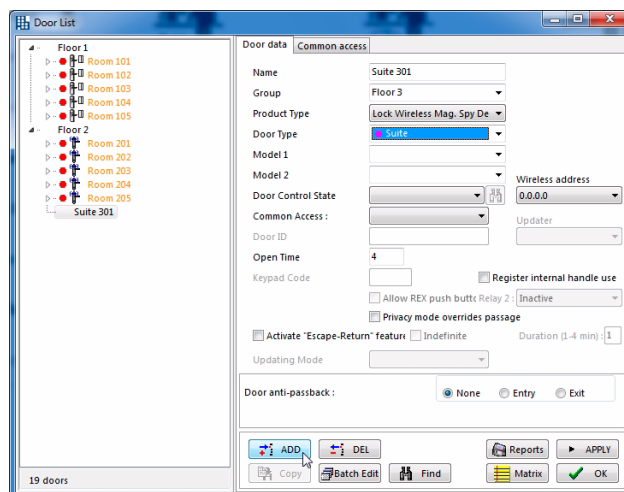


F

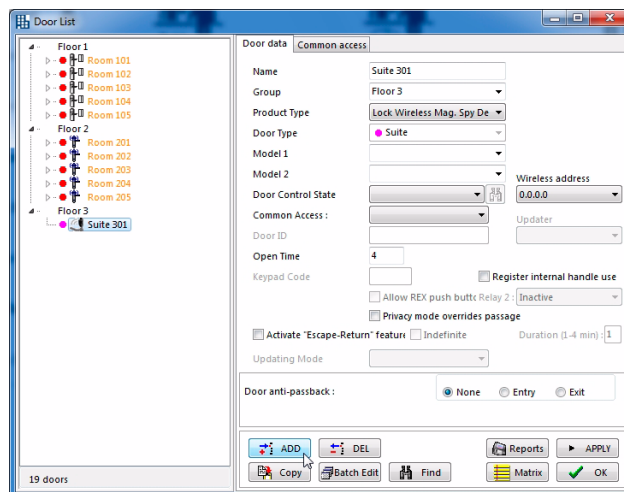
“Suite” doors

25 Create Suite 301 on Floor 3 by selecting the technology corresponding to the lock installed (Wireless) and the “Suite” door type.

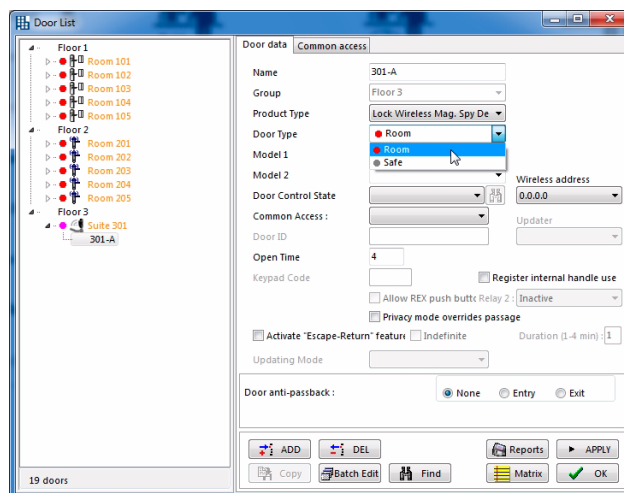
After filling out the fields, click on “Add” and accept the confirmation message.



26 Suite 301 is now defined on floor 3. Independent interior rooms can be created in the Suite, with their own lock. To do this, select the Suite (marked in blue) and click on the “Add” button.

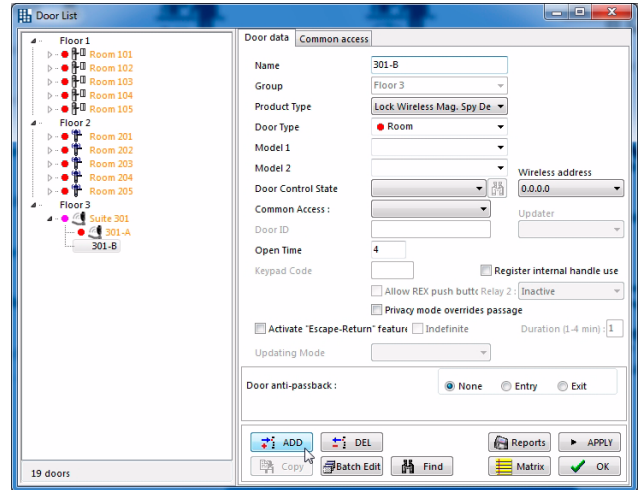


27 As can be seen in the “Door type” field, both safes and interior rooms can be associated. We create an interior room with the name “301-A” and click on “Add”. Accept the confirmation message that is displayed.



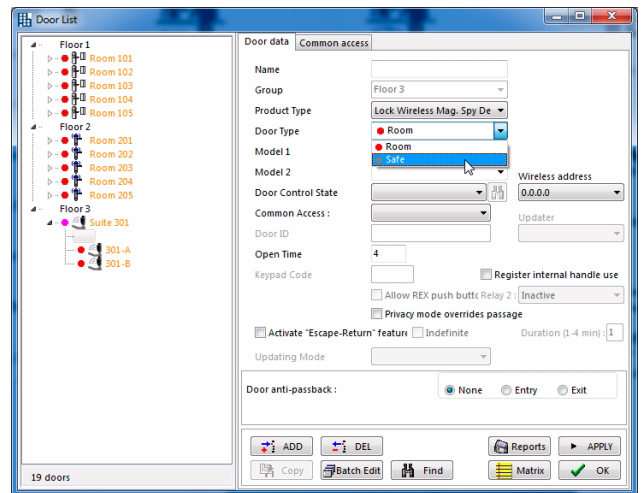
Creating the Locking Plan

28 You can create a second room (301-B) in the same way. After filling out the fields, click on “Add” and then accept the confirmation message that is displayed.



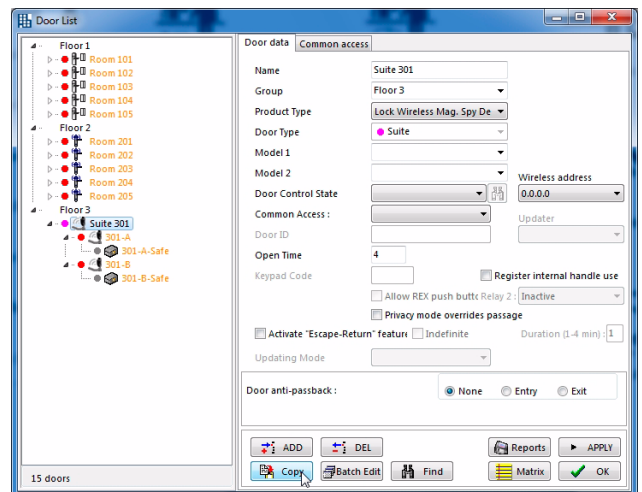
29 To finish defining Suite 301, you can add the safe associated to each room.

After filling out the fields, click on “Add” and accept the confirmation message that is displayed.



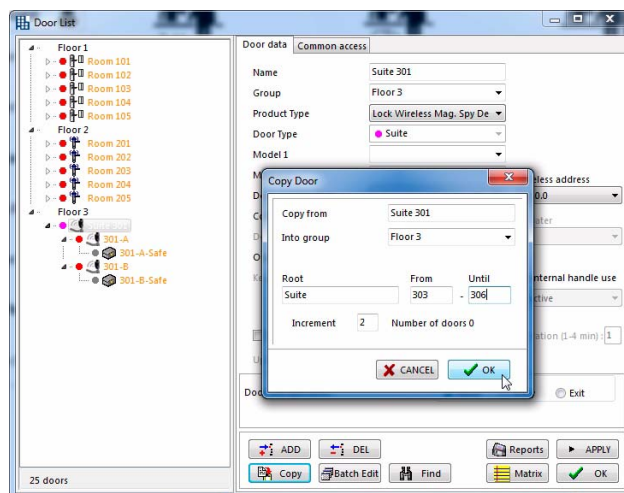
30 As you can see, Suite 301 is now created with its interior rooms and safes.

To create Suite 302, which is similar to 301, select Suite 301 (highlighted in blue) and click on “Copy”.



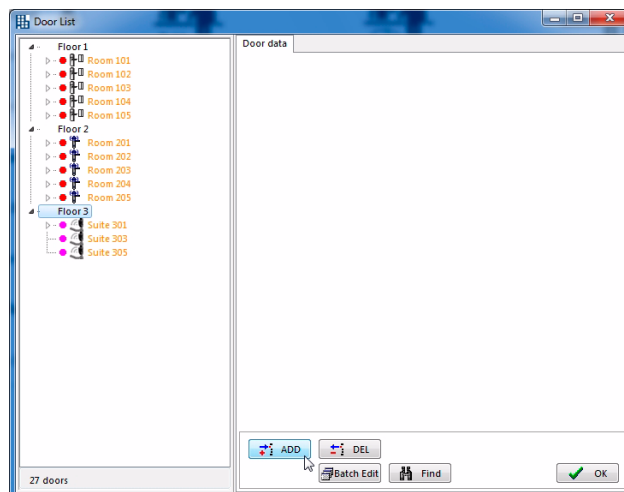
31 After clicking the “Select” button, the corresponding screen is displayed:

In the example, we wanted to number the suites with odd numbers, so in the “From” box we filled in the number 303 and in the “To” box we put 306, indicating in the corresponding field that the increment should be 2. The software indicates that 2 doors will be created. Click “OK” to confirm.



32 As we can see, all the rooms (with their safes) and the suites (with their interior rooms and safes) in the hotel have now been created.

We now need to create the “Common Access” and “Access Control” doors.



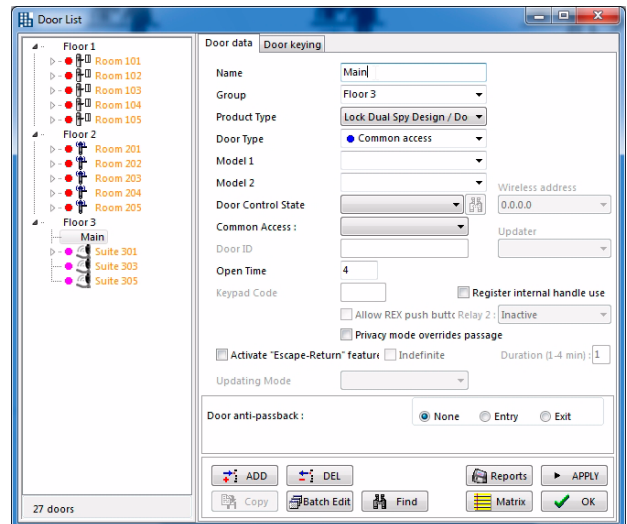
“Common Access” doors

“Common Access” doors are those which are accessible for both guests and staff of the hotel. The example hotel will have the following “Common Access” doors:

- The doors of the corridors of each floor (which will also have a special states table)
- The lock of the main door (which will also have a special states table)
- The wall reader of the garage (which will also have the special Garage grant)
- The common access lock of the swimming pool (which will also have the special Swimming Pool grant)

33 First of all, we create the Main Door by clicking on the “Add” button.

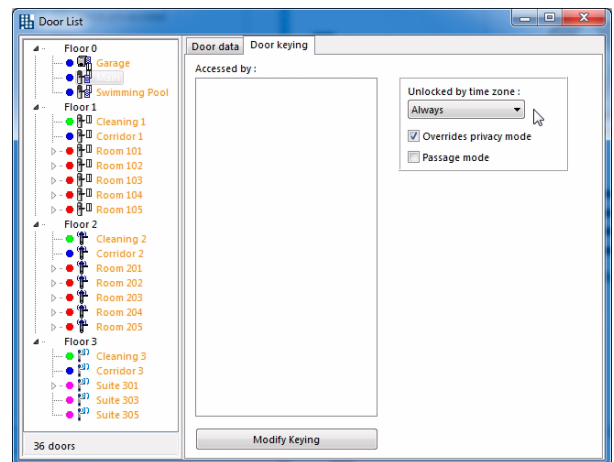
- In the “Name” field, we write “Main”.
- In the “Group” field, we write “Floor 0”.
- In the “Technology type” field, we select “Dual Lock”, as this means both guests with magnetic cards (those from Floor 1) and those with proximity cards (from Floor 2) can gain access.
- In the “Automatic Changes” field we select “MAIN”, as we created it specifically for this door.
- We leave the “Grants” field blank as it does not require a special grant.



We can see that for this door type, the “Door keying” tab is displayed. On this tab, we can select the guests who will have access to the main door.

In this example, all the guests will be able to access via the main door.

- The “Opened by” door indicates which guests will have access via this door. It is empty, which means no guest can gain access.
- The “Opened with timezone” field indicates the times at which the guest will have access. The “Always” and “Never” options are available, as are the timezones we define.
- The “Overrides Privacy” option allows the guest to open the door even if it is blocked from the inside with the privacy lever.
- The “Can leave door open” option allows the guest to change from “Open” to “Normal” mode or vice versa (not recommended).

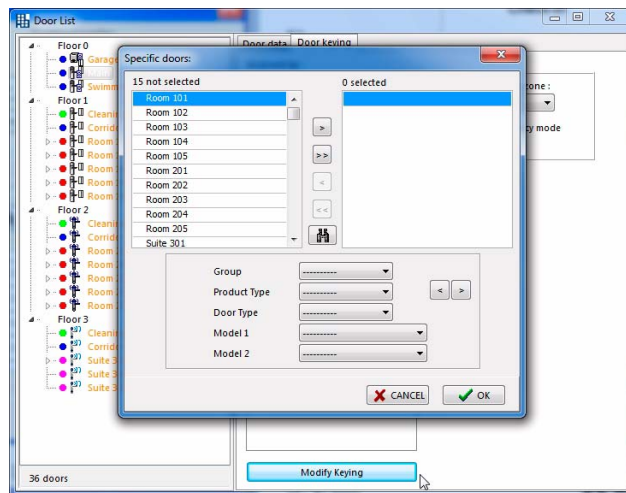


F

As can be seen, the “Opened by” field is displayed empty, meaning no guest can gain access via this door.

To add guests, click on “Modify keying”. A window is displayed that allows you to select the guests who will be able to gain access via this door (the Main Door). Since this is the main door, we select all the guests (“>>” button) and click “OK” to confirm.

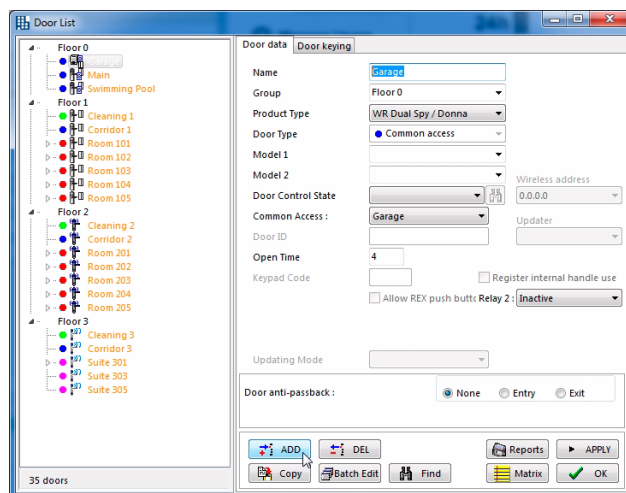
Finally, we return to the “Door Data” tab, click on the “Add” button and accept the confirmation message.



34 After creating the main door, we create the “Garage” door. The differences from the main door are:

- Name: garage
- Technology: Dual reader
- Door states: none (blank)
- Grants: Garage (even though all the guests are authorised in the keying, only those with the “Garage” permit will be able to gain access.

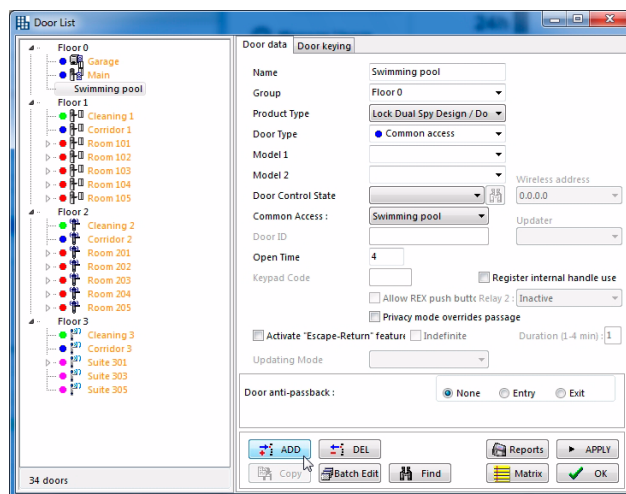
After filling out the fields, click on “Add” and accept the confirmation message.



35 After creating the main door and the garage, we create the “Swimming Pool” lock.

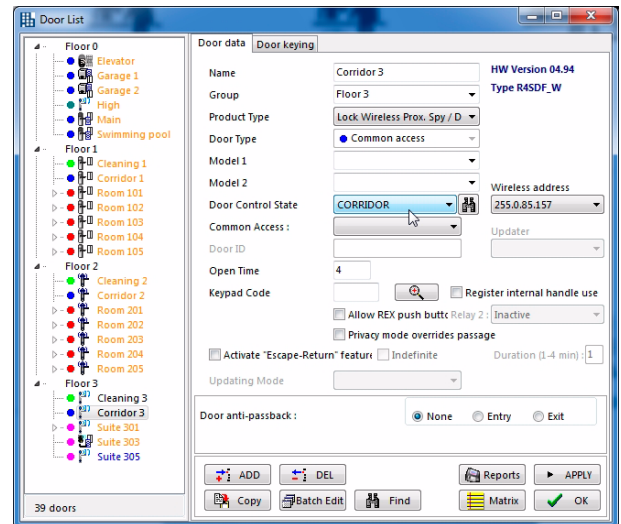
It is similar to the Main Door, the sole difference being that it requires the “Swimming Pool” grant.

After filling out the fields, click on “Add” and accept the confirmation message.



36 Finally, we create the doors of the corridors of each floor. The peculiarities of these doors are:

- It must use the same technology as that used in the rooms on that floor.
- In the “States” field, the states table we have defined for the corridors must be selected.
- The door keying must be performed in the corresponding tab, so as to allow guests to access.

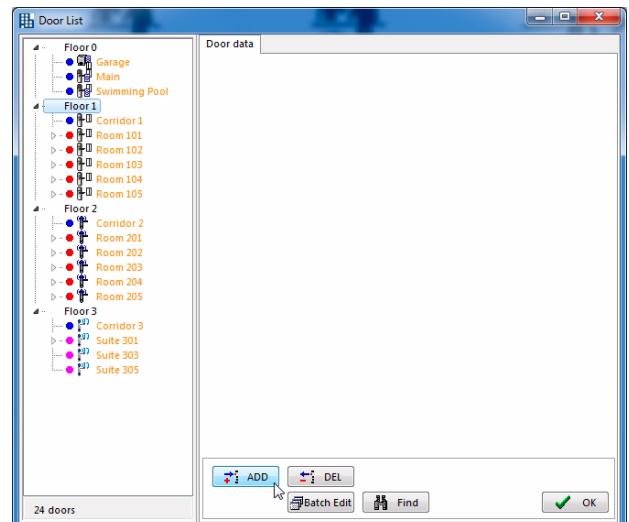


“Access Control” doors

“Access Control” doors are those dedicated exclusively to the hotel staff, for example the offices, the cleaning room, etc.

37 At this point we create the door corresponding to the cleaning room on floor 1.

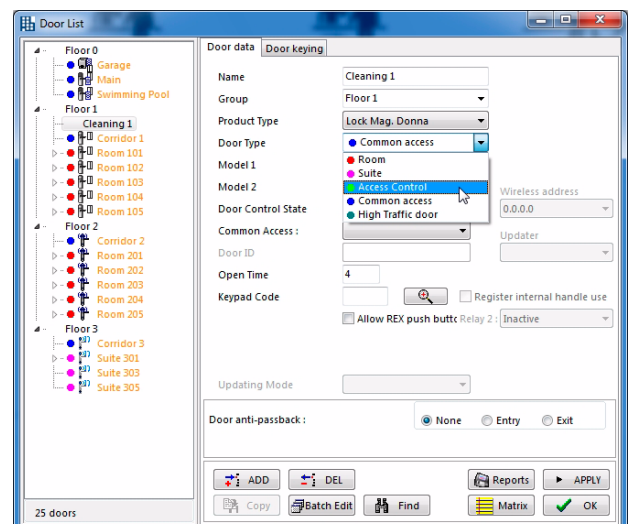
To do so, select the “Floor 1” group (highlighted in blue) and click “Add”.



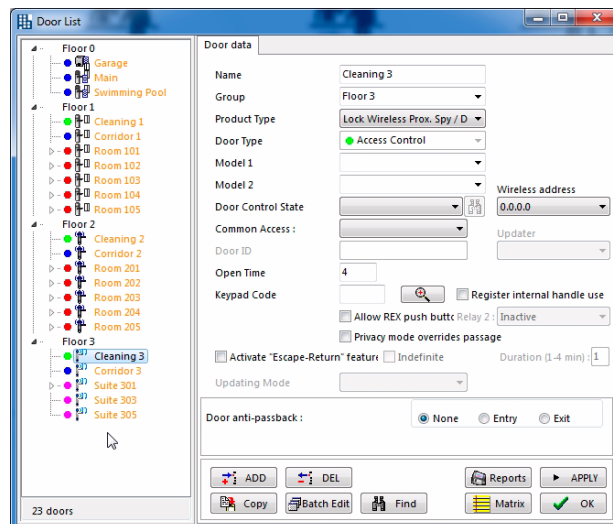
38 Fill out the fields displayed in the same way as in the previous cases. We should highlight the following:

- Name field: “Cleaning 1”
- Technology field: “Donna magnetic lock”, so that it coincides with the other locks on that floor.
- Door type: “Access control”.

When you have finished filling out the fields, click on “Add” and accept the confirmation message that appears next.



39 Create the other cleaning rooms on each floor in the same way, using the same technology type as that used on the floor in question.



Updater Reader

The updater reader is a special device with which a virtual on-line network system is obtained with no need for wires.

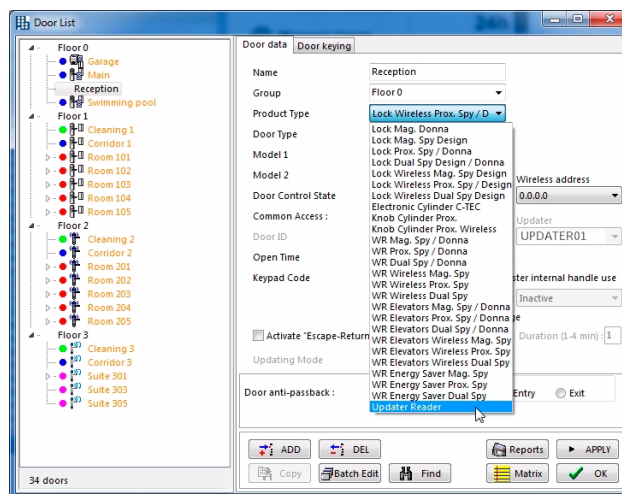
It is a wall reader connected to a mini updater PC inside the TESA Hotel network, which in addition to controlling a door by means of a relay, is capable of encoding and reading the cards by accessing the database in real time.

It also allows connection of a second wall reader, an open door detector and an emergency opening push button, always communicating with the TESA Hotel server PC in real time.

To create an Updater Reader on Floor 0, select the floor in question (highlighted in blue) and click on "Add".

Bear in mind that the updater reader must be previously connected to the TESA Hotel network and have accessed the database (consult the updater reader manual to see how this is done).

At this point the updater will appear in the "Updater" field of this window.



High Traffic Door

The cylinders, as well as the locks and wall 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 239.

For doors where it is necessary to provide access to more than 1,500 users, the TESA Hotel 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 expiration 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 expiration 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 in the *Matrix* of the system, since it does not require any other condition for granting access or not.

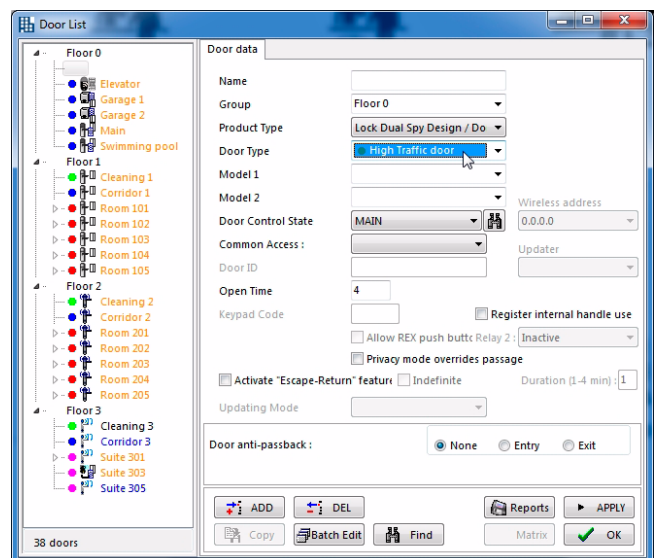
For a door to work as a high traffic door, this option must be selected in the “Door type” field when the door is being created.

You can see that the “Matrix” button ceases to be operative for this door.

For high traffic doors, it is important to consider that a user with a credential belonging to the site, but without an expiration 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 196).

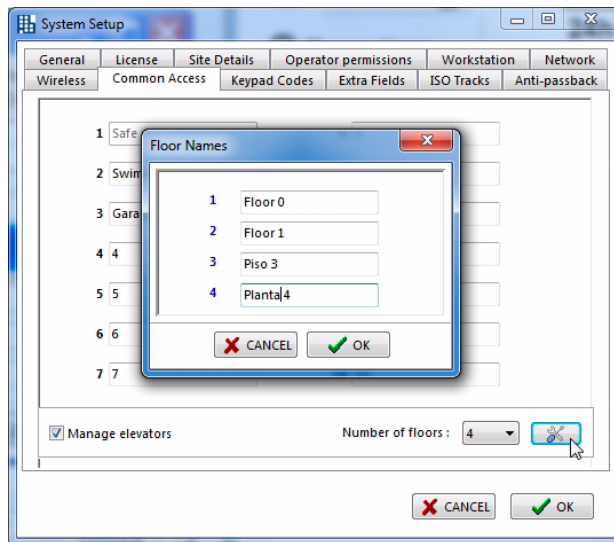


Elevator Wall Reader – 8-relay panel

In the “Setup” menu, “Grants” tab, the floors to be controlled by means of an Elevator Wall Reader are defined.

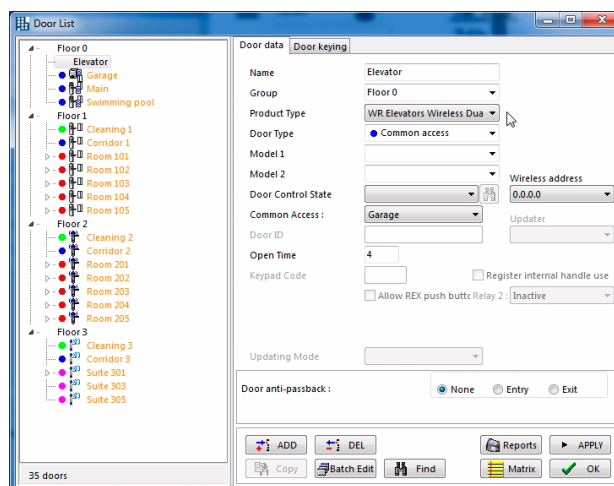
To do this, we define the number of floors we wish to control in the “Number of floors” field of this menu (up to a maximum of 40, installing a maximum of five 8-relay panels in series).

After defining the floors, we can change the name of each floor as appropriate (for example, 'piso', 'planta', floor, etc.).



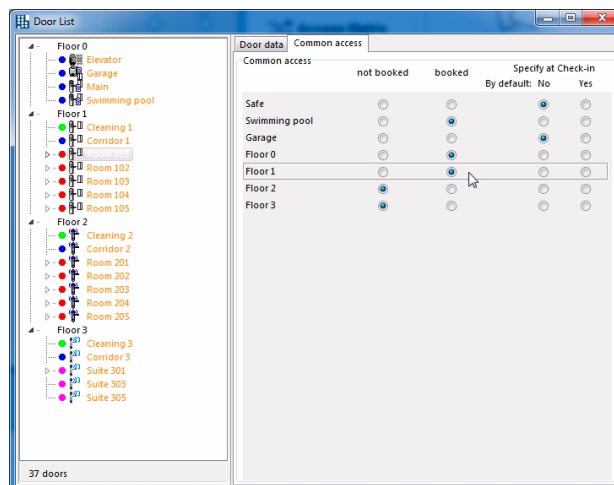
Next, the wall readers are created in the doors list, defining the technology type correctly (stripe / dual / wireless elevator reader).

It is also necessary to key the reader in order to define which guests have or do not have access to it, having defined the wall reader as a “Common Access” door.



Finally, in the room menu, we individually assign the grants of the guest for the floors we will give them access to. In this way, when the card is inserted in the elevator wall reader, the reader will activate the relays (grant = relay activated; grant 3 = relay 3 activated) to which the guest has access. This means that a guest from floor 1 will only access floor 1.

It is always possible to assign more grants to a guest if we want them to be able to access more floors (which are communal areas for all guests).



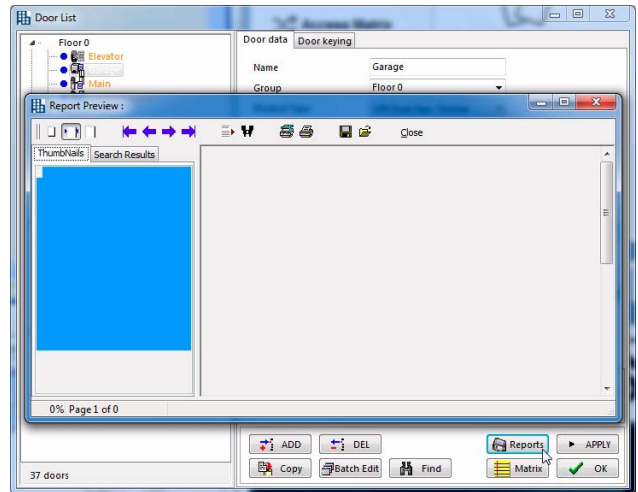
For more information on the Elevator Wall Reader, consult the instructions manual.

Reports

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

The information shown by the reports is the following:

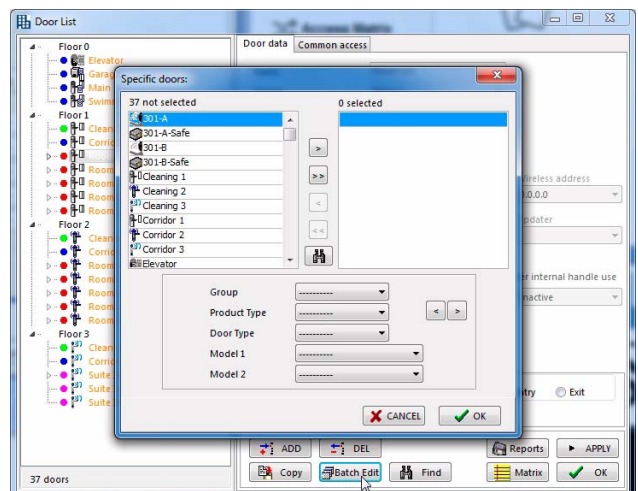
- **Door:** door name.
- **Group:** name of the group the door belongs to.
- **User:** user name.
- **Timezone:** this indicates whether the user is granted access or not and whether this is restricted to a timezone.
- **Open:** if the “@” symbol is displayed, then the user can leave the door in open mode. For more information on the “Can leave door open” concept, see “F.5 Matrix” on page 114.
- **Privacy:** if the “@” symbol is displayed, then the user overrides privacy. For more information on the “Overrides privacy” concept, see “F.5 Matrix” on page 114.
- **State:** this indicates the situation which the user is in at the door.
 - An arrow pointing to the right (\Rightarrow) 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 (\Leftarrow) indicates that the changes made in the locking plan of a user in that door have already been transferred to the credential, but are pending confirmation by the software
 - A blank space () indicates that the changes in the locking plan of that door have been transferred to the TESA Hotel system.



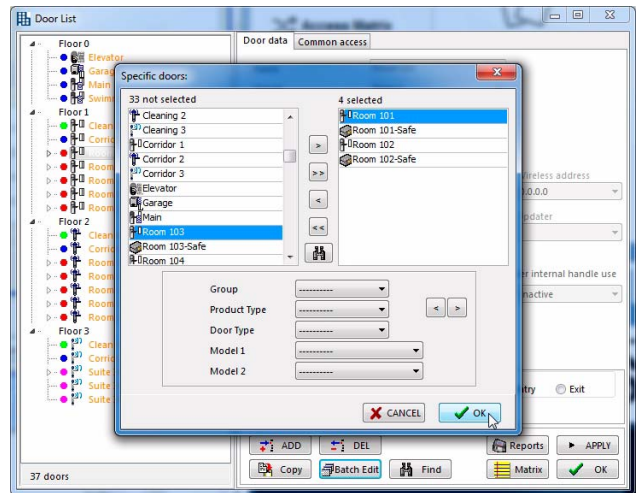
Batch

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

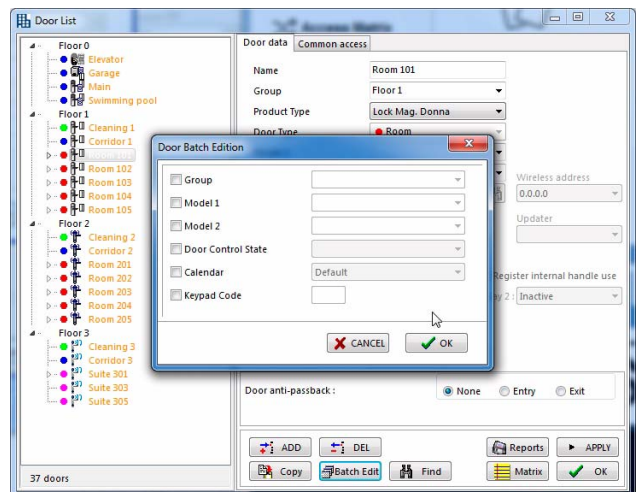
- 1 Click the “Multi” button; the following screen is displayed:



- 2 Select the doors whose properties you want to modify and click "OK".



- 3 Select the options you require, make the modifications in the corresponding field and click "OK" to accept the changes.

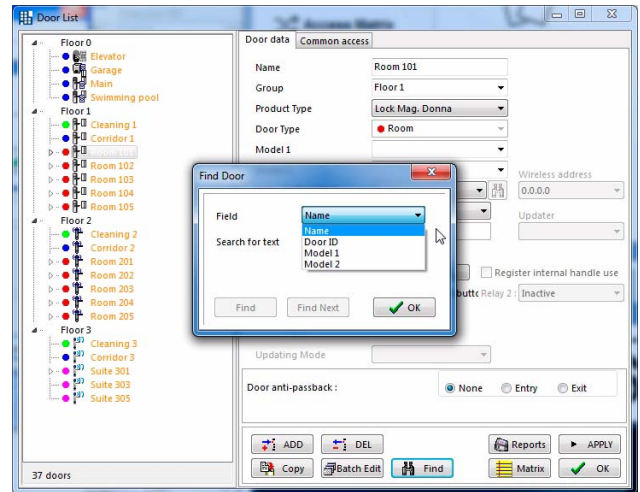


Find

The “Find” button allows conducting quick searches, which is very useful if the doors 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.

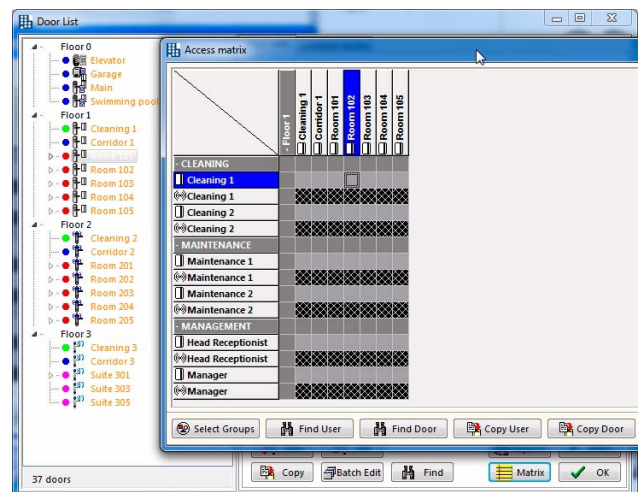
The search can be conducted by *Name*, by *Door ID* or by any of the *Door Extra Fields* which have been defined.



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 “Room 101” is selected, which belongs to the “Floor 1” group, only the doors belonging to the “Floor 1” group will be displayed.

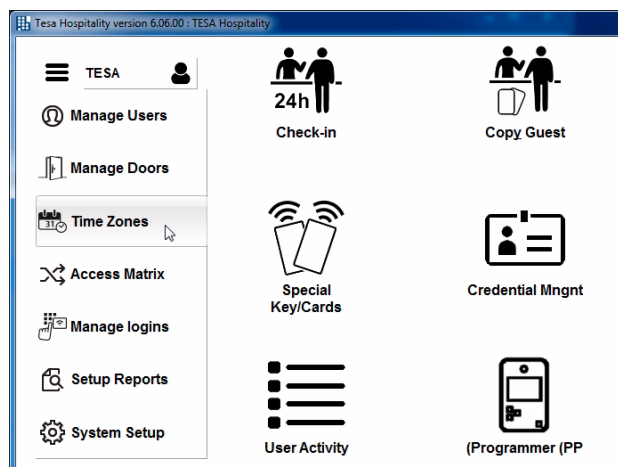


F.4 “HOURS” MENU

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

The electronic locks have a real-time clock and calendar, which allows us to restrict access by users according to the time and day.

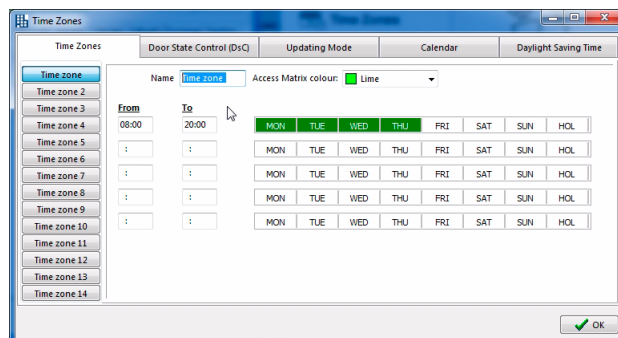
In order to access the “Hours” menu, click this option on the main screen of TESA Hotel.



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

- Hours
- State table
- Updating Mode
- Calendar
- Daylight Saving Time

These tabs are described in the following sections.

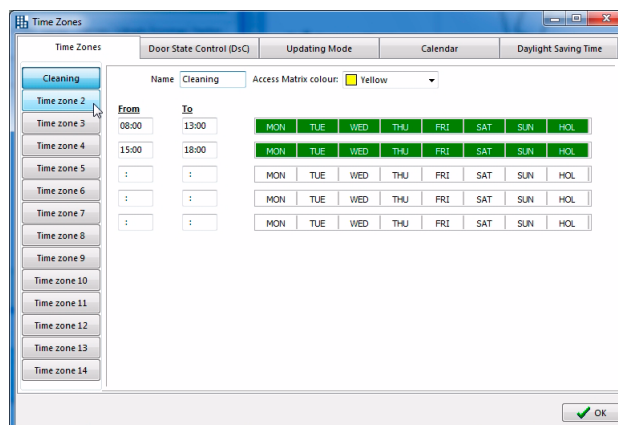


“Hours” tab (timezones)

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

As an example, presumably the Management and Maintenance staff will always have access to the doors and the cleaning staff will have access according to shifts (timezones).

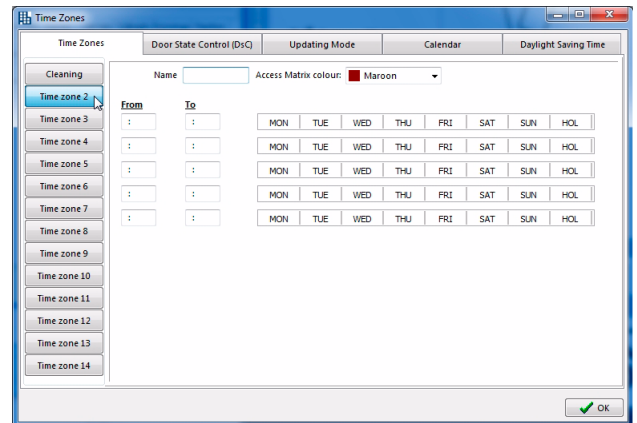
As a result, we create a Timezone which we call “Cleaning”, the working hours of which will be from 08:00 to 13:00 and from 15:00 to 18:00 every day of the week, including holidays.



If you wish to, you can define more timezones.

In order to define a timezone, 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.

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 in the matrix, which allows the timetable assigned to each user-door combination to be quickly distinguished in the matrix.

States

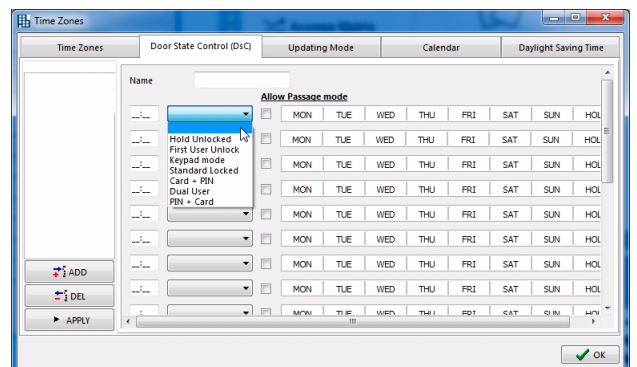
These are only available for Electronic Locks and Wall Readers.

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

It is possible to define up to 16 states tables, with a maximum of 20 zones or state changes in each of the tables.

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

- Open:** the door passes to open mode (free passage) at the time scheduled.
- First User:** the door operates in standard mode until the first user with granted access goes through it, 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).
In this mode of functioning, the locks and wall readers continue to work with the proximity credentials.
- 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 staff 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 lockings with a built-in keypad (magnetic stripe readers and locks).
This mode of functioning is not compatible with the *Read and Write* system.

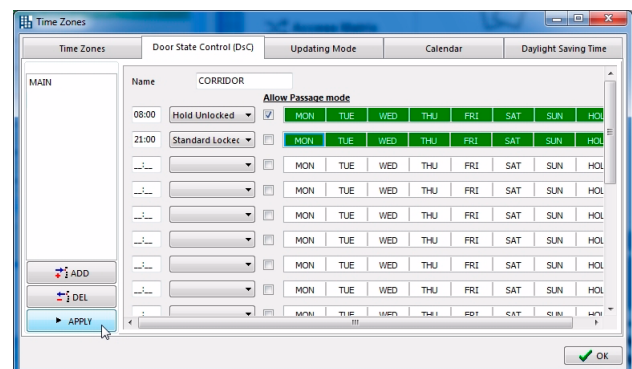
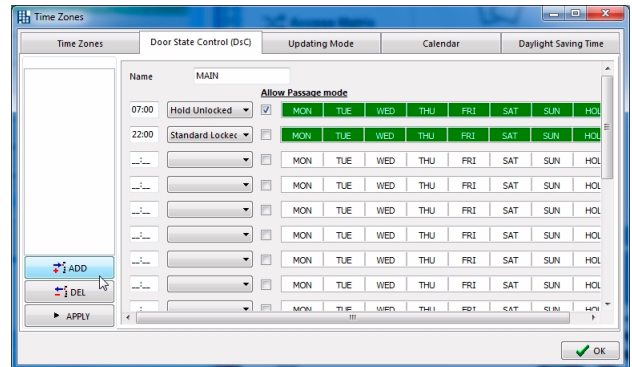


- **Dual User:** the door opens only if two credentials from authorised users are used in the lock successively.
- **PIN + Card:** in order to open the door, it is necessary in the first place to type the access code and then pass through the card associated to that code. This code is programmed in the “Users” menu.
This is the only dual identification option available in UoC (Read and Write) systems.
It is also compatible with wireless systems.

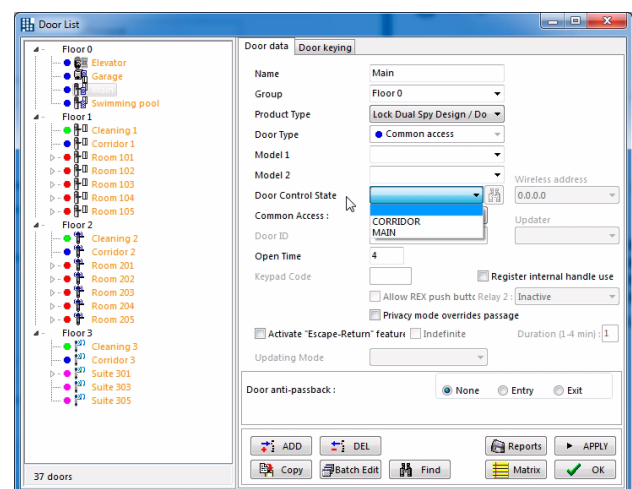
In order to create a new State, click “Add” and enter the desired data in the corresponding fields. The days are selected by double-clicking the corresponding day. Once you have finished, click “Apply” to encode the data.

Example: in a hotel, the MAIN door is required to be open (passage) every day of the week from 7 am to 10 pm. In addition, the doors of the CORRIDORS are required to be open from 8 am to 9 pm every day of the week. Therefore, two states tables are needed.

Moreover, we have marked the possibility of modifying the door state whilst it is open, by checking the “Door can be left Open or Closed” box. If this box is checked, the authorised users can change the state of the door from Open to Closed and vice versa, by passing their credential through it twice in a row.



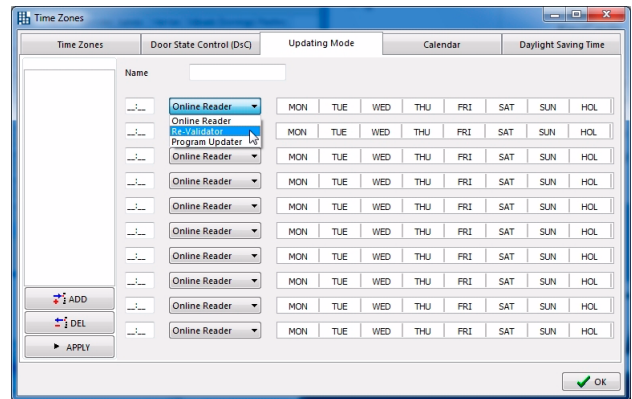
Once a door state has been created, a new Door States field is displayed in the “Doors” menu:



“Updating Mode” tab

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

- On-line 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 and revalidates 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 expiration of the credentials and modifying the grants assigned to the user. It can be used in updaters either 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 for reading and encoding the card is longer. It collects events, writes the locking plan crosses still to be encoded, renews the expiration of the credential and modifies the grants. It can be used in updaters either with or without door control.

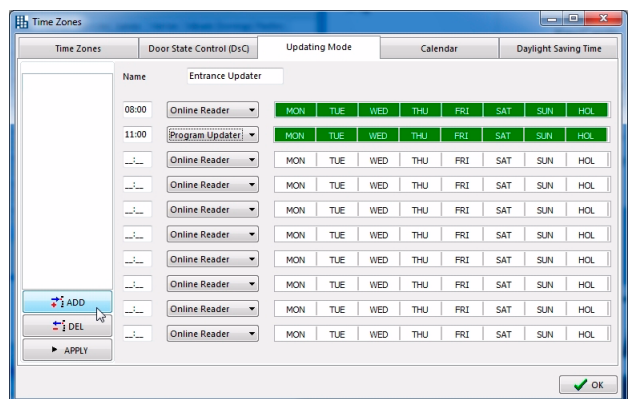


The main functions of an Updater Reader are reading, re-encoding and revalidating the cards in the Read and Write system. Performing all these functions in 4K Mifare cards with all their memory full can take a few seconds, and at times of high traffic can give rise to queues of users. To prevent this, the Updater Reader can be configured to work only as an on-line reader during high-traffic periods and so alleviate the traffic of people.

In the example, we have envisaged that early in the morning (at 8 am) it should work only as an on-line reader, so as not to create queues, and that from 11 am it should work in complete mode until 8 am the following day.

After filling out the fields, click on “Add” and accept the confirmation message that appears next.

You can add more updating modes if you wish to.

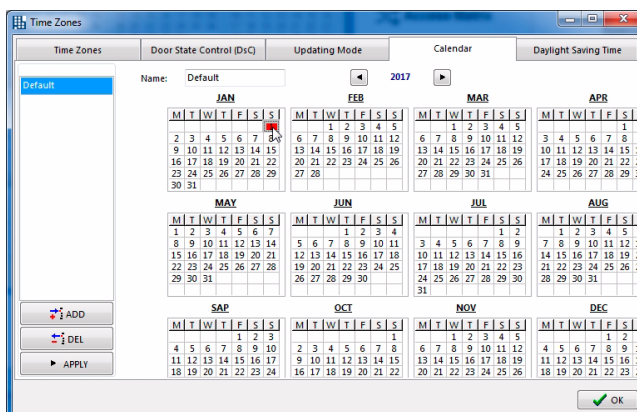


Calendar

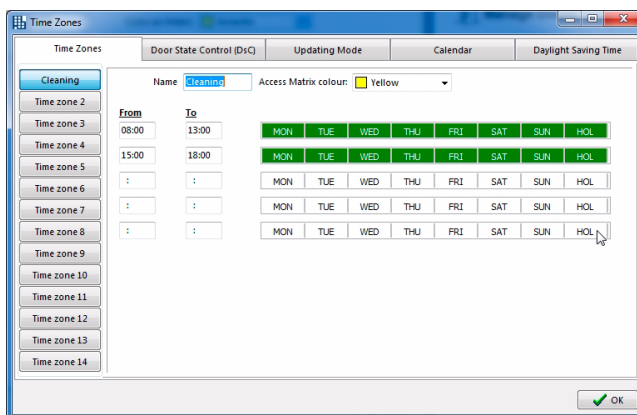
The locks have an internal calendar that enables them to recognise the day of the week, but not holidays. The “Calendar” tab allows the hotel’s holidays to be defined.

For this purpose, double-click the holidays for them to turn red. You can also define the holidays of the coming years, changing the year using the corresponding arrows.

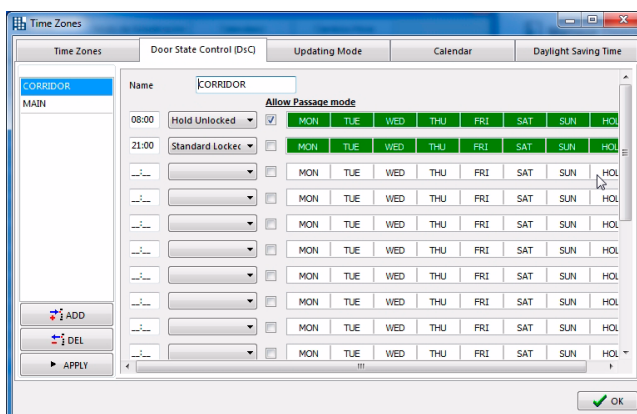
It is possible to define different calendars of holidays. In order to define a new calendar, click “Add” and write a name in the field “Name”. Select the holidays by double-clicking the corresponding days. Once you have finished, click “Apply”. The new calendar is displayed in the column on the left.



After setting the holidays by means of the “Calendar” tab, it is possible to restrict the access to the users on holidays, using the “Hours” tab, and clicking on “Holiday”, which is after “Sunday”.



We can also define different modes of functioning for the doors on holidays, using the “States” tab.



“Daylight Saving Time” tab

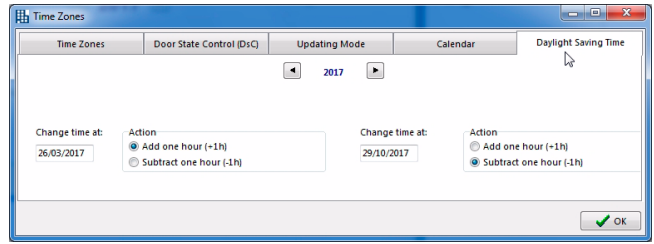
This allows setting the time changes for summer and winter (DST).

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.

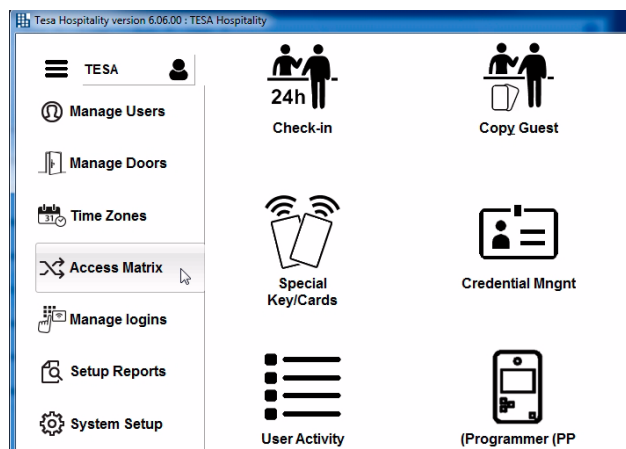
In the wireless systems, this information is sent automatically on the 1st of each month.



F.5 MATRIX

Once the staff 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.

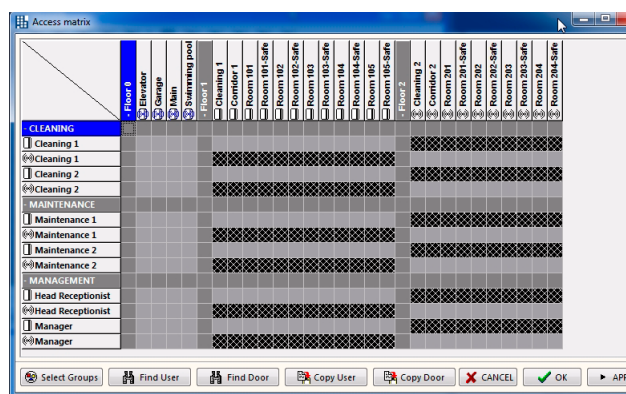
In order to access the “Matrix” menu, click this option on the main screen of TESA Hotel.



The matrix relates a user to a door, by means of a square.

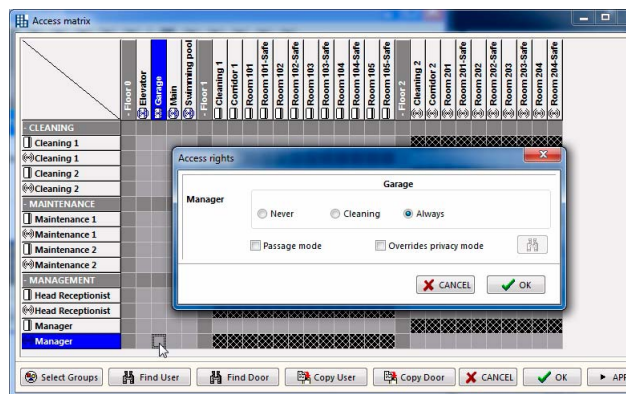
This square is referred to as a “Cross”. A *Locking plan cross* indicates whether or not that specific user has access granted to the door. By default, the first time the matrix is opened, no user has access to any door.

In the example, one can see the groups of users and doors that have been created in the previous sections of this chapter.



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


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

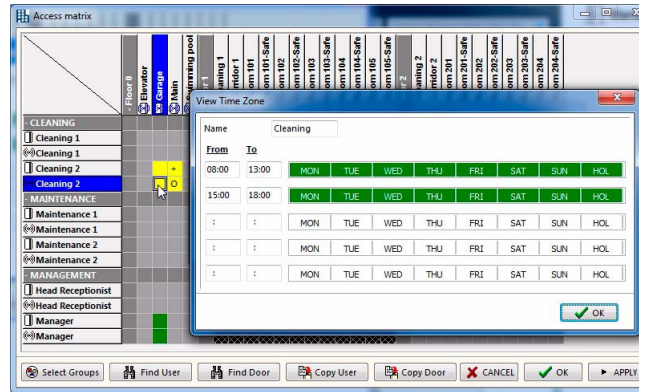


- **Can leave door open** check box: if this check box is enabled, the user can leave the door open, by acting as follows: passing their credential through the door once and, immediately afterwards, passing it through once again, while the lock is still open. In this way, the door remains open permanently. For the door to close again (for example, at night), it is necessary to define a *State* (see “States” on page 109), or repeat the same operation of swiping the card through.
- **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 thumbturn is engaged. Otherwise, they cannot gain access to it, even if authorised to do so, because the privacy thumbturn is engaged.

Creating the Locking Plan

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

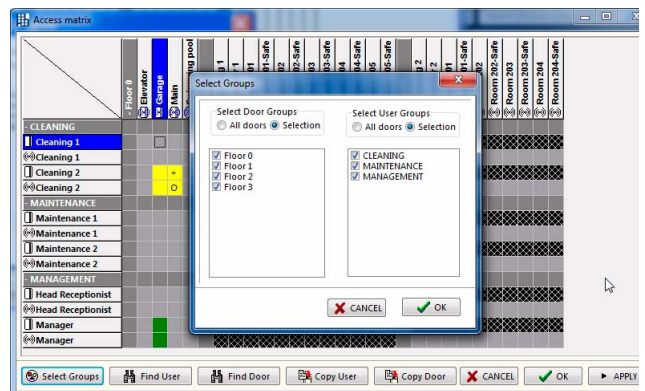
- **Black stripes:** The user's technology does not match that of the door (for example, user has a magnetic stripe and door has proximity card)
- **Grey:** never has access
- **Green:** always has access
- **Other colours:** access according to timetable defined with that colour. In order to see the 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.
- **+**: indicates that the user Overrides privacy.
- **0:** indicates that the user can leave the door open.



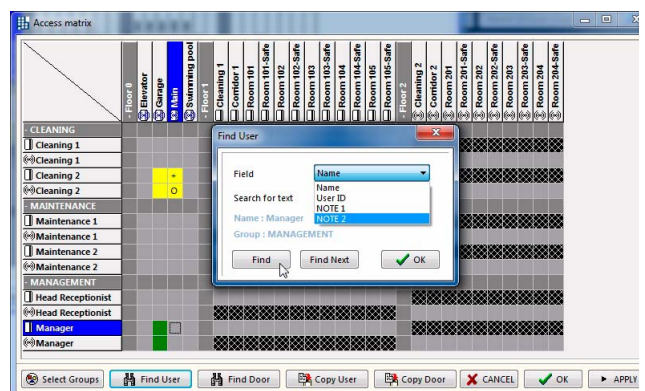
The following buttons are available at the bottom:



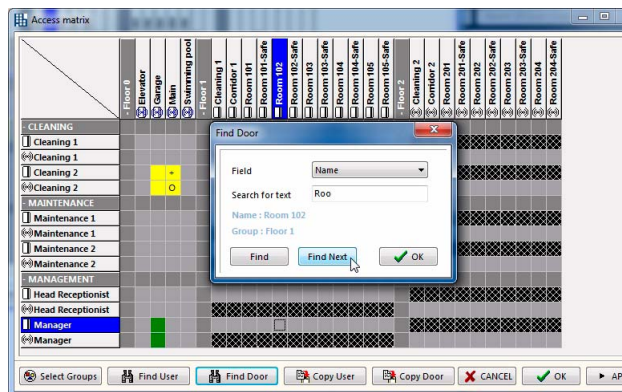
- **Select Groups:** this allows defining which groups of doors and users are displayed on the screen, which is very useful when the matrix is large.



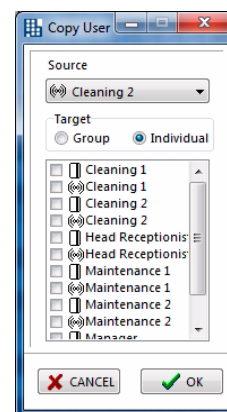
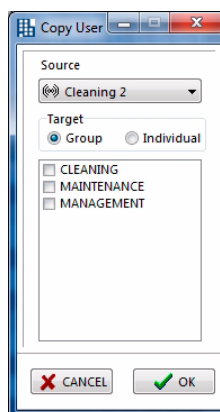
- **Find User:** a window is displayed when this button is clicked, which allows finding a user quickly. The marker is placed on the name of the user sought. The search can be conducted by *Name*, by *User ID* and by any of the *User Extra Fields* which have been defined.



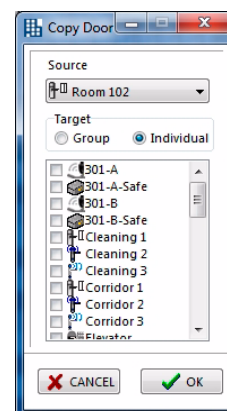
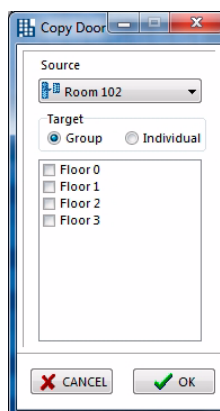
- **Find Door:** this allows finding a door easily, by means of a search window, in a large-sized matrix. The marker is placed on the name of the door sought. The search can be conducted by Name, by Door ID and by any of the Door Extra Fields which have been defined.



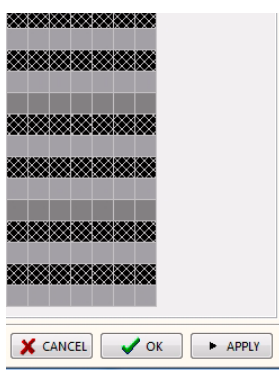
- **Copy User:** allows copying the accesses of one user to a series of individual users, or to one or several groups of users.



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



- **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

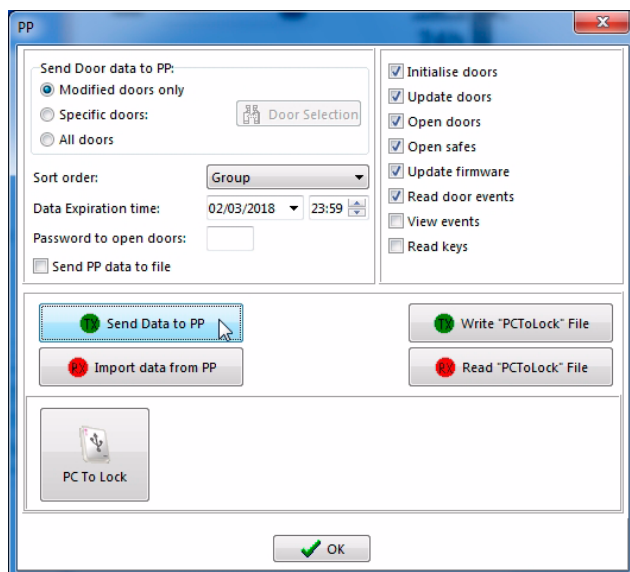
Once the locking plan has been created, it is necessary to transfer this information to the portable programmer and, subsequently, initialize the locks, readers and/or cylinders.

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



☞ The most usual procedure is to select the “All” field in “Send Doors to PP” and click on “Send Data to PP”, as explained in the section “1.2 Transmitting and receiving data by means of the portable programmer” on page 142.

It is also possible to store the data in a file in order to send them to a device that is connected to the PcToLock converter or communicate directly with the PcToLock device connected to the same machine.



G – Operators and Operator Levels

- Introduction 121
- Operator Levels 121
- Operators 123
 - “Key / Card User” field 124
 - “Operator Name” field 125
 - “Password” field 125
 - “Security Level” field 126
 - “Cards Validity Limit” field 126
 - “Show users and doors groups” field 127
 - “Managed door groups” and “Managed user groups” fields 128
 - “Add” and “Close” buttons 128



G – OPERATORS AND OPERATOR LEVELS

G.1 INTRODUCTION

In order to access the TESA Hotel software, 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 or staff card 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 TESA Hotel 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.

This operator will be assigned to a staff card user. If we need to create an operator who will not hold a physical staff card, we can create a “virtual” staff user whose card does not have to be encoded and even if it were, it would not open any doors, as this card is not keyed in the matrix.

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

G.2 OPERATOR LEVELS

On the TESA Hotel main screen, access the “Setup” menu, by clicking the corresponding button.



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

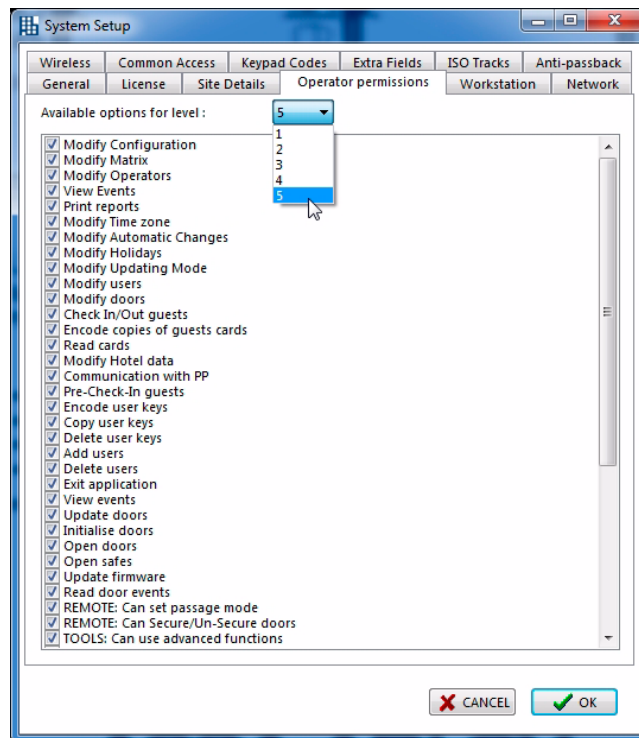
As can be seen, there are 5 different Operator Levels.

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 you wish to grant for that level.

Do the same for the other 4 levels.

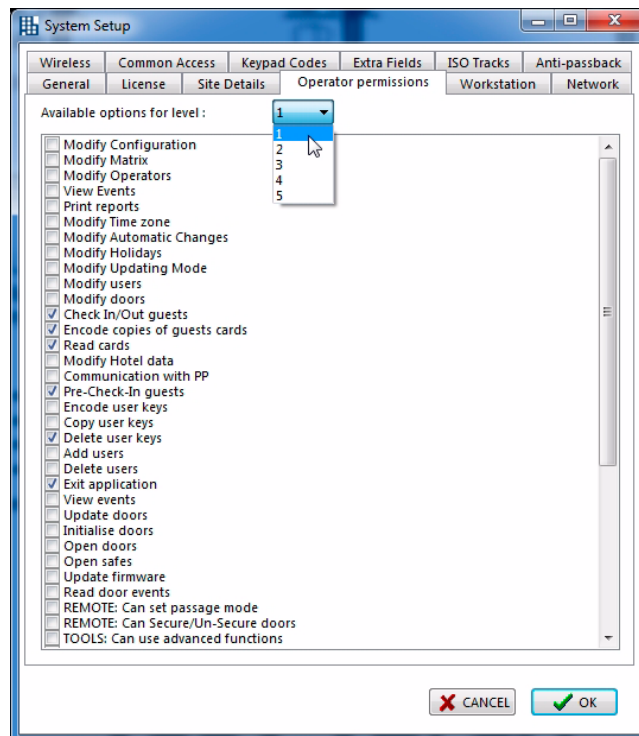
Afterwards, each Operator should be assigned the Level which is considered appropriate.



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

By default, all the levels have the “Close application” option enabled. This is important to prevent an operator leaving the application open and not being able to exit it. 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.

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



G.3 OPERATORS

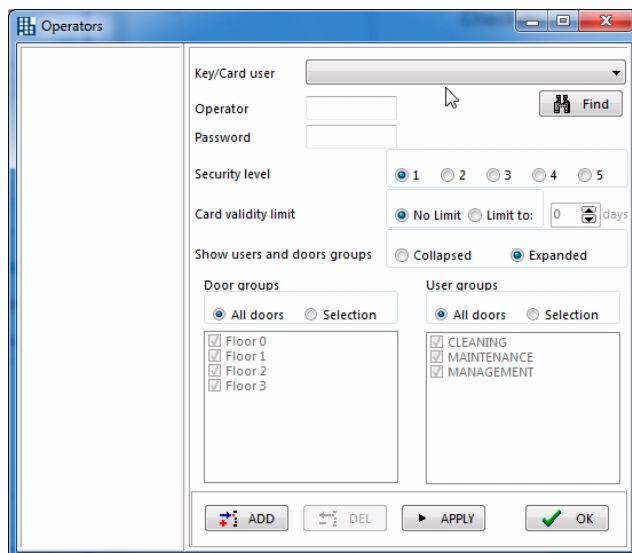
On the TESA Hotel main screen, access the “Operators” menu by clicking the corresponding button.



The “Operators List” screen is displayed:

This screen allows adding the Operators to the system.

The meaning of the different fields is explained below.

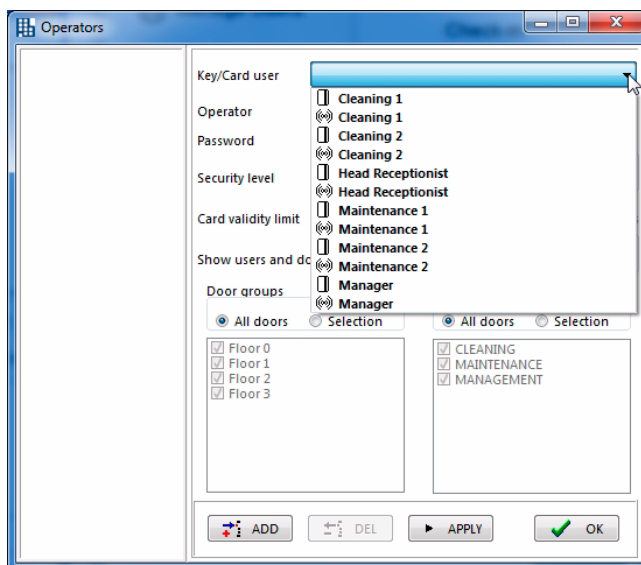


“Key / Card User” field

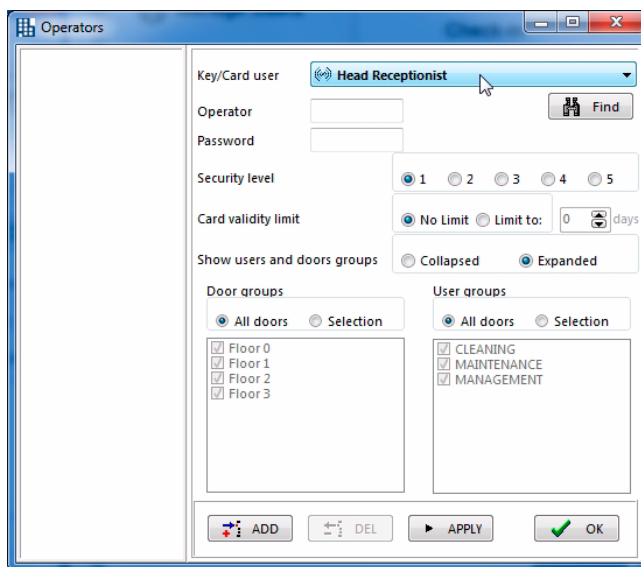
This field allows selecting, from among all the Users of the system, the one who is to be added as an Operator.

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

If you need to create an Operator but do not want them to have a credential that opens doors, virtual users can be created in the “Users” menu so that they are later displayed in the “Operators” menu.



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



“Operator Name” field

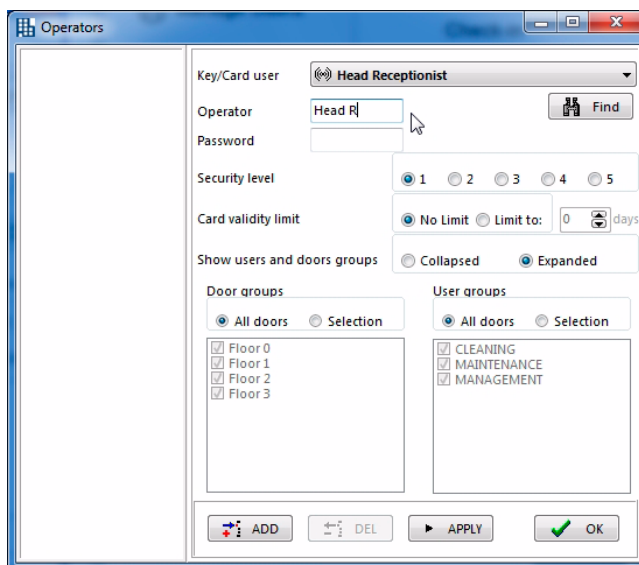
This field allows assigning an Identification Name to the Operator who is being added. This name need not match the User name.

Type the Operator name in the corresponding field.

You can choose an “alias” with 1 to 10 digits for the Operator name.

Either capital or lower-case letters may be used in the Operator name, as they are not distinguished.

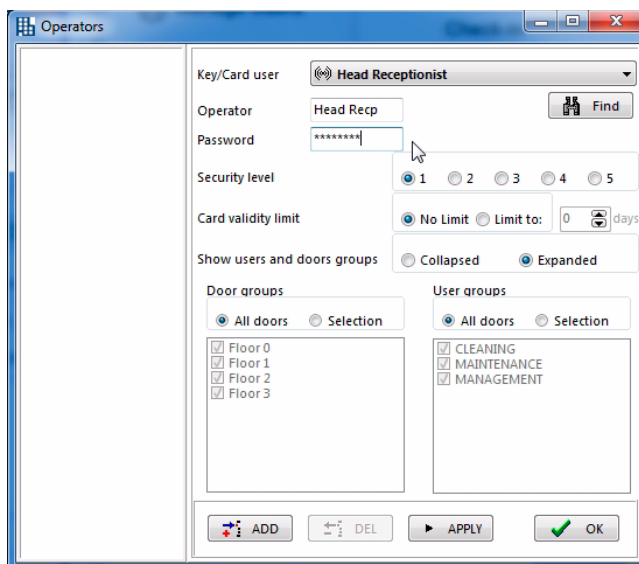
Once the Operator has been added, they will be displayed in the column on the left with the assigned Operator name in this field.



“Password” field

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

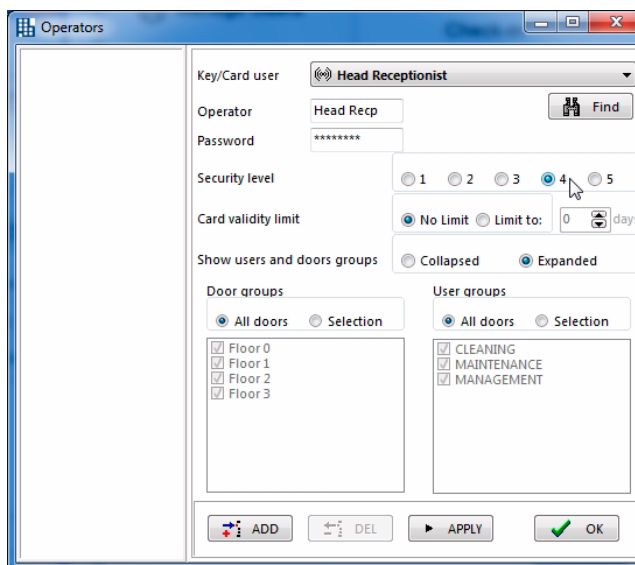
When entering the password, for security, this is shown as asterisks on the screen.



“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 121, it was explained how to define the operations allowed for each level.



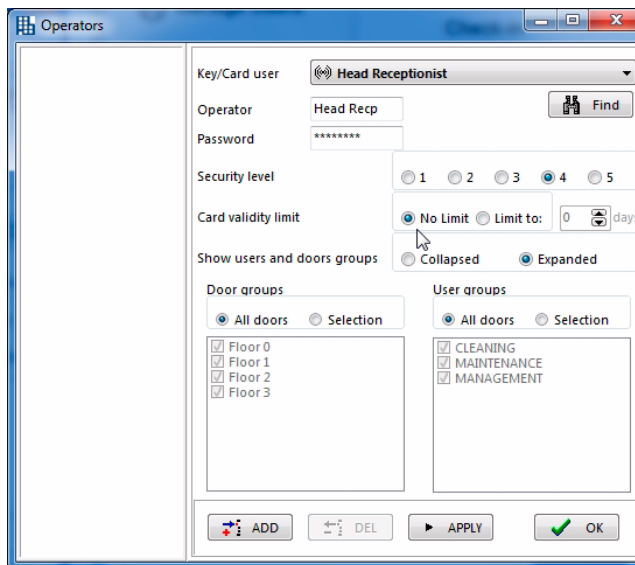
“Cards Validity Limit” field

This field allows preventing certain operators from encoding user cards with no expiration limit. When encoding a user card, it is possible to set an expiration 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.

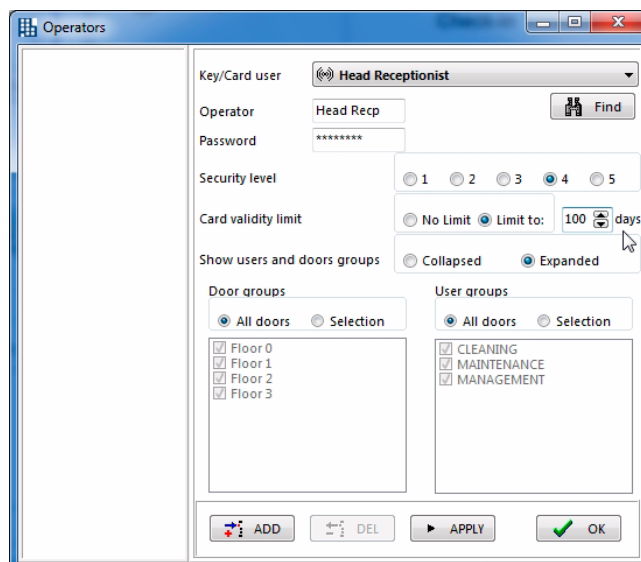
“No Limit” setting:

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



“Limited to” setting:

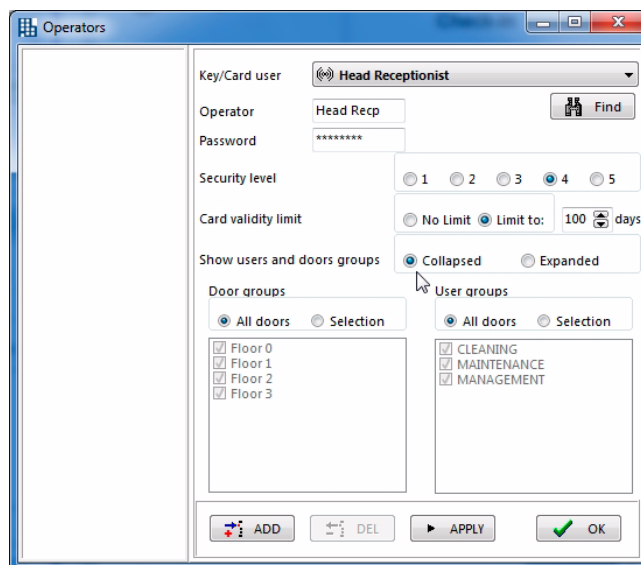
This option allows entering a number of days (from 1 to 730; 100 in the example) after which the card will expire, even if the operator had not entered an expiration date when encoding it.



“Show users and doors 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.

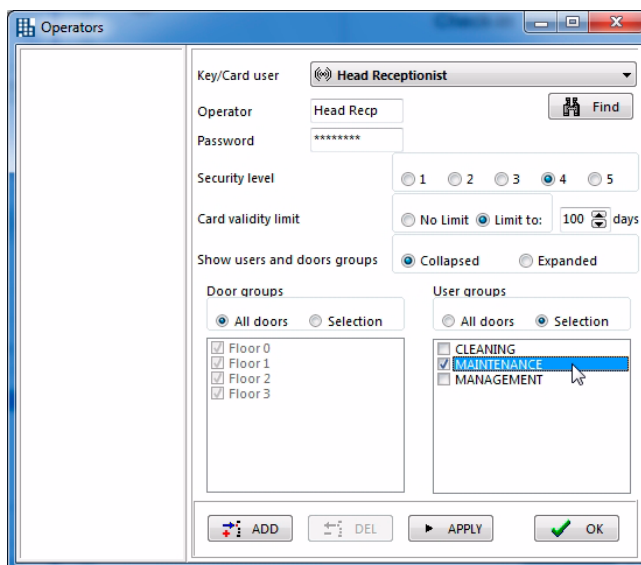


“Managed door groups” and “Managed user groups” fields

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.

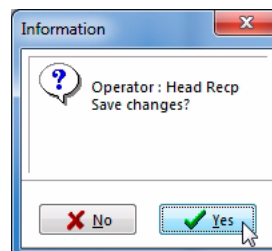
If you want to apply a restriction, tick the option “Selection” in the corresponding group (doors, users or both) and tick the groups which the operator is going to manage (“Management” in the example).



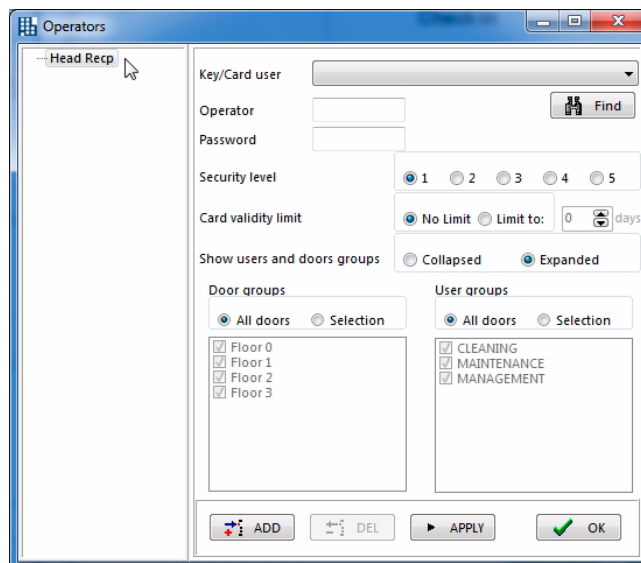
“Add” and “Close” buttons

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.



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



H – Grants

Introduction	131
Operation without Grants	131
Operation with Grants	132
Using Grants	133
Defining the Grants	133
Assigning grants to the doors	135
Updating the matrix	136
Updating the doors	136
Assigning the grants to the users (hotel staff / master)	137
Assigning grants to the guests (rooms and suites)	138

H – GRANTS

H.1 INTRODUCTION

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 Hotel” 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 to reprogramme this access.

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 expiration 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 expiration 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 a *Read and Write* 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 *Read and Write* 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 TESA Hotel software, 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 *Read and Write* 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 *Read and Write*, 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:

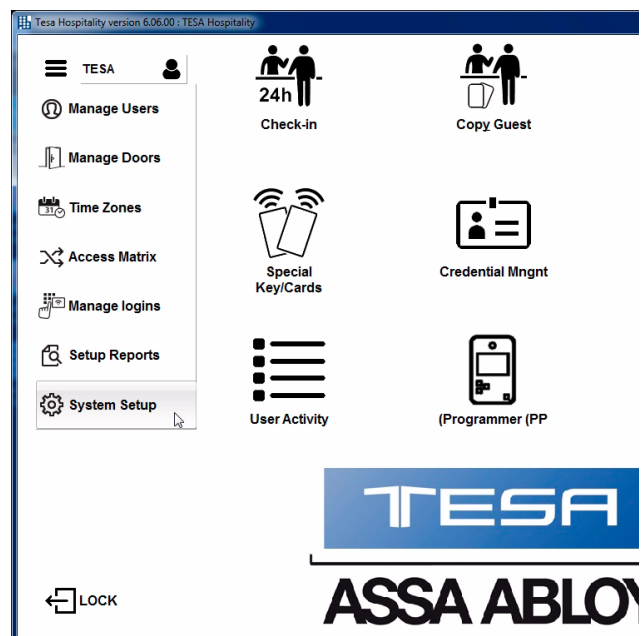
- 1 “Defining the Grants”
- 2 “Assigning grants to the doors”
- 3 “Updating the matrix”
- 4 “Updating the doors”
- 5 “Assigning the grants to the users (hotel staff / master)”
- 6 “Assigning grants to the guests (rooms and suites)”

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 TESA Hotel settings menu.



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

It is possible to have up to 48 different grants.


By default, the system has the “Safe” grant predefined, so we can define a further 47 grants depending on our needs.

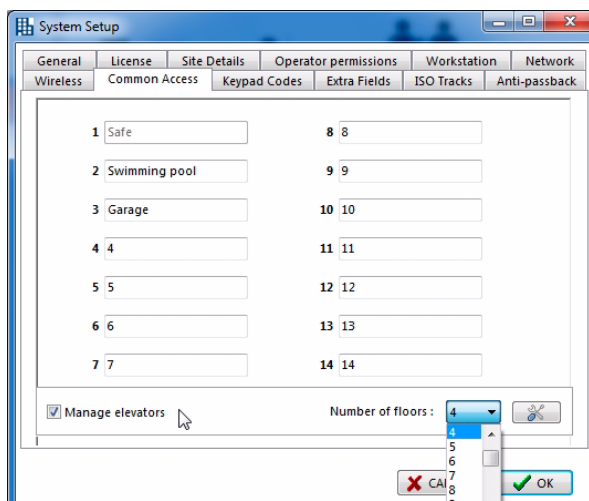
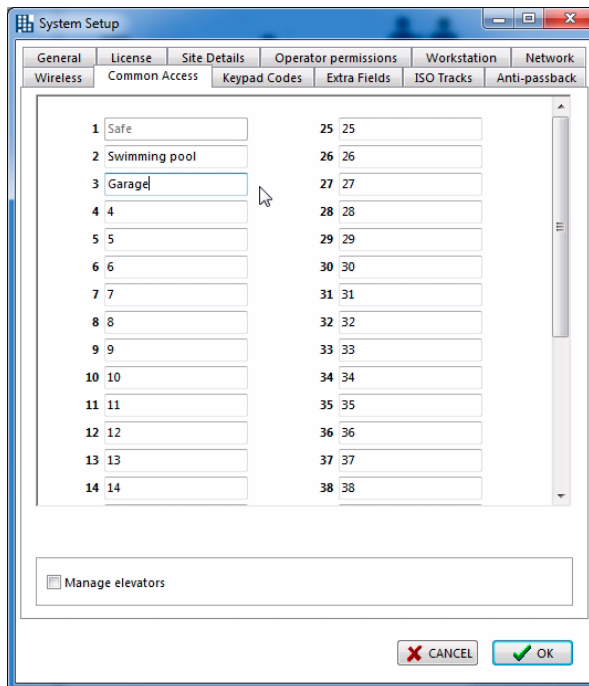
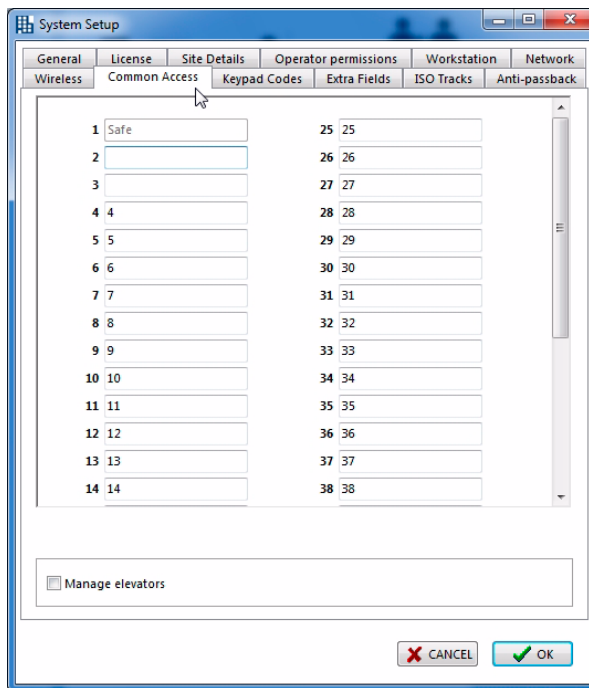
To create grants, all you have to do is write the corresponding name in each field: For example:

- Swimming pool
- Garage
- Floor 1
- Floor 2
- Floor 3

To finish, click on the “OK” button.

The “Manage elevators” option allows creating grants according to the floors the hotel has, which enables us to regulate the traffic of users in the hotel when there are elevator readers with 8-relay panels Up to a total number of 40 floors can be controlled, but in turn the grants will go from a total of 48 to 14. In the “Number of floors” field, we will define the number of floors the hotel has.

If you wish to customise the number of floors, click on the  button and a window will be displayed allowing you to do so.



Assigning grants to the doors

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

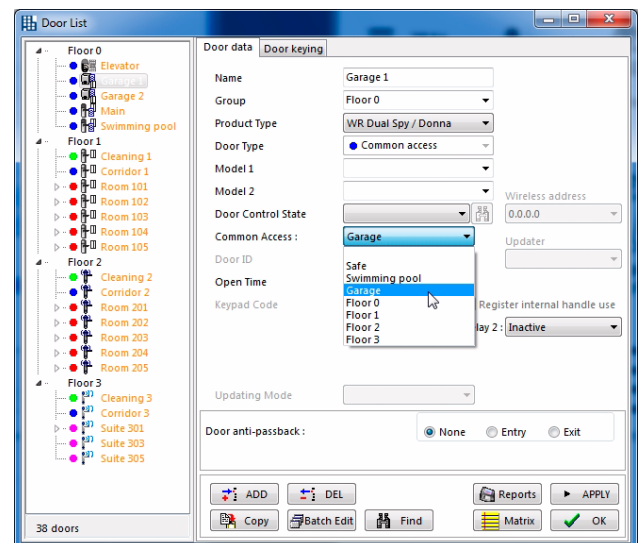
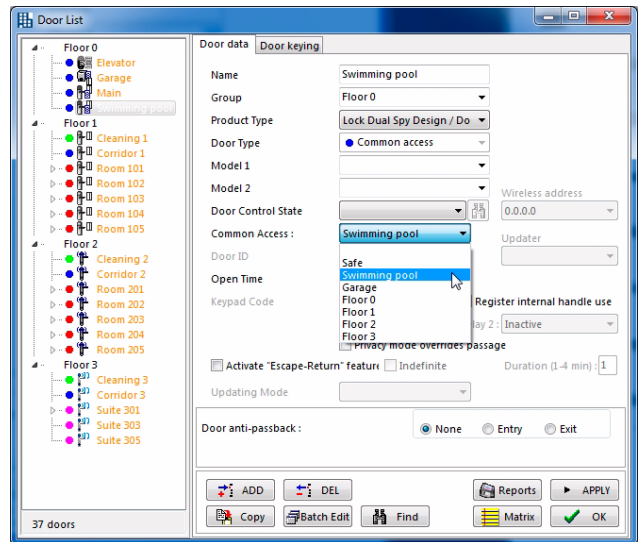
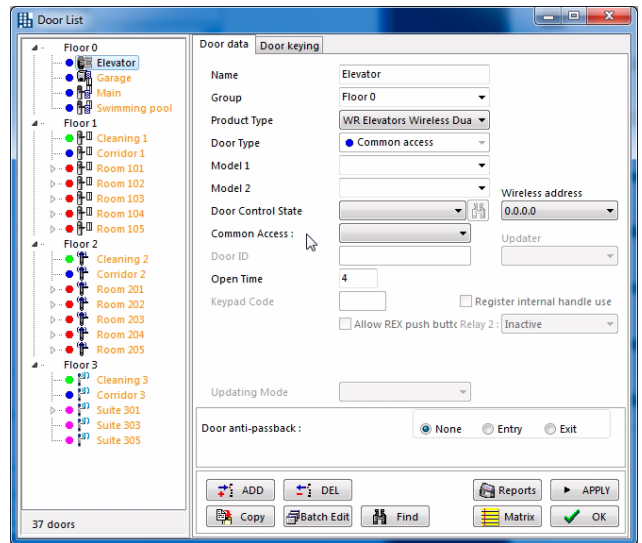
If this field is blank, it means that that door does not require any grant and, therefore, its operation mode will be like the one explained in section “H.2 Operation without Grants” on page 131.

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

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

Finally, the “Apply” button is clicked.

If desired, the same grant can be assigned to several different doors. For example, if there are 2 garage doors on a floor (Floor 0), it is possible to define a grant called “Garage” and assign it to the 2 doors of the garage.



H

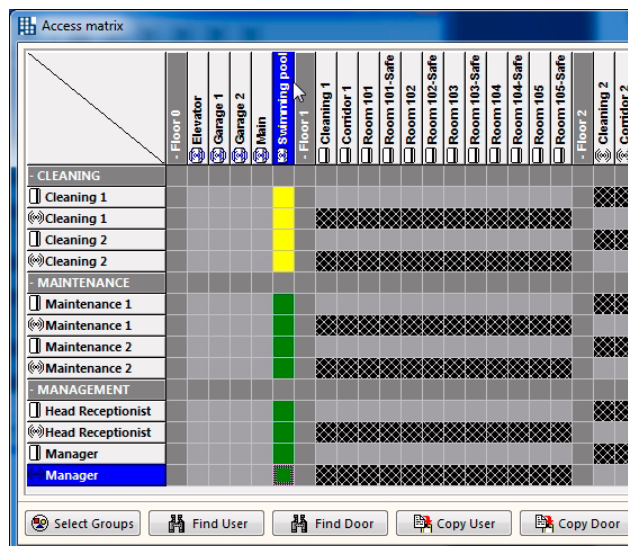
Updating the matrix

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 timezone “Always” (green colour) or according to any of the TimeZones 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 (encoded in the credential).

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



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 initialize them.

This is done in the following steps:

- 1 Transmitting the data to the portable programmer
- 2 Updating and/or initializing the affected doors using the portable programmer

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

Assigning the grants to the users (hotel staff / master)

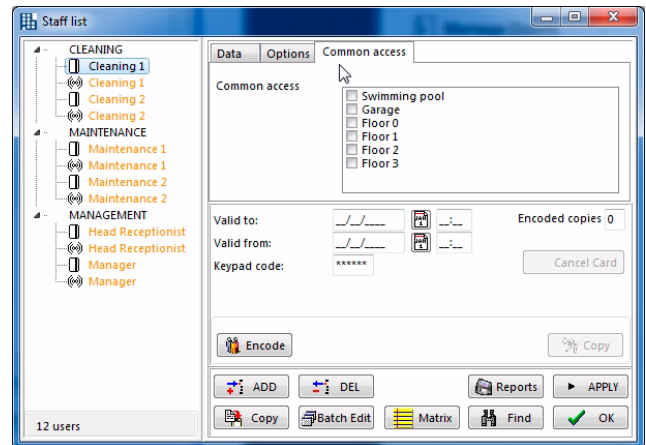
In the Users menu (Staff List) the grants are assigned to the hotel staff.

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 (staff list).

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 check the box for that grant.

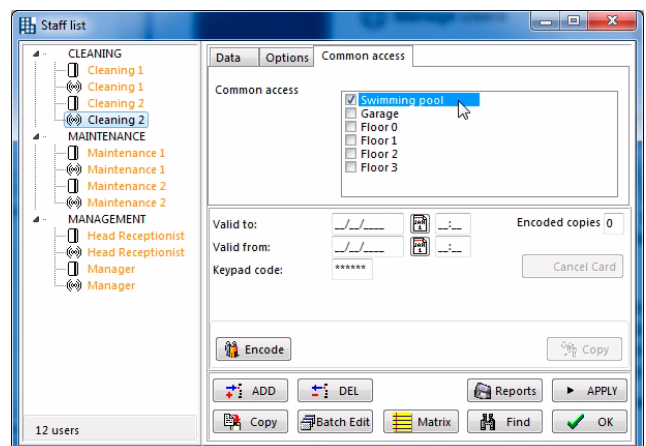
The assignment of grants can be modified as many times as desired; you only need to encode the credential of the user again each time the assignment is modified.



In the example, the grant Swimming Pool has been assigned to the user Cleaning 2.

Once the credential of Cleaning 2 has been encoded (proximity), he will be able to access the swimming pool without carrying out any other process.

In order to prevent Cleaning 2 from accessing the swimming pool, you only need to remove the selection from the grant swimming pool and encode his credential again.



If the system is *Read and Write*, the encoding can be carried out manually in an encoder or when the user goes through an updater.

Assigning grants to the guests (rooms and suites)

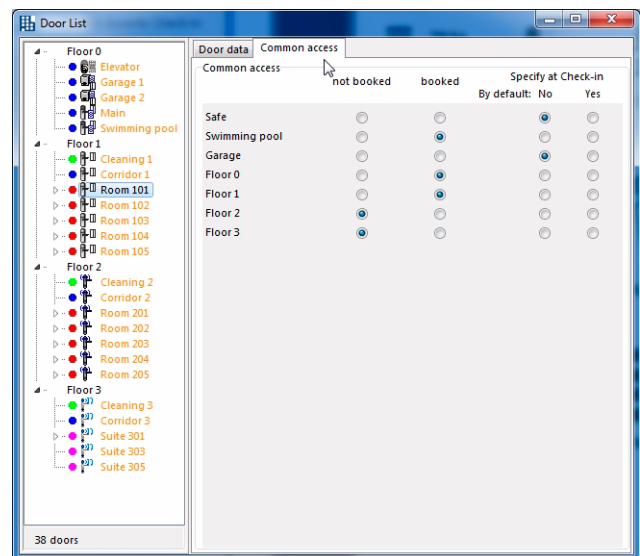
The grants of the guests are defined in the Doors menu (Doors List), in the corresponding rooms and suites.

Usually, in a hotel there are some services for guests that are optional, for which a supplement has to be paid in order to enjoy them. These services may be the garage, the swimming pool, the safe, etc. It is also possible to regulate the traffic of guests around the different floors of the hotel, creating grants by floors, which allow or deny access to certain floors via the elevator.

After creating these grants as indicated in *“Defining the Grants”* on page 133, they are assigned to the guests in their respective rooms and suites, on the *“Guest's Grants”* tab of the *“Doors”* menu (Doors List).

The grants that are assigned to a guest are determined on the *“Guest's Grants”* tab. There are four possibilities for each grant:

- **Not assigned:** the guest will never have access to the doors that require this grant.
- **Assigned:** the guest always has access, because the grant is encoded on his/her credential.
- **Specify at Check-In, by default Yes:** the guest has access to these doors by default, although the grant can be denied during Check-in.
- **Specify at Check-In, by default No:** the guest does not have access to these doors by default, although the grant can be assigned during Check-in. This is the most frequently used way of managing the grants for services requiring rental.



The example shows that the guest of room 101 has unrestricted access to the swimming pool and around floors 0 and 1, but access to the garage and safe of his/her room can be assigned when his or her card is encoded.

I – Encoding keys and programming doors

Introduction	141
Transmitting and receiving data by means of the portable programmer	142
“Send Doors to PP” field	143
“Available operations” field	145
“View doors sorted by” field	145
“PP data expiration” field	146
“Password to open doors” field	146
Send PP data to file	147
“Send Data to PP” button	148
“Get Data from PP” button	148
“PCToLock” button	149
“Write PCToLock File” button	150
“Read PCToLock File” button	150
Initializing the doors of the site	151
Introduction	151
Initialization by means of the Portable Programmer	151
Initialization by means of PCToLock	153
Encoding of (staff) credentials	154

I – ENCODING KEYS AND PROGRAMMING 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 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, keyrings, wristbands, watches...): Proximity Encoder
 - Magnetic Stripe Cards: Magnetic Stripe Encoder

- Programming 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

I.2 TRANSMITTING AND RECEIVING DATA BY MEANS OF 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 initialize the cylinders, locks and/or readers with that data.

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

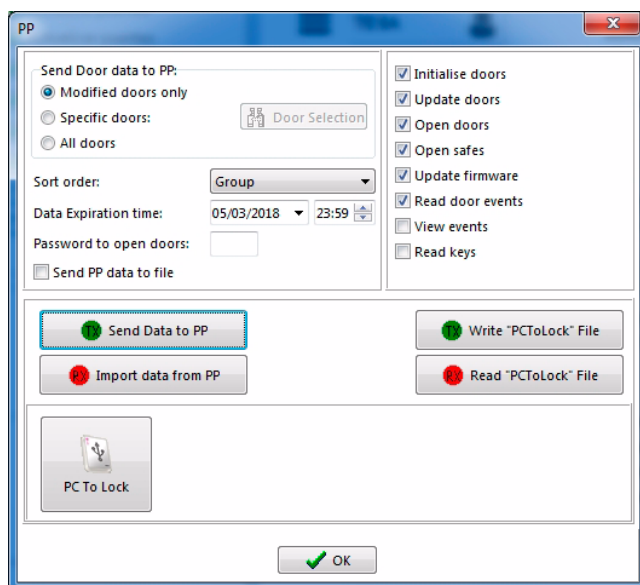
- ☛ Refer to the Instruction Manual of the Programmer used to see how it is connected, installed and managed.

After installing and connecting the Programmer to the PC, click the “PP” button on the TESA Hotel 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:



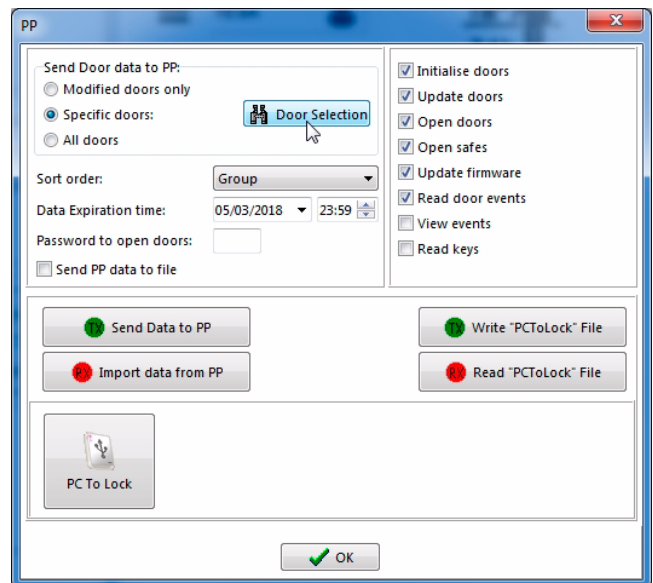
“Send Data to PP” field

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.

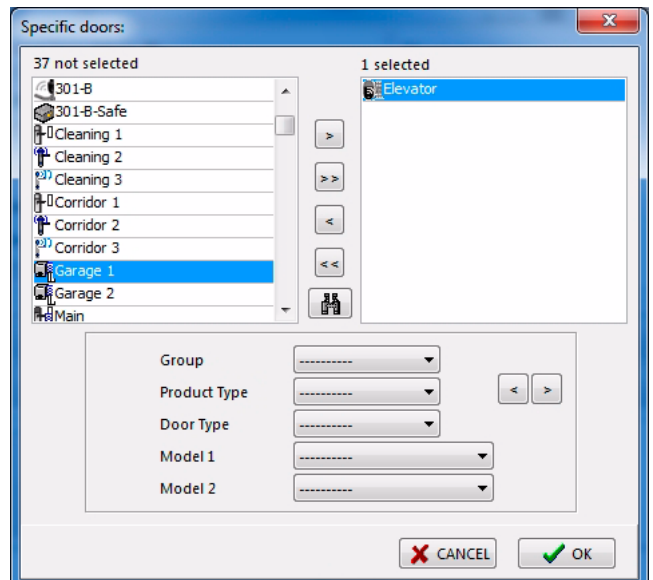
- The option “**Doors Selection**” allows selecting the doors which are needed: this option is selected and then the “Select” button is clicked.



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

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.



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.

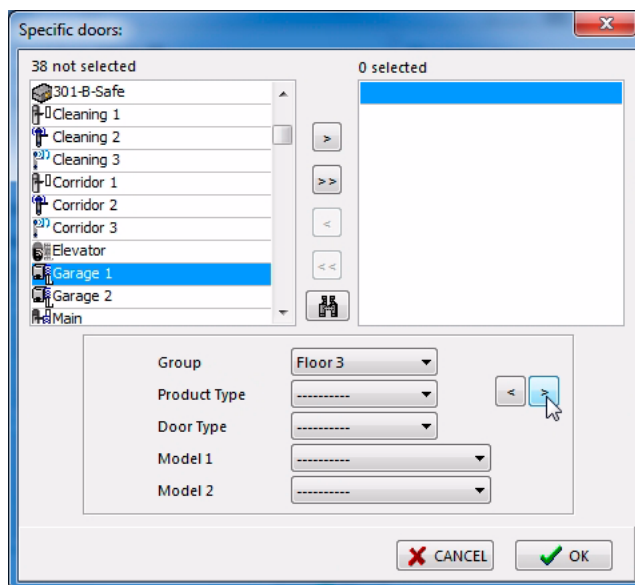
In the example, the group “Floor 3” is being selected.

- 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, it may serve for example to select all of the doors of a floor of the hotel, or of a specific department, 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”, “Suite”, “Common Access”, “High Traffic Door” and “Safe”.

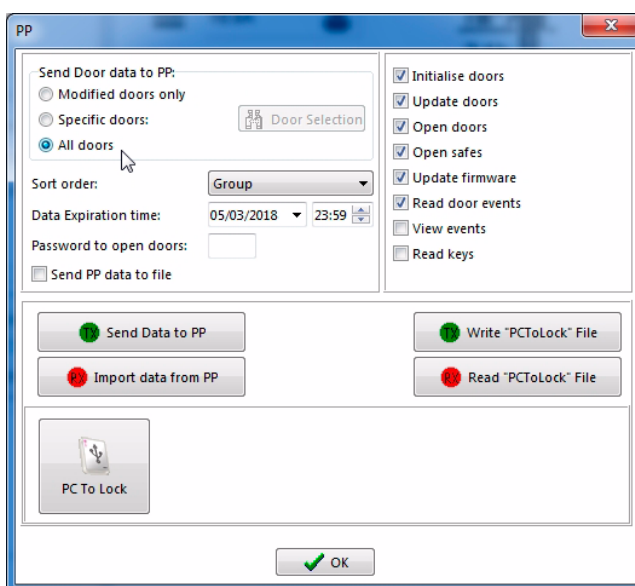
The selection of doors to be sent to the Portable Programmer may involve several individual selections made successively, that is to say, it is possible to select first the “Floor 3” Group and, then, the “Floor 0” Group.

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.



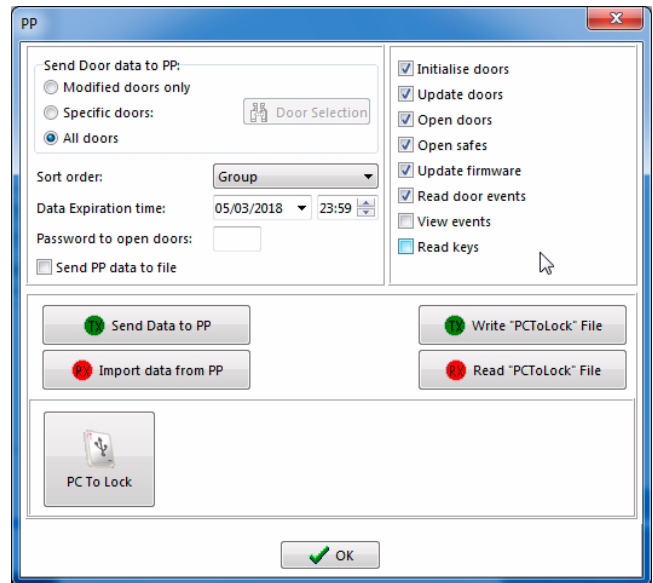
- The option “All” loads all the doors into the Portable Programmer.



“Available operations” field

Before sending the data to the Portable Programmer, it is possible to select the operations we wish to perform with said Programmer. They are the following:

- Initialize doors
- Update doors
- Open doors
- Open safes
- Update firmware
- Read openings from doors
- View openings
- Read keys
- View openings (by default No)
- Read keys (by default No)

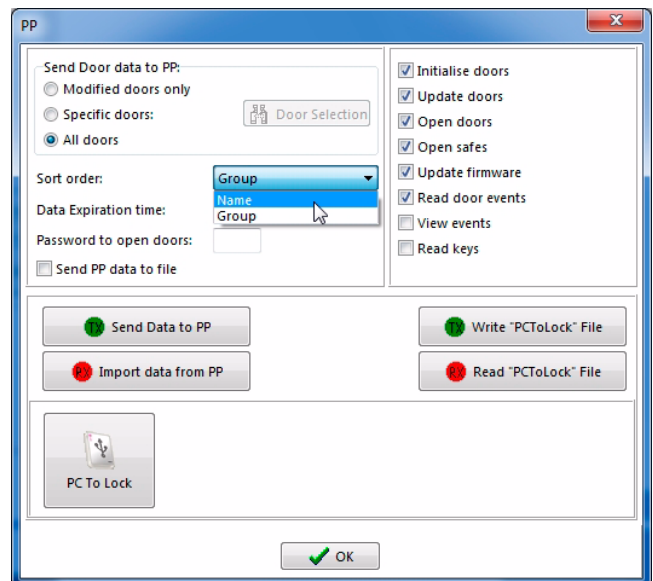


Select only the operations you want to carry out, by ticking the corresponding check box.

“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 “Floor 0” group first, followed by all the doors of the “Floor 1” group.
- The option “Sort by Name” will arrange the doors sorted by alphabetical order, without taking into account the group they belong to.



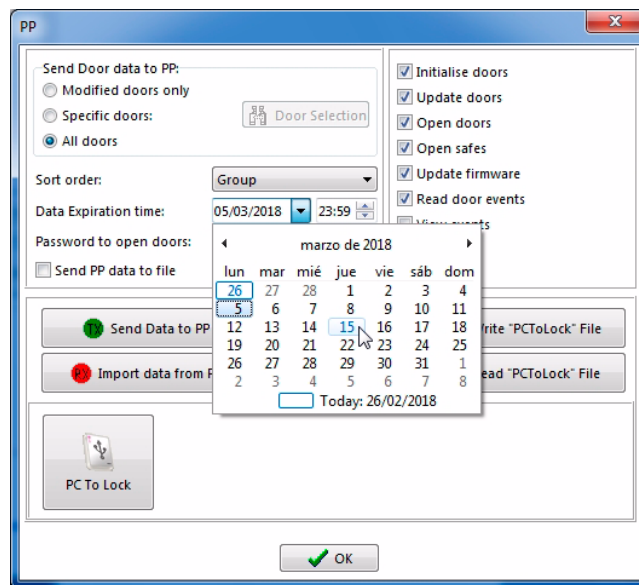
“PP data expiration” field

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

The expiration 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

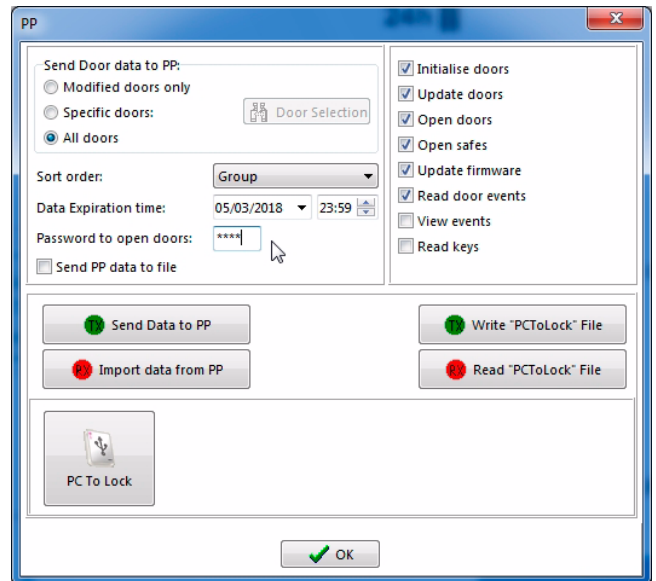
From the Portable Programmer, it is possible to carry out emergency openings of the cylinders, as well as of the locks and wall readers. In the Portable Programmer, this function is called “Open doors” and it can be found in the “F2: Doors” menu.

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, 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.

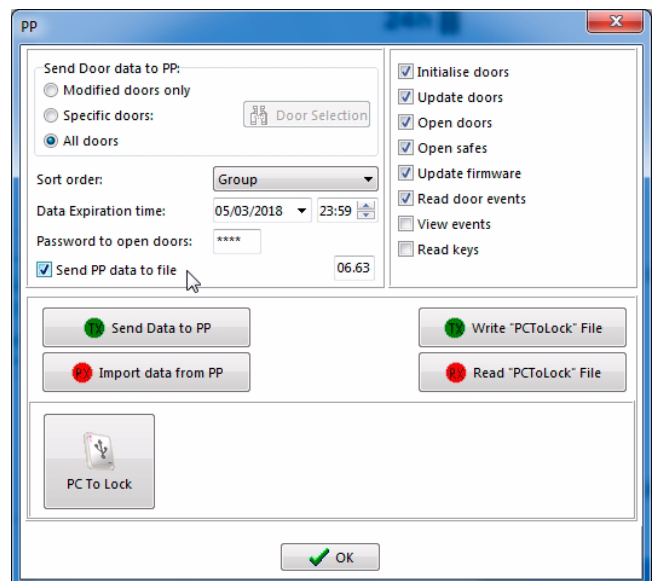
As a matter of security, the password remains hidden, represented by asterisks.



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.

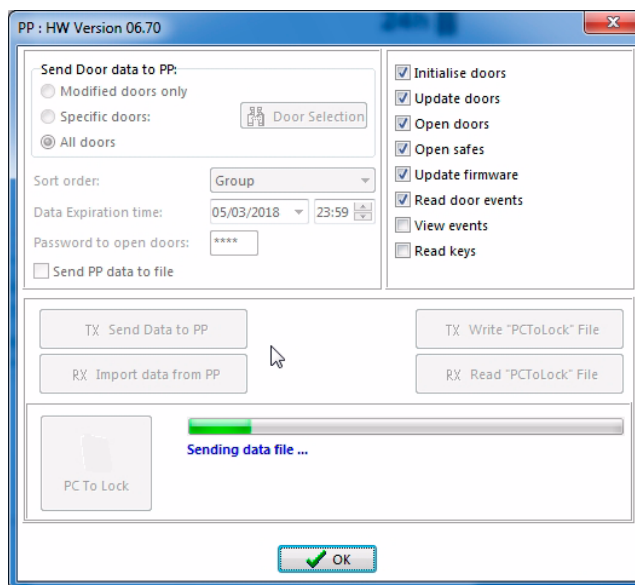
Nowadays, this option is not used any more.



“Send Data to PP” button

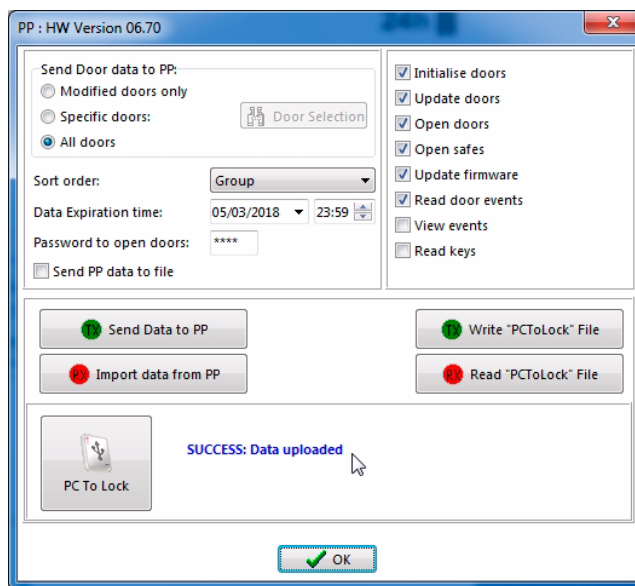
After following the previous steps, it is possible to send the data to the Portable Programmer, by clicking on “Send Data to PP”.

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



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 “Initialize doors”, which is described in “1.3 Initializing the doors of the site” on page 151.



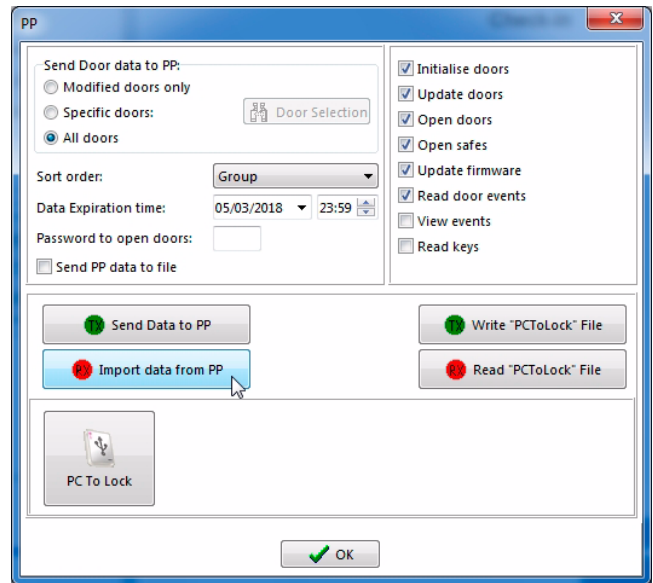
“Get Data from PP” button

With the Portable Programmer, it is possible to carry out various operations on the doors, such as Initialize 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 TESA Hotel 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 TESA Hotel.

This operation is essential, after having initialized 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).

- 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

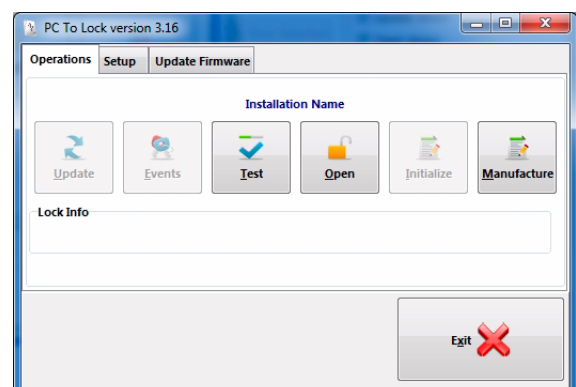
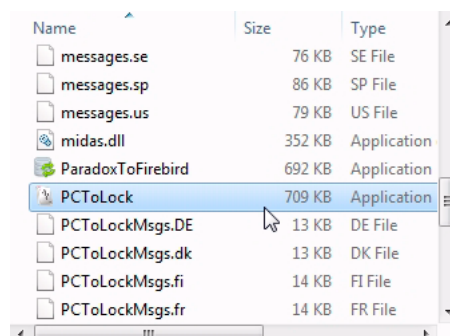
There is another method, an alternative to the Portable Programmer, to send the data to the doors, initialize and update them, as well as to read their openings. This system is called “PC To Lock”. It consists of the following components:

- 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 (*tablet*) with Windows XP, Vista, Windows 7, Windows 8.1 or Windows 10 operating system.
- “PCToLock” software to manage the communication with the doors. This software is automatically installed in the same directory as TESA Hotel, when installing the latter.

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

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

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

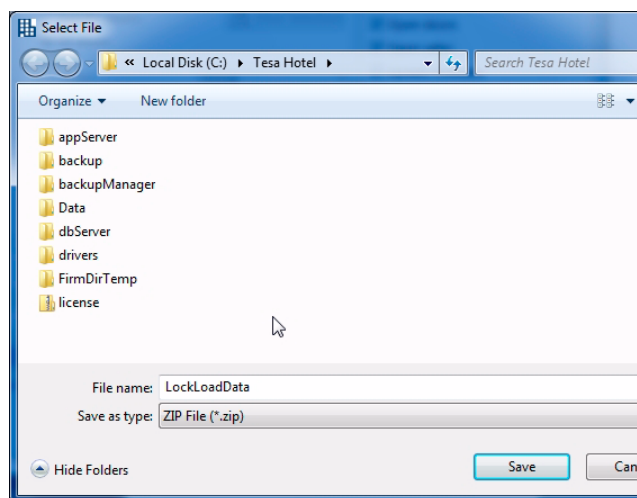


“Write PCToLock File” button

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 TESA Hotel 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 TESA Hotel has not been installed, in order to be able to work more conveniently at the doors of the site, it is necessary for 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 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 Initialize doors, Update doors, or collect events recorded in the doors (Auditor) to analyse them with TESA Hotel, etc.

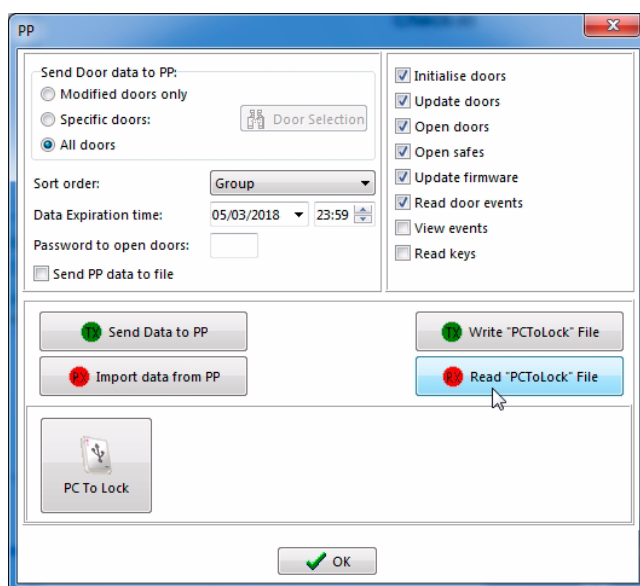
After carrying out these operations, the data are recorded in the file loaded into the “PCToLock” software, so that, for the database of the site to be updated, it is necessary to process this file using the TESA Hotel software.

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

This downloading process is carried out by transferring the data file from the portable PC or tablet to any TESA Hotel 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 TESA Hotel software.



I.3 INITIALIZING THE DOORS OF THE SITE

Introduction

The initialization 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 initialization 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.

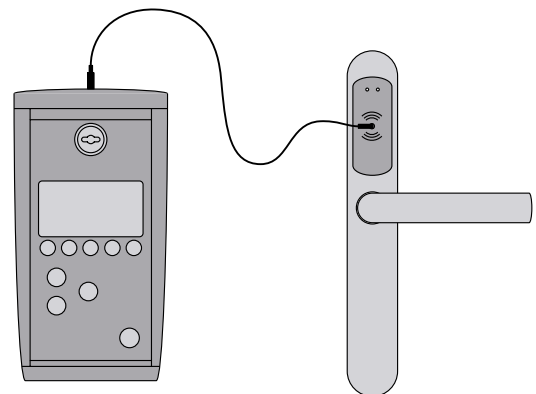
When it is initialized, the lock loses all the information previously stored in it. If still set to factory settings (as delivered from the manufacturer), it will cease to be so.

Once a cylinder, lock or wall reader becomes part of a site, it can only be initialized anew with information from another door of the same site. That is to say, once initialized, you can change their location as many times as you wish, but always within the site they were initialized for.

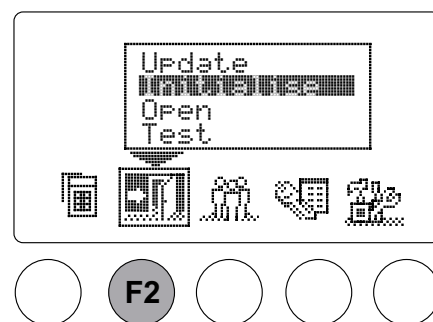
If a lock was already initialized previously and is initialized again, all of its parameters are rewritten, and the record of openings stored in it is deleted entirely.

Initialization by means of the Portable Programmer

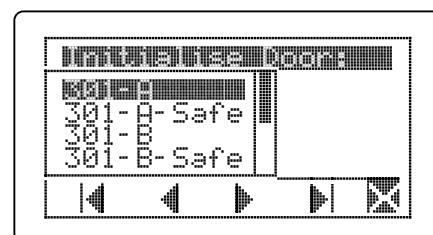
For initialization using the Portable Programmer, it is necessary to connect it to the Electronic Cylinder, Lock or Wall Reader.



The process is carried out at each door, by means of the Portable Programmer, in the menu "2- Doors" > "Initialize" > "Select Group1" > "Select Door" > "OK".



For more information, refer to the instructions for the Portable Programmer.



After initializing the door using the Portable Programmer, it is possible to collect the openings from it so that there is a record of its date and time in the system.

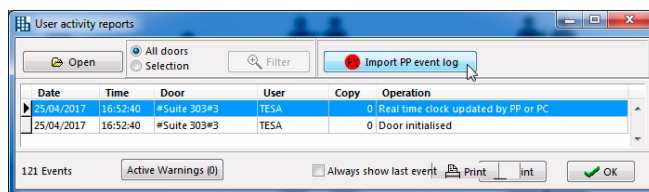
This last step is very important for the information of the work done at the doors to be recorded in the database and for the pending actions to be recognised as completed, so that the affected doors and users are highlighted in black, rather than orange or blue, in the corresponding menus.

In order to do this, connect the Portable Programmer to the TESA Hotel 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.

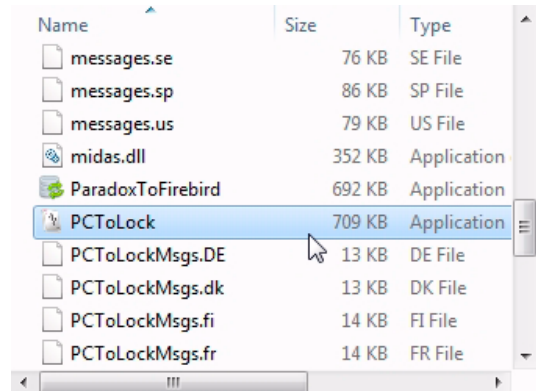
After this operation has been carried out, the door initialization process is finished.



Initialization by means of PCToLock

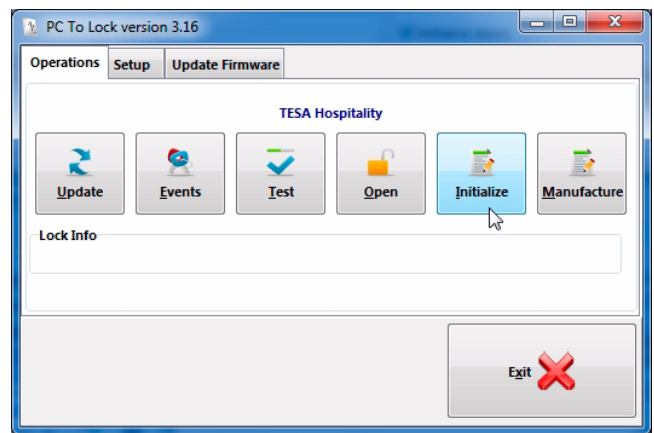
It is also possible to initialize the door with the “PCToLock” software and the “USB-KCOM” device connected to a portable PC or equivalent device, rather than using the Portable Programmer.

For this purpose, run the “PCToLock.exe” software on the PC where the “PC-ToLock” device is connected.



The initialization of the doors is carried out by means of the “Initialize” button.

For full information, refer to the instructions for the “PCToLock” software.

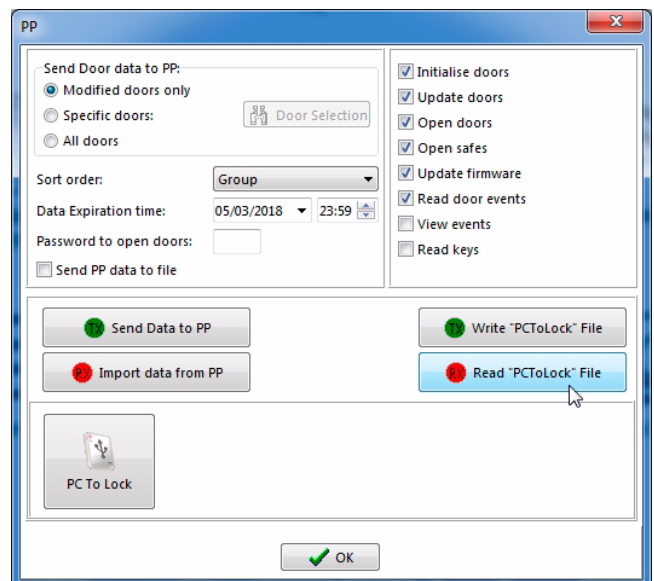


After the initialization, it is necessary to update the information of the system. For this purpose, click the “Read PCToLock File” button in the “PP” menu of TESA Hotel.

For more information, refer to ““Read PCToLock File” button” on page 150.

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.



I.4 ENCODING OF (STAFF) CREDENTIALS

NOTE: particularly in the *Read and Write* systems, the encoding of credentials must be carried out once the doors have been initialized and the database updated with the information of that initialization, 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 TESA Hotel software. The information encoded on each credential is, basically, what can be seen in the Users tab, encrypted.

NOTE: the encoding of the guest credentials is part of the *Check In*, and is therefore not explained in this section. For more information on the *Check In*, see “K.2 Check In” on page 182.

In order to encode the credentials, it is necessary to have the Card Encoder 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.

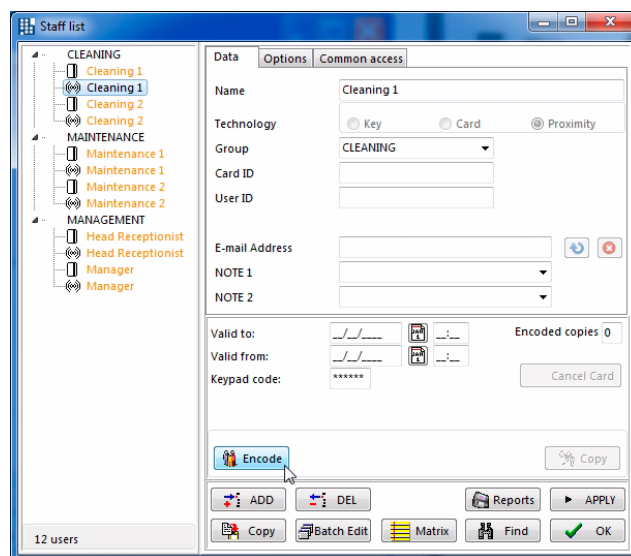
As a guide, the procedure for the different types of technology is shown below:

- **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 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, 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 List” screen of the TESA Hotel, select the user name (highlighted in blue) whose credential you want to encode.

Modify the Expiration and Activation dates in the corresponding fields if necessary, and the grants to be encoded on the credential using the “Grants” tab.

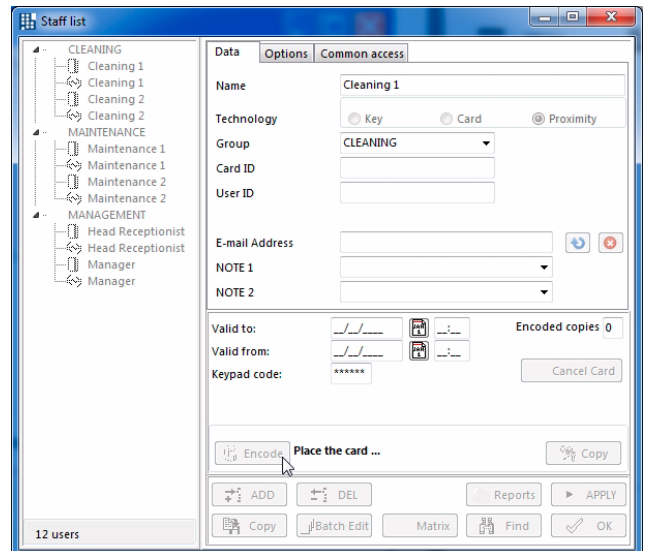
Once the user has been selected, click the “Encode” button.



Encoding keys and programming doors

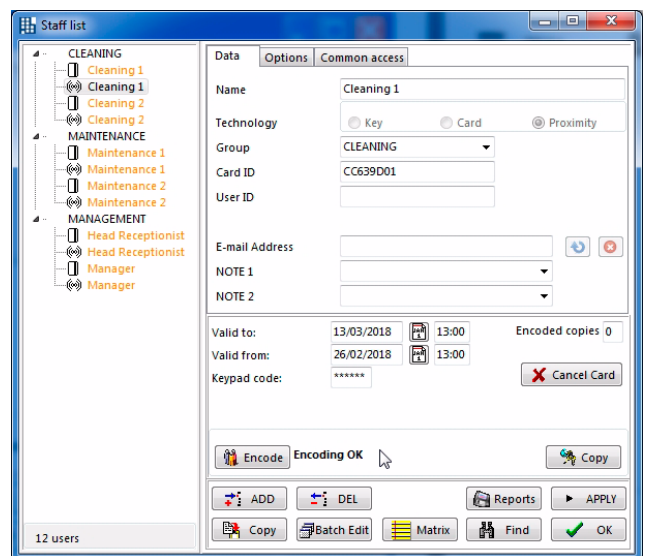
The software prompts you to present the credential to be encoded:

- Proximity: Place the card...
- Magnetic Stripe: Insert the card...
- Electronic Keys: Insert the key...



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.



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 (Staff List) 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 Staff 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 orange 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 expiration dates of a user, it will be necessary to encode their credential again.

J – Wireless System

Wireless system architecture	159
Wireless system configuration	160
Hub setup	160
Configuration and initialization of the Hubs by means of InitHubIP	160
Initial network parameters of the Hub	160
Configuring the network parameters of the PC for it to be able to communicate with the Hub	161
Configuration of the Hubs by means of InitHubIP	164
Resetting the network parameters of the PC to the previous configuration	166
Adding the Hubs to the system	168
Autolink function	169
Adding wireless devices to the Hub (manual link)	171
Advanced setup	173
Change Channel	173
Frequency change (from 868 MHz to 915 MHz or 902MHz)	174
Multiple Wireless Server mode	175
Remote Hubs	176
Firmware update	177
Management of wireless devices	178

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, 915 MHz or 902 MHz. The information sent between the devices is encrypted (AES128 standard encryption).

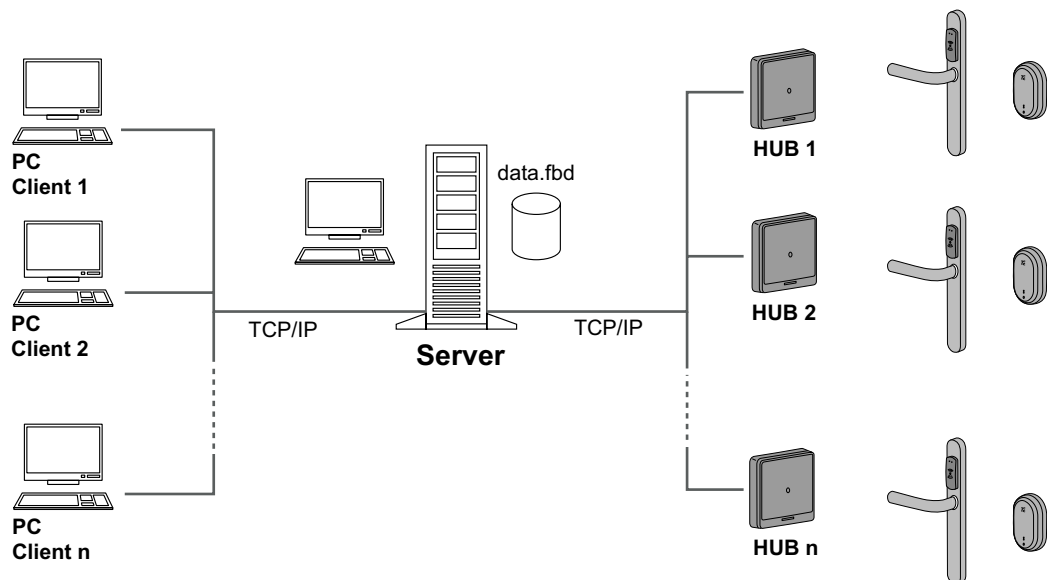


Fig. 4 Wireless system architecture, with a single centralised server

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 metres in a closed environment or up to 100 metres 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 initialization 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 Hotel Server application is installed, as well as the "InitHubIP" tool, which is used to configure the IP parameters of the Hubs and initialize them.
- Connect the power supply of the Hub. In some cases, the power supply arrives through the Ethernet connector (PoE - Power Over Ethernet) and in other cases, it is necessary to use a parallel external feeder. It is possible that you may also have to turn on the 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 initialization of the Hubs by means of InitHubIP

The steps to be carried out are the following:

- 1 Learning the [initial network parameters of the Hub](#) (initializing 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 initializing them for the TESA Hotel 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

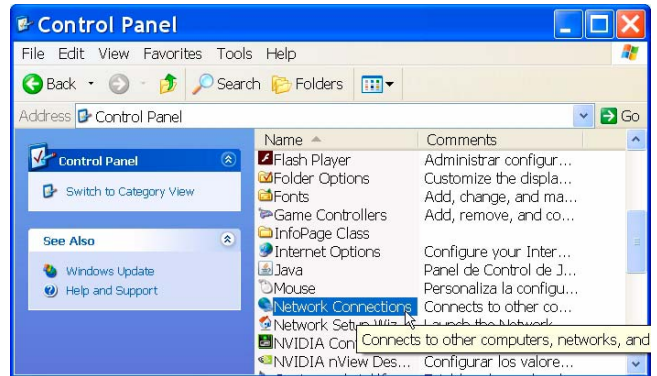
- ☞ If the Hub has been used before and the parameters are not known, the factory parameters can be recovered by resetting the Hub. The reset involves, with the Hub off, pressing the Reset button and, without releasing it, turning on the Hub, and keeping the Reset button pressed for approximately 5 seconds. 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 initialized 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

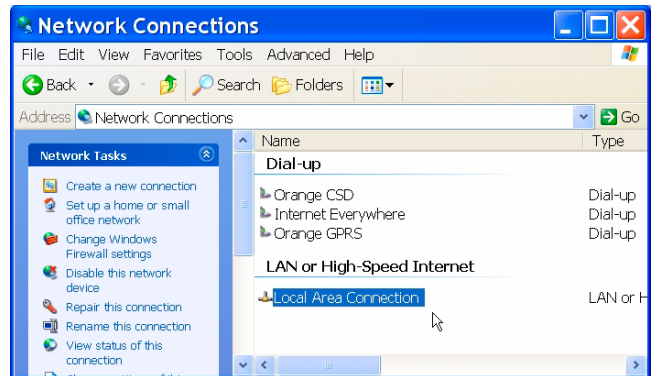
Once the parameters of the Hub are known, it is necessary to configure the corresponding parameters of the PC for it to be able to communicate with the Hub (the IP of the PC has to be configured to lie in the same range as that of the Hub, with the same subnet mask and the same gateway).

Proceed as follows (these steps may vary depending on the Operating System installed on your computer):

- 1 Access “Network connections” in the “Control Panel”.

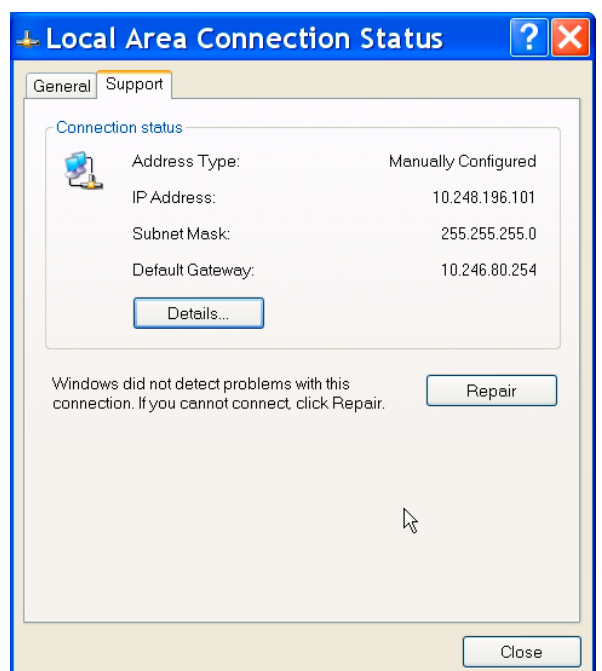


- 2 In “Network connections”, select “Local area connection”.

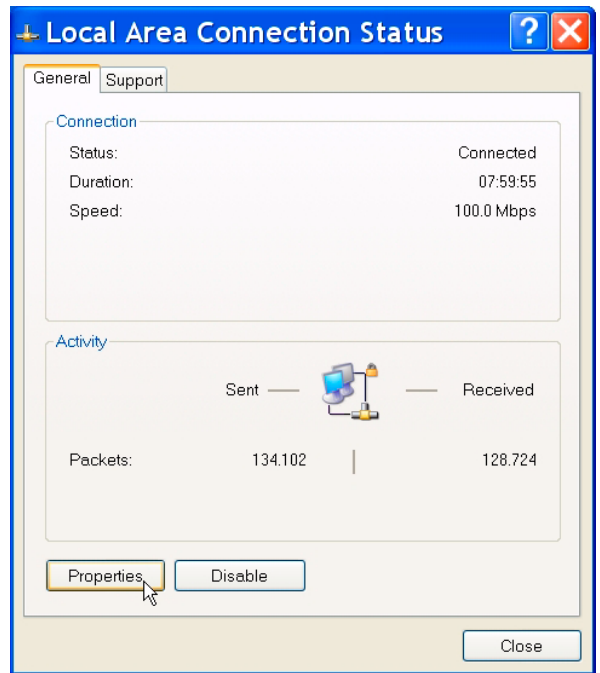


- 3 Select the “Support” tab. The current configuration of your PC is displayed. Note it down, since you will have to modify it and then restore it. In the example, the parameters are:

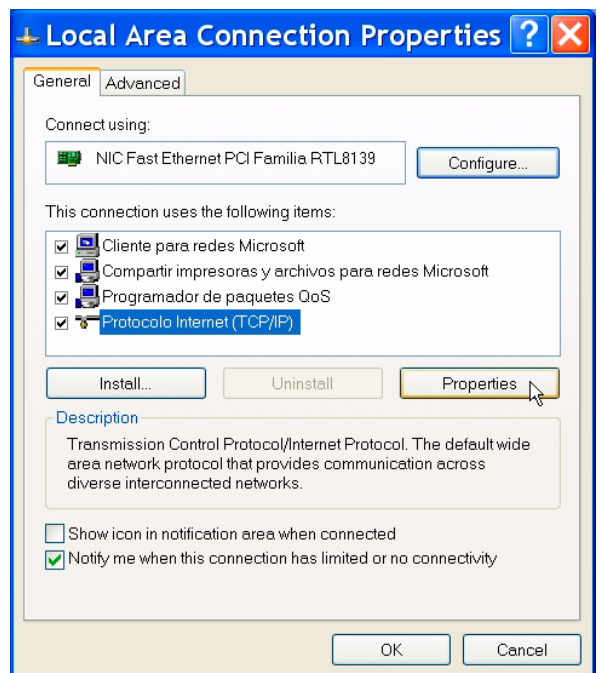
- IP address: 10.248.196.101
- Subnet mask: 255.255.255.0
- Gateway: 10.246.80.254



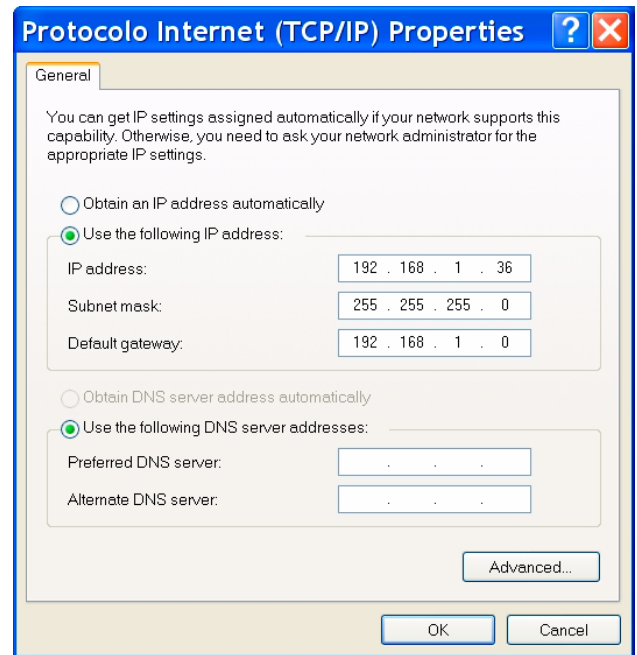
- 4 In the "General" tab, click the "Properties" button.



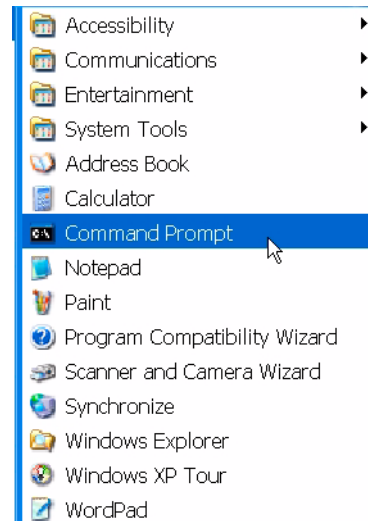
- 5 Select "Internet Protocol (TCP/IP)" and click the "Properties" button.



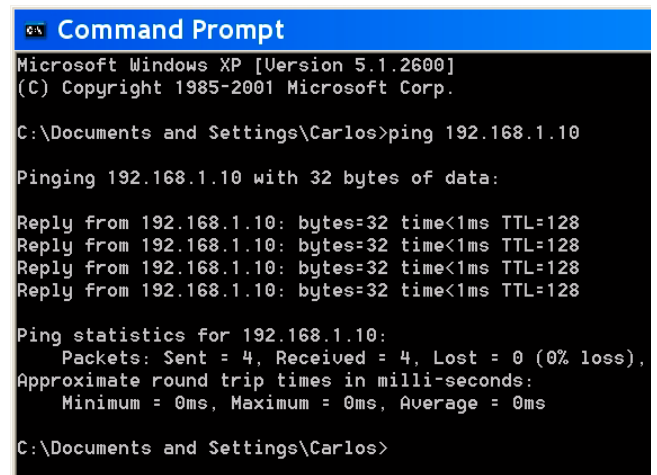
- 6 Change the IP address and enter one which is in the same range as that of the Hub, with the same subnet mask and gateway. For example:
- IP address: 192.168.1.36
 - Subnet mask: 255.255.255.0
 - Gateway: 192.168.1.0



- 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.



At this moment, since the PC and Hub are communicating properly, it is possible to initialize the Hub by means of the "InitHubIP" tool, as explained in the following section.

Configuration of the Hubs by means of InitHubIP

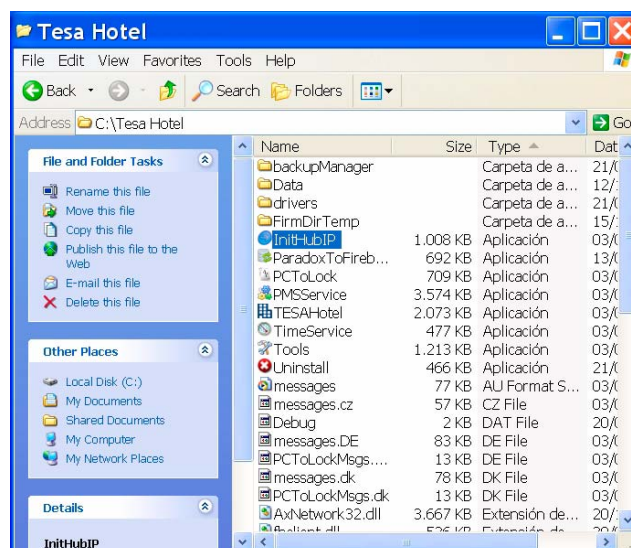
The “InitHubIP” tool is used to configure the network parameters of the Hubs (assigning them a fixed IP address, provided by the network administrator) and to initialize them.

- ☞ 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 TESA Hotel software 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.

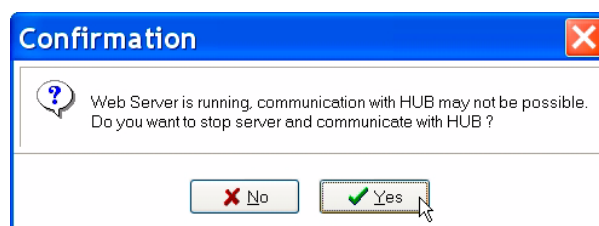
The steps to be followed in order to run the InitHubIP application are shown below, on the same PC where the TESA Hotel Server application is being run:

- 1 Run the InitHubIP application, which is installed in the same folder as TESA Hotel.



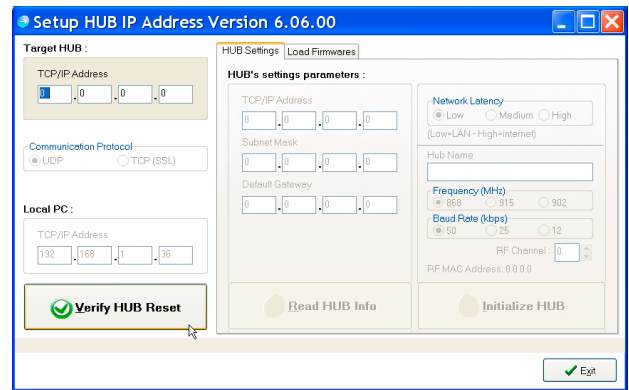
- 2 A message is displayed, requesting permission to stop the “TESA_APPSERVER Glassfish Server” service. Confirm this by clicking “Yes”.

This window is not displayed if the application is being run from a PC which does not have the TESA Hotel installed.



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 initialize the Hub by means of its corresponding Reset button in order to restore the factory values.



- **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 176.

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 or 902 MHz)" on page 174.

Baud rate (kbps): data transmission speed. Allows selection of the most suitable speed for your site.

RF channel: allows conflicts with other devices operating at the same frequency in the same site to be avoided.

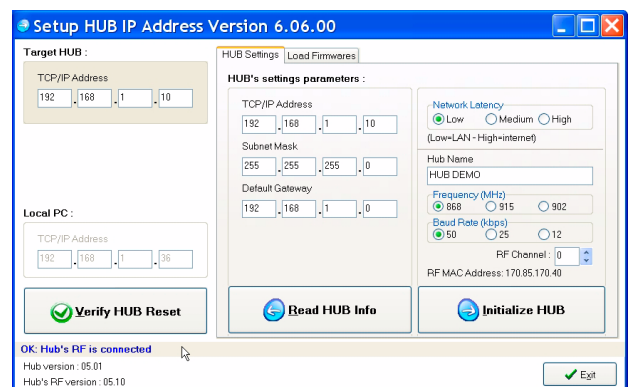
For more information, see "Channel change" on page 173.

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.
- **Initialize 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 160).

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.

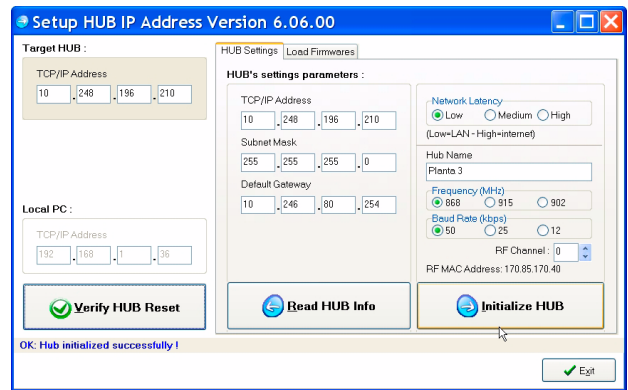


- 5 Once the connection with the Hub has been verified, enter the new parameters (**the network parameters must be provided by its administrator**).

In the example:

TCP/IP = 10.248.196.210,
Subnet Mask = 255.255.255.0,
Gateway = 10.246.80.254,
Name = Floor 3.

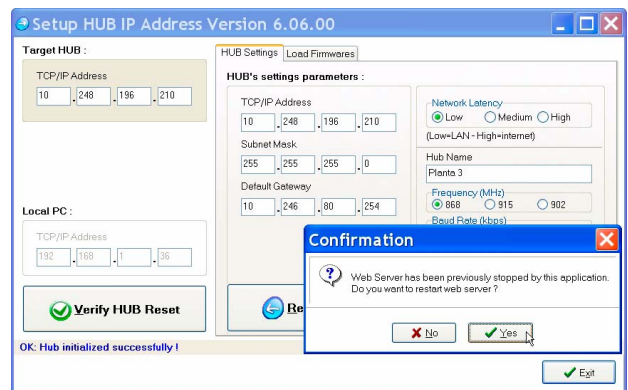
Click "Initialize HUB" to confirm. The confirmation message "OK Hub initialized successfully!" will be displayed.



- 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.

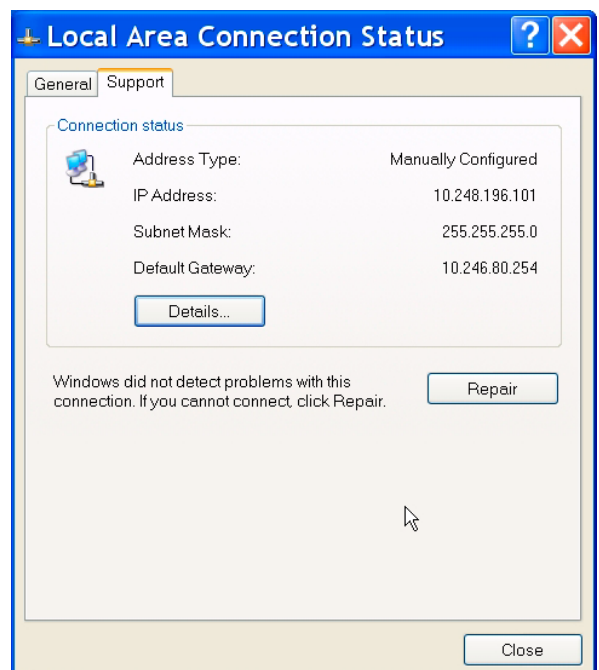
This window is not displayed if the application is being run from a PC which does not have TESA Hotel installed.



- 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

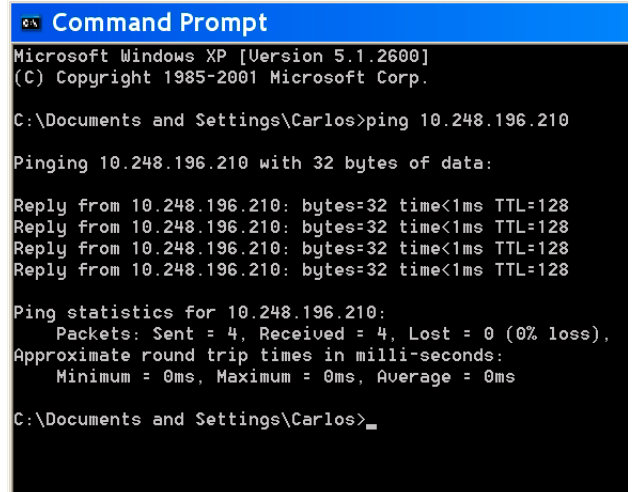
After initializing all the Hubs by means of InitHubIP, as explained in the previous section, it is necessary to reset the PC to its original IP value, since this was modified in section "Configuring the network parameters of the PC for it to be able to communicate with the Hub" on page 161.



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.



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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=128
Reply from 10.248.196.210: bytes=32 time<1ms TTL=128
Reply from 10.248.196.210: bytes=32 time<1ms TTL=128
Reply from 10.248.196.210: bytes=32 time<1ms TTL=128

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 initializing the Hubs, it is necessary to add them to the system, by means of the TESA Hotel application, in the “Setup” menu, “Wireless” tab.



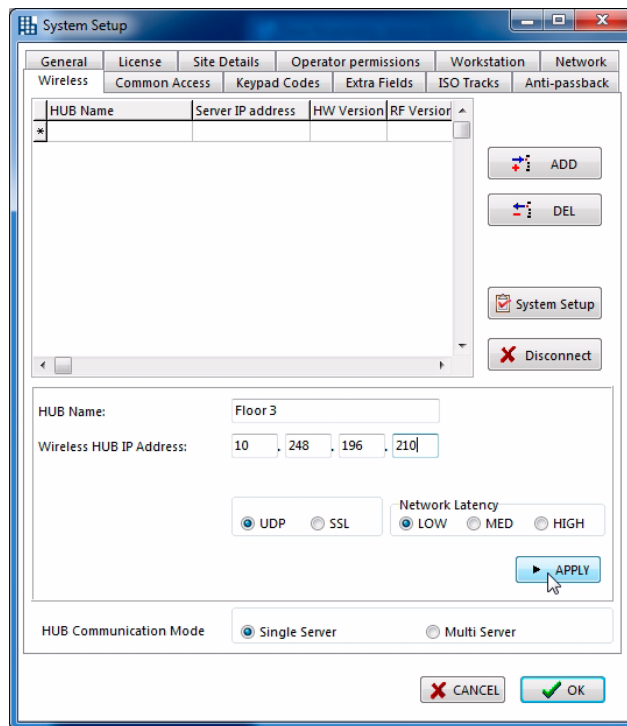
Each Hub is identified with a name or number differentiating it from the rest and a fixed IP address provided by the network administrator (as explained in “Configuration of the Hubs by means of InitHubIP” on page 164).

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 initializing the Hub by means of InitHubIP.

Network Latency field: use the same option applied when initializing 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.



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:

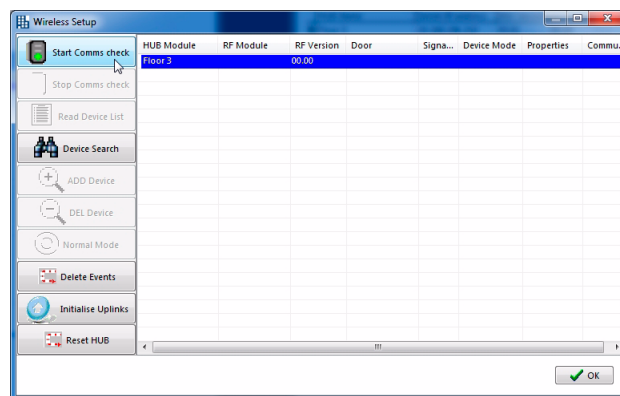
- When they are turned on/activated (battery change).
- After being initialized or having the time updated with the Portable Programmer (version 6.70 or higher) or by means of the PCToLock (V3.11 or higher).
- Every time a *New Event* is generated in a device which has not previously been linked to a 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 initialize, 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).

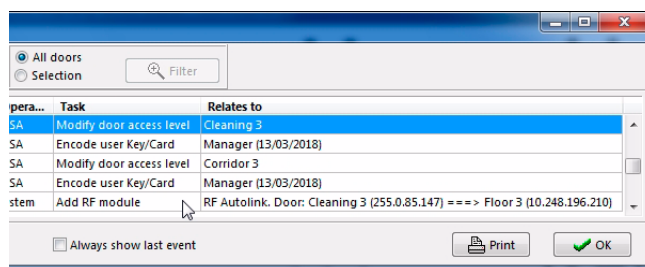


For the automatic link process, bear the following in mind:

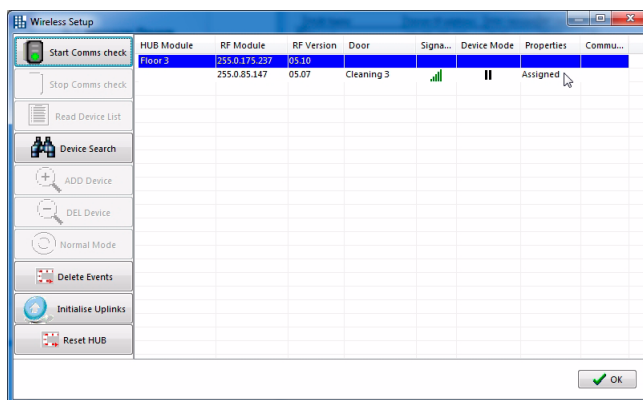
- When a door device tries to link automatically, it will search for Hubs which are within its coverage range. If more than one Hub is found, it will automatically select the Hub with the strongest coverage signal.
- The device will only link to the Hubs which belong to the same site.
- When a device 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”

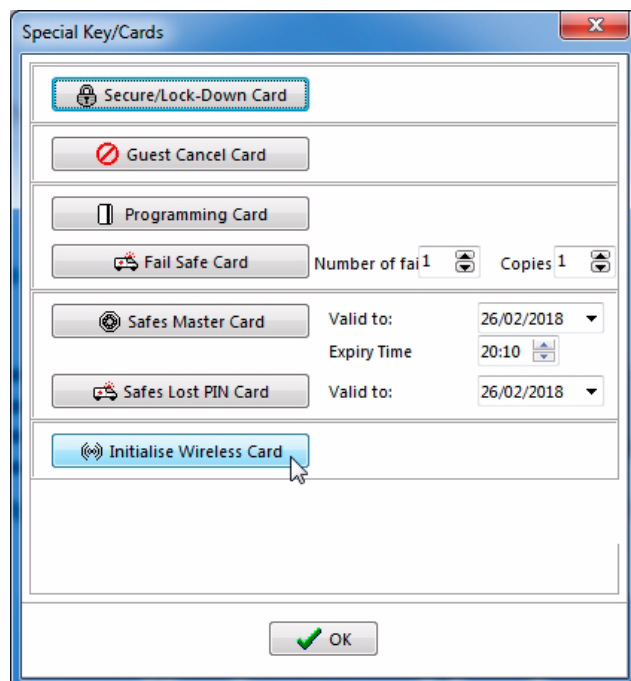


The V3 wireless door device will automatically be displayed in the Wireless menu as “Assigned” to the Hub.



If, during the initialization 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 171.
- Bringing the “Init Wireless Card” special card close to the lock. This card is encoded in the *Reception Menu*, “Special Keys/Cards” tab, “Init Wireless Card” button.
- By means of the Update of the lock either with the PP or PCToLock.



In any of the above cases, if the Wireless device does not find a Hub with coverage, its link to a Hub will remain pending and battery consumption will be extremely high during this process. This must be remembered if the Wireless devices are initialized and the Hubs are not going to be installed or linked for a long time.

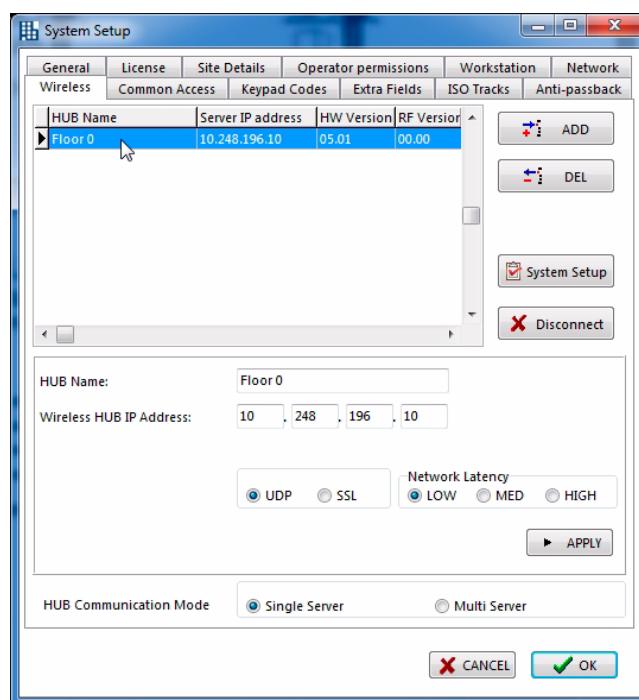
Adding wireless devices to the Hub (manual link)

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.

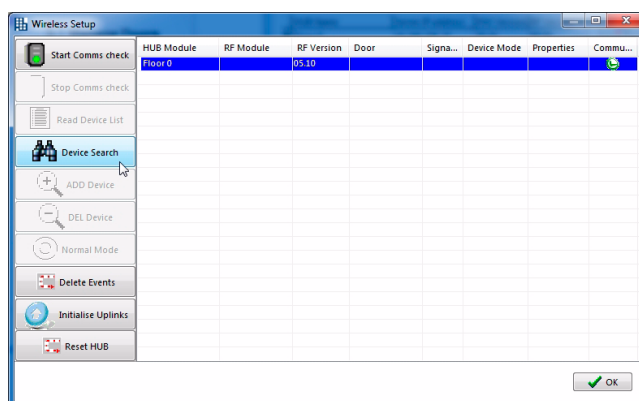
NOTE: the devices of the V3 wireless system have the “Autolink” function, which has been explained in the previous section, for adding them to the Hub. Therefore, it is not necessary to apply what has been explained in this section for V3 devices, since they have “Autolink”. However, it may be useful in particular cases, for example: if the Hubs were not connected when the doors were initialized 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 82 if you do not know how to do this).
- 2 Initialize the wireless device if it has not been initialized yet (see “1.3 Initializing the doors of the site” on page 151 if you do not know how to do this).
- 3 In the TESA Hotel programme, in the “Setup” menu, “Wireless” tab, double-click the Hub chosen.



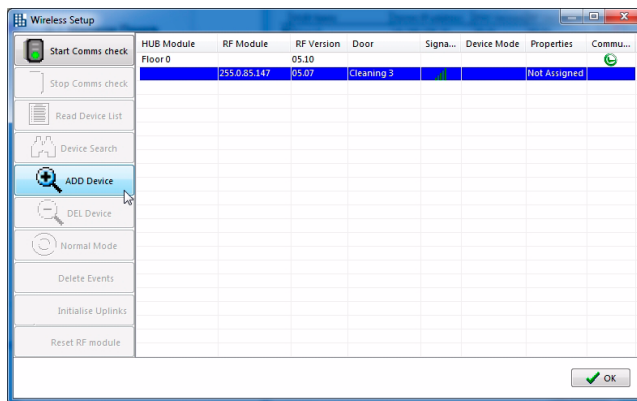
- 4 The following screen is displayed:
Click the “Find New RFs” button.



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.

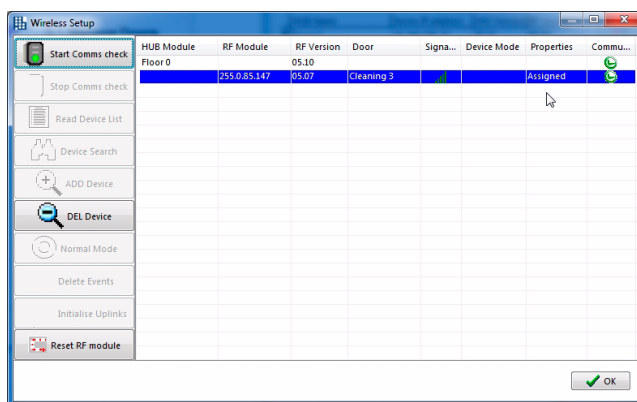
From this moment, it is possible to communicate with the “Cleaning 0” wireless lock through the PC, by means of the “Wireless” menu of the *Reception Menu* of TESA Hotel, as explained in “J.3 Management of wireless devices” on page 178.



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:

- **Start Diagnostics:** verifies the state of the wireless device.
- **Stop Diagnostics:** 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 to make remote operations possible.
- **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 initialization process (both with the InitHubIP application and the Portable Programmer or PCToLock, respectively).

It is also possible for the site to have a Wireless 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).

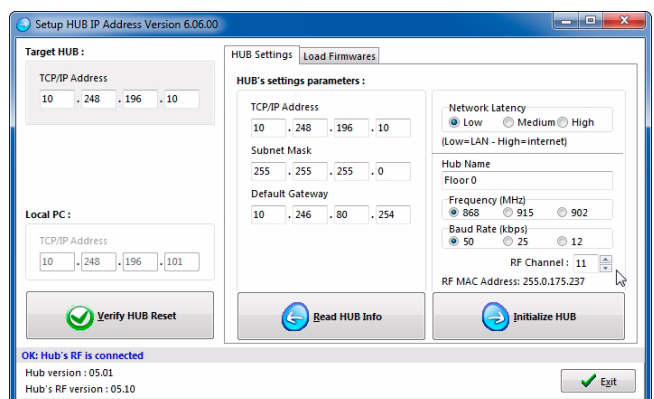
The V3 wireless communication system allows changing the communication channel within values ranging from 0 to 31, in three steps:

- 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 “License” tab of the TESA Hotel software Setup menu.
 - 3 Initializing the door devices, by means of the Portable Programmer or PCToLock.
- 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.

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 initialized 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 “Initialize Hub” button.



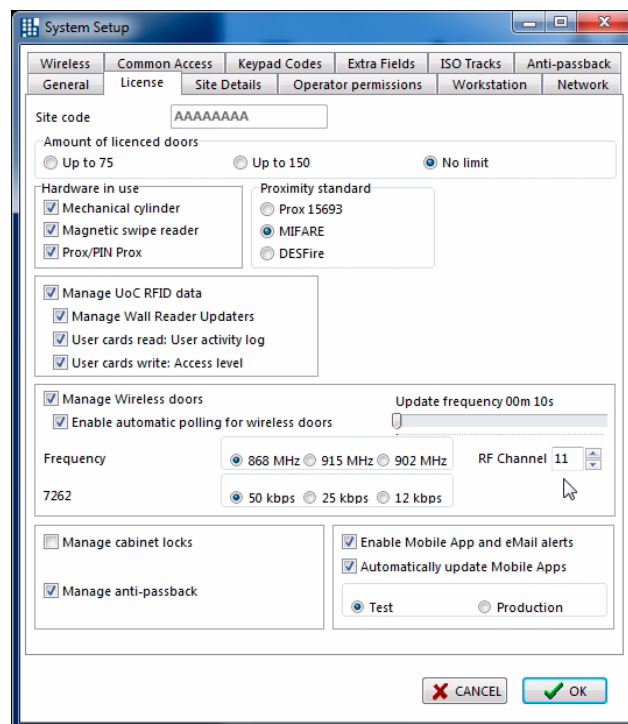
- 2 Configuring the channel in the door devices.

This is performed in the TESA Hotel software, in the “Setup” menu, “License” tab.

Select **the same channel selected for the V3 Hubs** (11 in the example) and click the “OK” button to confirm.

- 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 Initializing 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 or 902 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) or 902 MHz.

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 “License” tab of the TESA Hotel software “Setup” menu.
- 3 Initializing the door devices, by means of the Portable Programmer or PCToLock.

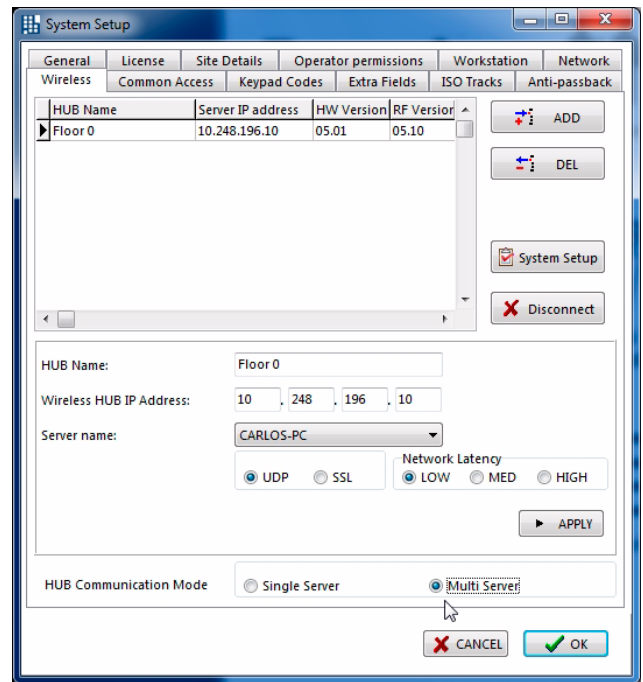
Multiple Wireless Server mode

Similar to what is 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 159).

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.



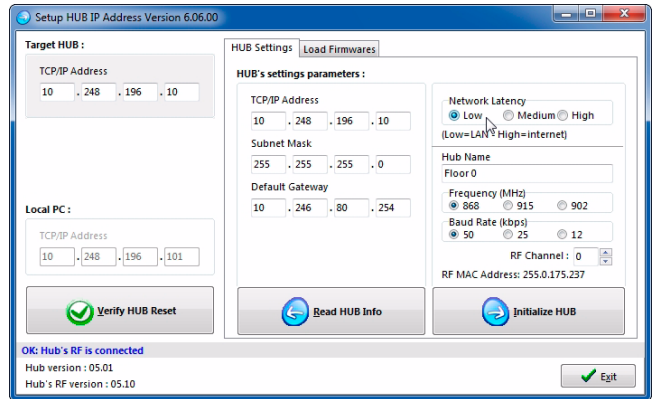
Remote Hubs

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 facilitate 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.



- 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).

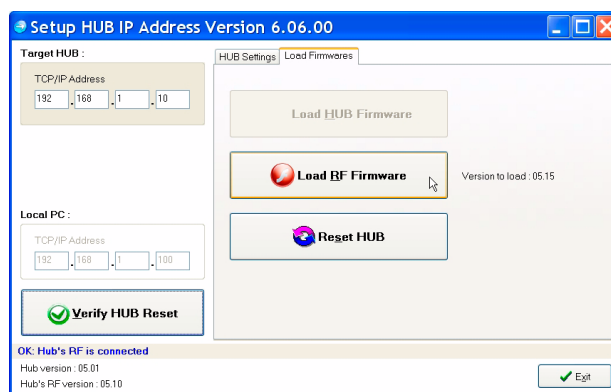
Device versions required:

- 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.

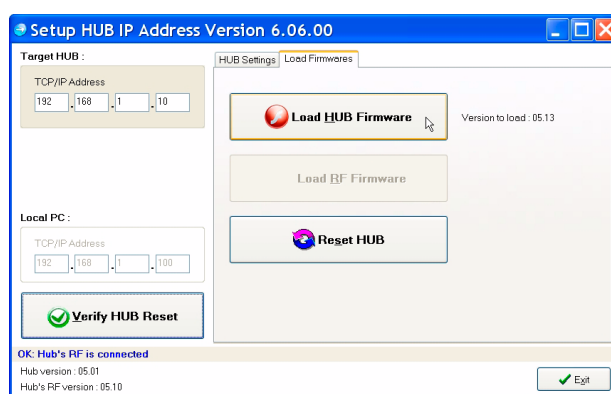
It is also possible to update by means of the “InitHubIP.exe” application, using the “Load RF Firmware” button.

For this “Load RF Firmware” button to be activated, the file with the new version of the firmware (e.g. “R5RF0515.zip”) must be placed in the same file where the “InitHubIP.exe” application is installed (by default, “C:\Tesa Hotel”)



- 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 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.

For this “Load HUB Firmware” button to be activated, the file with the new version of the firmware (e.g. “R5HUB0513.zip”) must be placed in the same file where the “InitHubIP.exe” application is installed (by default, “C:\Tesa Hotel”)

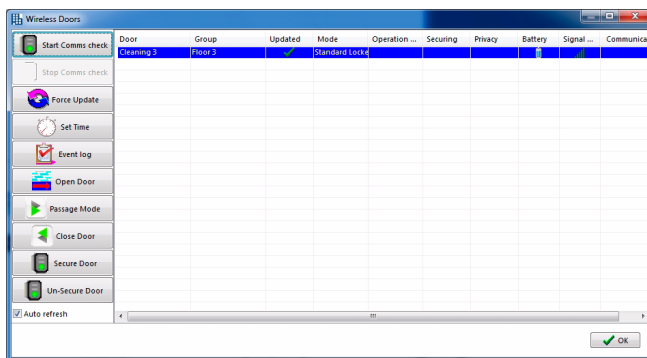


J.3 MANAGEMENT OF WIRELESS DEVICES

The management of wireless devices (locks, wall readers) is carried out by means of the “Wireless” menu of the Reception Menu of TESA Hotel.



In the Wireless menu, the table with the wireless devices controlled by the Hubs connected to that PC is displayed.



By selecting a device (in the example, the “Clean 0” lock), it is possible, using the buttons on the left, to carry out the following operations:

- **Start Diagnostics:** a message to test communication between the PC and the locks is sent in order to verify the connection.
- **Stop Diagnostics:** 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.
- **Audit Trail:** 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.
- **Block:** blocks the lock so that it can only be opened by users who have the option “Can open blocked doors” enabled.
- **Unblock:** unblocks the lock if it is blocked, setting it to Standard mode once again.

K – Site management

Introduction 181

Check In 182

Copy Guest 186

Pre-check In 188

Check Out 189

 Modify Grants 191

 Extend guest stay 191

Other cards 192

 Blocking Card 193

 High Traffic Cancelling Card 196

 Guest Cancel Card 198

 Programming Card and Fail Safe Card 200

 Encode Programming Card 200

 Encode Fail Safe Card 202

 “Safes Master” Card 205

 “Safes Lost PIN” Card 207

 “Init Wireless” Card 210

Read cards / keys 213

Openings 216

 Openings read from Doors by means of the Portable Programmer 216

 Openings read from Credentials by means of the Portable Programmer
 Portable or Encoder (in the Read and Write system) 218

 Analysis of the openings collected 218

 Filter 219

 Print 222

 Open 223

 Active Alerts 224

 Scroll automatically to last event 224



Portable Programmer (P.P.) 225

Auditor 226

Login and Logout 228

Logout 229

Customisation of Main Menu 229

Site management through the Web 230

 Users menu 231

 Doors menu 231

 Matrix 231

 Wireless Doors 232

 Hours 232

 Openings 233

 Auditor 233

 Alerts 233

 Options 234

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.

The system setup, and creation of the locking plan seen in the previous chapters, was performed via the different menus on the *Setup Menu*. For day-to-day management of reception, the *Reception Menu* will be used.

The *Reception Menu* is displayed in the figure below:



The *Reception Menu* has the following screens:

Check In, Copy Guest, Check Out, Other cards/keys, Keys/Cards, Wireless, Openings, P.P. (portable programmer), Auditor.

K.2 CHECK IN

The “Check In” operation consists of:

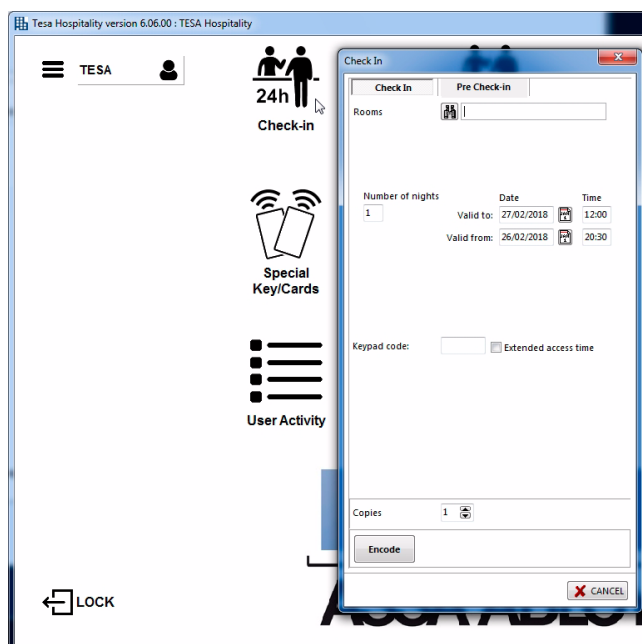
- assigning a free room to a new guest and
- encoding the card for this guest.

The card will be encoded with an expiration date, which will be the date/time at which the guest will leave the hotel.

Below is a step-by-step description of the process for *Check In*.

- 1 Click on the *check in* icon on the Reception Menu of the TESA Hotel programme. The following screen is displayed:

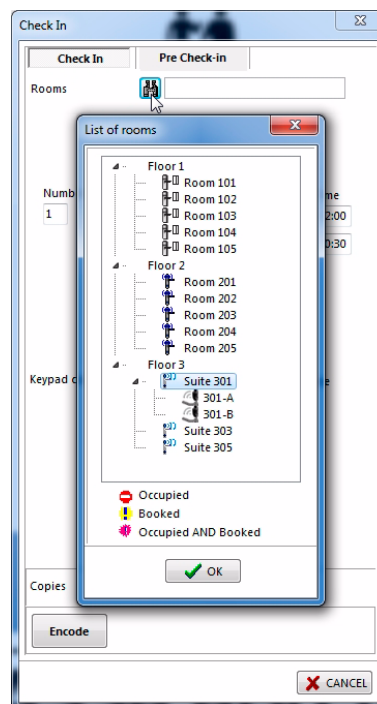
To see which rooms are available in the hotel, click on the button with the binoculars in the “Rooms” field.



- 2 The list of rooms in the hotel will unfold. On it, the rooms that are NOT available, and therefore occupied, are shown in red. The rooms that are available are shown in black. In the example, all of them are available.

On the list, select the available room you wish to assign to the new hotel guest.

Click “OK” to confirm.



- 3 The next field indicates the number of nights the guest will stay at the hotel. The number 1 appears by default.

The Expiration Date activates automatically depending on the number of nights selected.

The expiration time displayed (12:00 am) is the time established by default in the TESA Hotel programme. The "General" tab of the "Site" menu establishes the default expiration time of the guest's cards in the hotel. Both the date and the time can be modified manually.

By default, the Activation Date and Time of the card correspond to the moment the guest's *Check In* is being performed. The activation date is available because this option is selected on the "General" tab of the "Site" menu. The activation date matches the date/time from which the encoded card begins to be valid in the locks. Obviously, the expiration date must be later than the activation date.

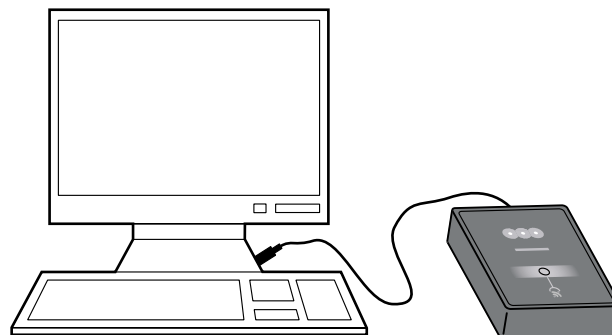
- 4 The "Grants" field displays the grants available for the guest of this room. In this case, the client is optionally assigned the corresponding grants for access to the safe in their room and the garage.
- 5 The "Disabled (ADA)" option doubles the opening time in the doors to which this specific guest has access (this option is not available for electronic cylinders).
- 6 The "Keypad Code" field will be the personal PIN the guest for whom we are performing the *Check In* must use in access doors in which the lock has a keypad and is functioning in "Card + PIN" mode. To open this door, the guest will insert their card and then key in their PIN code. This option is rarely used in hotel rooms, except for the *Check In PIN* functionality.

K

- 7 In the event that there are dual locks on rooms, a new field is displayed: "Guest Carrier". This field allows selection of the technology of the credential (magnetic stripe or proximity card) for the guest whose *Check In* we are performing. The option that we have previously chosen on the *Doors* menu will be activated by default.
- 8 If the site has intelligent energy savers, when a guest's card is encoded, one relay (activates the first relay of the energy saver) or two relays (activates both relays) can be selected. This is useful when the second relay (relay 2) of the energy saver is connected to an electrical device that can be rented (Air Conditioning, TV, etc.). Optionally, by selecting one or two relays the information necessary for activating said relays in the energy saver installed in the room of the guest in question is encoded.

- 9 "Copies" field: allows the number of cards we wish to encode to be inserted. All of the cards will be exactly the same, with the same characteristics, and the successive copies will be numbered for the openings record.

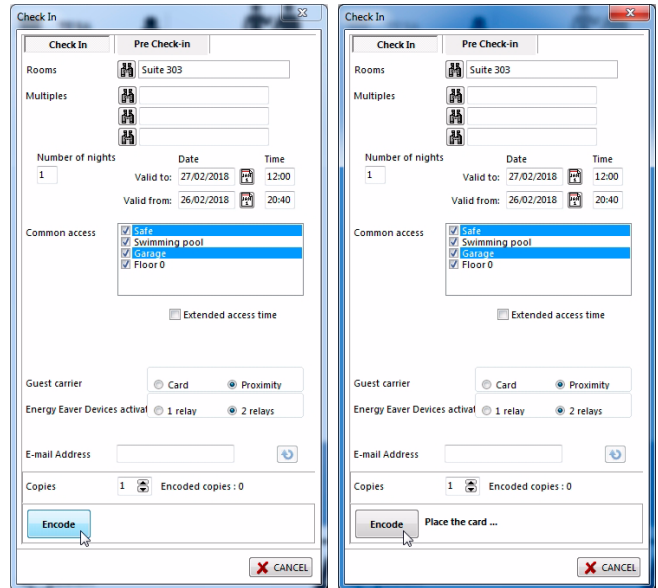
- 10 After all the fields on the form have been defined, it is time to encode the card for the new guest. To do this, the card encoder/encoding device must be switched on and connected.



11 Press the “Encode” button and place the card on the encoder, which will encode it.

The software will indicate the state of the encoding process by means of messages.

12 If we have requested 2 or more copies, the programme will then indicate that the second card should be placed on the encoder, and then the third, and so on consecutively until all the cards are encoded.



When the guest leaves the hotel on the day of the *Check Out*, their card will expire in accordance with the date/time encoded during *Check In*.

If for any reason the guest leaves the hotel earlier than expected and takes the card, it will automatically be cancelled when it expires or when a new guest inserts their card into the lock of the same room. That is to say, a guest's card automatically cancels the card of the previous guests if it has not already expired.

If there is no new guest in the hotel to whom the same room is allocated, and we need to cancel the card of a guest who has already left the hotel with an unexpired key, there is a special card called “Guest Cancel Card” (for more information, see “*Guest Cancel Card*” on page 198).

K.3 COPY GUEST

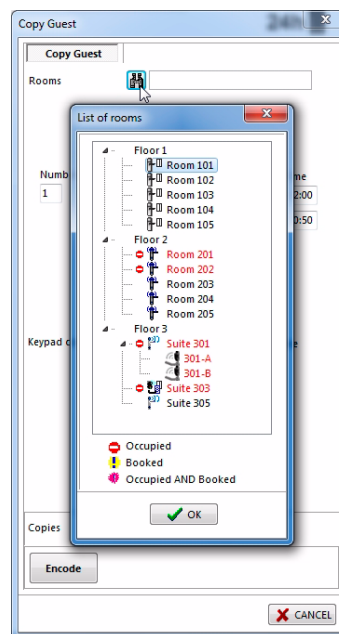
When the *Check In* of a new guest is carried out, it is possible to make as many copies as we wish of this guest card. The card and the copies of it will have all of the same characteristics and functions enabled. It may be that we do not want the same functions to be enabled (safe grant, additional access to pool, etc.) in all the copies, or that the guest requests additional copies for their room after *Check In*.

The system allows copies to be made of a previously-encoded guest card using the “Copy Guest” option on the Reception Menu.

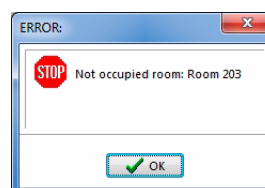


On the screen displayed, select the room number for which you wish to make the copy of the card. It must be a room for which the Check In has already been performed, that is to say, it must be a room that is occupied.

To select a room, click on the binoculars button and the list of the hotel's rooms will be displayed. The occupied rooms (i.e. those for which there is already at least one unexpired guest card encoded) are shown in red, and the available rooms (i.e. without guests) are shown in black. To make a copy of a guest card, select an occupied room from the list.

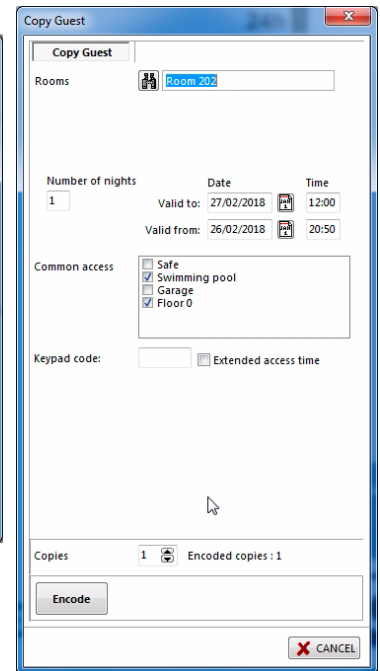
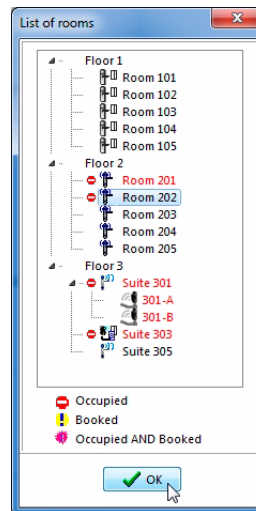


If you select a free room and click on “OK”, when you try to encode the card an error message will be displayed, as shown in the figure.



When you select an occupied room (for example, room no. 202) and click on “OK”, the previous screen is displayed, on which room 202 will be selected and showing the characteristics with which the original card was encoded during *Check In*.

On this screen, one can see that the “original” card has certain characteristics. For copy/copies of the card we can modify the grants, the activation/expiration date/time, ADA, relays etc.; indeed any parameter of the card can be modified. A maximum of 10 copies can be made.



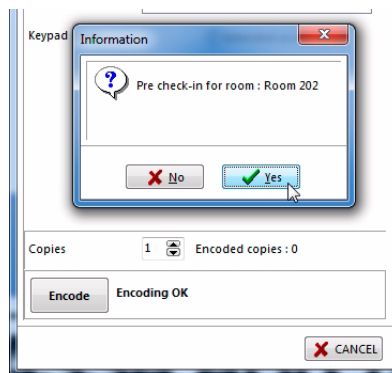
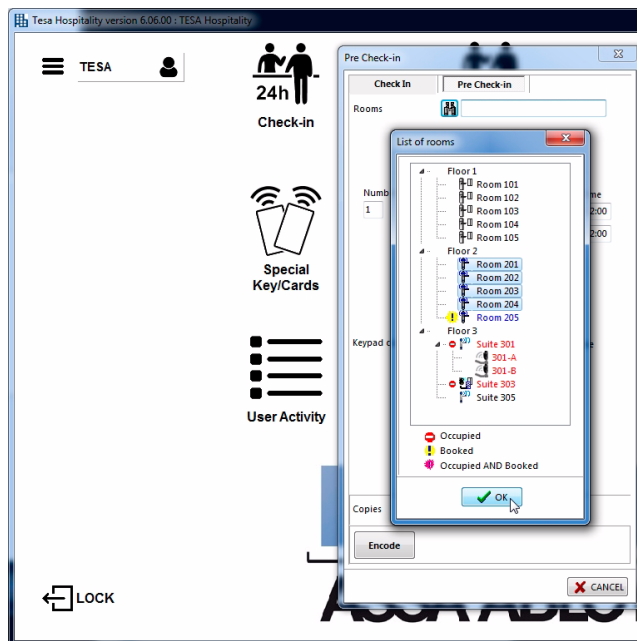
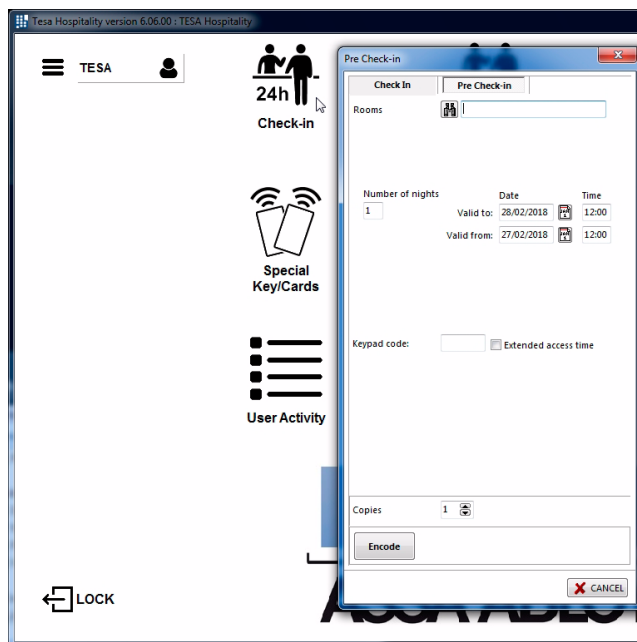
K.4 PRE-CHECK IN

The *Pre-check In* consists of the allocation of rooms to guests who will be staying at the hotel in the coming hours or days without the rooms having to be free. That is to say, *Check In* is performed as described in the section “K.2 Check In” on page 182, filling out all of the fields required by the corresponding form, but the date and time at which the card will be activated is also defined.

This option is extremely useful for managing groups that arrive in the hotel, simply by having the guest forward the *Check In* details before their arrival.

It is possible to carry out *Pre-check In* in several rooms simultaneously if desired, in the event that they all have the same characteristics. The method for achieving this is described below:

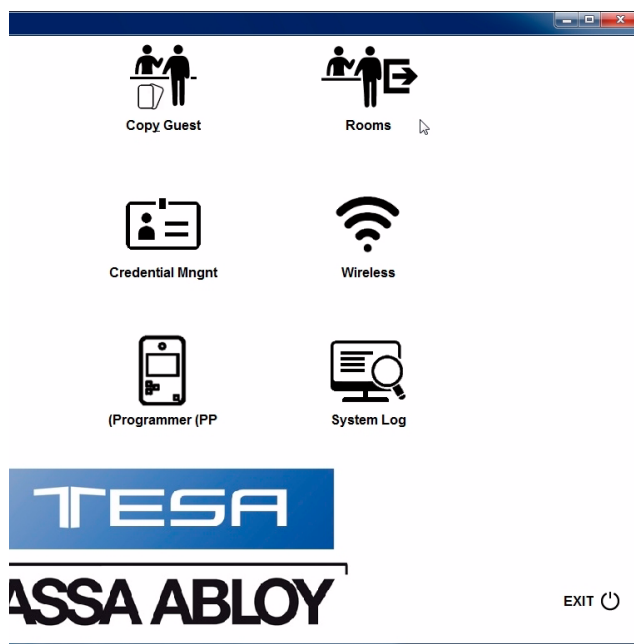
- 1 Make sure the card encoder is functioning.
- 2 Select all of the rooms you wish to assign simultaneously and click OK.
- 3 Click the “Encode” button.
A message is displayed telling you to place the card on the encoder.
- 4 Place the card of the first room to be encoded on the encoder.
A message is displayed indicating the card was encoded correctly and then, a dialogue box is displayed asking whether you wish to perform the pre-check in for the next room.
- 5 If you click on “No”, the encoding process of the cards will end. If you click on “Yes”, a message will appear telling you to place the card on the encoder.
- 6 Continue in the same way to encode the rest of the cards.



K.5 CHECK OUT

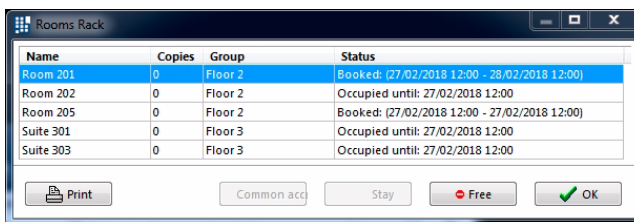
A room will be “officially” occupied until the expiration date/time established during *Check In* is reached. Whilst the room is occupied, no other *Check In* can be performed for this room. That is to say, the room is not available.

The room will automatically be available again when the expiration date is reached, and the *Check Out* will be carried out automatically. If a guest leaves the hotel before the established expiration date is reached (whatever the reason), and we need to make the room available, the *Check Out* will have to be performed manually to make the room available again.



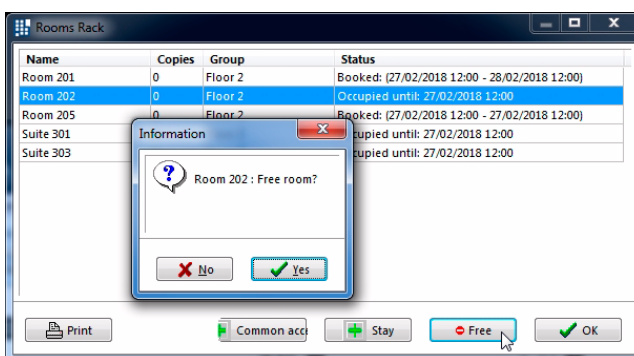
To perform the *Check Out* of a room manually, click on the “Check Out” icon on the Reception Menu and the “Check Out” form will be displayed.

This form displays the list of occupied rooms in the hotel at that time. To carry out the *Check Out* of one room in particular, select said room, for example room 201.



After selecting the room, click on the “Free” button and the software will perform the *Check Out* of the room, which will become available again in the list of free rooms in the *Check In*.

Before performing the *Check Out*, the software will request confirmation.



K

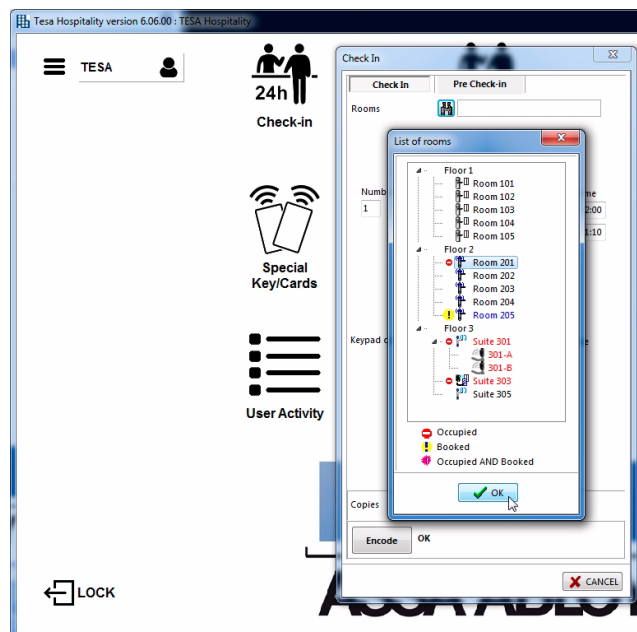
As can be seen, the room in question disappears from the list of occupied rooms on the *Check Out* list.

Name	Copies	Group	Status
Room 201	0	Floor 2	Booked: (27/02/2018 12:00 - 28/02/2018 12:00)
Room 205	0	Floor 2	Booked: (27/02/2018 12:00 - 27/02/2018 12:00)
Suite 301	0	Floor 3	Occupied until: 27/02/2018 12:00
Suite 303	0	Floor 3	Occupied until: 27/02/2018 12:00

The *Check Out* operation can also be carried out from the *Check In* form.

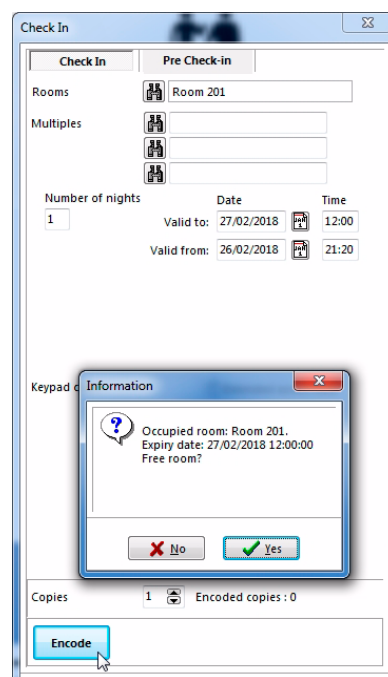
For example, the *Check In* of a new guest is being prepared and we wish to allocate them a room we know is free, but which shows up as occupied in the system. On the *Check In* form, click on the “Room” field to see the list of rooms.

For example, to allocate them room 201 which shows up as occupied, but which we know is available, select said room (despite being in red, indicating it is not available), and click on the “OK” button.



Next, click on “Encode”, and the software presents a message indicating that said room is occupied and asking whether you wish to free the room.

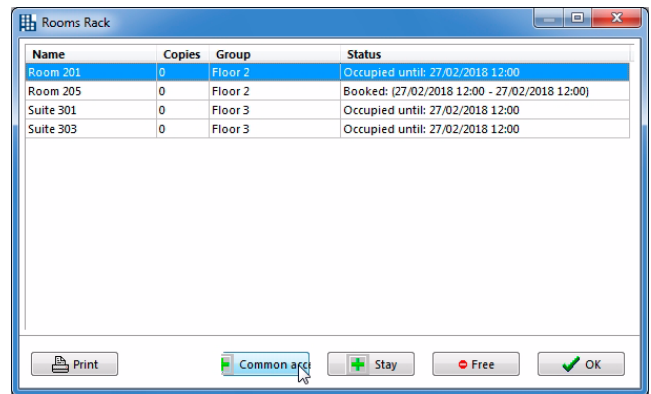
Click on the “Yes” button and the programme will automatically perform the *Check Out* of the room, and select it to carry out the *Check In* of the guest in said room. The *Check In* process continues as explained in the previous section.



Modify grants

The “Check Out” window enables us to perform other operations. One of them is the modification of the guests' grants.

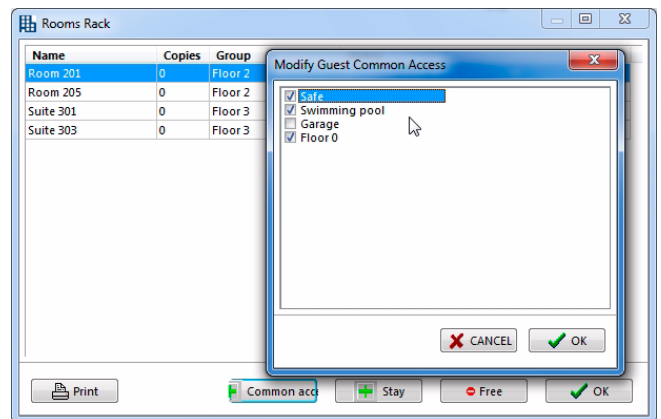
To modify the grants, select the room whose grants you wish to change and click on the “Grants” button.



A window appears with the grants.

Modify the grants as desired and click on “OK” to confirm.

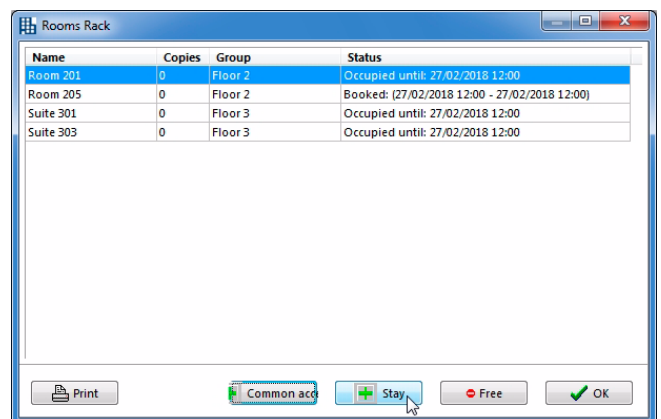
The grants will be encoded on the guest's card only in the *Read and Write* system and only when the card is swiped through an updater in the site.



Extend guest stay

From the “Check Out” window it is also possible to extend the stay of guests who are already occupying a room.

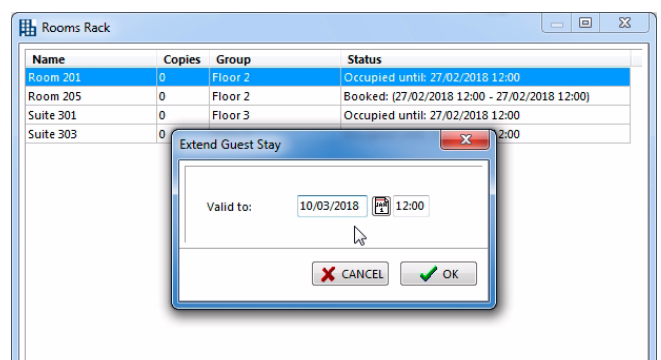
To do so, click on the “Stay” button.



A window is displayed enabling selection of the new date on which they will leave the hotel.

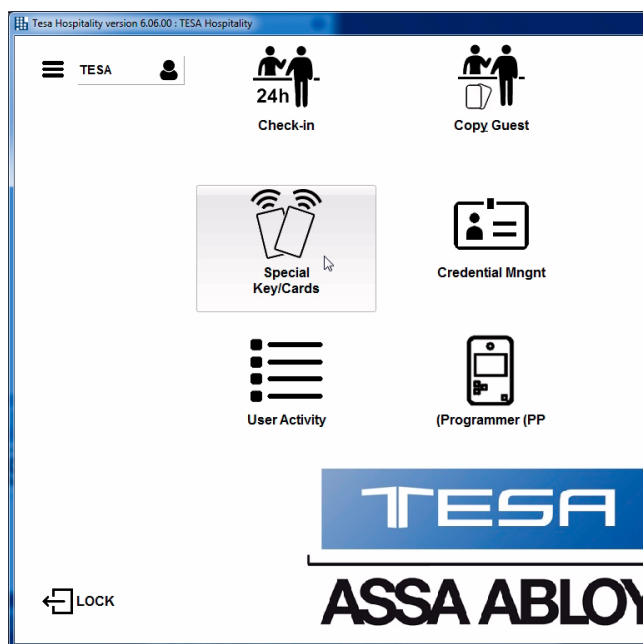
Select the desired date and click “OK” to accept.

The new date/time of *Checkout* will be re-encoded on the guest's card only in the *Read and Write* system and only when the card is swiped through an updater in the site



K.6 SPECIAL KEY/CARDS

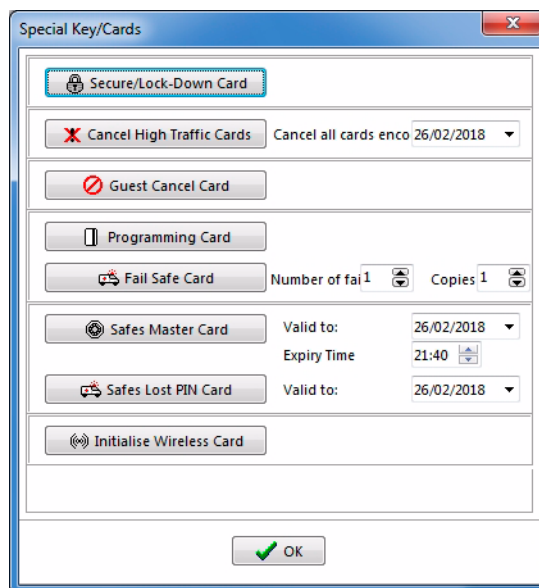
The TESA Hotel system offers a series of cards with special functions. This section explains each of these cards and how to encode and use them.



If you click on “Special Key/Cards” in the Reception Menu of the TESA Hotel programme, the “Other Cards/Keys” form is displayed.

The following special cards and keys are available:

- Blocking Card
- High Traffic Cancelling Card (this option is only displayed if a “High Traffic” door has been created).
- Guest Cancel Card
- Programming Card
- Fail Safe Card
- Safes Master Card
- Safes Lost PIN Card
- Init Wireless Card



Each of these special cards is described below.

Blocking 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.

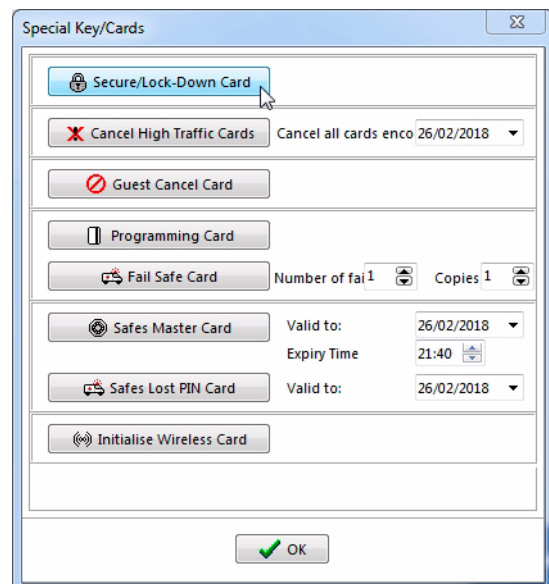
By default, the hotel guests can never open blocked doors.

To “unblock” a blocked lock, repeat the operation of inserting and removing the same blocking card used to block it. When a lock is unblocked, it returns to its previous state, once again allowing access to all users who have it according to the locking plan.

The blocking card is extremely useful in a hotel, for example when for some reason or other we wish to block a guest's access to their room, but do not wish to cancel their card. Or when an area or guest room is being refurbished and the management considers nobody should access it, etc.

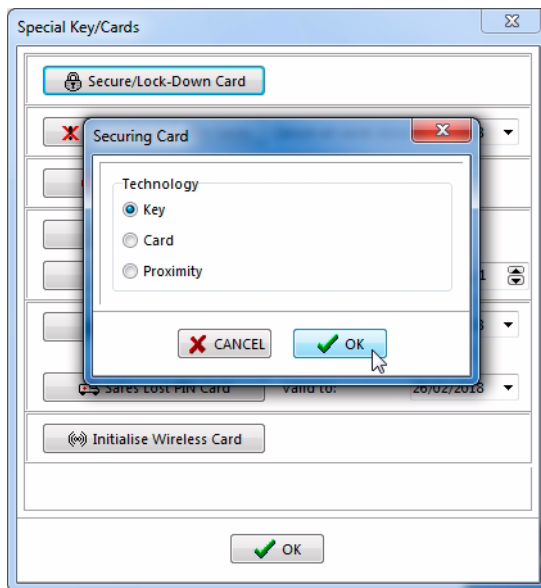
In order to encode the blocking card, proceed as follows:

- 1 In the Reception Menu, click on the “Other Cards/Keys” button.
The “Other Cards/Keys” form is displayed. Click on the “Blocking Card” button.



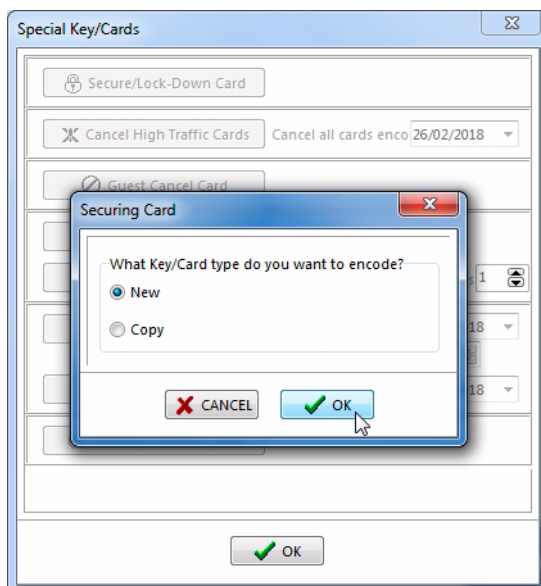
- 2 A window is displayed for selecting the technology of the credential (Key, Card, Proximity).

Select the technology corresponding to the credential you are going to record and click "OK" to accept.

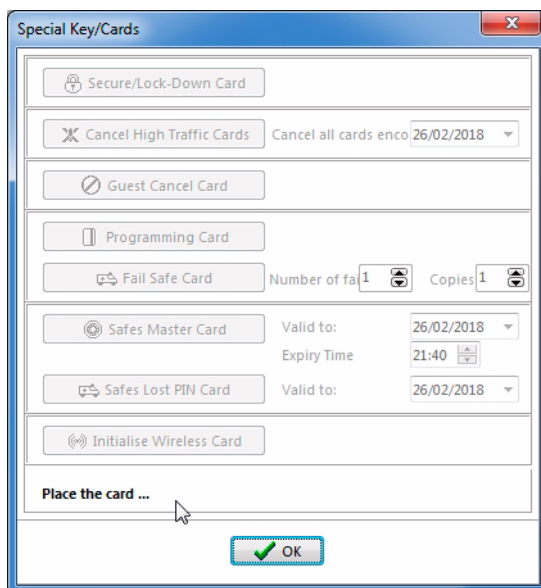


- 3 A screen is displayed asking whether you want a "New" card (cancels the previous blocking card) or a "Copy" (which does not cancel it).

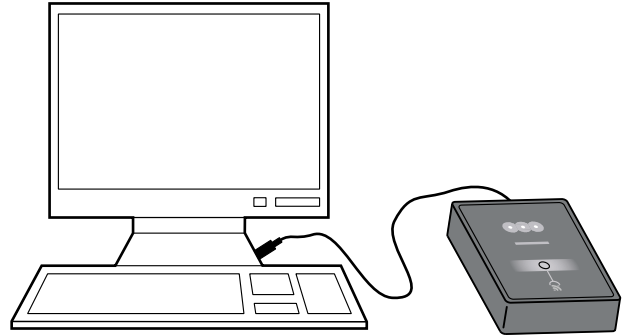
Choose the desired option and click "OK" to accept.



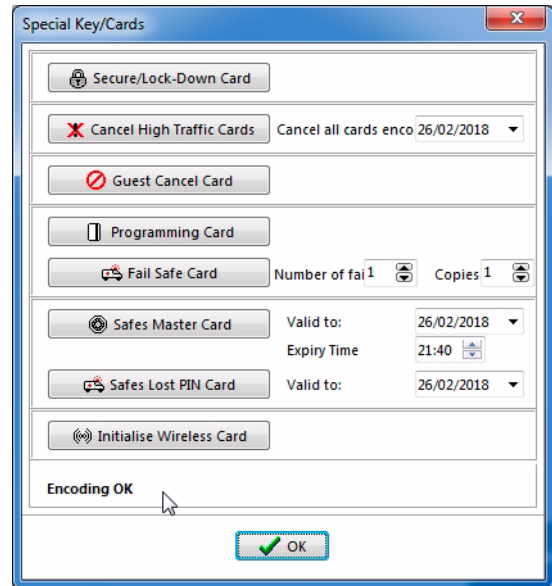
- 4 A message is displayed telling you to place the card on the encoder to encode it.



- 5 Place the card on the encoder.



- 6 At the end of the process, a message is displayed indicating that the encoding has been completed correctly.



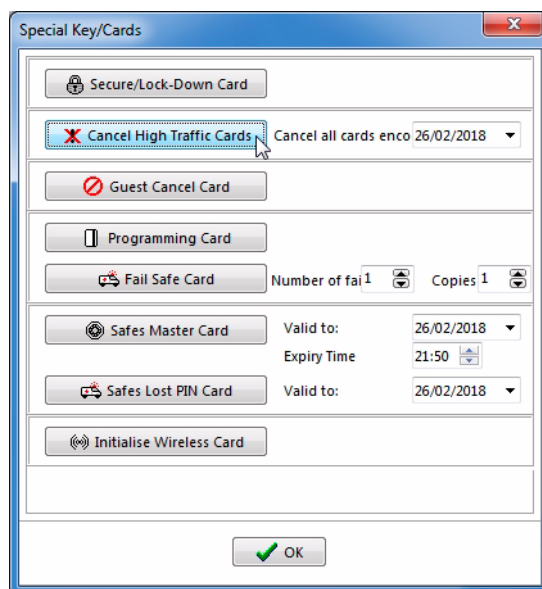
High Traffic Cancelling Card

A High Traffic Door can be opened with any credential which belongs to the system, whose dates are correct, and which holds the necessary permissions. That is to say, a user with a credential belonging to the site, but without an expiration 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.

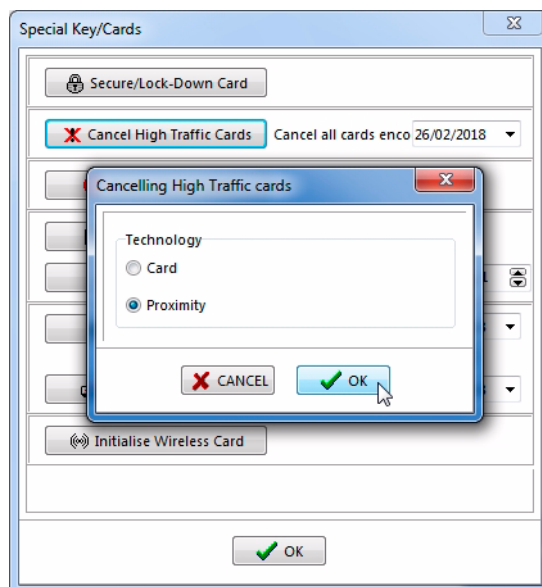
For more information on high traffic doors, see “High Traffic Door” on page 103.

The High Traffic Cancelling Card allows cancelling the credentials which have been encoded before the date selected in the field “Cards encoded before”.

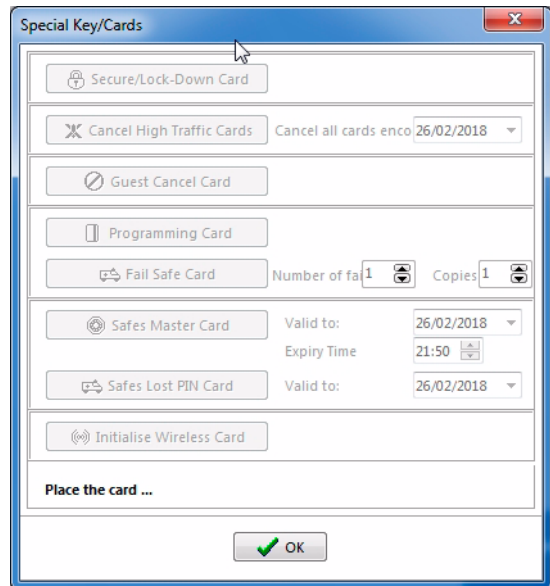
Select the date desired, connect the card encoder, and click on the “High Traffic Cancelling Card” button.



Select the type of technology of the card (Magnetic Card or Proximity Card) and click “OK” to confirm.

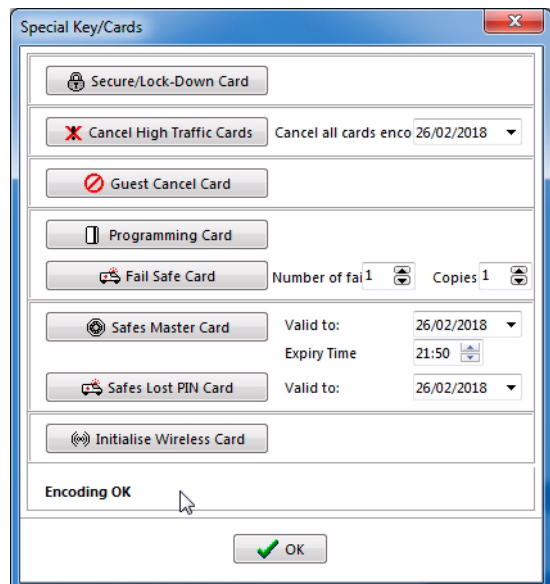


Place the card on the encoder as indicated in the message.



When the card has been encoded correctly, a confirmation message is displayed.

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.



Guest Cancel Card

The guest cancel card serves to cancel guest cards that are active in the locks of the system.

To cancel an active guest card in any room, simply insert the guest cancel card in said lock. The guest card and copies active at that time will automatically be cancelled.

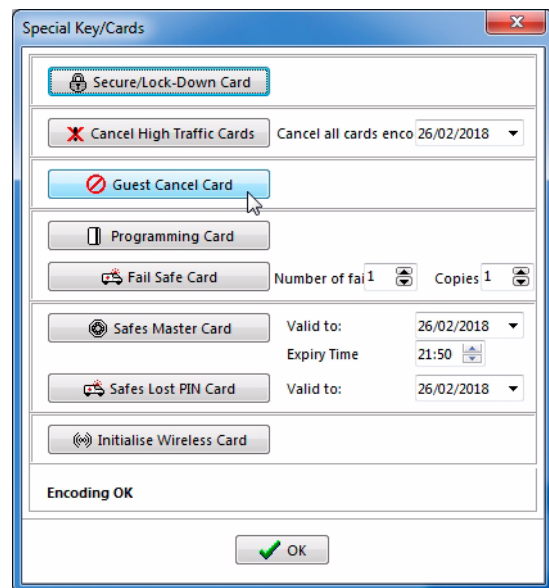
This card is very useful when a guest leaves the hotel earlier than expected and there is no new guest in the hotel for said room: when a guest performs the *Check In* in the hotel, they do so for a certain number of nights, so the card will not expire until 12 o'clock on the day set as the day of departure. To put it another way, the card will be active in the system until that date and time.

If for any reason this guest leaves the hotel earlier than expected and does not hand in their card, said card will continue to be active until a new guest performs the *Check In* for the same room or until it expires. Remember that a guest's room card is automatically cancelled for the lock by inserting a new guest card for the same room into the lock. That is to say, every time the *Check In* is carried out for a room, a guest card is encoded for said room and used in the lock.

When this card is inserted into the lock of the room, the lock automatically cancels the card of the previous guest. If there is no new guest, there is no need to encode a new guest card for the same room, so the card of the guest who left the hotel earlier than expected will remain active until it expires.

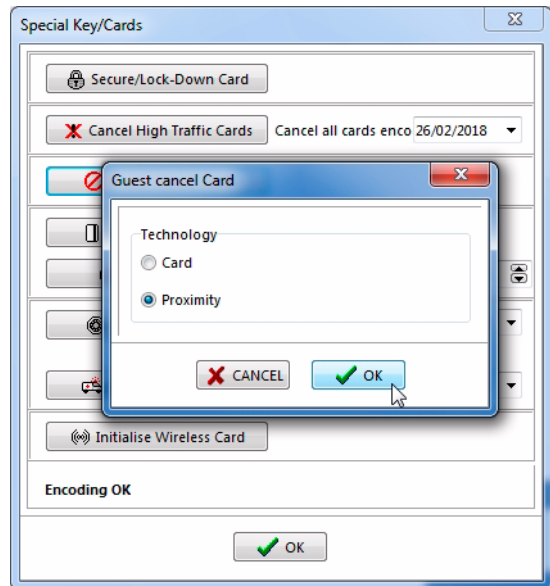
To prevent said guest from accessing the room they rented during the period from when they left the hotel until expiration of the card, we use the guest cancel card.

- 1 To encode this card, click on the "Guest Cancel Card" button.



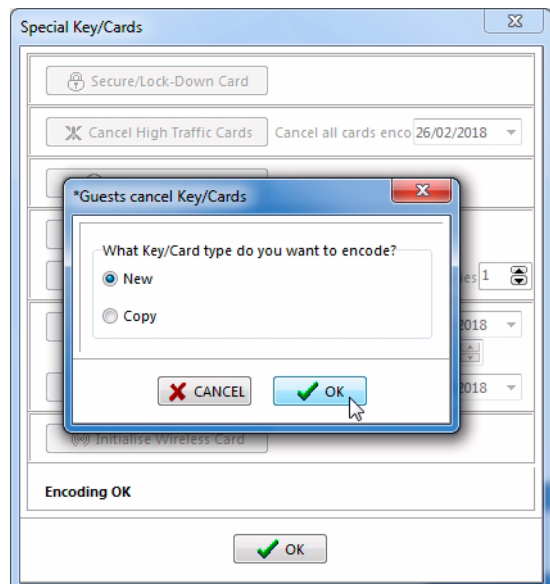
- 2 A window is displayed for selecting the technology of the credential (Card or Proximity).

Select the technology corresponding to the credential you are going to record and click "OK" to accept.



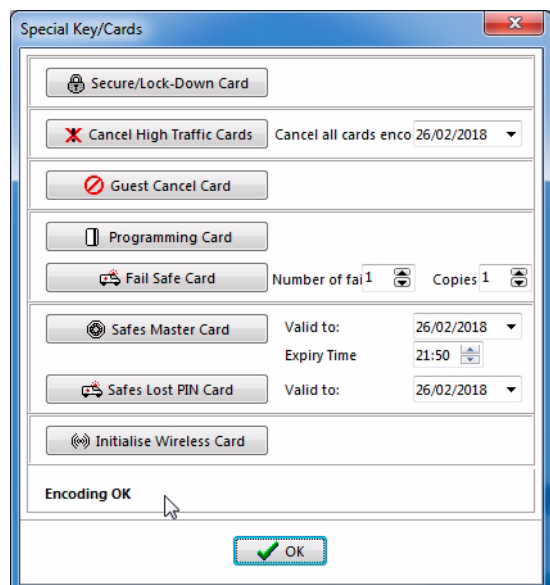
- 3 A screen is displayed asking whether you want a "New" card (cancels the previous card) or a "Copy" (which does not cancel it).

Choose the desired option and click "OK" to accept.



- 4 A message is displayed telling you to place the card on the encoder to encode it.

- 5 Place the card on the encoder. At the end of the process, a message is displayed indicating that the encoding has been completed correctly.



K

Programming Card and Fail Safe Card

The programming card and the fail safe cards are special cards designed to help if there is a failure in the system that prevents operation with the TESA Hotel software and encoding of guest cards.

If for any reason the TESA Hotel programme cannot be run, or the card encoder does not work, etc., and it is not possible to perform the guest *Check In* normally, as an emergency measure we can use the programming card and the fail safe cards to perform the *Check In* manually.

The functioning is as follows:

In the hotel reception, two programming cards and at least as many fail safe cards as the number of rooms in the hotel will be reserved. If the system fails, to perform the *Check In* of a guest to a room, insert the programming card in the lock of the room and then insert a fail safe card. From this moment on, the fail safe card will become the guest's card for that room. Operating in this way, it is only possible to have one card per room if the encoding system has not yet been recovered.

When this guest leaves the hotel, they must give the card in to reception and the card will be given to the next guest for said room.

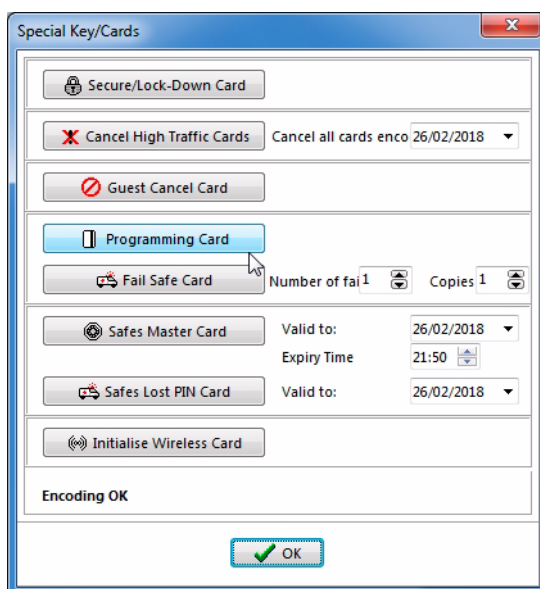
If the guest who leaves the hotel does not hand in the card, the operation will have to be repeated and a new fail safe card programmed. That is to say, the programming card will be inserted in the lock, and then a new fail safe card; this card will become the new guest card for this room and the previous one will be cancelled.

When the system is working again, the *Check In* will be performed as normal and when the new guest card (now encoded with the card encoder) is inserted in the lock of the room, the fail safe card that was operational will be cancelled.

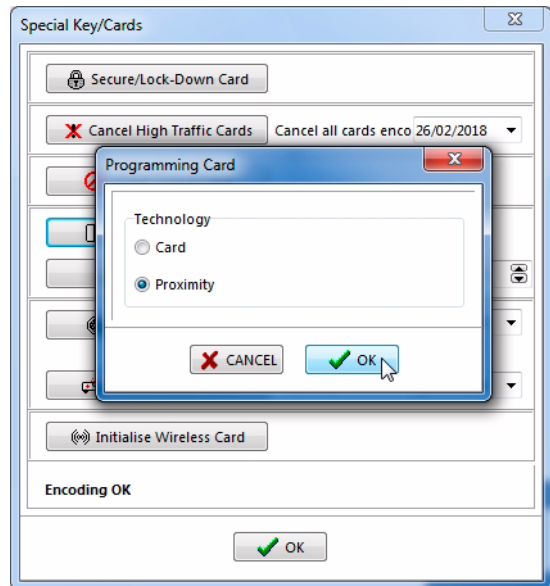
Encoding the Programming Card

In order to encode this card, proceed as follows:

- 1 Click on the "Programming Card" button.

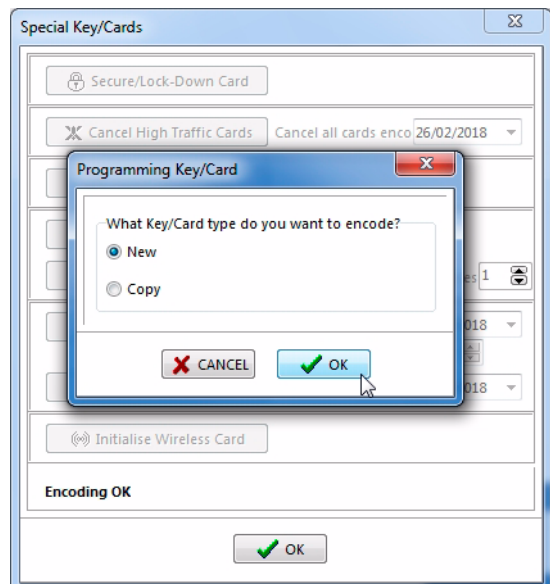


- 2 Select the type of technology of the card (Magnetic Card or Proximity Card) and click "OK" to accept.

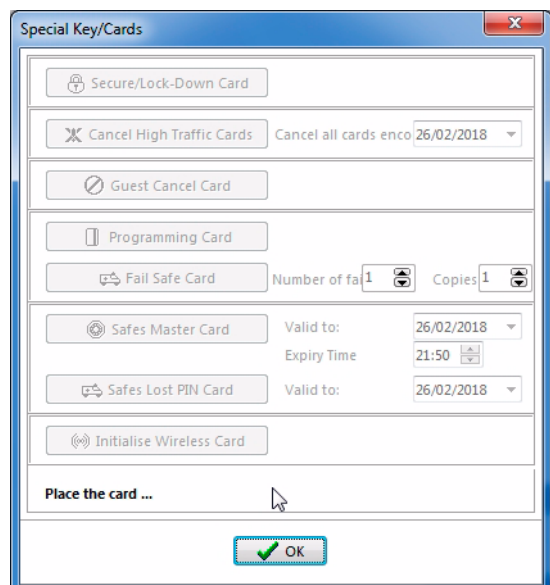


- 3 Choose the desired option (New Card or Copy) and click "OK" to confirm.

If you select "New" the previous card encoded will be cancelled, but if you select "Copy" it will not. Encoding of a New Card, and of a couple of Copies afterwards, is recommended.

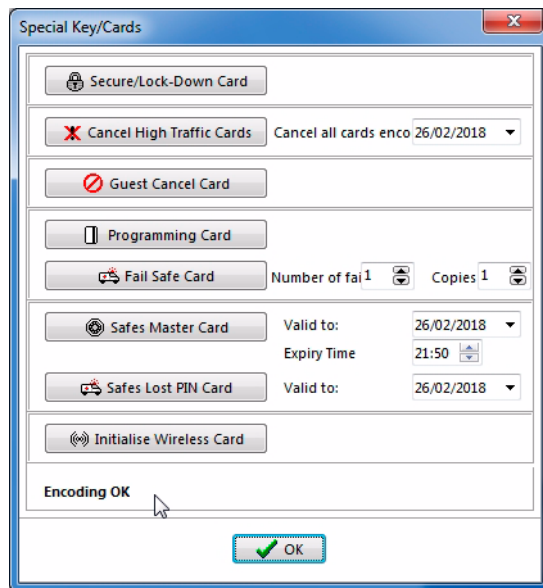


- 4 Place the card on the encoder as requested in the message.



K

- The encoding takes place and the corresponding confirmation message is displayed.



Encoding the Fail Safe Cards

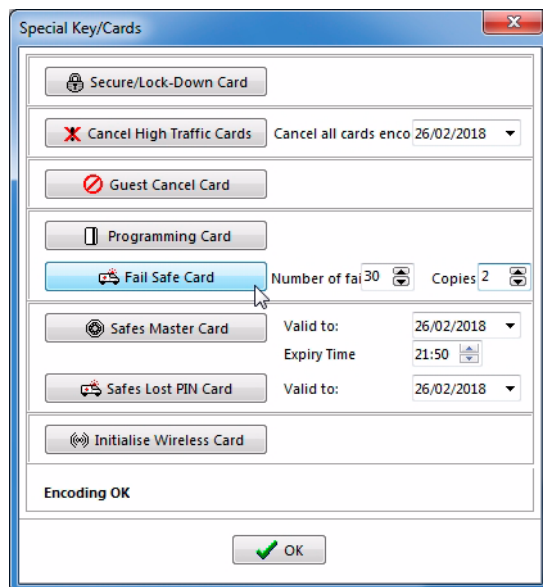
Before encoding the Fail Safe Cards, the number of Fail Safe Cards that will be required must be determined. In this way, all of the cards will be encoded consecutively, one after the other.

After determining the number of Fail Safe Cards needed, proceed as follows:

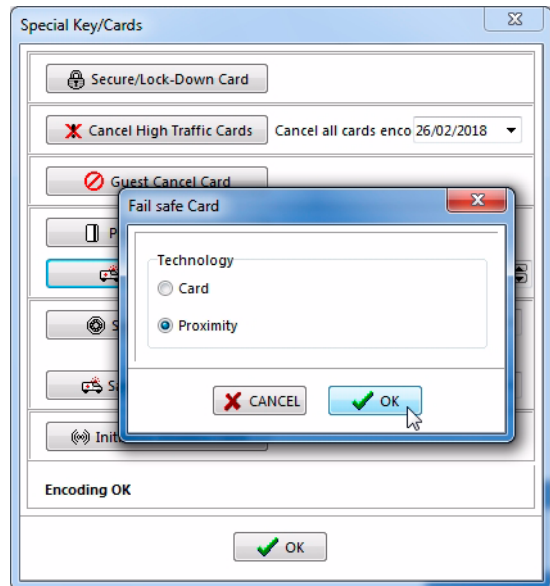
- Complete the “No. of cards” and “Copies” fields and click on the “Fail Safe Card” button.

If copies are encoded, it is important to afterwards keep the cards properly with their pair - the original and its copy together.

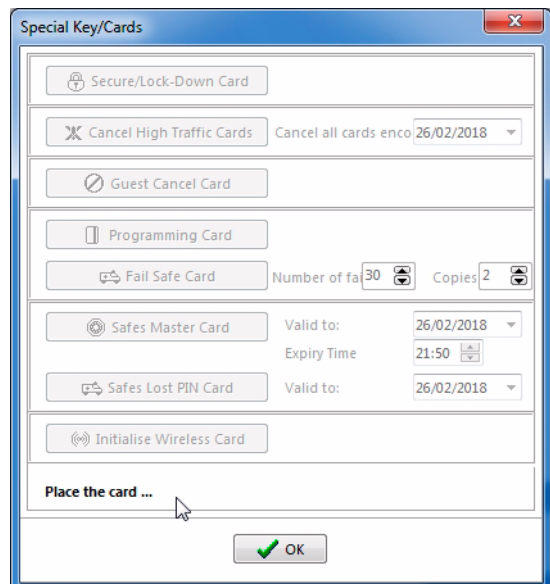
If copies are encoded, two cards may be given to the guest for their room, as it is sufficient to programme just one of them in the room.



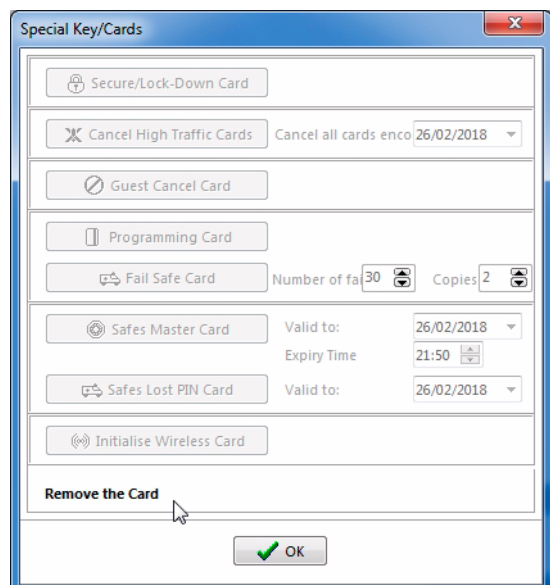
- 2 Select the type of technology of the card (Magnetic Card or Proximity Card) and click "OK" to accept.



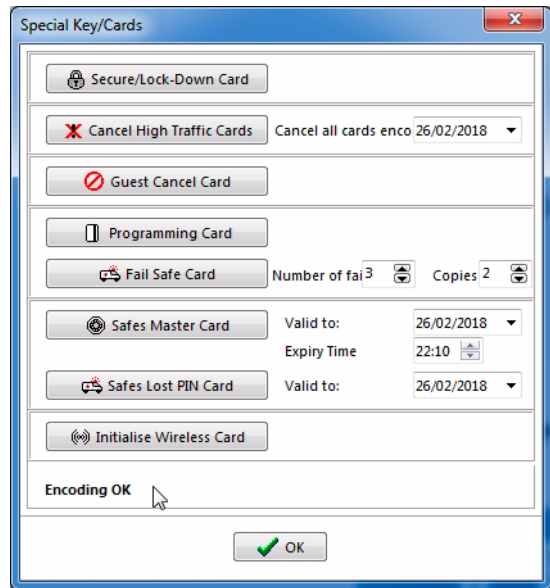
- 3 Place the card on the encoder as requested in the message.



- 4 After the first card is encoded, remove it (as indicated in the message).
- 5 A new message will be displayed telling you to place the next card to be encoded on the encoder.
- 6 Repeat the process until all the cards are encoded.



- When all the cards are encoded, the "Encoding OK" message is displayed.



“Safes Master” Card

When a guest who has had access to the safe in their room leaves the hotel, they should leave the safe open so that the next guest can use it.

If they leave it closed, the new guest will not be able to use the safe and will call reception for emergency opening of the safe in question to be performed.

For this purpose, we have the *Safes Master* card. This is a card that opens ALL the safes in the hotel. Because it can open all the safes in the hotel, this is a high-security card and therefore few operators should have the possibility of encoding it and keeping it in a safe place.

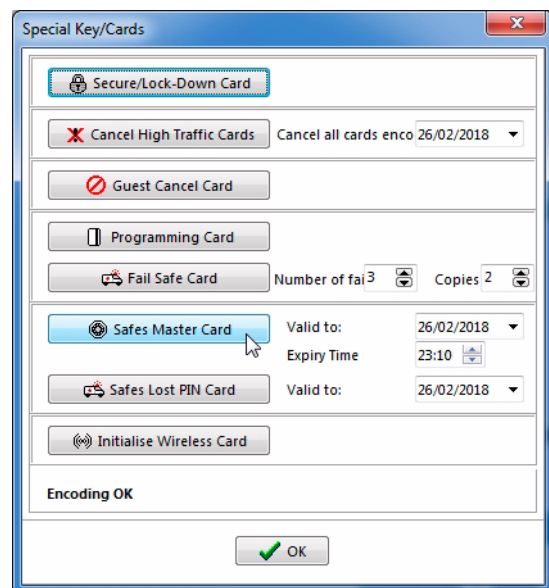
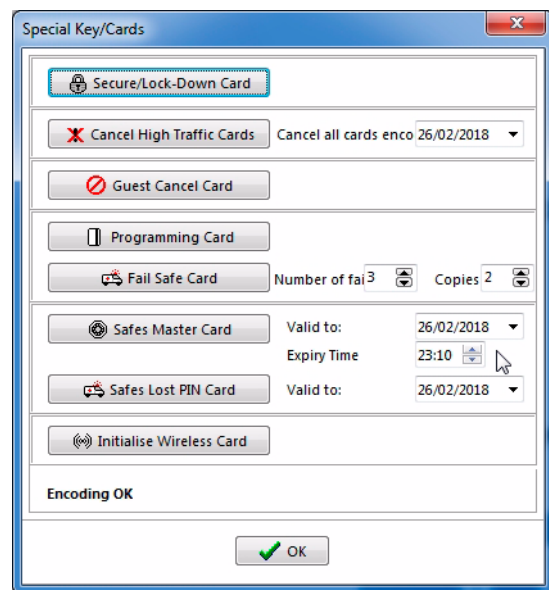
Moreover, since it is such a “high risk” card, when it is encoded, there is the possibility of selecting a very short expiration period, so that it practically serves for one day only. Thus, every time it is needed we will have to encode it again, and this is something only authorised operators will be able to do.

To encode the safes master card, we must first select the expiration day and time. By default, the same day on which the card is recorded and ten minutes' time will be assigned.

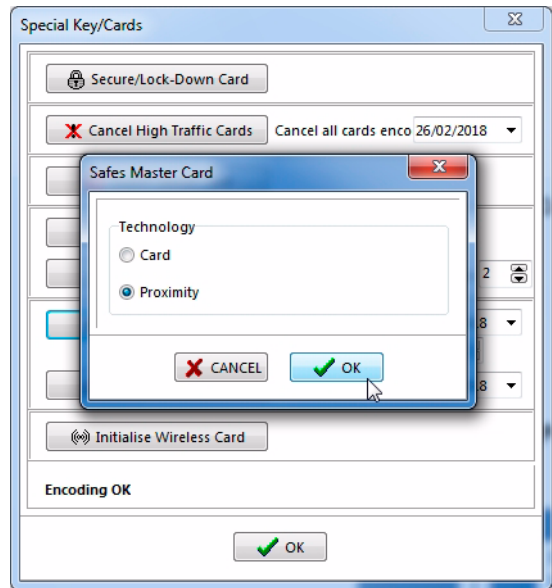
To select the day, click on the arrow in the “Expiration Date” field and select the day.

Select the “Expiration Time” field in the same way and set the time.

After selecting the day and time, click on the “Safes Master Card” button and the card will be encoded.

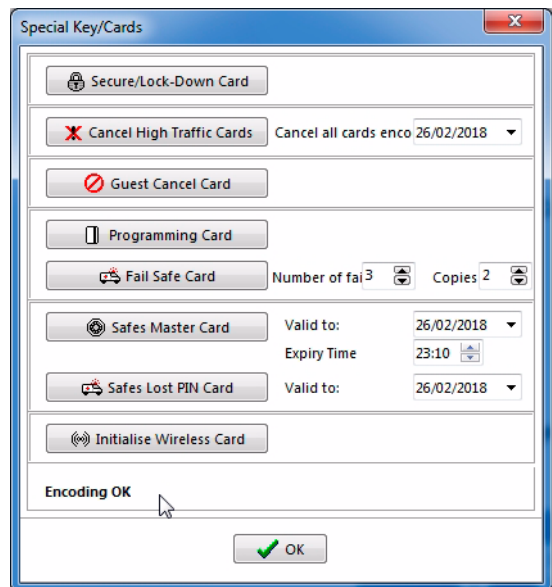


Select the type of technology of the card (Magnetic Card or Proximity Card) and click "OK" to accept.



Place the card on the encoder for encoding.

After the encoding, the corresponding confirmation message is displayed.



“Safes Lost PIN” Card

Another different situation in relation to safes is when a guest forgets the code they had chosen on programming the safe.

The functioning of the safes when they are working in “Card + PIN” mode is as follows: when the guest arrives in the room, to operate the safe they insert their guest card and then enter a 4-digit code of their choice and press the green key. They enter the code again to confirm the operation and then press the green key again. If the operation is completed successfully, when they press the green key for the second time, the safe will close. From this moment on, the guest will simply have to key in their code and press the green key to open or close the safe. When the guest leaves the hotel, they will leave the safe open and when the new guest arrives, they will repeat the operation with a new code of their choice.

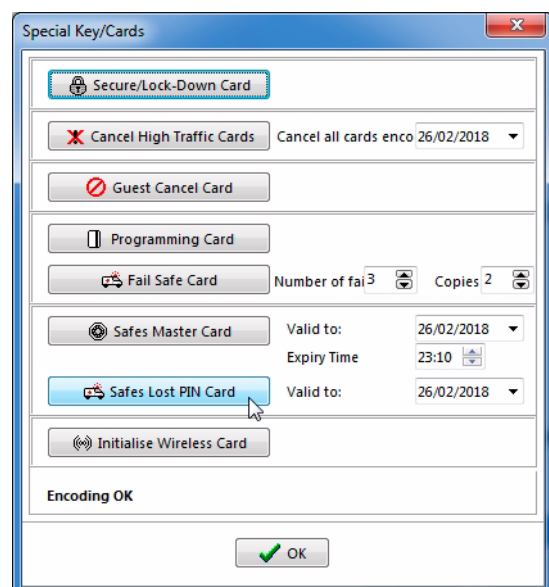
With the safe functioning in this mode, only the guest knows the keypad code to open or close the safe, as it is they who have programmed it.

If for any reason the guest does not remember that code, we will need to perform an emergency opening of the safe. To carry out the emergency opening in this situation, the TESA Hotel programme has a special card called the “Safes Lost PIN” card. The guest will call reception explaining what has happened. Reception will encode a “Safes Lost PIN” card and the receptionist will go to the room where the guest is. The safe will be opened in emergency mode, with the combination of the “Safes Lost PIN” card and the guest card: the receptionist will insert the “Safes Lost PIN” card and the safe will now require the guest card. When the guest inserts their card after the Safes Lost PIN card, the safe will open.

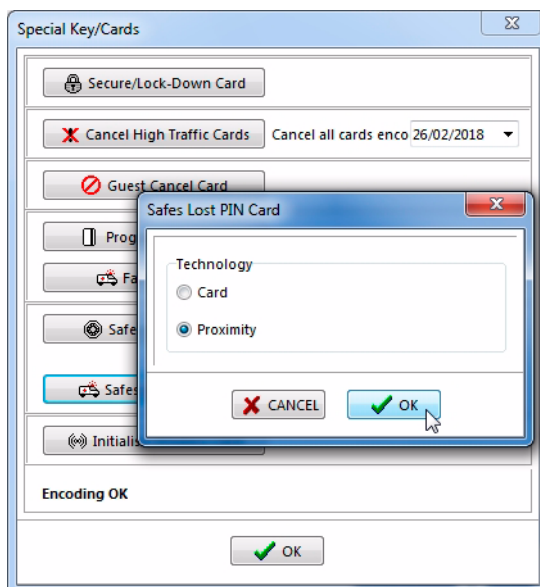
This is therefore a complete security measure both for the guest (as the guest will see that nobody can open their safe if they are not present) and for the hotel. The “Safes Lost PIN” card is identical to the “Safes Master” card, a high-security card, so restriction to operators must be stringent, and the expiration time must be short.

As with the “Safes Master” card, before encoding the card we must select the expiration date of it, which by default will be 24H00MN on the same day as it is encoded.

After selecting the expiration date, click on “Safes Lost PIN”.

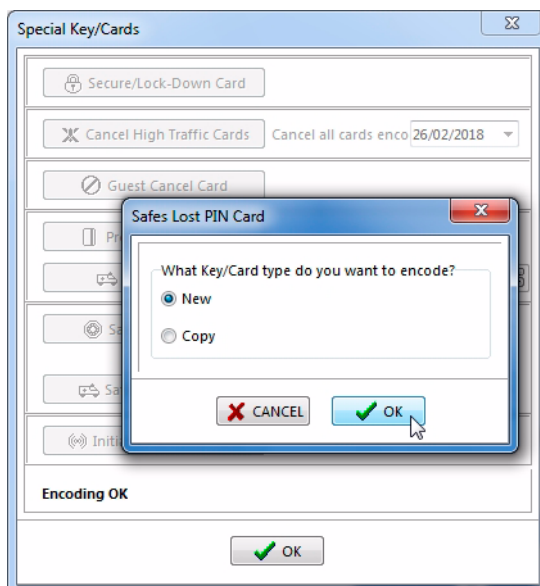


In the window displayed, select the type of technology of the card (Magnetic Card or Proximity Card) and click “OK” to accept.

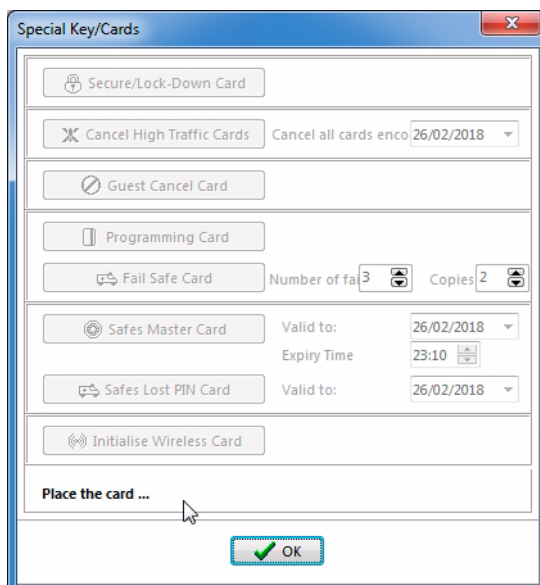


Choose the desired option (New Card or Copy) and click “OK” to confirm.

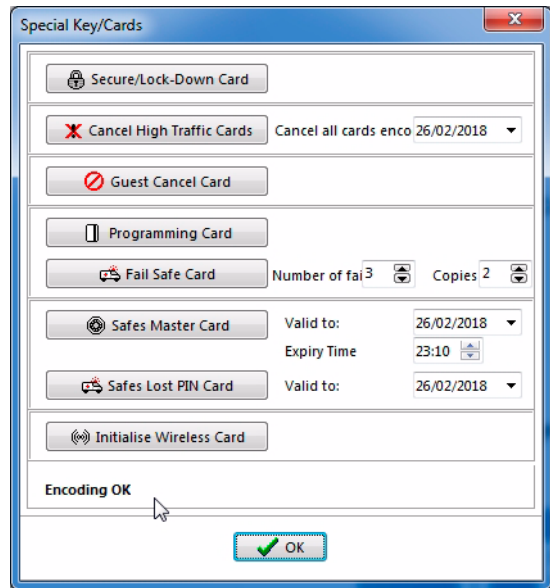
The new card or key will cancel any previous one encoded, but the copy does not.



Place the card on the card encoder, as indicated in the message in the window.

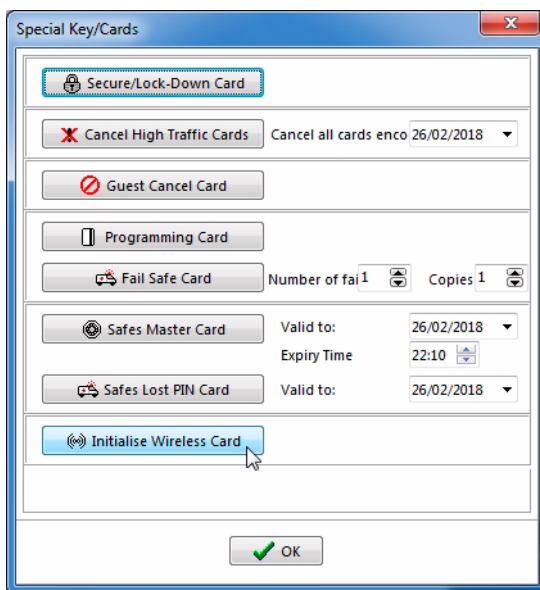


When the card has been encoded correctly, a confirmation message is displayed in the window.



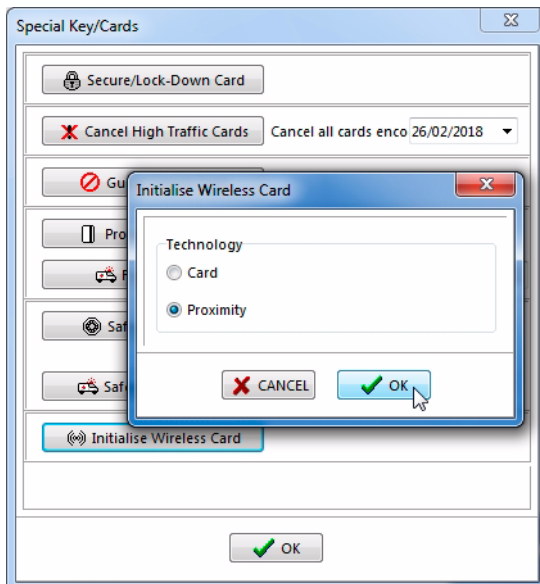
“Init Wireless” Card

The “Init Wireless” Card is used in V3 wireless systems to automatically link the doors to the Hub having the strongest coverage available.

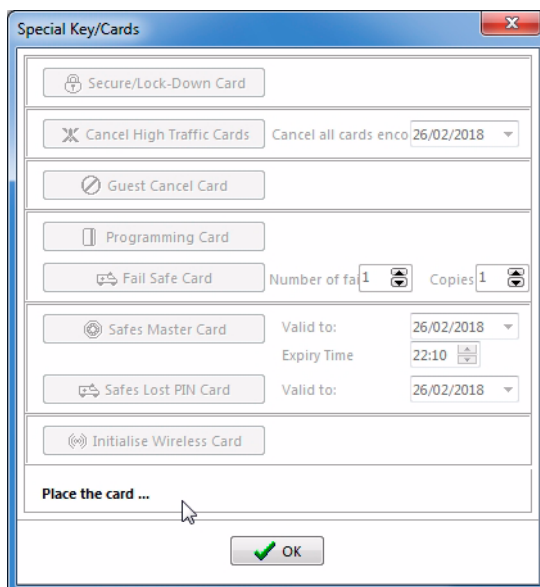


In order to encode the card, connect the card encoder and click the “Init Wireless Card” button; a window is displayed asking you to choose the technology of the card.

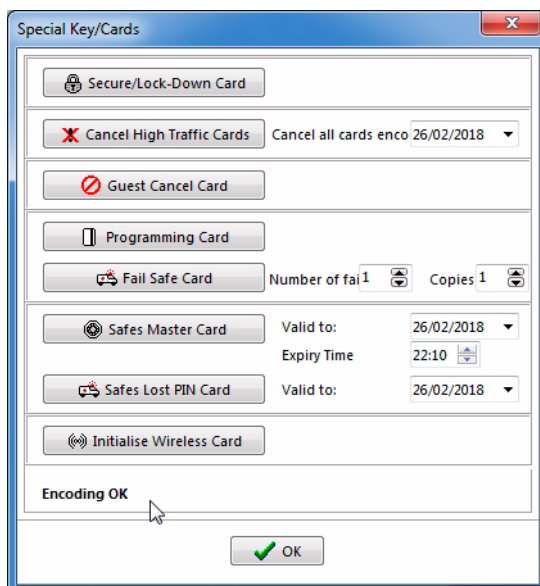
Select the technology applicable to your card and click “OK”.



A message is displayed indicating you to bring the card close.



Place the card on the encoder. After a brief moment, the card will be encoded, and a confirmation message will be displayed.



Once the initialization 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 "Keys/Cards" menu.

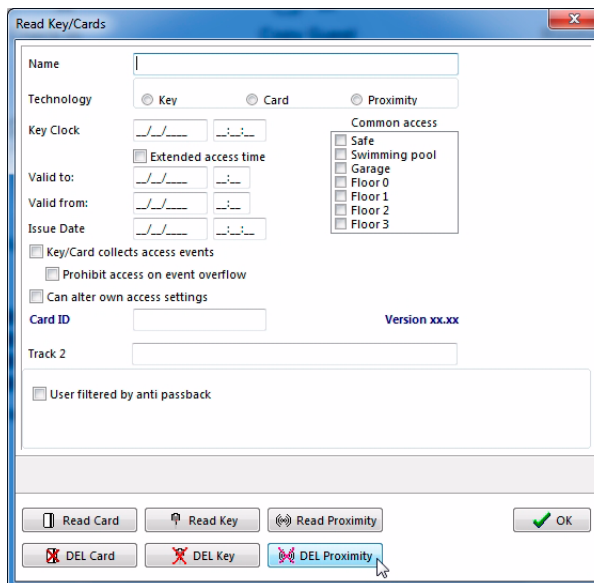


K

The window “Read Cards/Keys” is displayed: click the “Delete Proximity” or “Delete Card” button, as appropriate.

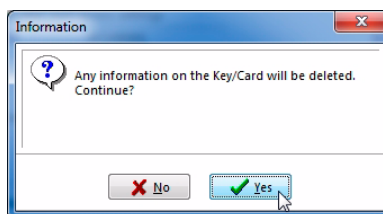
With the card encoder previously connected, click the corresponding deletion button and place the card on the encoder.

First, the encoder reads the card, showing the information encoded on it on the screen.

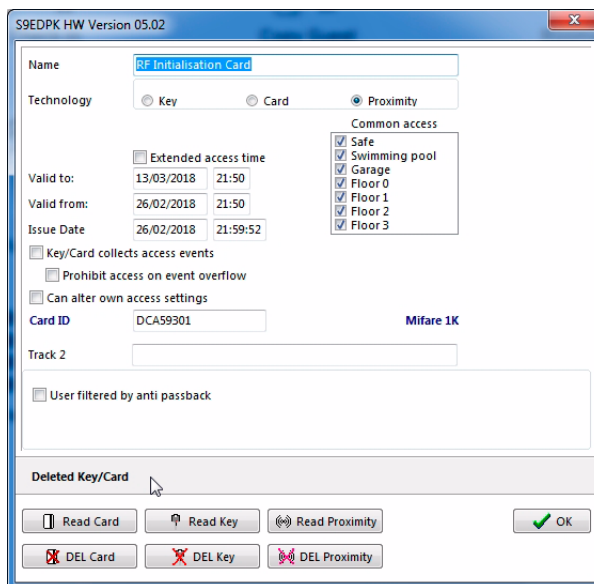


A message is displayed asking you to confirm the deletion of the card.

If the information you wish to delete is correct, click on “Yes” to confirm.



The deletion takes place and a confirmation message is displayed.

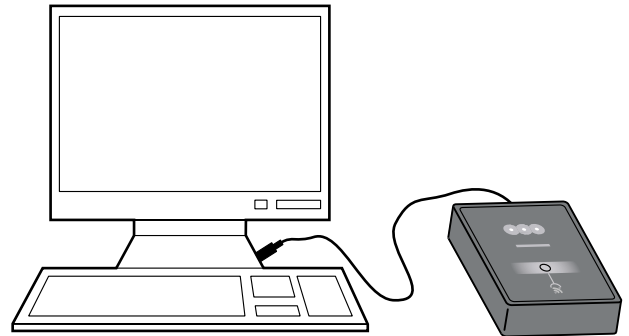


K.7 READ CARDS/KEYS

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.

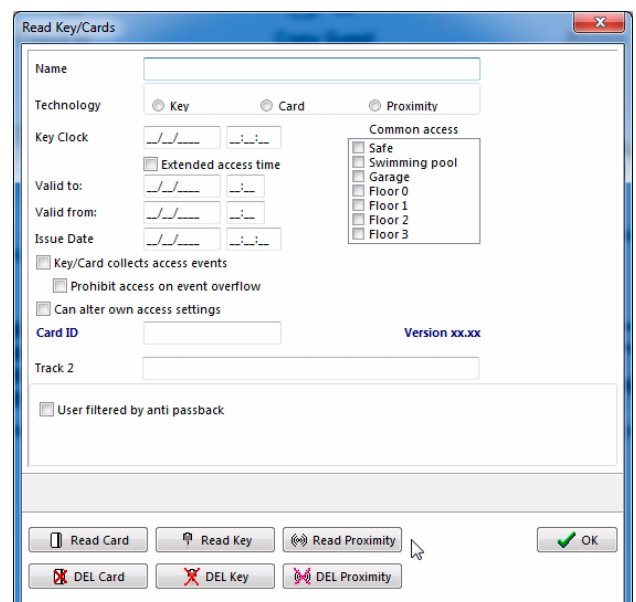


After connecting the Device to the PC, click on “Read Keys/Cards”, on the TESA Hotel Reception Form.



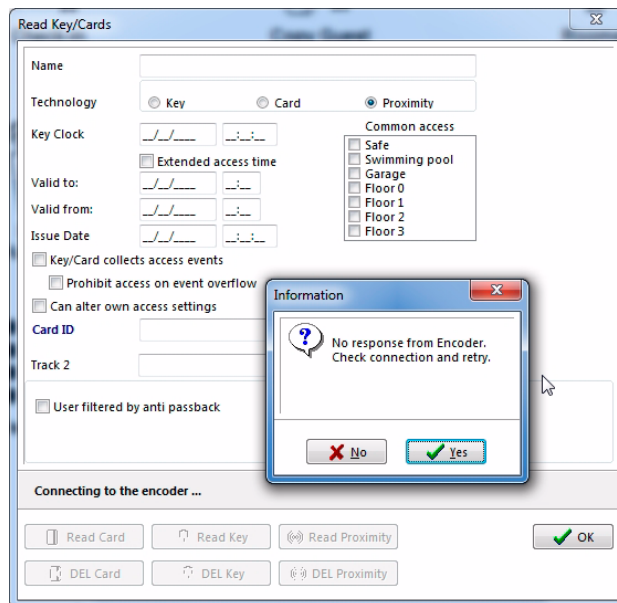
The “Read Cards/Keys” window is displayed.

Click on the button corresponding to the credential you wish to read (Card, Key or Proximity).



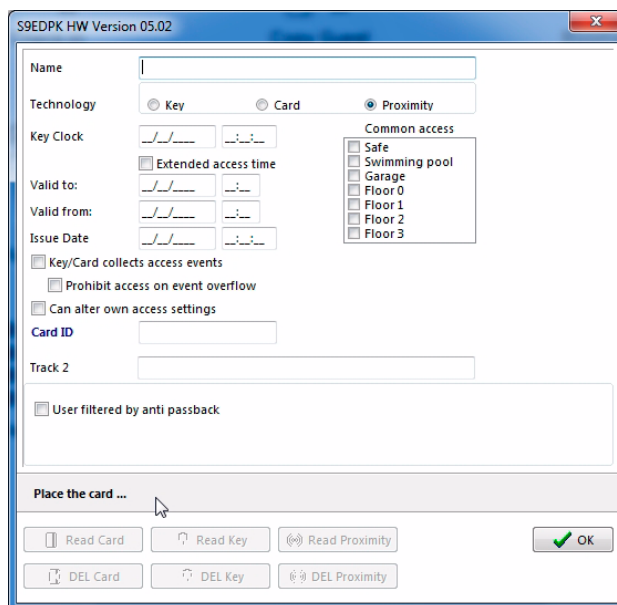
K

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".



Once communication has been established, a screen is displayed, with the fields to be read shown empty, where a message appears requesting the card to be brought closer.

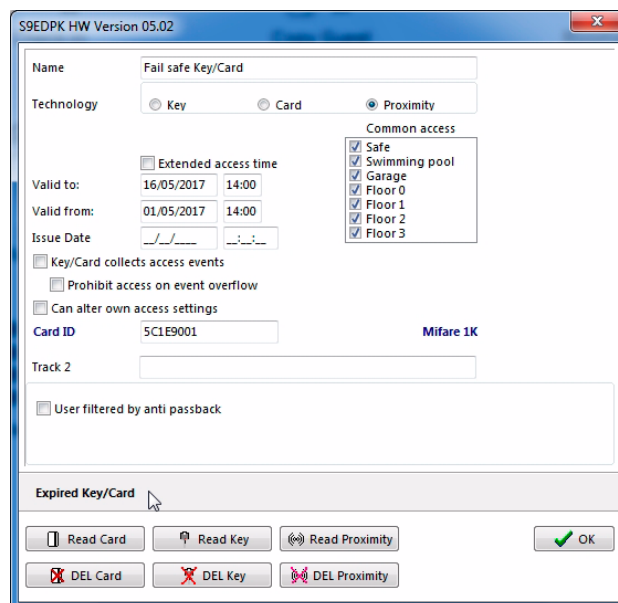
At the top of the window, both the model and version of the Encoder being used to read the card are shown.



After bringing the card closer, the information related to the User is displayed on the screen, in addition to the message “Reading OK”.

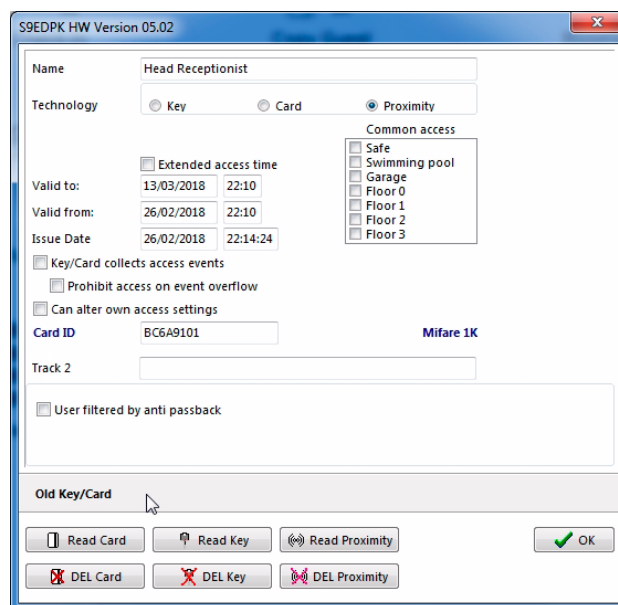
If the expiration date has been exceeded, the “Card/Key expired” message is displayed.

If you want another card to be read, you only need to bring it closer to the Encoder and click the “Read Proximity” button.



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 Electronic Key and Proximity 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 (in the Read and Write system)” on page 218).



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.8 OPENINGS

The TESA Hotel 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 TESA Hotel system allows checking all these events by means of the Opening Register. In order to be able to check these events by means of TESA Hotel, 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 TESA Hotel software, 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 in the *Read and Write* system).
- 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 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” sub menu.
 - 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:

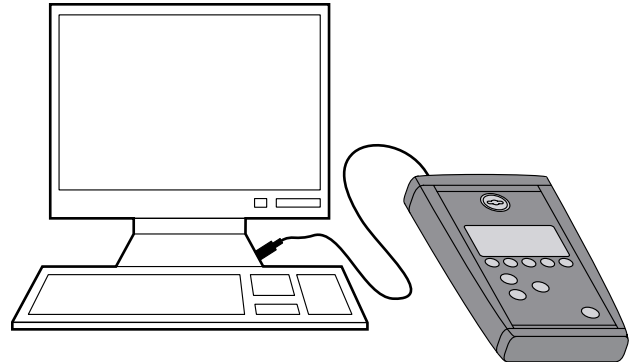
- Viewing the event in the Portable Programmer (in the F4 “Openings” menu, “See Openings” sub menu).
- Transmitting the records to the PC and viewing them in the TESA Hotel software

The first option is more appropriate when you wish to quickly view a specific event related to a given door.

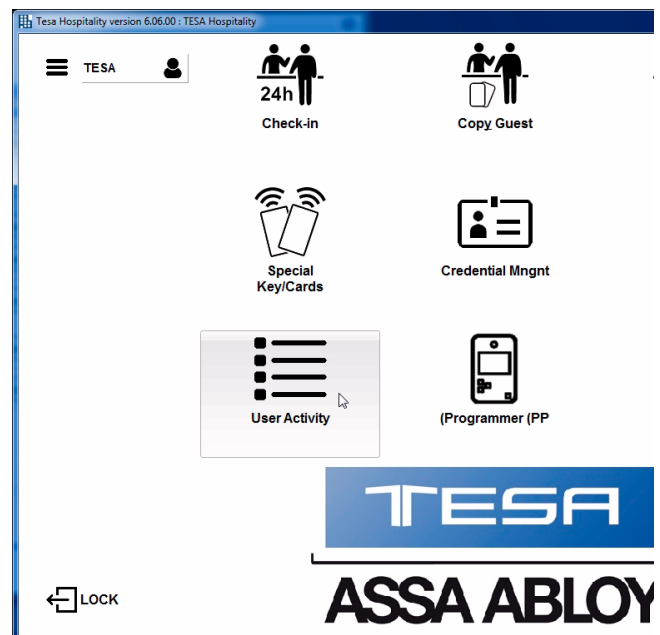
For any other case, the second option is, in principle, more convenient.

The second option is carried out as follows:

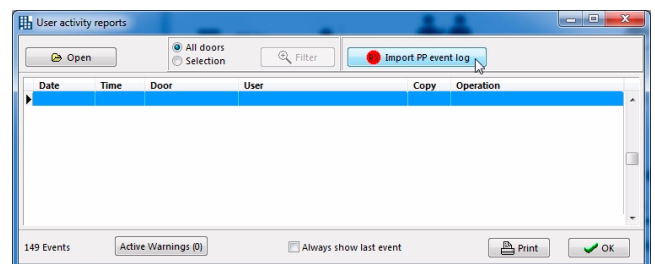
- 1 Connect the Portable Programmer to the PC with the corresponding serial cable (this can be USB or RS-232, depending on the model).



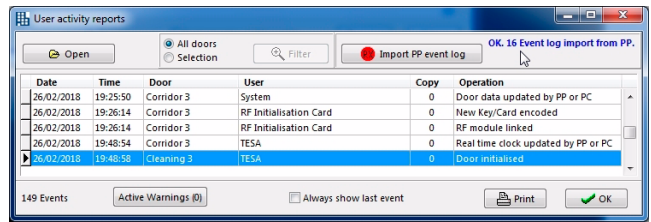
- 2 Access the “Openings” menu in the TESA Hotel Reception Menu.



- 3 The following screen is displayed: Make sure the Programmer is on (it turns off automatically after some minutes of inactivity) and, on the TESA Hotel screen, click the “Collect Openings from PP” button.



- 4 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.



Openings read from Credentials by means of the Portable Programmer or Encoder (in the Read and Write system)

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.

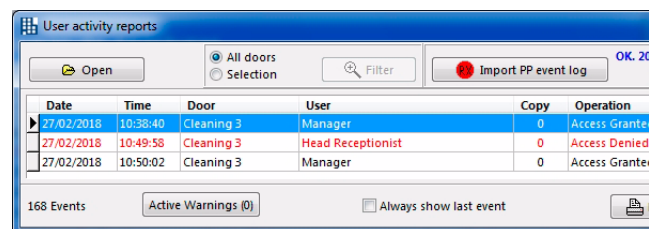
The process involves taking the credential of the user and reading it from the “Cards” menu, as has been explained in section “K.7 Read cards/keys” on page 213. In addition to finding the form of the credential, the system collects, records and deletes from it all the events stored.

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.
- **Copy:** number of the user's copy of the card in the event the card is a copy. If “0” is displayed, this means it is an original card.
- **Operation:** the event itself, that is to say, what happened. For example: “Initialization of door”.

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 initialization, time setting, etc.

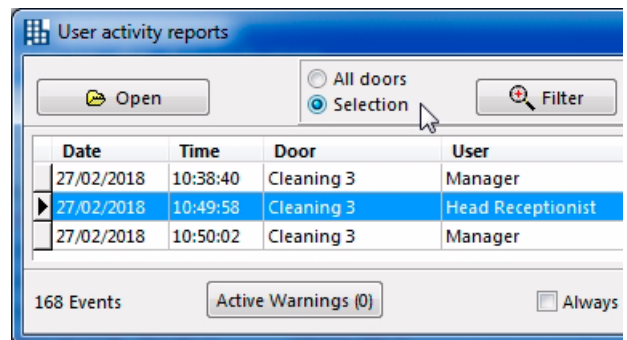
The information presented on this screen can be managed by means of the “Filter” and “Print” tools, which are included on it:

- 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 can be imported from 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.

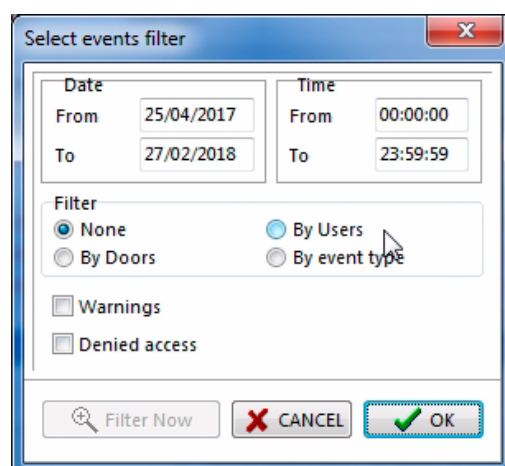
By selecting the option “Selection”, the “Filter” button is enabled.



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.

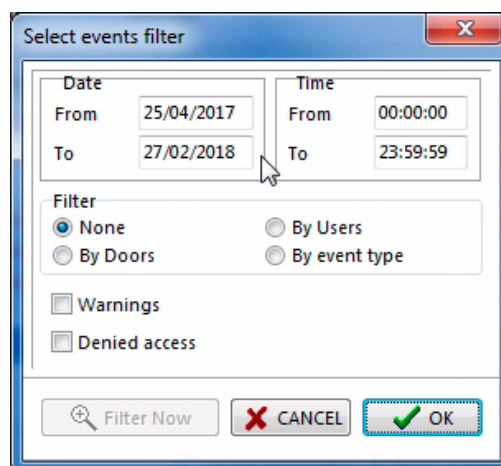
It is also possible to select the options “Only Warnings” or “Only Rejections”.



- **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.




- **Filter by Doors:**

In the field "Filter", the option "By Doors" is selected and the following screen is displayed:

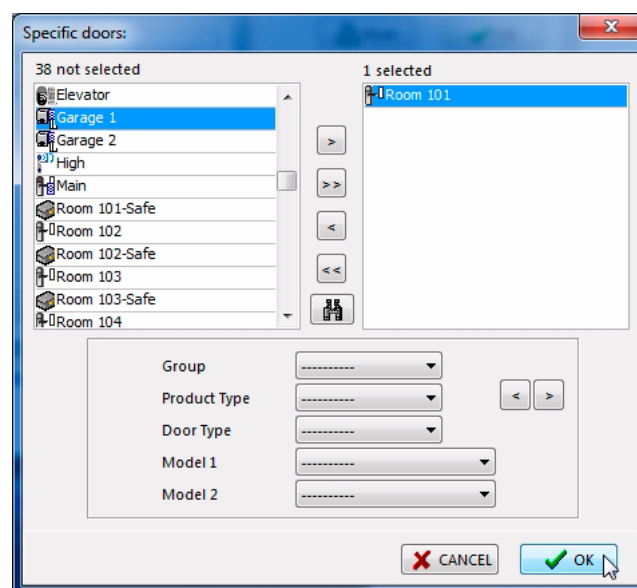
This screen allows selecting the doors whose events you want to see.

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.



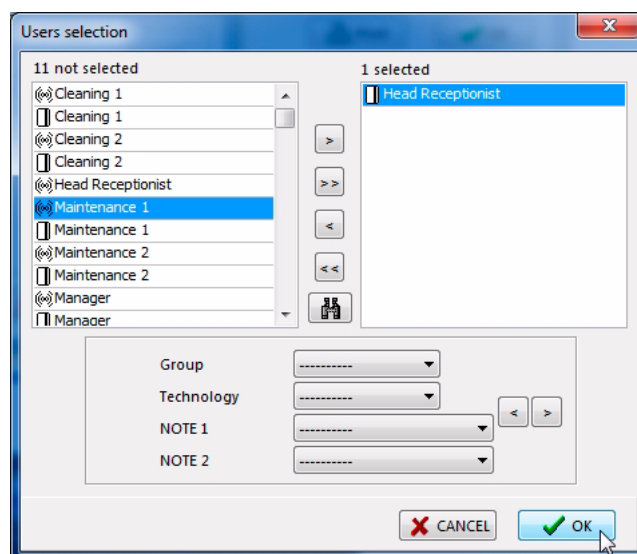
- **Filter by Users:**

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.

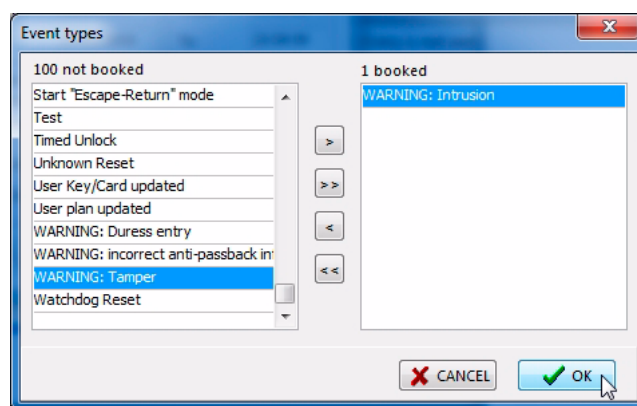


- **Filter by Operations:**

In order to set filters according to the operations carried out, select the option “By Operations” and the following screen will be displayed:

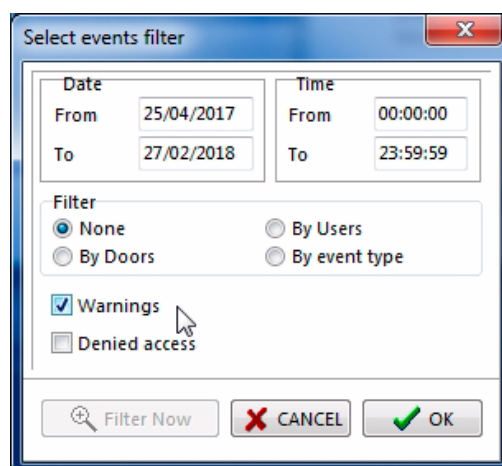
This screen allows selecting, from among the different types of possible operations, the ones whose events you want to see.

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.



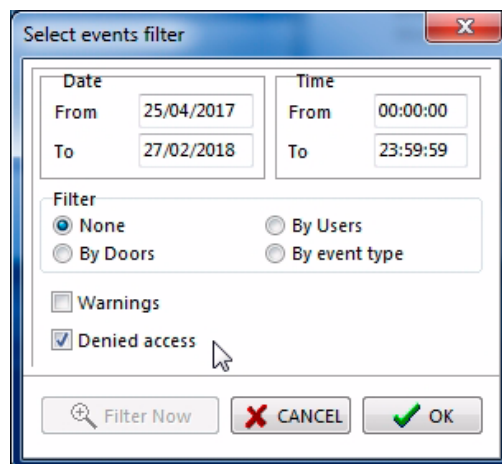
- **“Only Warnings” filter:**

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”.



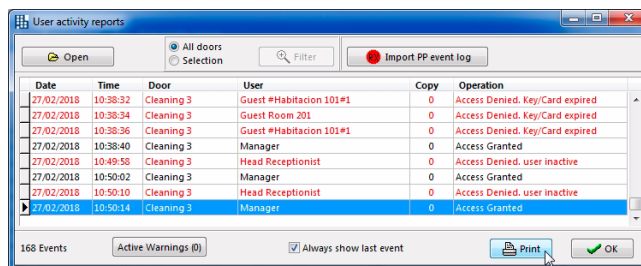
- “Only Rejections” filter

You also have the possibility of filtering to view only the rejections. Select the option “Only Rejections” and, then click “OK”.



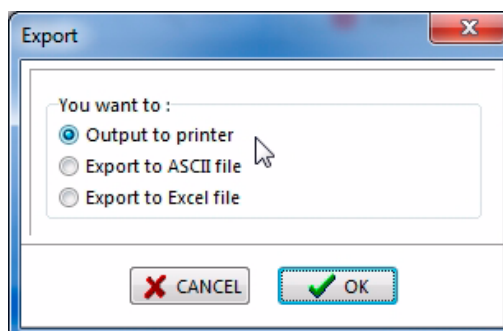
Print

It is possible to print the opening register by clicking the “Print” button located at the bottom right.

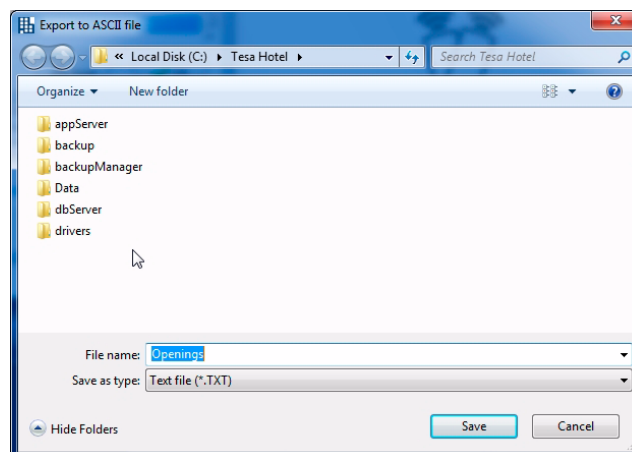


After clicking the “Print” button, three possible options are displayed:

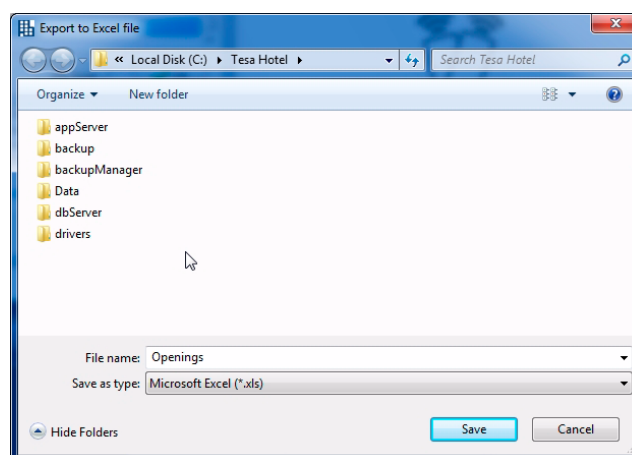
- **Output to printer:** allows printing the opening register on the default printer of the computer being used.



- 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.



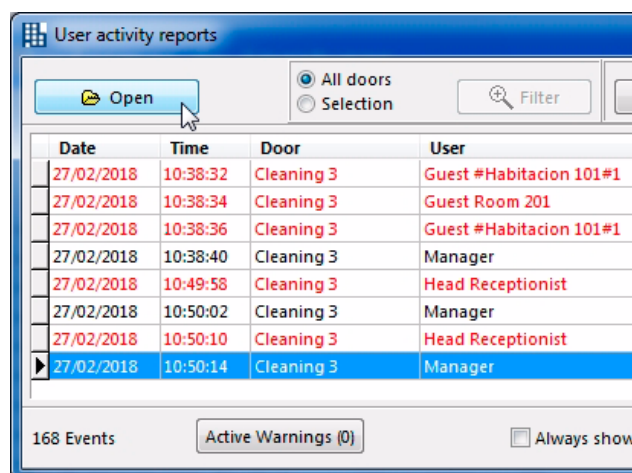
- Export to Excel file:**
 by selecting this option and, then, clicking “OK”, a window will be displayed which allows selecting the location to which you want to export the “Openings.xls” text file, which is created to hold the events.
 It is also possible to modify the name of that file as you wish.



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.

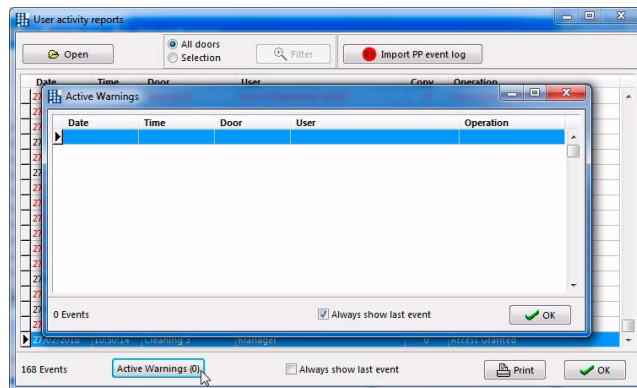


Active Alerts

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.

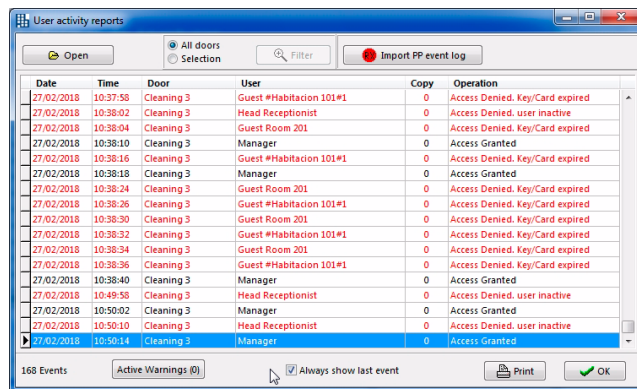
For more information on alerts, see “Alerts” on page 233.



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.

This is useful if the register is very large because, by selecting this check box, the most recent events will be automatically shown.



K.9 PORTABLE PROGRAMMER (P.P.)

The TESA Hotel Reception Menu allows communication with the Portable Programmer (P.P.).

To access the communication form, click on the corresponding button.



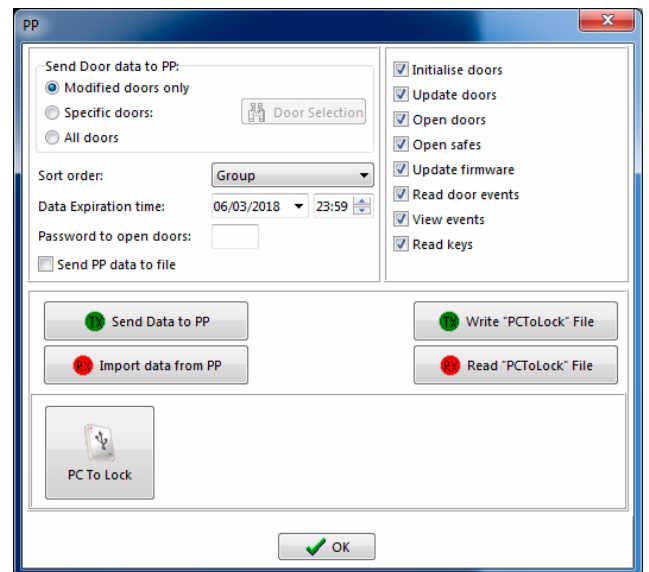
The "PP" screen is displayed:

This screen allows sending of data to the Portable Programmer, and also data reception.

Using the Portable Programmer, the doors are initialized and are sent the locking plan and its modifications.

It is also possible to read the event log of the doors.

For more information, see "1.2 Transmitting and receiving data by means of the portable programmer" on page 142.



K.10 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 TESA Hotel management software, which allows filtering and viewing as desired.

To access the Auditor, click on “Auditor” in the TESA Hotel *Reception Menu*.



The following screen is displayed:

On this screen, all the operations carried out in TESA Hotel 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.

Date	Time	PC	Opera...	Task	Relates to
19/04/2017	19:36:22	RROTS-DB41BI	TESA	Add door	Habitacion 101
19/04/2017	19:49:54	RROTS-DB41BI	TESA	Add door	Habitacion 101-Saf
19/04/2017	19:49:55	RROTS-DB41BI	TESA	Modify door access level	Habitacion 101-Saf
19/04/2017	20:07:17	RROTS-DB41BI	TESA	Add door	Habitacion 102
19/04/2017	20:07:17	RROTS-DB41BI	TESA	Add door	Habitacion 102-Saf
19/04/2017	20:07:17	RROTS-DB41BI	TESA	Add door	Habitacion 103
19/04/2017	20:07:17	RROTS-DB41BI	TESA	Add door	Habitacion 103-Saf
19/04/2017	20:07:17	RROTS-DB41BI	TESA	Add door	Habitacion 104
19/04/2017	20:07:17	RROTS-DB41BI	TESA	Add door	Habitacion 104-Saf
19/04/2017	20:07:18	RROTS-DB41BI	TESA	Add door	Habitacion 105
19/04/2017	20:07:18	RROTS-DB41BI	TESA	Add door	Habitacion 105-Saf
19/04/2017	20:12:24	RROTS-DB41BI	TESA	LOCK	TESA HOSPITALITY
20/04/2017	13:53:43	RROTS-DB41BI	TESA	UNLOCK	TESA HOSPITALITY - Server: localhost [
20/04/2017	17:27:47	RROTS-DB41BI	TESA	Modify door	Habitacion 201
20/04/2017	17:27:47	RROTS-DB41BI	TESA	Modify door name	Habitacion 101 -> Habitacion 201
20/04/2017	17:31:17	RROTS-DB41BI	TESA	Delete door	Habitacion 201-Saf
20/04/2017	17:31:17	RROTS-DB41BI	TESA	Delete door	Habitacion 201
20/04/2017	17:31:44	RROTS-DB41BI	TESA	Add door	Habitacion 101

Just as with the Opening Register, filters can be applied to the information in the Auditor file.

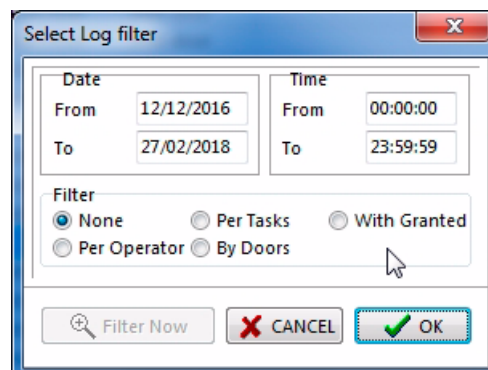
By selecting the option “Selection”, the “Filter” button is enabled in the field “Filter”.



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

This screen allows applying filters:

- by Date and Time,
- by Operator,
- by Tasks,
- by Doors,
- by Safes.



The way to proceed is similar to that for the Openings menu, explained in “Analysis of the openings collected” on page 218.

K.11 LOGIN AND LOGOUT

Clicking “Logout”, on the main screen, 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.12 LOGOUT

In order to exit the programme, click the “Exit” button, which closes the main window.

This is the way to leave the programme.



K.13 CUSTOMIZATION OF MAIN MENU

The main menu can be customized with the logo or name of the hotel or chain, with the contact of your official TESA technical service, etc.

The customisable card is displayed in the upper right-hand corner of the Main Menu.

The customisable card is a graphic file in JPG format in which the desired information, logo or graphic file can be displayed. The file can be created with any graphics editor. It only has to comply with a series of requisites:

- Name of file: logo.jpg
- Recommended size: 567 x 163 pixels
- Recommended resolution: 72 ppi



After creating the file, you simply have to copy it directly into the TESA Hotel software setup directory (b default, C:\Tesa hotel). When the application is opened (TESAHotel.exe) the card is automatically displayed in the upper right-hand corner of the main menu.

The graphic file has to be copied onto all the PCs where the application is installed, regardless of whether it has been installed as a server or as a guest, in the same location.

K.14 SITE MANAGEMENT THROUGH THE WEB

It is also possible to manage the site by means of the Web application, without accessing the TESA Hotel software. For this purpose, it is necessary to have the GlassFish service installed and running.

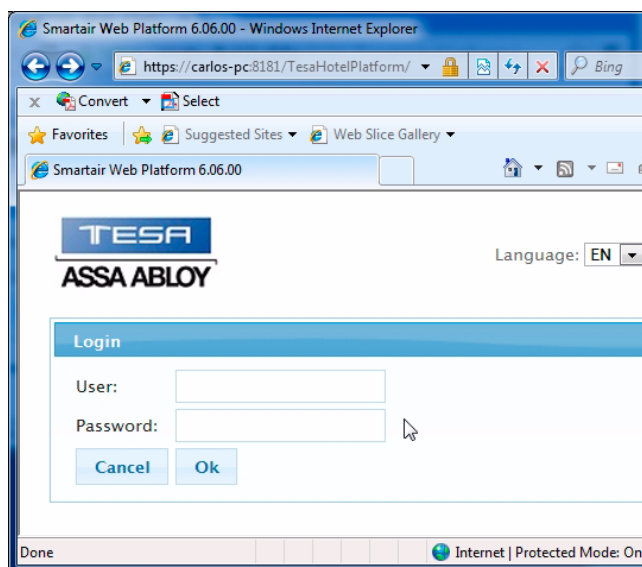
The Web application is accessed through the following URL address:

<https://host:8181/TesaHotelPlatform>

host can be the IP address or name of the server PC

The application is accessed through an operator (User and Password) defined in the TESA 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 TESA Hotel 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 (staff cards)” on page 72.

Sync	User	Group	User ID	Card ID	Expiration
<input type="checkbox"/>	Cleaning 1	CLEANING			
<input type="checkbox"/>	Cleaning 1	CLEANING			03/13/2018
<input type="checkbox"/>	Cleaning 2	CLEANING			
<input type="checkbox"/>	Cleaning 2	CLEANING			03/13/2018
<input type="checkbox"/>	Maintenance 1	MAINTENANCE			
<input type="checkbox"/>	Maintenance 1	MAINTENANCE		DC4E9201	03/14/2018
<input type="checkbox"/>	Maintenance 2	MAINTENANCE			
<input type="checkbox"/>	Maintenance 2	MAINTENANCE		1C289101	03/14/2018
<input type="checkbox"/>	Head Receptionist	MANAGEMENT			
<input type="checkbox"/>	Head Receptionist	MANAGEMENT			03/13/2018
<input type="checkbox"/>	Manager	MANAGEMENT			
<input type="checkbox"/>	Manager	MANAGEMENT		1CA69301	03/13/2018

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 82.

Sync	Door	Group
<input type="checkbox"/>	Elevator	Floor 0
<input type="checkbox"/>	Garage 1	Floor 0
<input type="checkbox"/>	Garage 2	Floor 0
<input type="checkbox"/>	Main	Floor 0
<input type="checkbox"/>	Swimming pool	Floor 0
<input type="checkbox"/>	Cleaning 1	Floor 1
<input type="checkbox"/>	Corridor 1	Floor 1
<input type="checkbox"/>	Room 101	Floor 1
<input type="checkbox"/>	Room 102	Floor 1
<input type="checkbox"/>	Room 103	Floor 1
<input type="checkbox"/>	Room 104	Floor 1
<input type="checkbox"/>	Room 105	Floor 1
<input type="checkbox"/>	Cleaning 2	Floor 2
<input type="checkbox"/>	Corridor 2	Floor 2
<input type="checkbox"/>	Room 201	Floor 2
<input type="checkbox"/>	Room 202	Floor 2
<input type="checkbox"/>	Room 203	Floor 2
<input type="checkbox"/>	Room 204	Floor 2
<input type="checkbox"/>	Room 205	Floor 2

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 114.

Sync	Group	User	Group	Door	Access	Can leave open	Over-privilege
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Elevator	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Elevator	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Garage 1	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Garage 1	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Garage 2	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Garage 2	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Main	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Main	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Swimming pool	<input checked="" type="checkbox"/>	No	No
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 0	Swimming pool	<input checked="" type="checkbox"/>	No	No
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Cleaning 1	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Cleaning 1	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Corridor 1	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Corridor 1	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Room 101	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Room 101	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Room 102	<input type="checkbox"/>		
<input type="checkbox"/>	CLEANING	Cleaning 1	Floor 1	Room 102	<input type="checkbox"/>		

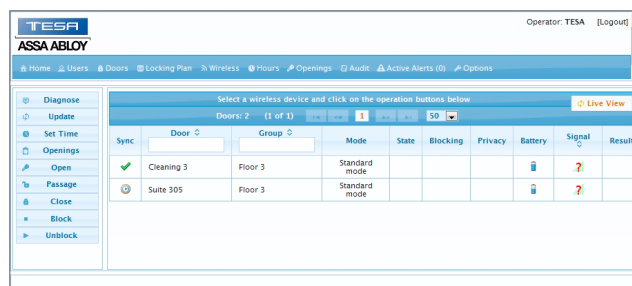


Wireless Doors

It is possible to interact with the wireless devices which have been configured, the following operations being available:

- 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.

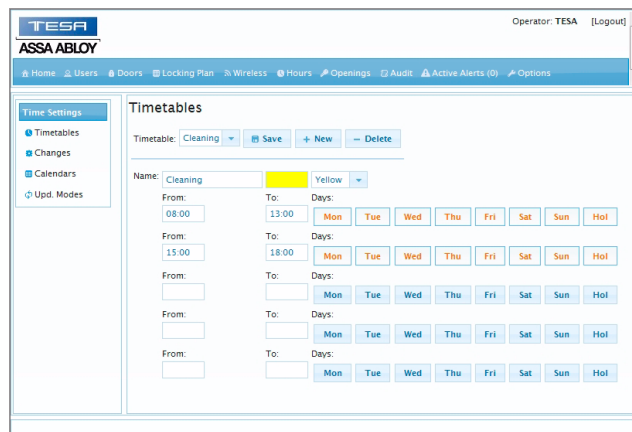
For more information on these functions, see “J.3 Management of wireless devices” on page 178.



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 108.



Openings

The events of the door devices are shown in this tab, it being possible to apply filters.

For more information, see “K.8 Openings” on page 216.

Date	Time	Door	User	Operation
02/27/2018	1:34:46 PM	Suite 305	System	Door data updated by PP or PC
02/27/2018	1:34:46 PM	Suite 305		Real time clock updated by PP or PC
02/27/2018	1:33:16 PM	Suite 305	System	Door data updated by PP or PC
02/27/2018	1:33:16 PM	Suite 305		Real time clock updated by PP or PC
02/27/2018	12:44:10 PM	Suite 305	System Operator	Real time clock updated by PP or PC
02/27/2018	12:42:34 PM	Suite 305	„Suite 305	Granted access
02/27/2018	12:41:56 PM	Suite 305	System	Door data updated by PP or PC
02/27/2018	12:41:56 PM	Suite 305		Real time clock updated by PP or PC
02/27/2018	12:41:46 PM	Suite 305	System	Door data updated by PP or PC
02/27/2018	12:41:46 PM	Suite 305		Real time clock updated by PP or PC
02/27/2018	12:40:36 PM	Suite 305	System	Door data updated by PP or PC
02/27/2018	12:40:36 PM	Suite 305		Real time clock updated by PP or PC
02/27/2018	12:40:14 PM	Suite 305	System Operator	Door initialized

Auditor

The Auditor shows all the operations carried out in the system, as well as who performed them.

For more information, see “K.10 Auditor” on page 226.

Date	Time	Machine	User	Operation	Referred to
02/26/2018	7:55:53 PM	CARLOS-PC	System	Login	Server Initialization
02/26/2018	7:50:33 PM	CARLOS-PC	System Operator	View Auditor	
02/26/2018	7:49:39 PM	CARLOS-PC	System Operator	View Auditor	
02/26/2018	7:49:03 PM	CARLOS-PC	System	Add RF module	RF Autolink, Door: Cleaning 3 (255.0.85, Floor 3 (10.248.196.210))
02/26/2018	7:47:37 PM	CARLOS-PC	System Operator	Delete RF module	Floor 3 - (TESA HOSPITALITY 6.06.00) (S
02/26/2018	7:47:11 PM	CARLOS-PC	System Operator	Delete RF module	Floor 3 - (TESA HOSPITALITY 6.06.00) (S
02/26/2018	7:46:47 PM	CARLOS-PC	System Operator	View Auditor	
02/26/2018	7:44:16 PM	CARLOS-PC	System Operator	View Auditor	
02/26/2018	7:28:56 PM	CARLOS-PC	System	ERROR: Automatic updating of wireless door	ERROR: COMMUNICATION_LOCK, NO Cleaning 3

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	Hub	User	Operation
No records found.					

Settings

- **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 or doors you wish to check and, in the column on the right, select the events desired.

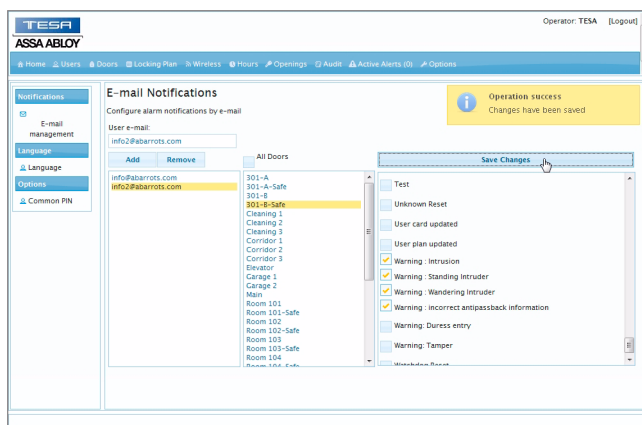
The notifications will be received at the address selected when the events selected take place at the door selected.

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 “License” tab of the “Setup” menu of the TESA Hotel must be selected (for more information, see section “License” tab on page 61).

- **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 67.



L – Other Functions

Introduction	237
Special Functions (Setup menu)	237
Use PMS interface	238
Lock's Audit trail	239
Proximity setup	239
PP asks for password to collect openings	239
Disable event register	241
Manage Esc/Return feature	242
Intelligent Energy Savers (magnetic or proximity)	243
ISO tracks	244
Reports	246
Doors List, Users List (Type 1)	246
Timezones List, Door States List, Holidays List (Type 2)	248
Doors form, Users form, Locking plan of doors Locking plan of users (Type 3)	249
Check In PIN	251
Configuration of the database	251
Use of the Check In PIN functionality from the Reception software	254
Wireless APP	258
Configuration of the database	258
Use of the "Wireless APP" functionality from the Reception Menu	259
Use of the "Wireless APP" functionality from the Web Server (only for master cards).....	264

L – OTHER FUNCTIONS

L.1 INTRODUCTION

TESA Hotel Software has several functions which are not used frequently, but are of great interest on occasions.

Some of them are characteristic of certain setups. 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 these functions mean and how they work.

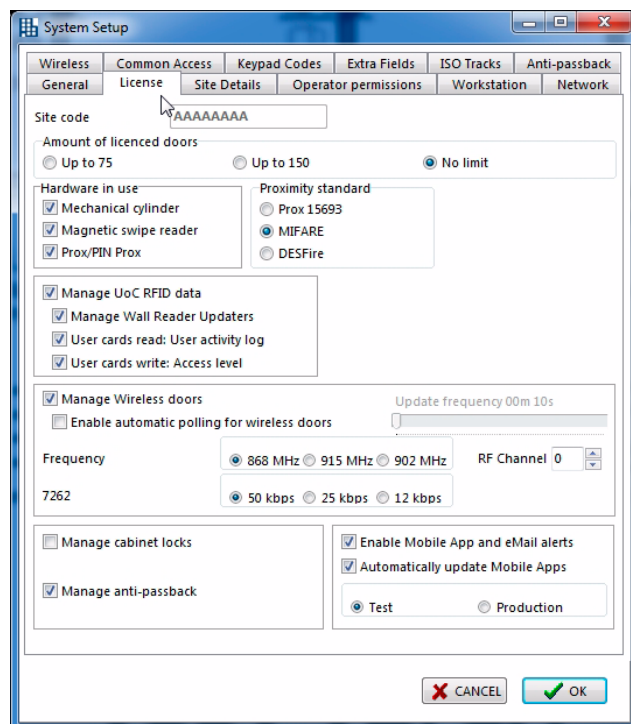


L.2 SPECIAL FUNCTIONS (SETUP MENU)

If TESA 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: "License" 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 "License" 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 "License" tab on page 61.

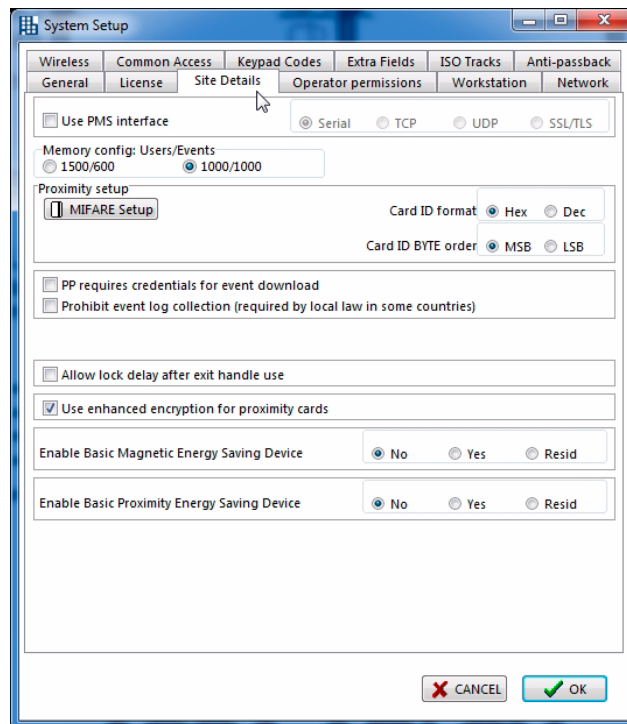


The “Facility” tab allows defining a series of special functions which will only be used in certain specific cases.

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 Esc/Return feature
- Use enhanced encryption for proximity cards
- Magnetic Intelligent Energy Savers
- Proximity Intelligent Energy Savers

These functions are described below.



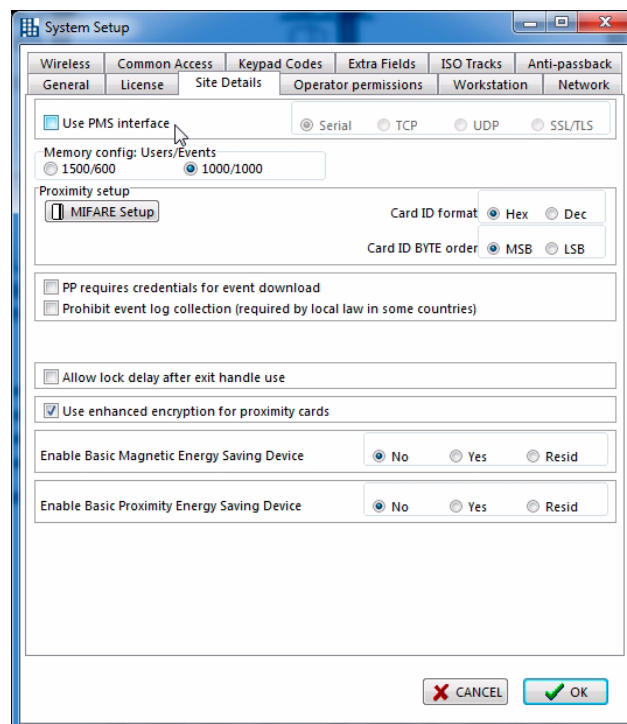
Use PMS interface

On the market, there are systems for the management of hotels for different uses. These systems are called PMS (Property Management Systems).

It may be the case that, in the building where the TESA Hotel 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 TESA Hotel software, but rather prefers to manage it from the PMS management system itself.

TESA Hotel offers the possibility of integrating the 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, consult your distributor or the “PMS Communications” manual.



Lock's Audit trail

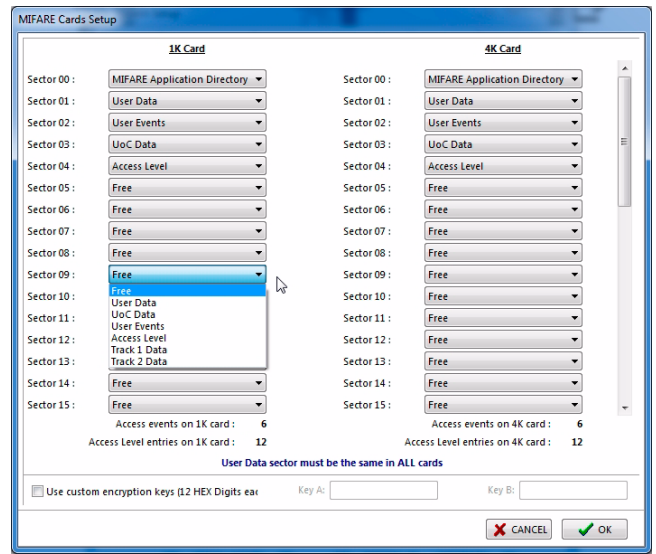
The field "Lock's Audit trail" allows choosing between two settings: Standard and Extended:

- 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. This second Lock's Audit Trail is the most recommended.

Proximity setup

This field allows configuring the cards (Mifare) to calculate how many events and locking plan crosses are stored, as well as for multiapplication with other systems.

For more information, consult the "Read and Write" system manual.



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:

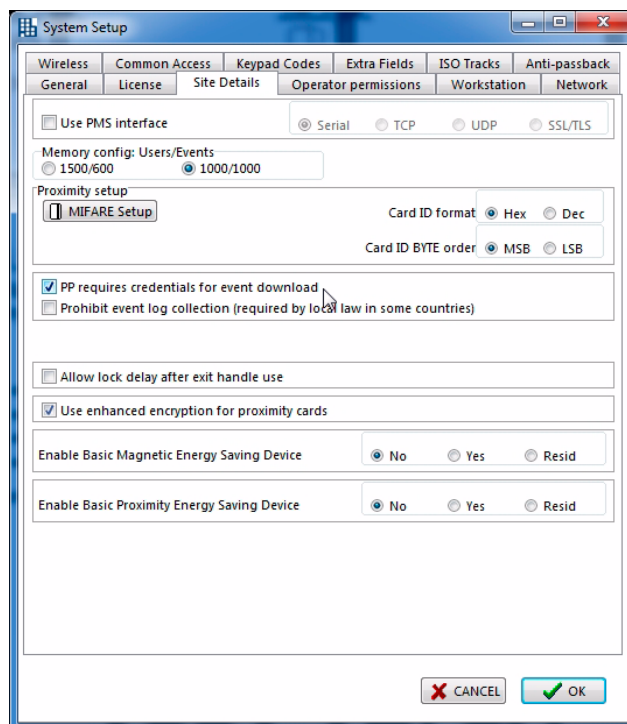
- Viewing the event register in the Portable Programmer.
- Transmitting the information to the PC to view it from the TESA Hotel software.

When the event register of a lock is read, it is not deleted from its memory. 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.

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 TESA Hotel Reception Menu.

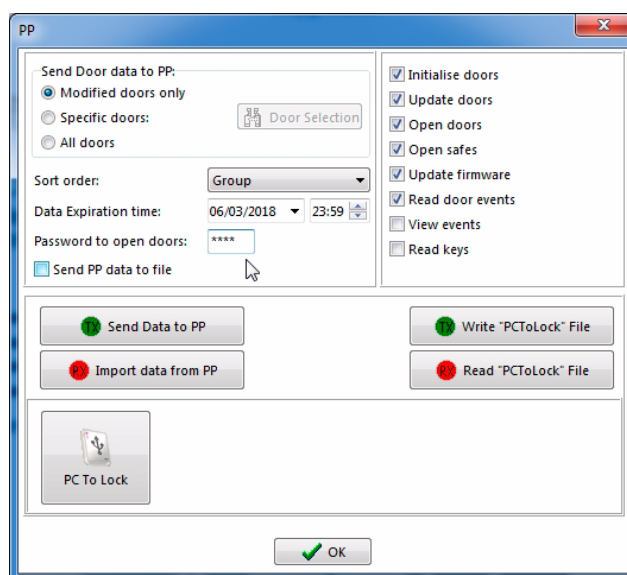
In order to establish this password requirement, carry out the following steps:

- 1 In the “System Setup” menu, “Set-up” tab, tick the option “PP asks for password to collect openings”.
- 2 Click “OK” to accept it.



- 3 In the “PP” menu of the Reception Menu, “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 sending to the PP, where it actually is stored. The next time this window is opened, the default values will be shown again.

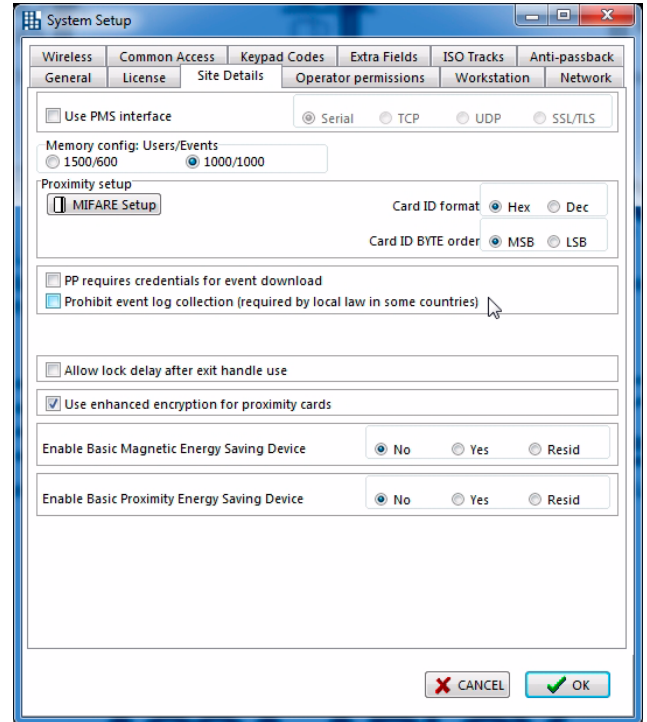


Disable event register

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.

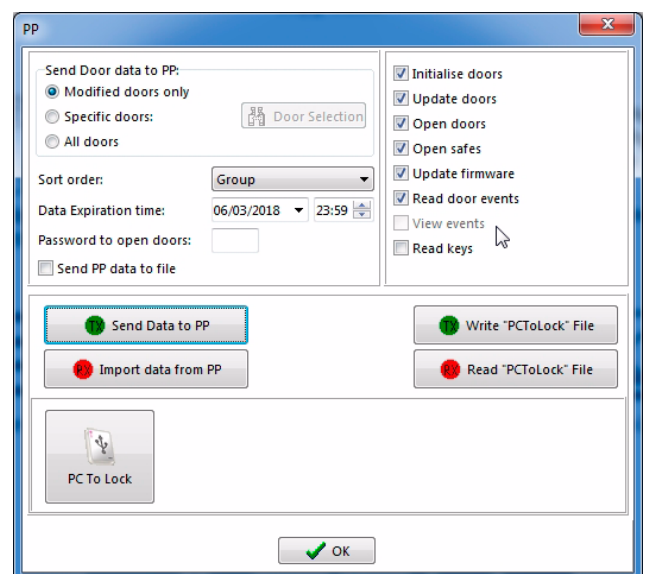
For this reason, the TESA Hotel programme offers the possibility of “Disabling the event register”.

In order to disable this register, tick the option “Prohibit event log collection (required by local law in some countries)” and then, click “OK” to accept it.



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 Reception Menu).
- In the event register of the TESA Hotel software (“Openings” menu), the authorised accesses by the users are not recorded.



Manage Esc/Return feature

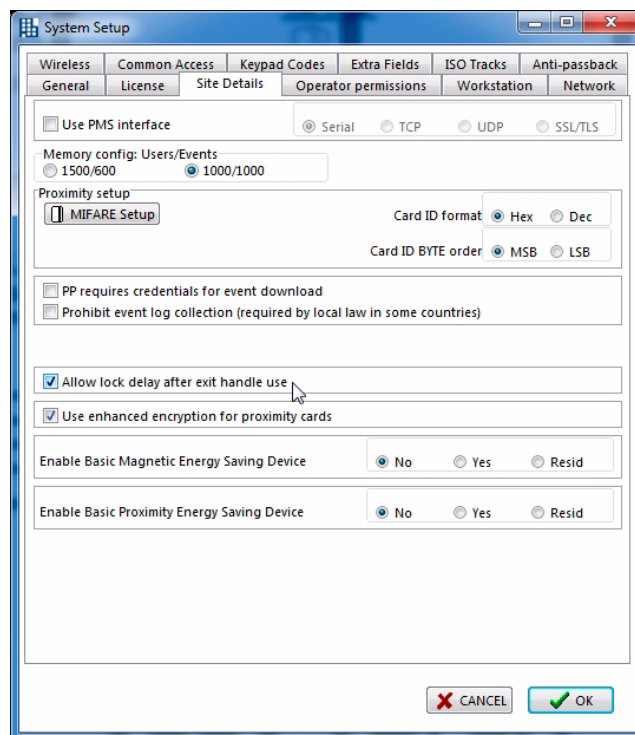
In some European countries, regulations demand that when a user opens a door from the inside, it must remain in a state which allows it to be opened from the outside (as well).

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.

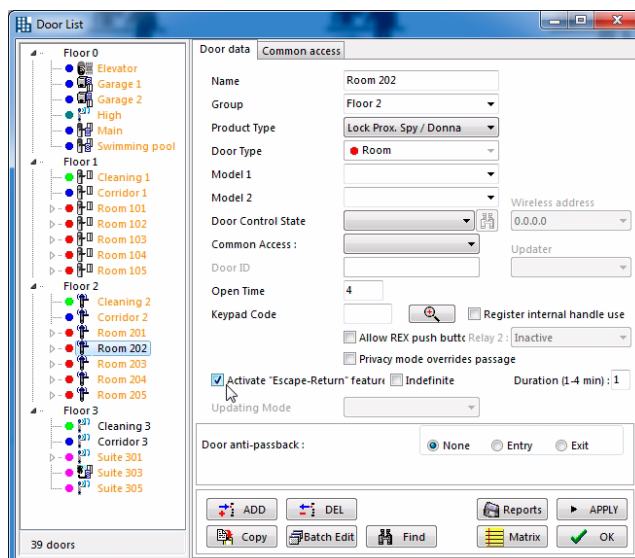
This function is called “Esc/Return”.

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.



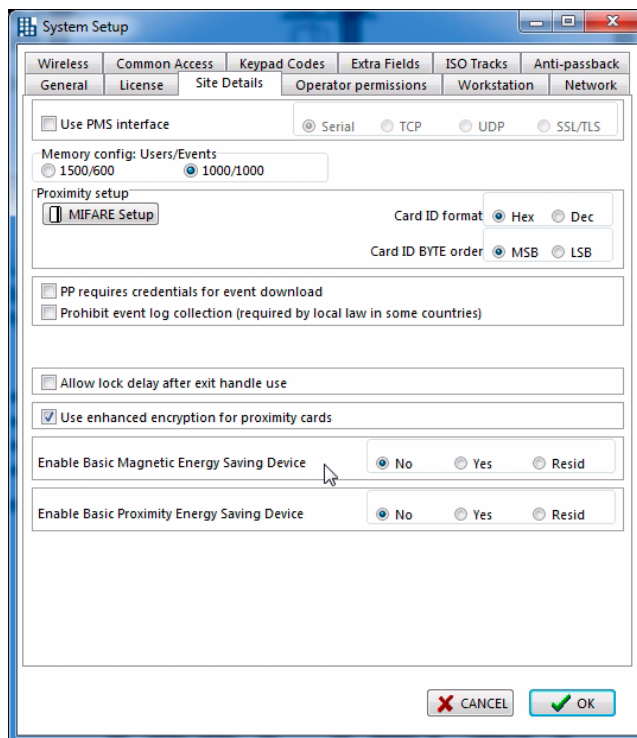
When the function “Esc/Return” is enabled, the field “Activate Esc/Return” is displayed in the “Doors” menu, which allows enabling the function for that door, as well as the field “Indefinite”, which allows leaving the door open indefinitely, and the field “Duration (1...4 min)”, which allows selecting the time it will remain open.



Intelligent Energy Savers (magnetic or proximity)

In the event that the setup has intelligent energy savers, in the Magnetic and/or Proximity Intelligent Energy Savers option, select whether the start-up will be in Basic mode or in Residential mode. The information necessary to use the energy savers, if they are present in the setup, will be encoded in the user cards.

- “Basic” mode generates a system code for all the energy savers in the hotel. Its simplicity makes it the perfect solution for hotels: only the cards of that particular hotel will be recognised by the intelligent energy savers.
- The “Residential” option generates a system code individually for each energy saver. The solution is ideal in some cases, for example, nursing homes, as it prevents residents from being able to exchange cards during their stay to activate the energy savers of rooms other than their own.



For more information, refer to the corresponding instruction manual of the Proximity Intelligent Energy Saver.

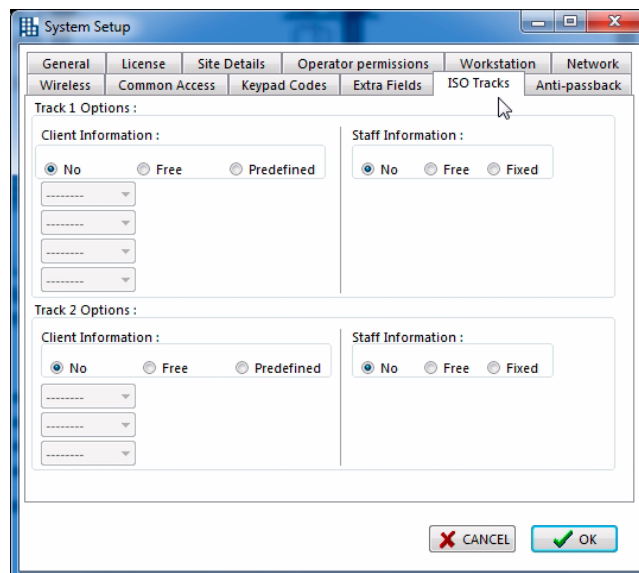
ISO tracks

If magnetic stripe electronic locks are used, the corresponding magnetic stripe cards have three tracks on which the information can be encoded, that can subsequently be read by the locks.

RFID proximity cards do not have any tracks; and have an internal memory instead, but the “ISO Tracks” menu can also be used for this purpose: encoding additional information on the cards so that they are compatible with other systems, for example with TPV systems.

The TESA Hotel system uses only the third of the three tracks a standard magnetic stripe has for the locks, and therefore track 1 and track 2 are left free, allowing them to be codified in accordance with guests' needs.

By default, the system will select the option NO for both track 1 and track 2, both for guests' cards and staff cards.



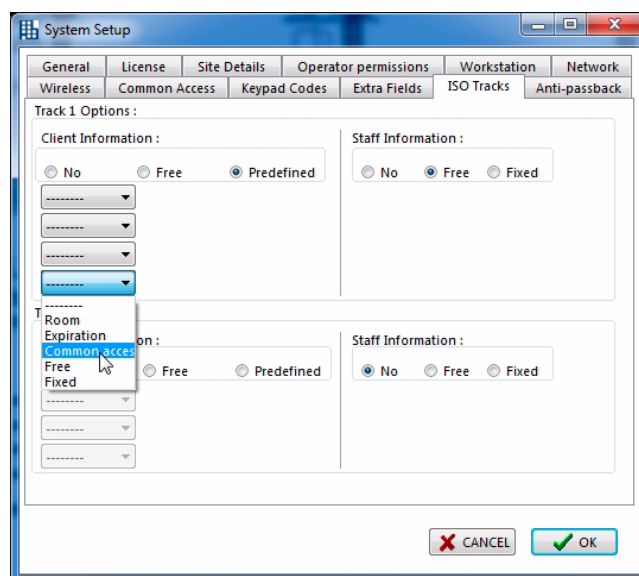
By selecting the “Free” option in “Guest Information”, the selected track can be encoded upon *Check In*.

In the case of “Staff Information”, if the “Free” option is chosen, the selected track can be encoded when the staff cards are encoded.

In “Client Information”, if we select the “Predefined” option, the fields situated directly below will be activated.

Opening these fields gives one the option of using the track to encode the information on Room, Expiry, Grants, Free or Fixed we wish to have available on the guests, in other management systems of the hotel (for example in the Restaurant, etc.).

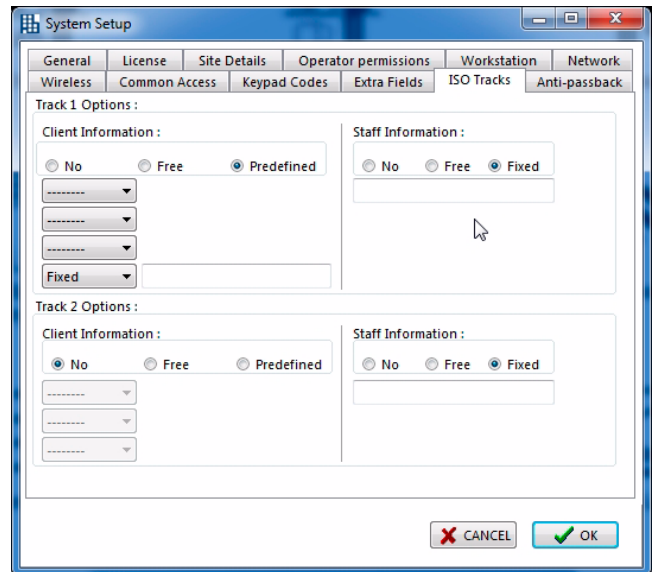
If the “Fixed” option is selected, a new field is displayed in which we can record the hotel guests' code we wish to control.



In “Staff Information”, instead of the “Predefined” option, there is the “Fixed” option.

If this option is selected, a new field is displayed in which we can record the hotel staff code we wish to control.

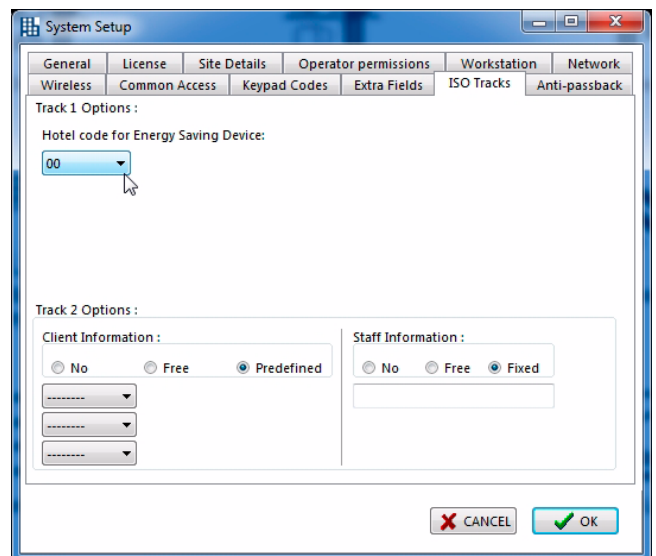
The “Fixed” option can also be selected in “Client Information”, inside the “Predefined” option.



If magnetic intelligent energy savers are used, track 1 is reserved for them.

The “Hotel code for energy savers” identifies a unique system code for the energy savers.

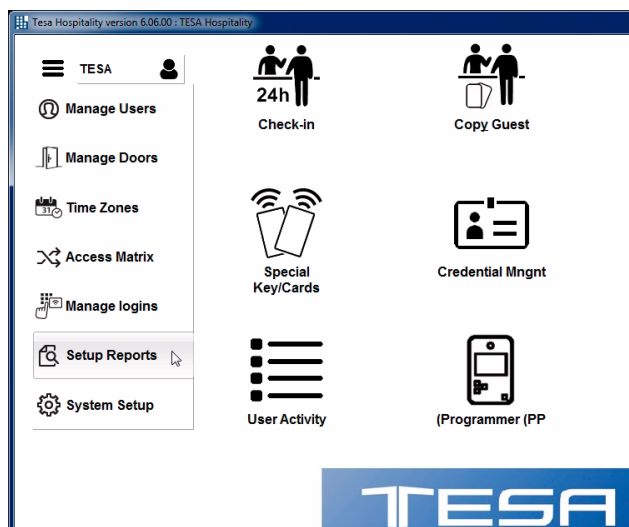
We recommend using a different code for each hotel.



L.3 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.

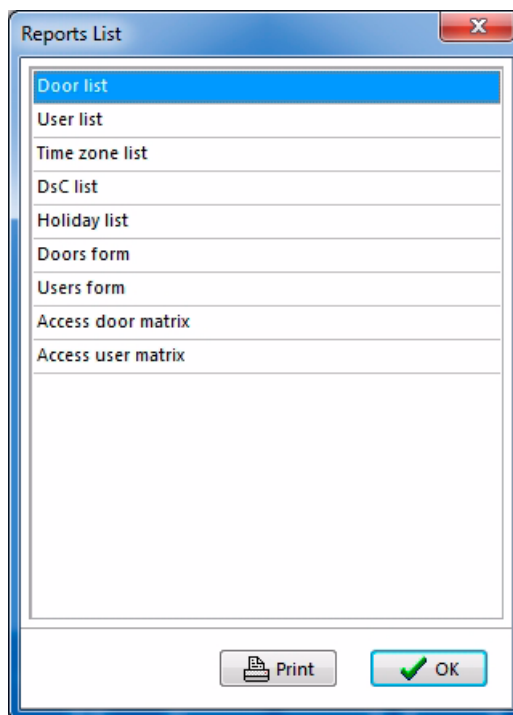
To access the “Reports” screen, in the *Setup Menu* of TESA Hotel, click on “Reports”.



The following screen is displayed:

All the types of reports which can be printed are displayed on this screen.

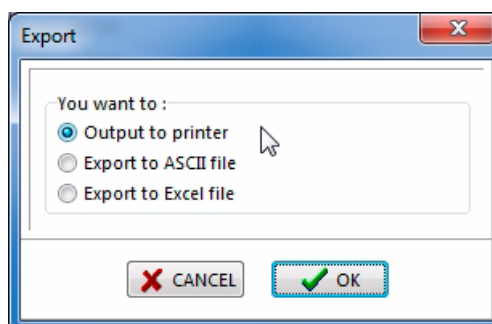
There are three different types of processes to be followed in order to print successfully, depending on the type of report selected. Each of the three types is explained below.



Doors List, Users List (Type 1)

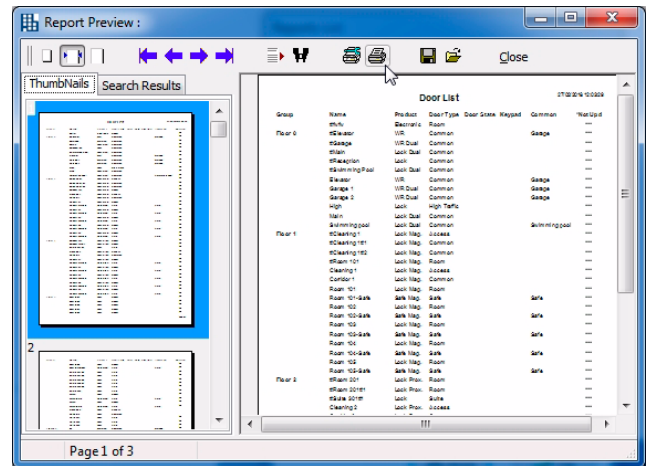
If the Doors List or Users List is selected and the “Print” button is clicked, a screen is displayed where three options are shown:

- Output to printer
- Export to ASCII file
- Export to Excel file



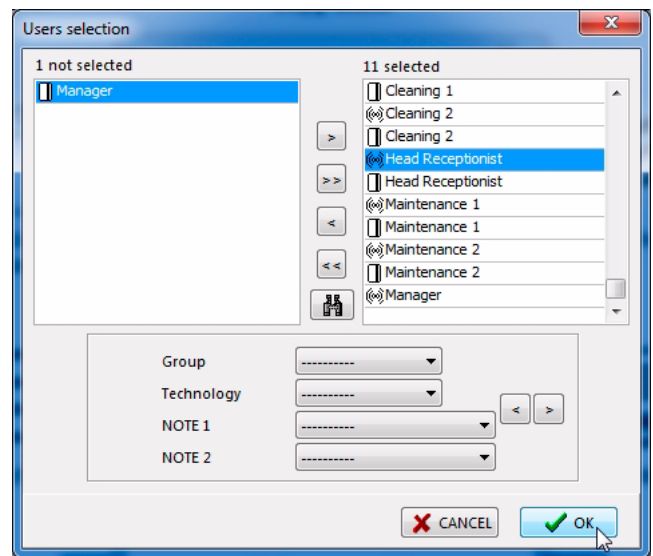
If the option “Output to printer” is selected, a screen is displayed with a preview of what will be sent to the printer.

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.



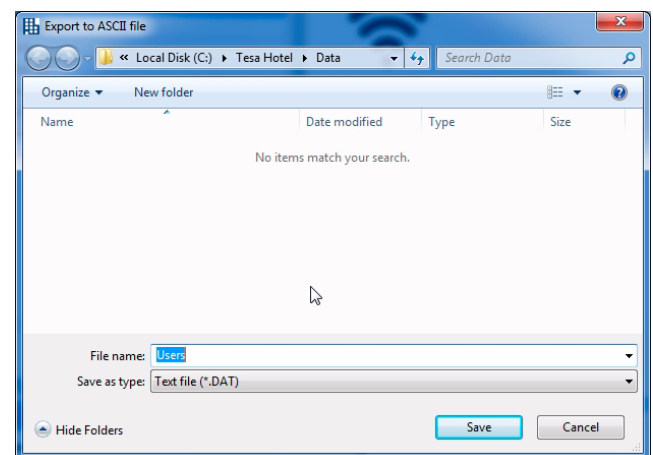
If the option “Export to ASCII file” is selected and the “OK” is clicked, a window is opened which allows selecting the doors (or users) you want to be displayed on the list. By default, all the doors (or users) selected are displayed.

After selecting the doors (or users) you want, click “OK”.

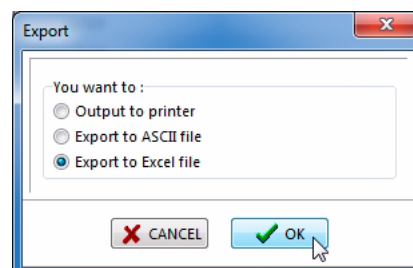


After clicking “OK”, a window is displayed requesting the location to which to save the “Doors.dat” (or “Users.dat”) file.

If you wish, the name of this file can be changed.



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.

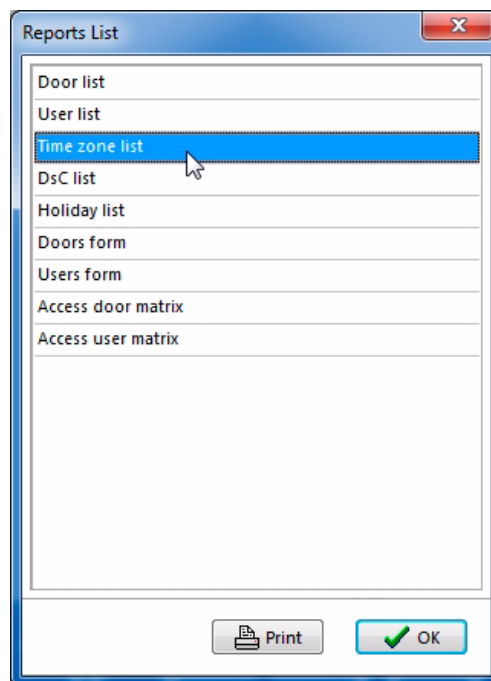


Timezones List, Door States List, Holidays List (Type 2)

If, in the “Reports” window, any of these reports is selected:

- timezones list,
- door states list,
- holidays list,

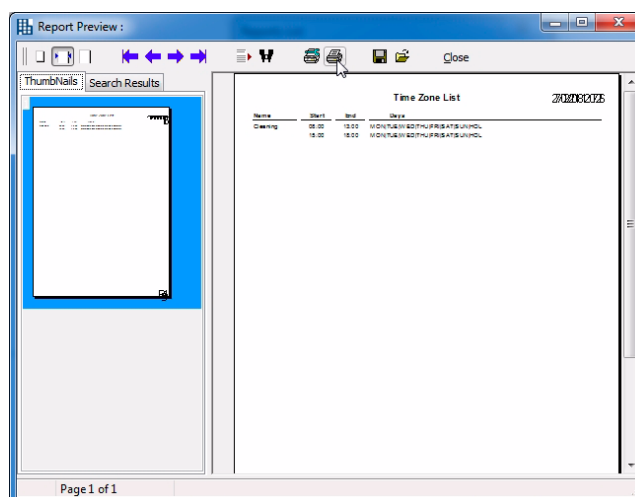
and then “Print” is clicked, a window is displayed showing a preview of what will be sent to the printer.



The window showing the preview allows configuring the printer with the “Printer Setup” button.

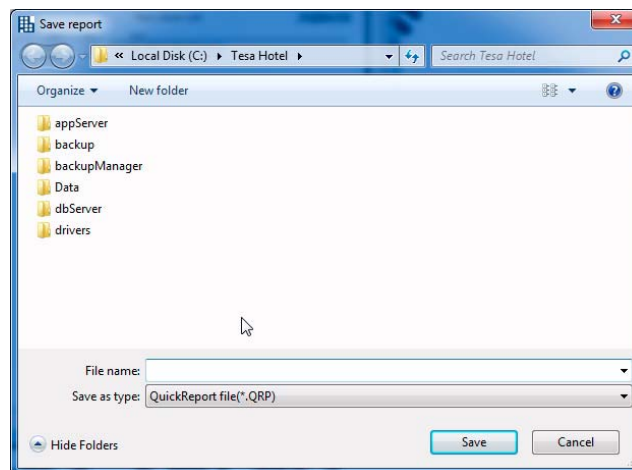
In order to print, click the “Print” button.

Using the corresponding buttons, you can conduct searches for specific pages and texts, which allows you to select what you want to print.



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.

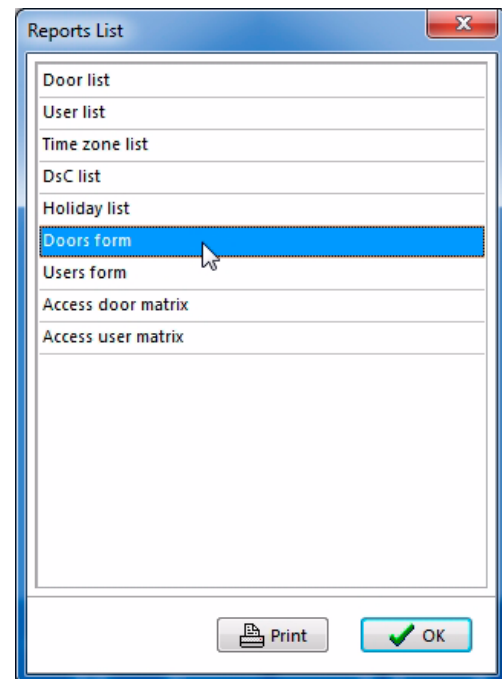


Doors Form, Users Form, Locking Plan for a Door, Locking Plan for a User (Type 3)

If, in the “Reports” window, any of these reports is selected:

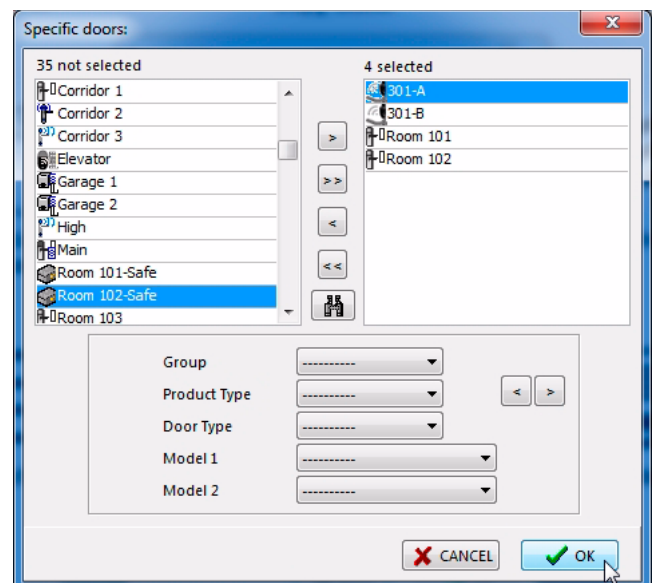
- doors form,
- users form,
- locking plan for a door,
- locking plan for a user,

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”.

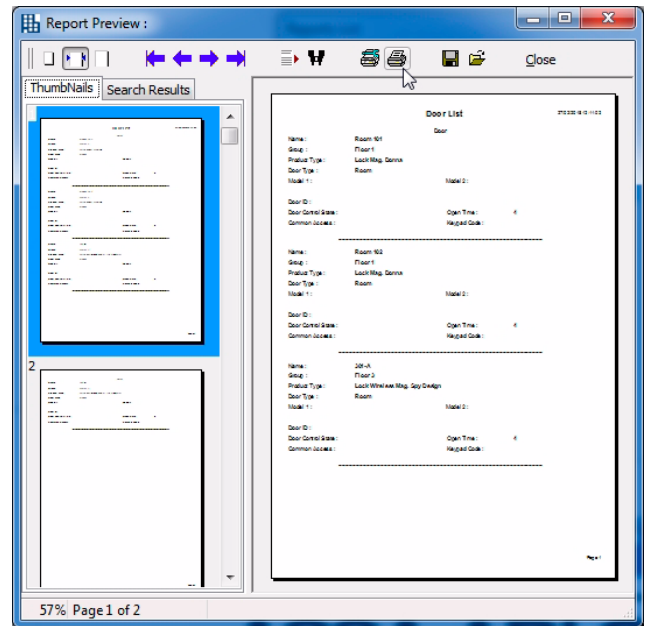


After clicking “OK”, a window is displayed where the preview of what will be sent to the printer is shown.

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 “Print”.

In order to exit without printing, click “Close”.



L.4 CHECK-IN PIN

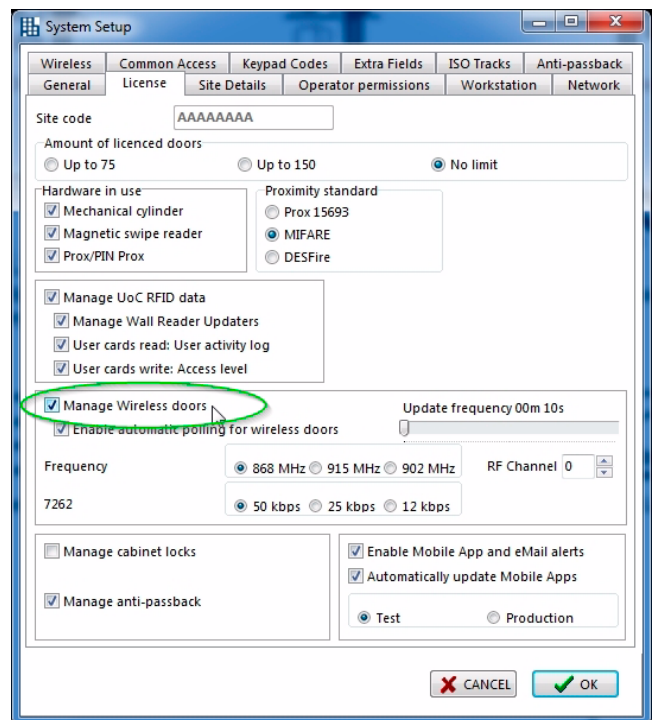
The *Check In PIN* functionality is available for *Wireless V3* devices (locks and wall readers) with a keypad.

In addition to the usual proximity card as a credential for opening electronic locks, in the *Wireless* system, and only for devices with a keypad, the system allows for generation of a keypad code during *Check In* to the room, which will be valid in the door throughout the time the room is occupied by the guest. The system automatically sends the guests an e-mail informing them of the PIN code of the keypad which provides them with access to their room, and of the date/time of arrival and departure for their stay.

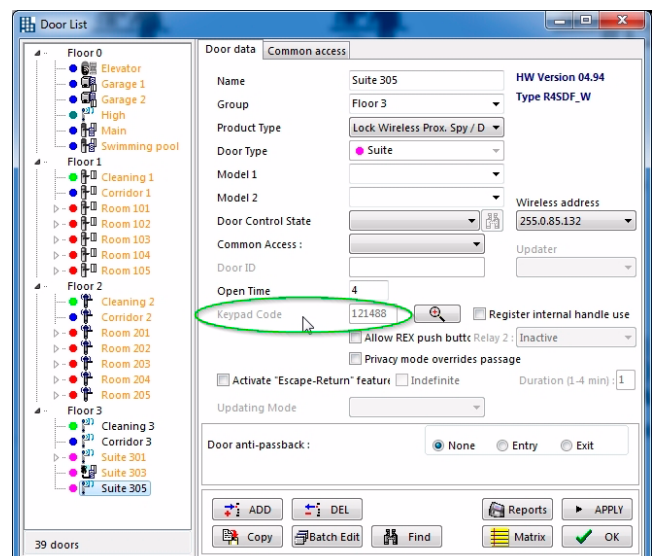
The PIN code is cancelled automatically on the *day/time* of the *Check Out*. In this way, guests can open their lock using both the card and the keyboard assigned to them.

Configuration of the database

- 1 Check that the “Manage wireless doors” option is activated in the “System Setup” menu, “License” tab.

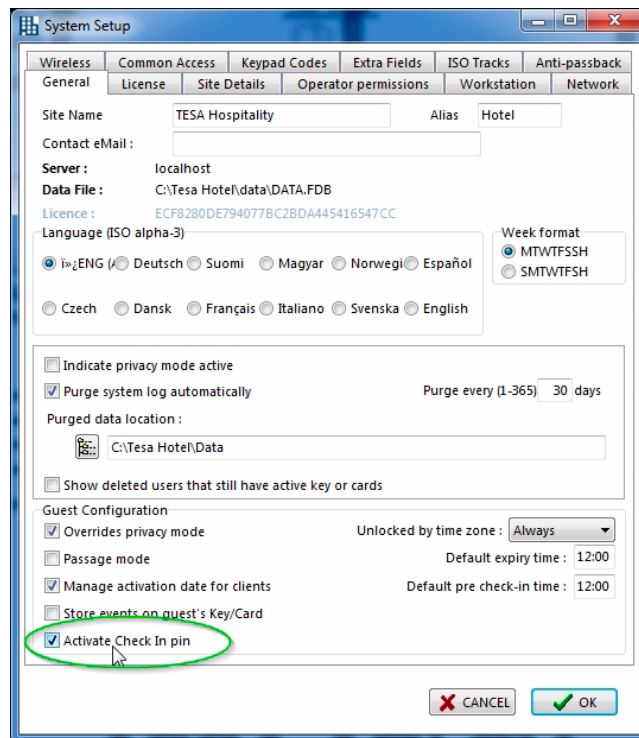


- 2 The “Pin Code” field of the “Door Data” tab in the “Doors list” menu is locked by the system. In it, the *Check In Pin* code will appear when it is created.



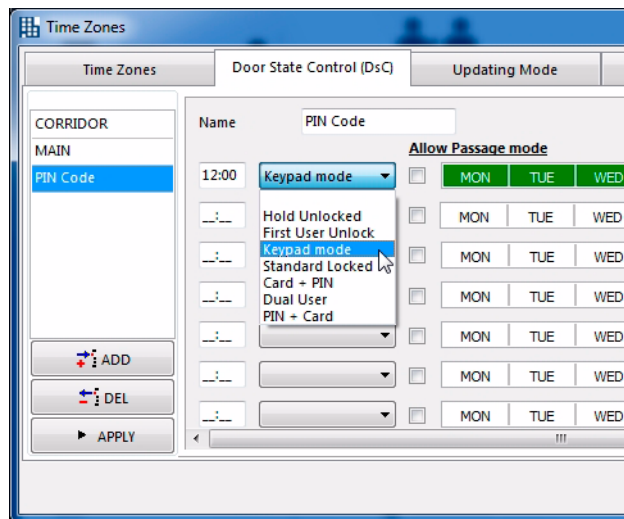
- 3 This “Pin Code” ceases to be editable as soon as the “System Setup” menu, “General” tab, “Activate Check In Pin” is selected.

From this moment on, the “Common Keypad” field will be for the exclusive use of the functionality *Check In PIN*, and it cannot be modified manually.



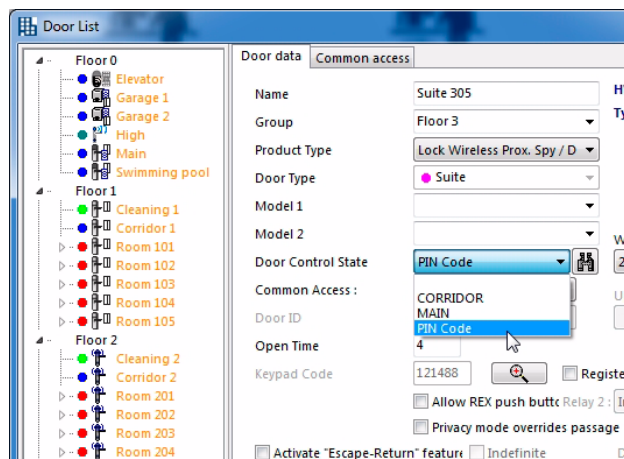
- 4 In order for use of the keypad to start in the wireless lock, an extra configuration must be added to the lock/reader: activate a change of “PIN Code” state in the “Hours” menu.

Access the “Hours” menu, “States” tab and create the new change in state, in the example “PIN Code”. Once this change has been assigned to the locks, it will activate the keypad in them every day of the week at 12:00 pm (on the drop-down menu, the mode is called “PIN Code” = Keypad activated). After activating this mode in the lock, as well as allowing the keypad to be used, this lock will continue to function with the proximity cards, as it did before the state was assigned to it.



After creating this change in state, it must be assigned to all the locks in which we wish to activate the functionality (one by one or all at once by means of the “Batch” button-option), in the “Doors” menu, “Door Data” tab.

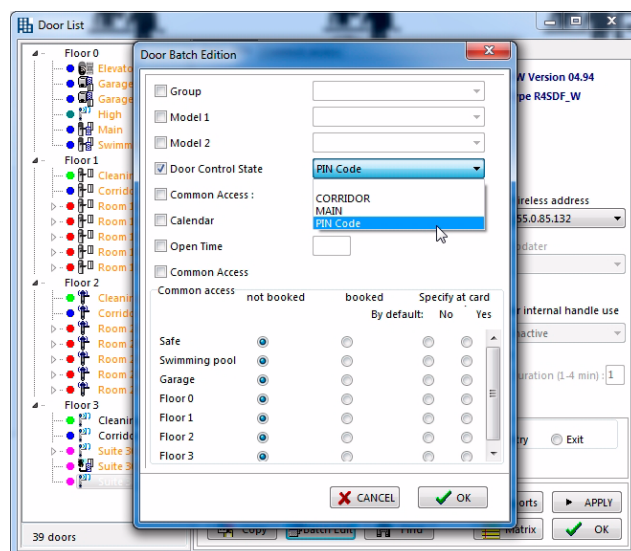
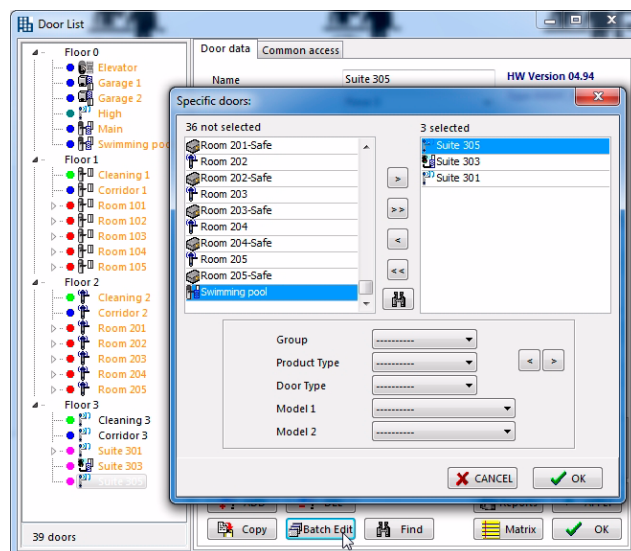
Select the lock in question and assign the “PIN Code” door state you just created in the previous step to it.



The “Batch” button allows you to assign the “PIN Code” state to several doors simultaneously.

After completing assignment of the new state to all the locks, if they are already initialized, they will be automatically updated by the Wireless system. If they have not been initialized, the Portable Programmer must be loaded and the doors initialized.

On the locks, use of the keypads can begin (“Check In PIN” state) as from 12:00 pm on the day in question. If this time has already passed, we have to wait until 12:00 am the following day. If we want use of the keypad to start on the same day, when creating the change in state we must select a moment later than the time when we know all the locks will be updated when their clocks reach said time.



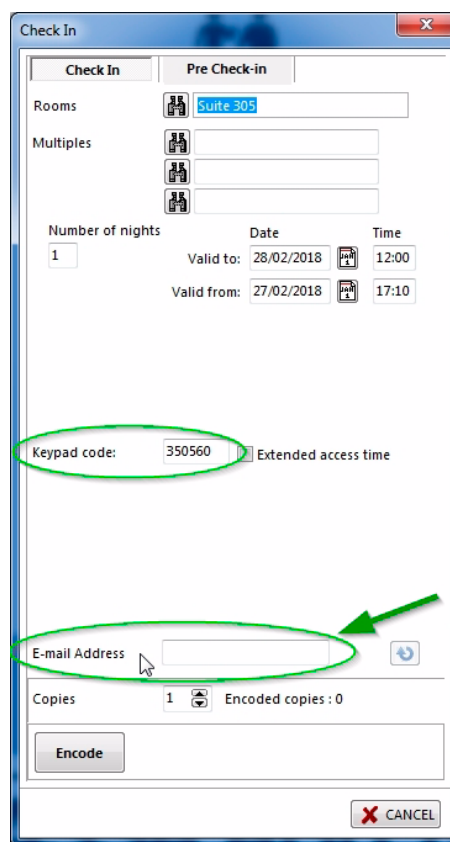
Use of the Check In PIN functionality from the Reception software

The system randomly and automatically assigns a 6-digit PIN code to the lock during generation of the *Check In*.

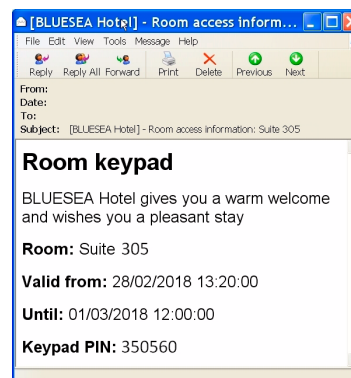
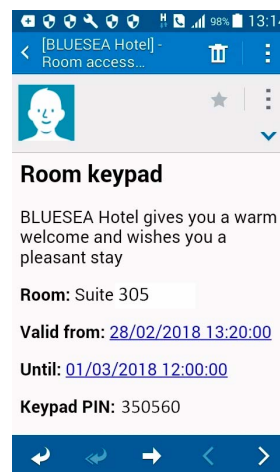
In the “Check In” menu, one can see the automatically-generated PIN code. The PIN code will automatically be sent by wireless to the lock immediately.

If during *Check In* the guest's e-mail is keyed into the “E-mail address” field, said guest will receive an e-mail with the name of the hotel, the room number/name, the dates of activation/expiry and the PIN code of the room. The texts that appear in the e-mail for these fields can be personalised, as shown under point 12 on page 256.

For the web server of the TESA Hotel application to send out the mail, a mail server must previously have been configured in its setup menu (consult section “Configuration of the E-mail Server” on page 38. in chapter “D – Setup”).



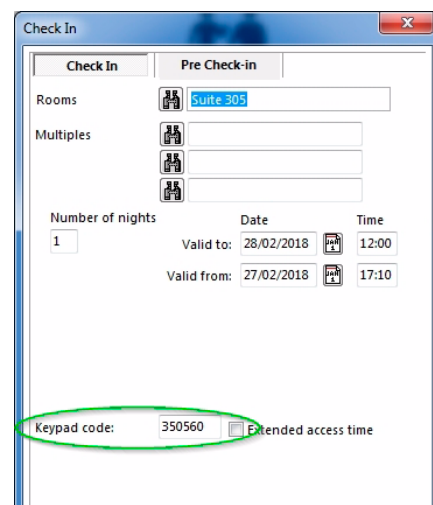
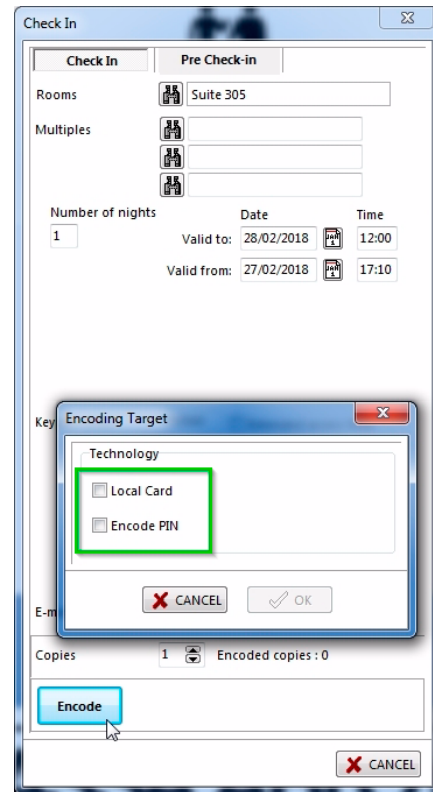
Here are some examples of the mail that reaches the guest (example of mail to mobile phone and example of mail to Outlook):



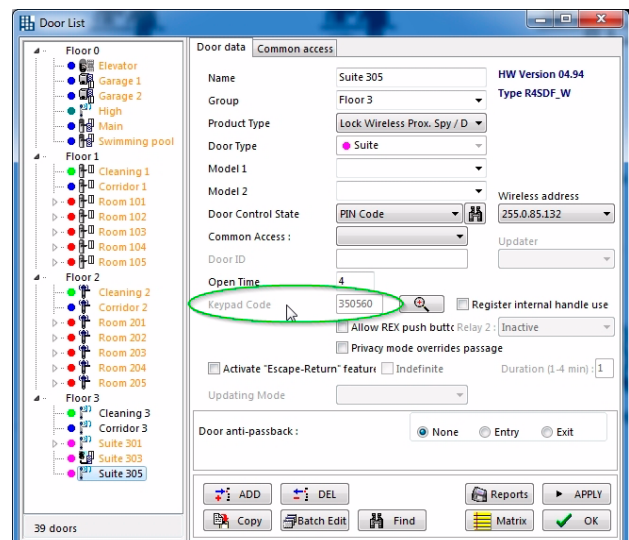
When we click on the “Encode” button, two options are displayed for selection:

- Local Card (encoding of a standard proximity credential in the proximity encoder connected to the USB port of the PC).
- Assign PIN: creation of the PIN Code for the guest of this door (if the “E-mail address” field has been completed, an e-mail will also be sent to the guest with their PIN code information).

It is possible to select either technology or both, without distinction.

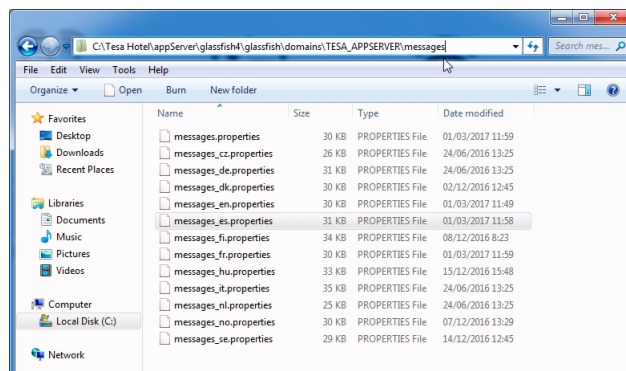


- 5 In the TESA Hotel software, the random PIN code sent to the lock and the guest's e-mail address can be checked by accessing the “Doors” menu, “Door Data” tab, “PIN Code” field.



- 6 When performing the *Check Out* of a room (either automatically or manually, because we wish to delete the guest before the expiry date of the original *Check In*), the PIN will be deleted from the system and updated immediately in the lock by wireless, and the PIN that was being used until then will be invalidated.
- 7 The *Check In PIN* function is not available in the “Guest Copy” menu.
- 8 If a *Pre-Check In* is performed, the PIN code will be activated automatically in the lock on the date and at the time set as the start date for the guest’s stay, that is, when going from *Pre-Check In* to *Check In*.
- 9 A *Check In PIN* invalidates any possible card encoded previously by means of *Check In* of the previous guest for this room.
- 10 A PIN-only *Check In* can be performed. If the Local Card and Assign PIN options are selected, first of all the credential will be encoded in the Proximity Encoder and then the system will create the *Check In PIN*.
- 11 In a lock in which the *Check In PIN* is activated, if electronic privacy is enabled from the inside, said electronic privacy does not restrict access to any user (guest or common staff PINs) who tries to open the door using only the keypad code. Before showing the green door open signal, the keypad signals that electronic privacy is set from the inside by means of brief red flashing.

- 12 The mail texts sent to the guest automatically can be modified so as to customise the welcome message, for example.



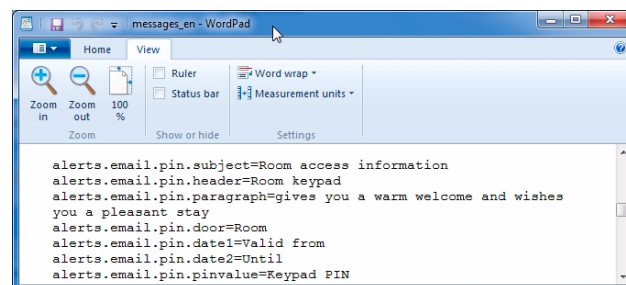
The file to be modified is in the following location:

C:\Tesa Hotel\appServer\glassfish4\glassfish\domains\TESA_APPSERVER\messages
 (C:\Tesa Hotel is the directory in which the application is initially installed)

Open the “messages_es” file (*Properties*-type file) if you wish to modify the texts in Spanish (_es), and search for the text lines that appear on the adjacent screen.

The texts displayed after the “=” can be modified to appear in the e-mail that is automatically sent to the guest during the Check In PIN.

For other languages, open the messages file of the corresponding language (_en: English, _fr: French, etc.).



Here is an example is the mail received, with the texts that can be modified in blue.

From:
Date:
To:
Subject: [BLUESEA Hotel] - Room access information: Suite 305

Room keypad

BLUE
BLUESEA Hotel gives you a warm
welcome and wishes you a pleasant stay

Room: Suite 305

Valid from: 28/02/2018 21:00:00

Until: 01/03/2018 12:00:00

Keypad PIN: 396149

L.5 WIRELESS APP

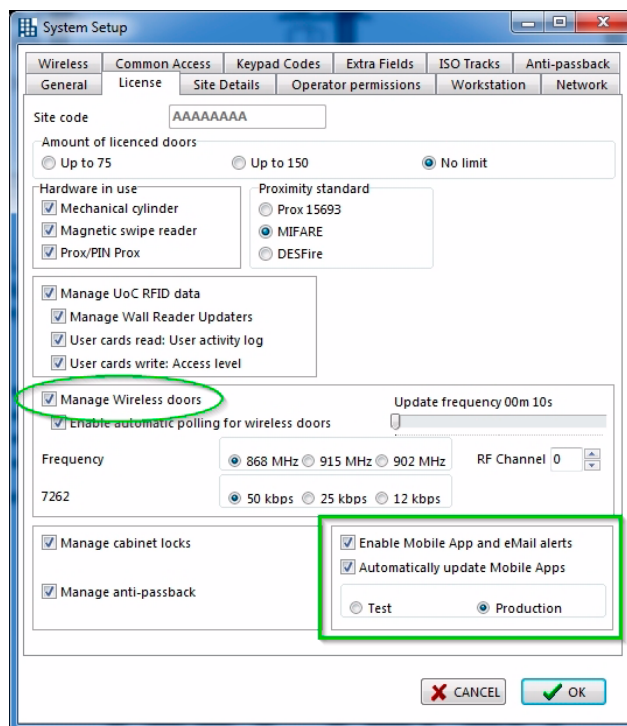
The TESA Hotel App allows hotel staff and guests to open the Wireless locks remotely from their *smartphone*, simply and safely.

During the *Check In* of the room and now via an e-mail from an end user, with which they have registered in the App, we can send a *push* notification to the *smartphone* with the user's credential. The credential will add the doors with wireless locks the user has access to into the App. The key will automatically disappear from the App when the expiry date is reached (or after completion of *Check Out*).

As well as the usual proximity card as a credential to open electronic locks, the Wireless system allows generation, during *Check In*, of an e-mail with the credential for dispatch to an e-mail account with which the user has registered after downloading the "TESA Hotel" App from any of the *markets* for Android or iOS. The App user will receive a notification that will add the key to the App to open the Wireless locks. This key on the App will be valid for the door for the time the room is occupied by the guest (or upon expiry of the staff credential).

Configuration of the database

- 1 In the "Setup" menu, "License" tab, check that both the "Manage Wireless doors" option and "Automatically update Mobile Apps" option are activated.
- 2 Also check that the "Production" field is ticked.



Use of the “Wireless APP” functionality from the Reception Menu

Before a key can be sent to a *smartphone*, the user (either a guest or hotel staff) must download the “TESA Hotel” App from the *markets* and register in it with an e-mail address, preferably one they can manage from the same *smartphone* onto which they have downloaded the App.

To download and register in the App, consult the end user's guide, “Quick Guide for Downloading and Using the TESA Hotel App”.

To send the credential to the App, after the end user has downloaded it and registered, follow the steps indicated below:

- 1 Configure a mail server in the Setup menu of the Web Server application (consult the section “Configuration of the E-mail Server” on page 38. in the chapter “D – Setup”).

- 2 In the “Check In”, “Pre-Check In”, “Copy Guest” and “User” menu, a new field is displayed, called “E-mail address”.


In this field, type the user's e-mail (guest or hotel staff) to which the *push* notification will be sent.

The screenshot shows the 'Check In' window with the 'E-mail Address' field highlighted by a green oval. The window includes fields for Rooms (Suite 305), Multiples, Number of nights (1), Date (26/02/2018), Time (12:00), Keypad code (215311), and an 'Encode' button.

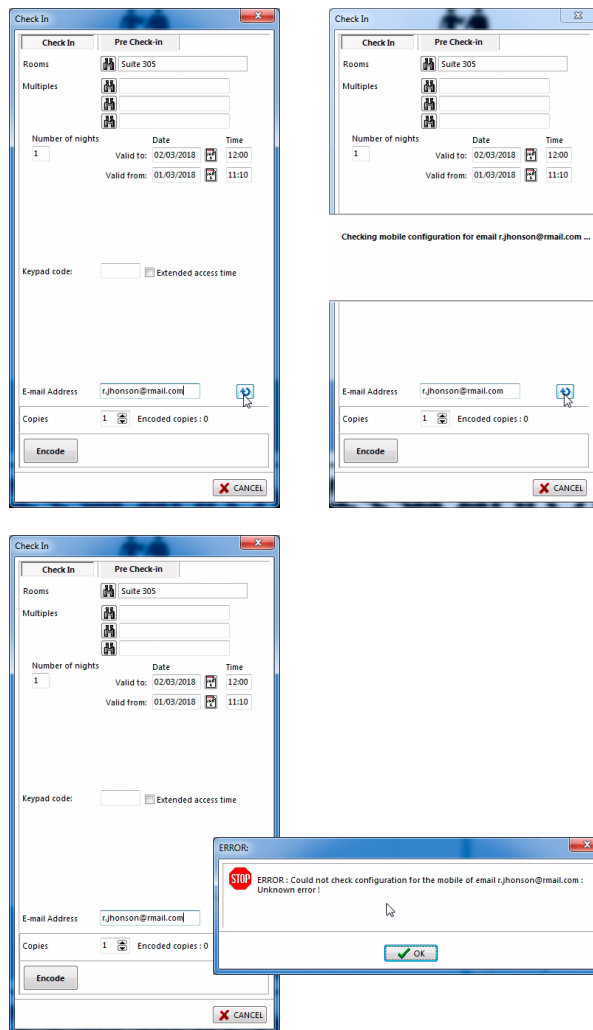
The screenshot shows the 'Pre Check-in' window with the 'E-mail Address' field highlighted by a green oval. The window includes fields for Rooms (Suite 305), Multiples, Number of nights (1), Date (01/03/2018), Time (12:00), Keypad code (251628), and an 'Encode' button.

The screenshot shows the 'Copy Guest' window with the 'E-mail Address' field highlighted by a green oval. The window includes fields for Rooms (Suite 305), Number of nights (1), Date (26/02/2018), Time (13:10), Keypad code (200890), and an 'Encode' button.

The screenshot shows the 'Staff list' window with the 'E-mail Address' field highlighted by a green oval. The window displays a list of staff members and their details, including Name (Head Receptionist), Technology (Key), Group (MANAGEMENT), Card ID (7CB49E01), and User ID. It also includes fields for Valid to (13/03/2018), Valid from (26/02/2018), Keypad code (*****), and an 'Encode' button.

- After filling in this field with the e-mail address, it is recommended you check whether the e-mail/user of the App to whom the credential will be sent has downloaded the App and has registered correctly using it, using this same e-mail address. To do so, before sending the key, check by pressing the button .

The system will perform a quick on-line check to see whether that e-mail address/user is capable of receiving the credential on their App or not.

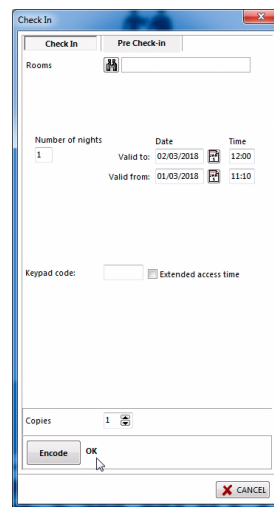
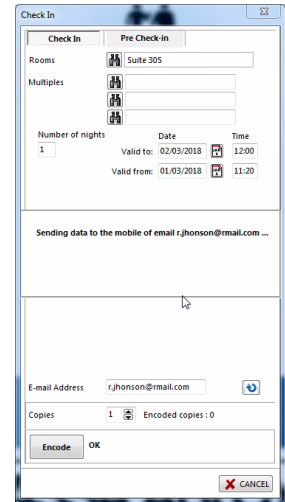
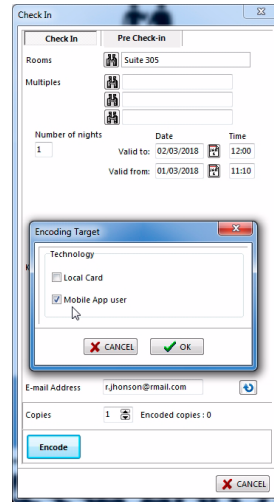


- 4 After performing the check (which is not indispensable), we proceed to encode the credential.

After completing the e-mail field, "E-mail Address", and clicking on the "Encode" button, two options will appear for selection:

- Local Card (encoding of a standard proximity credential in the proximity encoder connected to the USB port of the PC).
- Wireless App: dispatch of the credential to the guest/staff user of the door/s in question.

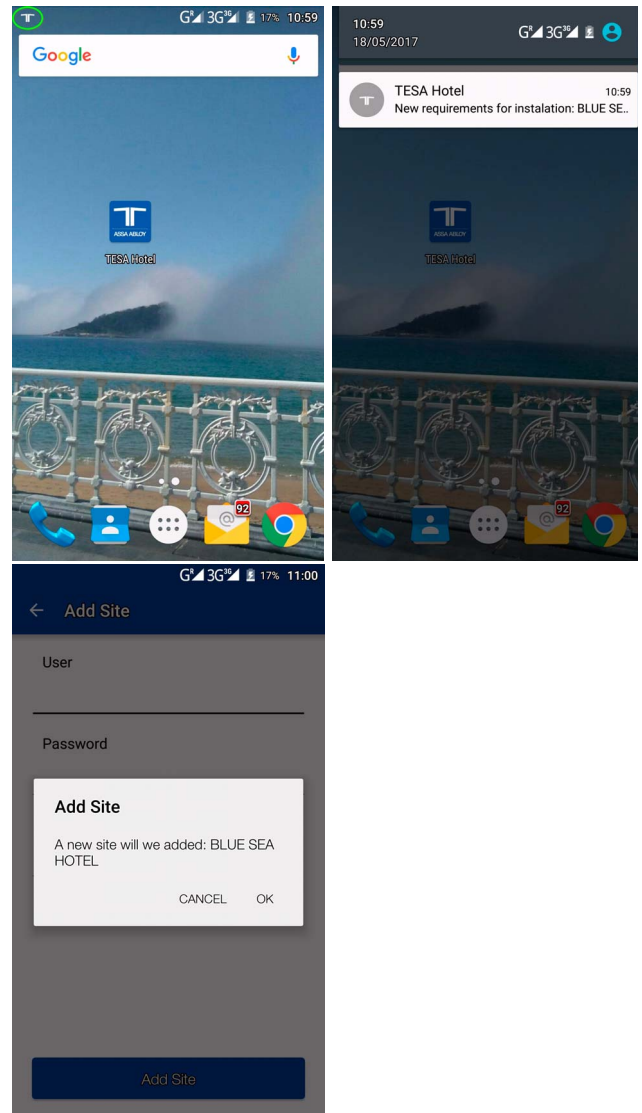
It is possible to select either technology or both, without distinction.



- 5 If the encoding is correct, the key will be sent to the App on the *smart-phone* registered and the user will receive a *push* notification on the screen, as shown in the example.

When the grants for installation of the notification are accepted, the TESA Hotel App will open automatically, asking for permission to add the new “Installation”/key.


After installation of the key has been accepted, the user can now utilise the App with their key to open the doors they have access to.



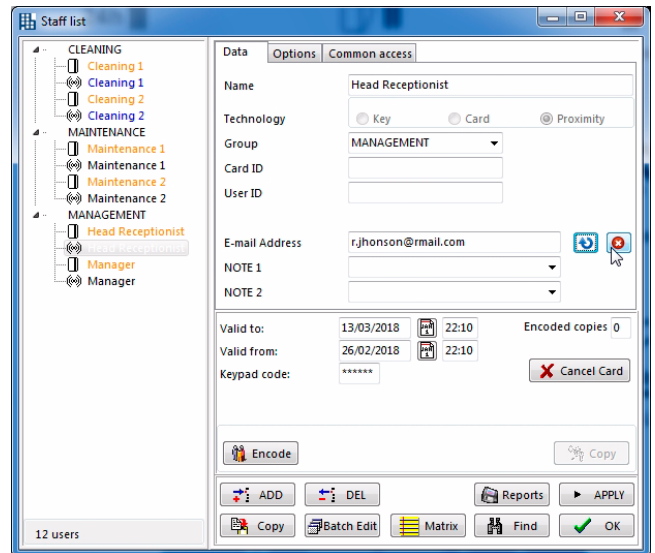
For information on use of the App, see the “Quick Guide for Downloading and Using the TESA Hotel App”.

- Español: www.tesa.es/hotel_app_guiausuario
- English: www.tesa.es/hotel_app_userguide
- Français: www.tesa.es/hotel_app_guideutilisateur

- 6 The procedure is the same for sending the staff keys to the installation employees (staff cards), accessing the “Users” menu of the TESA Hotel software configuration.
- 7 When performing the *Check Out* of a room (either automatically or manually, because we wish to delete the guest before the expiry date of the original *Check In*), the App credential will be deleted from the system and updated immediately in the lock by wireless, and the guest's access via the App will be invalidated.
- 8 If a *Pre-Check In* is performed, the credential will be activated automatically in the App on the date and at the time set as the start date for the guest's stay, that is, when going from *Pre-Check In* to *Check In*. In this way, the user does not receive the *push* notification until the date/time of *Check In* of their key.
- 9 A new *Check In* invalidates the key of the App (as does a new encoded card).

- To cancel/revoke a credential of a staff card on the App in real time, all one has to do is enter the Setup Menu of the TESA Hotel application, "Users" menu, and select the user one wishes to cancel from the List of Staff Keys, and finally click on the button .

The software will display a confirmation message when the action has been completed.



Sending data to the mobile of email r.jhonson@mail.com ...

Use of the “Wireless APP” functionality from the Web Server (only for staff cards)

This section describes how to send staff keys from the Web Server via the internet browser (it is not possible to send Check In - Guest cards).

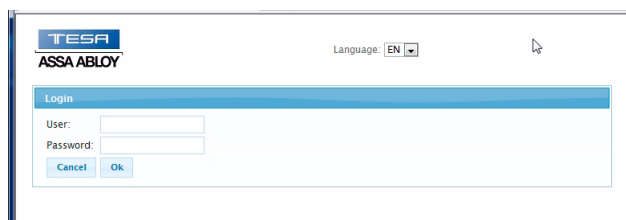
In this case, when the cards are sent from the Web Server or the user's App, they do not behave in the same way as if they had been sent/encoded using the reception software. In this case, the key sent to the App as a staff card does NOT cancel a staff card of the same user in the event that one is encoded previously.

- 1 Adding and checking a user through their e-mail.

To do this, first of all access the user menu of the Web Server by entering the URL address of the Web Server's user menu into the internet browser.

(for example: [https://localhost:8181\TesaHotelPlatform](https://localhost:8181/TesaHotelPlatform)).

Access with a user and password with a level valid for encoding or modifying users of staff cards/keys.



- 2 Access the “Users” menu, “Mobile app user” field and type in the e-mail of the user of the staff card.

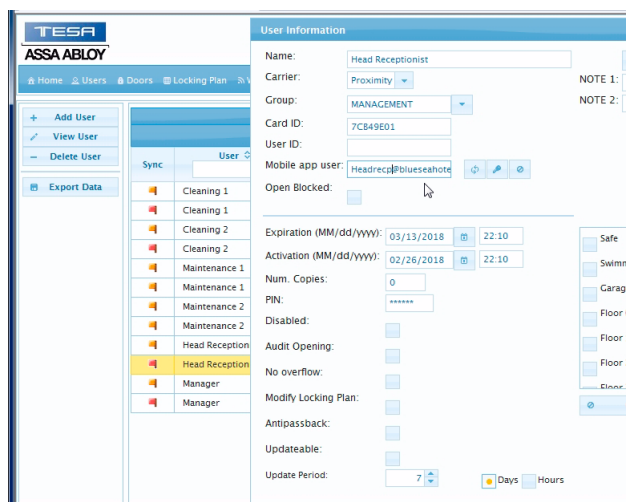
To check that the user has registered on the TESA Hotel App correctly, click on the “Refresh” button



To see how to register a user on the App, consult the “Quick Guide for Downloading and Using the TESA Hotel App” document.

If the user is not registered correctly, a “Stop” icon will be displayed next to the e-mail address.

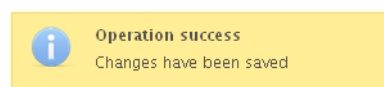
If the user has already downloaded the App and registered correctly, an “Ok” icon will be displayed next to the e-mail address.



- 3 To send the key to the user's App, click on the “Send” button.



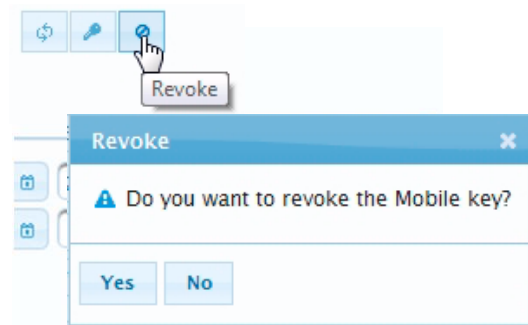
The Web Server will show the correct dispatch of the key to the App with the message “Operation Correct”.



- 4 To delete/eliminate a key on the App from the Web Server application, click on the "Revoke" button of the user to be deleted.

A confirmation message will be displayed; accept the revocation.

The key will be deleted from the user's App.



ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience



ASSA ABLOY

We are one of the largest manufacturers and suppliers worldwide of closure and access control solutions for hotels. Leaders in the hospitality market: hotels, student residences, geriatrics... We offer the unique electronic locks system with an integral solution. We are backed by 30 years of experience in developing electronic systems for hotels.

In TESA ASSA ABLOY we devise products that have allowed us to expand and be present in more than 70 countries, offering our quality and cutting-edge services to the global market in the 21st century. We do not stop thinking about the necessity of our clients and work on the development of the systems of the future: our ideas are destined to revolutionize access control systems in the hotel world as they are known today. TESA ASSA ABLOY is an accredited brand after more than 75 years, whose range of electronic products (locks, wall readers, safes or electronic cylinders) is complemented with a complete catalog of mechanical products including panic exit devices, mechanical cylinders, security locks, knobs and handles, door closers, electromechanical and electromagnetic solutions and armored doors.

We have developed a complete access control system for the hotel that offers an intelligent, safe, friendly, reliable and elegant evolution.

TESA ASSA ABLOY always one step ahead.

Talleres de Escoriaza S.A.U.
Barrio de ventas 35
20305 Irun
Gipuzkoa · España
T: +34 943 669 100
tesalocks@tesa.es
www.tesa.es/hotel