SALTO

inspiredaccess

www.saltosystems.com

Pro-Access READ/ WRITE ACCESS CONTROL

User Manual V. 11.04.x.x

1. INTRODUCTION: 8

2. PROGRAM INSTALLATION 10

MDAC 10

MDAC Installation on your system 11

SQL MS Server 12

3. SALTO SERVICE RW 26

4. SOFTWARE OPERATORS AND COMPETENCIES 33

Creating a new DB 33

Migrating an existing MS-Access DB to a MS-SQLServer DB 36

Operator competencies 37

IMPORT TOOL 43

Data type 43

Text file 44

Excel file 45

IMPORT FROM A SALTO DB (Merging) 48

Origin of the DB 49

Invalid DB version 50

IMPORTANT notes 50

5. EXPORT: 51

6. ADMINISTRATOR OPERATOR 54

Doors 55

Limited User Access 71

Zones 73

OUTPUTS 79

Automatic Outputs: 81

TIME PERIODS. 82

TIME ZONES. 85

CALENDARS 87

TIME CHANGE. 90

OUTPUT LIST FOR ELECTRONIC SAVING DEVICES (ESD) 92

Automatic changes 93

USERS ACCESS LEVELS 98

USERS LIST 106

User key assignment 118

Lockers 123
Define Lockers: 123
Define Free Assignment Zones: 125
Free Assignment Zone: 125
Multiple Free Assignment Zones: 125
Free Closing: 127
Types of Keys: 127
Time-limited Occupancy: 128
Lockers & Visitors: 128
Locker Initialization: 129

Visits: 131
Vistors Checkin : 132
Checkout visitors: 133

Blacklist 134

Blacklist Configuration 134

Automatic key up date 136

Using PPD. Initialization 138
Main menu: 138
Initializing doors: 138

7. ADVANCED OPTIONS 142

General info 142

PPD status 144

Encoder status 146

Configuration of Ethernet encoders 147

Lock status. 149

Advanced parameters 151

Automatic Purge 152

User 155

Writing extra info on track 1, 2 or 3 for staff keys 156

Writting extra info in users cards: 157

Show Key detect mode: 159

Show ROM code: 160

Wiegand Code: 161

Port ranges 164

AUTO LOGOFF 165

AUTOMATIC PURGED 166

PERMANENT USER DELETION: 169

AUTOMATIC KEY ASSIGNMENT 170

KEY ISSUING 174

INCREASSE THE OCCUPIED SECTORS LATER 177

DESFire Evolution 1 178

MIFARE PLUS 178

LEGIC PRIME AND ADVANT 180

AUDITOR 182

ON LINE 182

PERIPHERAL MENU 183

Monitoring On Line Control Units 184
Multiple Online Monitoring (only for Service) 189
Peripheral List 191
Peripheral Initialization 195
Inhibit Master communication 196
Encoder and PPD firmware update 198
Update the readers: 199

Roll-Call: 200
How to create a Roll-Call area: 200
Extra Area: 201
Example: 202
Monitoring of Roll-Call areas 202

Limited occupancy 206

Language. Language change. 208

Log-out. Change operator. 209

PPD connection. Portable programmer. 209

Audit Trail. Collecting door opening data. 213

New filter 216

Create a new filter 216
Save the filter: 221

AUTOMATIC AUDIT TRAIL EXPORT 221

BADGING 226

DEPARTMENT DATA BASE CONFIGURATION 231

Activate departments feature 232

How to create departments 233

Internal elements 235

Share elements 237

Users automatically shared 238

External elements 239

Operations 240

Operator Groups 240

How to work with external elements 242

Audit trail 246

Programming and spare keys 246

8. AUTOMATIC USER DATA SYNCHRONISATION TOOL 248

EVENTS STREAMS (SALTO SERVICE ONLY!) 253

9. SALTO HOST INTERFACE PROTOCOL SHIP 257

Activate communication SALTO (server) – Host (client) 257

Activate communication SALTO (client) – Host (Server) 258

MATRIX 259

Advanced option LOCATION_FUNCTION_MATRIX 259
Step 1. Activate “Location_Function_Matrix” 260
Step 2. Set up Groups for Locations and Functions 261
Step 3. Set up Location and Function 262
Step 4. Assign doors for Location and Function 263
Step 5. Assign Access and time right to user 264

SALTO WIRELESS 265
System Setup 265
RF Options 266
Lock parameters 266

WORKING WITH MODE 1 267
Gateways RF1 267
Repeaters RF1 268
Wireless Locks RF1 270
Monitoring of online locks 271
RF Network 273

WORKING WITH MODE 2 274
Gateways RF 2 274
Nodes RF2 275

Creating the LINK with DOORS 276

LOCKDOWN 277

AMOK 279

1.Introduction:

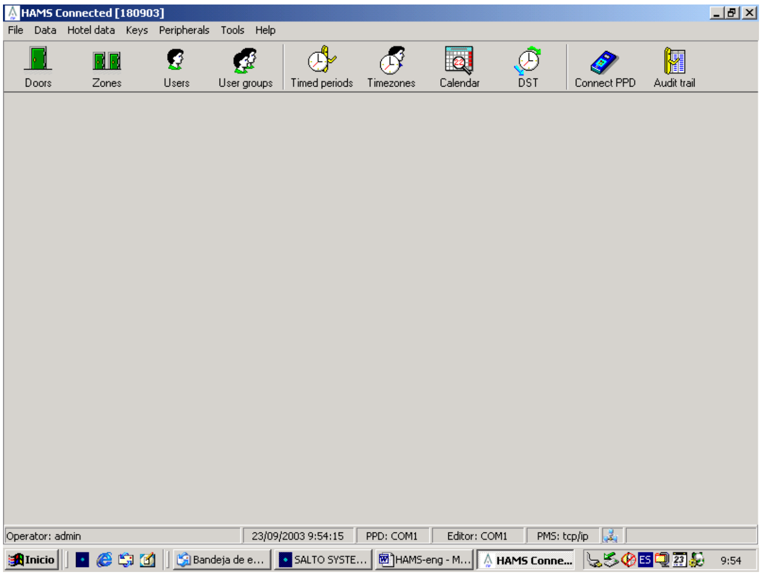
SALTO RW Pro-Access software has been developed to manage access control to buildings where *read-write* ID elements are used (smart cards).

Using this system two main tasks can be accomplished:

- Design the locking schedule and perform the first electronic lock initialization.

- Support an application usable by software operators to edit the user´s key cards.

The ability of managing online wall readers and updaters is a feature available from RW **PA100** software with 4 online doors, to no limit on RW **PA Departmental**.



Operator: admin | 23/09/2003 9:54:15 | PPD: COM1 | Editor: COM1 | PMS: tcp/ip

Figure 1.

Once the locking schedule has been designed, we can transfer it to every door within our facilities by PPD, a small portable programming device, which will be essential to implement the installation, and to audit doors whenever you want.

To sum up, you will need the following elements in order to manage the site access control:

1. Salto PA Software installed in 1 PC .
2. RW iD elements, both for hotel personnel and guests. (keys).
3. RW escutcheons for those doors with access control procedures.
4. 1 card editor. ECX000
5. 1 portable programmer (PPDX00)

2. Program installation

To install the software provided by SALTO, the minimum system requirement should comply with the following:

SQL DB

RAM: 1GB.
Processor: 1 GHz or higher. 32Bits or 64Bits.
Hard disk available space: 10 GB. (Aprox. depends on the DB)
Operating system: Windows XP, Windows Vista, Windows 7 (32bits and 64bits), Windows Server 2003, Windows Server 2008, Windows 8 (32bits and 64bits)
MS-SQL: MS-SQL 2000, MS-SQL 2005, 2008, 2008R2 and 2012 - *all editions, including MS-SQL Express* -
Minimum resolution: 1024x768

Specific points for the SQL+SERVICE platform:

MS-SQL: MS-SQL 2005, 2008, 2008R2 and 2012 - *including MS-SQLExpress* - (MS-SQL 2000 is not compatible!)
.NET Framework 3.5 (mandatory)
MS-Windows Installer 3.1
Machine Name Resolver (DNS - Domain Name System)
Domain Environment: Strongly Recommended

WARNING**: make sure that your PC clock has the right time, and that it set correctly, since the SALTO system time will be based on your PC clock.**

Salto software allows you to work with a multi-workstation configuration, that is to say, the program can be used on different PCs simultaneously, with the same data base. The main condition being that every user is provided access with read/write privileges to the SALTO DB within the SQL Server.

MDAC

Salto RW application requires MDAC (Microsoft Data Access Components) 2.1 version or higher installed on the system. This requirement is met by the latest operating systems such as Windows 2000 or Millennium, where MDAC 2.5 is a default installed option.

MDAC Installation on your system

SALTO installation program contains also the executable file “mdac_typ.exe”, that runs MDAC 2.5 version. Before proceeding to install this, perform the following steps:

- Check that your system has no MDAC or a lower version than 2.1 already installed (see previous paragraph).

- Close all currently active applications, above all those that could use MDAC such as: Word, Excel, Access, Power Point, Internet Explorer, Outlook, etc…

- With Windows NT, as a precautionary measure, log in as a user with administrator privileges.

- Double click the executable file “mdac_typ.exe” contained in the CD-ROM provided by SALTO in order to install in your hard disk 2.5 version. To localise this file, select the path: D:\Mdac\ Mdac2.5SP2\ Language\ mdac_typ.

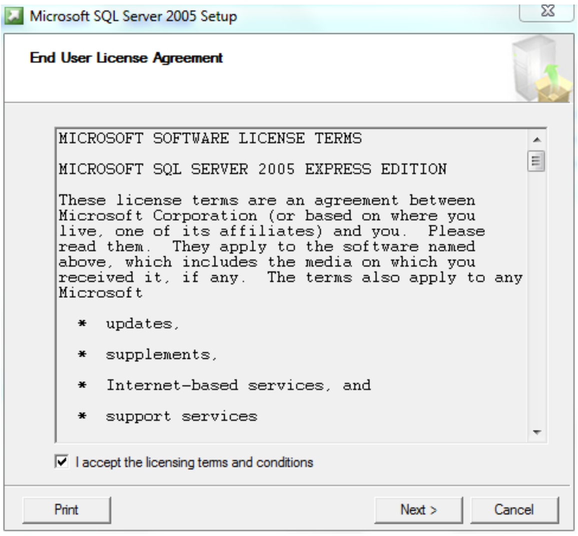
- It is advisable to read the mdac_readme file, to obtain more information.

SQL MS Server

To work with this application it is needed to have installed on the computer the MS SQL Server 2005 or 2008. Even it is recommended to have installed the Microsoft SQL Server management Studio as well.

The Salto software is available to work on the windows authentication and SQL authentication. This Software is available in the following site:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=220549b5-0b07-4448-8848-dcc397514b41



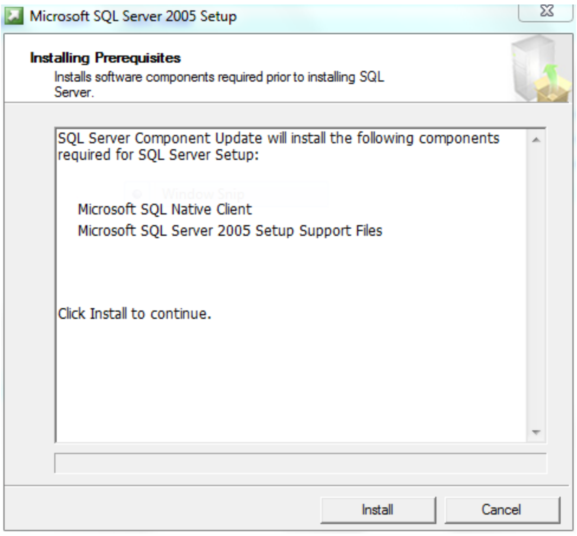
Microsoft SQL Server 2005 Setup

End User License Agreement

```
MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2005 EXPRESS EDITION

These license terms are an agreement between
Microsoft Corporation (or based on where you
live, one of its affiliates) and you.  Please
read them.  They apply to the software named
above, which includes the media on which you
received it, if any.  The terms also apply to any
Microsoft

  *  updates,

  *  supplements,

  *  Internet-based services, and

  *  support services
```

☑ I accept the licensing terms and conditions

Accept terms and conditions and click next.



Microsoft SQL Server 2005 Setup

Installing Prerequisites

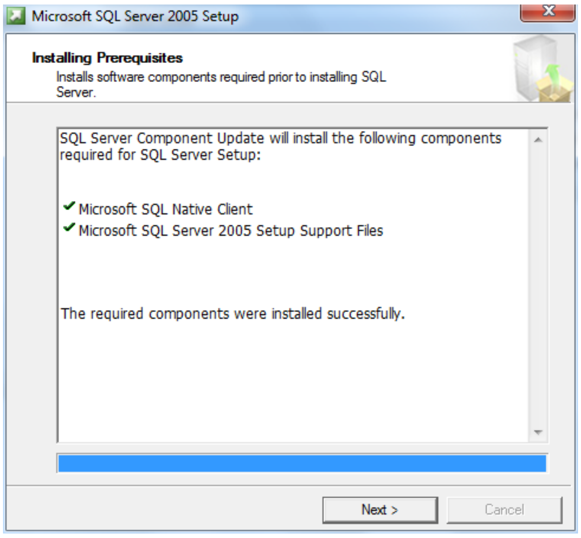
Installs software components required prior to installing SQL Server.

SQL Server Component Update will install the following components required for SQL Server Setup:

Microsoft SQL Native Client
Microsoft SQL Server 2005 Setup Support Files

Click Install to continue.

Installing Prerequisites, click Install



Microsoft SQL Server 2005 Setup

Installing Prerequisites

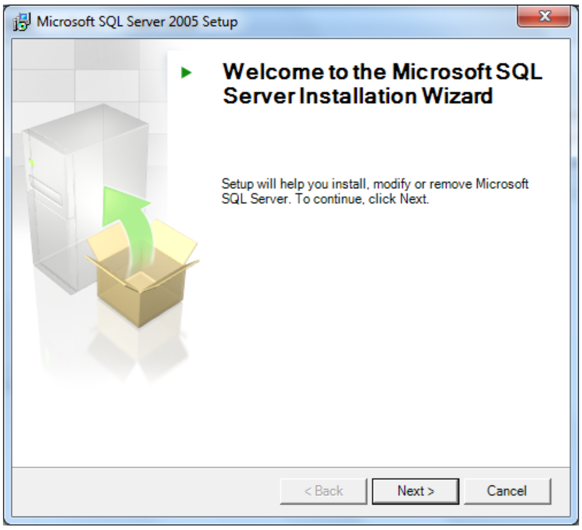
Installs software components required prior to installing SQL Server.

SQL Server Component Update will install the following components required for SQL Server Setup:

✓ Microsoft SQL Native Client
✓ Microsoft SQL Server 2005 Setup Support Files

The required components were installed successfully.

Prerequisites are installed, click next.

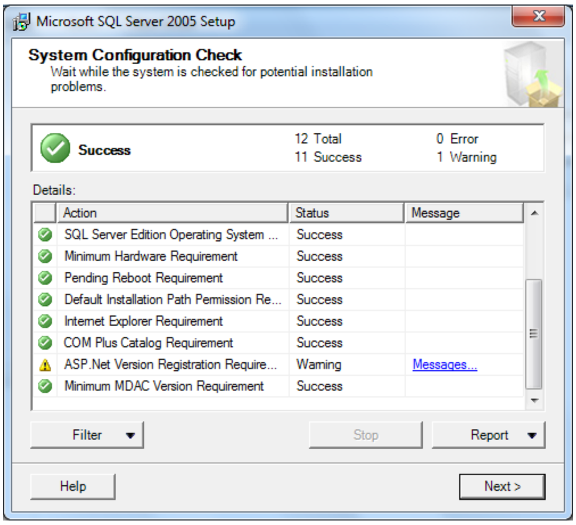


Microsoft SQL Server 2005 Setup

Welcome to the Microsoft SQL Server Installation Wizard

Setup will help you install, modify or remove Microsoft SQL Server. To continue, click Next.

Click next.



Microsoft SQL Server 2005 Setup

System Configuration Check

Wait while the system is checked for potential installation problems.

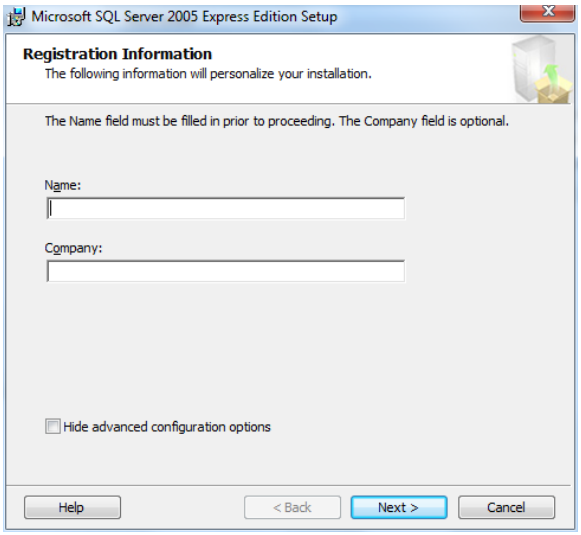
Success 12 Total 11 Success 0 Error 1 Warning

Details:

	Action	Status	Message
✓	SQL Server Edition Operating System ...	Success	
✓	Minimum Hardware Requirement	Success	
✓	Pending Reboot Requirement	Success	
✓	Default Installation Path Permission Re...	Success	
✓	Internet Explorer Requirement	Success	
✓	COM Plus Catalog Requirement	Success	
⚠	ASP.Net Version Registration Require...	Warning	Messages...
✓	Minimum MDAC Version Requirement	Success	

Once the checking will be done, click next.

In case of errors, they will have to be fixed before continuing with the installation. It is possible that the 'Microsoft .NET Framework 2.0 o superior' is missing. In this case, it will have to be installed before continuing with the installation.



Microsoft SQL Server 2005 Express Edition Setup

Registration Information

The following information will personalize your installation.

The Name field must be filled in prior to proceeding. The Company field is optional.

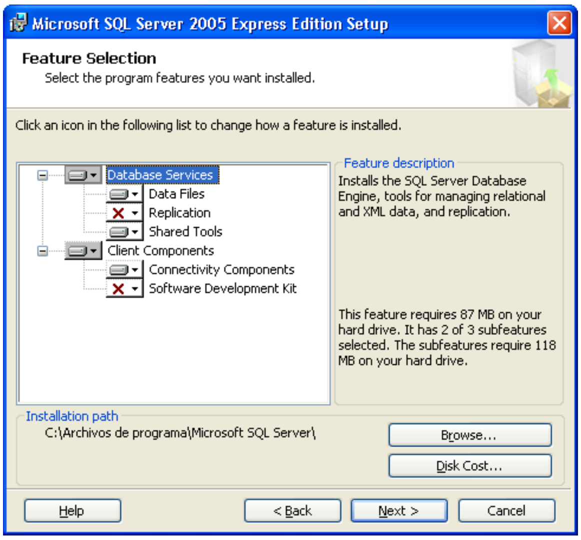
Name:

Company:

□ Hide advanced configuration options

Place the name and the company. The name must be written, the company is optional.

Unselect the "Hide advanced configuration options" mark and click next.



Microsoft SQL Server 2005 Express Edition Setup

Feature Selection

Select the program features you want installed.

Click an icon in the following list to change how a feature is installed.

- Database Services
  - Data Files
  - ✗ Replication
  - Shared Tools
- Client Components
  - Connectivity Components
  - ✗ Software Development Kit

Feature description

Installs the SQL Server Database Engine, tools for managing relational and XML data, and replication.

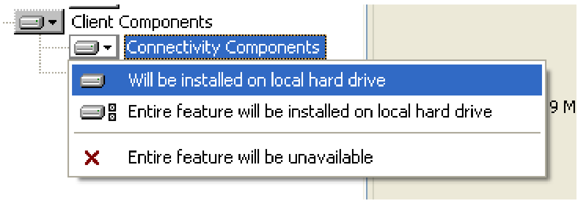
This feature requires 87 MB on your hard drive. It has 2 of 3 subfeatures selected. The subfeatures require 118 MB on your hard drive.

Installation path

C:\Archivos de programa\Microsoft SQL Server\

Select the path where the SQL Express and its components must be installed.

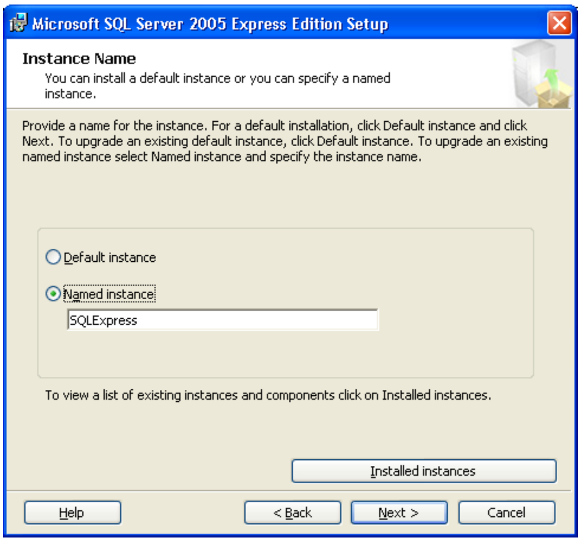
The following features must be installed; Data Files, Shared Tools, y Connectivity Components. In order to select them, click on the option to select and chose, 'will be installed on local hard drive'



Client Components

Connectivity Components

- Will be installed on local hard drive
- Entire feature will be installed on local hard drive
- Entire feature will be unavailable



Microsoft SQL Server 2005 Express Edition Setup

Instance Name

You can install a default instance or you can specify a named instance.

Provide a name for the instance. For a default installation, click Default instance and click Next. To upgrade an existing default instance, click Default instance. To upgrade an existing named instance select Named instance and specify the instance name.

○ Default instance

● Named instance

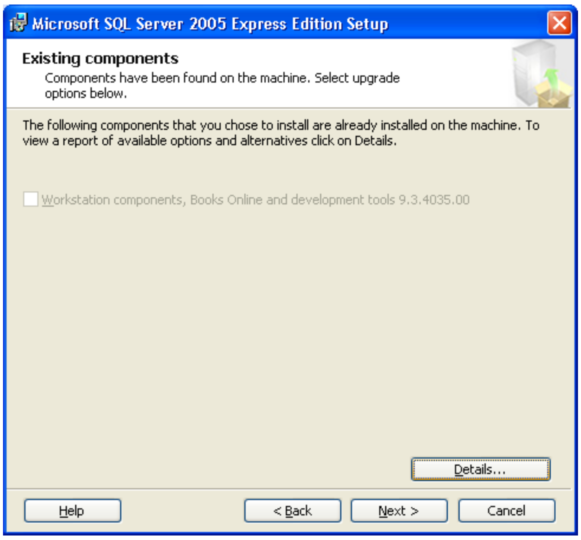
SQLExpress

To view a list of existing instances and components click on Installed instances.

Provide the name of the instance to be installed.

If only one instance will be installed in this machine, it is possible to select “Default Instance”. In this case, when opening the Salto DB it would be enough to place the PC’s name without the instance.

If an instance name is specified, in order to connect to a DB, it will be necessary to place; **‘Server_name\Instance_name’**



Microsoft SQL Server 2005 Express Edition Setup

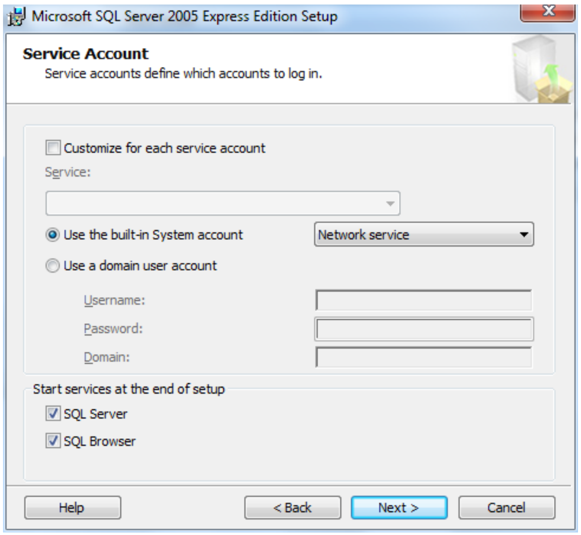
Existing components

Components have been found on the machine. Select upgrade options below.

The following components that you chose to install are already installed on the machine. To view a report of available options and alternatives click on Details.

□ Workstation components, Books Online and development tools 9.3.4035.00

After all the PC’s components have been updated, click next.



Microsoft SQL Server 2005 Express Edition Setup

Service Account
Service accounts define which accounts to log in.

☐ Customize for each service account

Service:

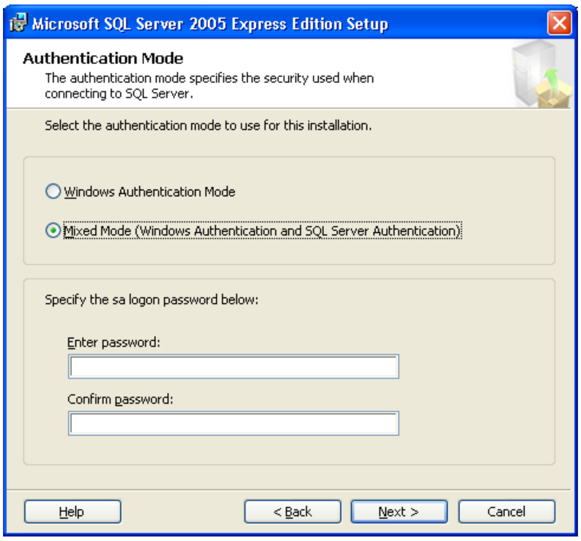
● Use the built-in System account — Network service

○ Use a domain user account

Username:
Password:
Domain:

Start services at the end of setup
☑ SQL Server
☑ SQL Browser

Make sure to select the “Start services at the end of setup” option, SQL Server and SQL Browser.



Microsoft SQL Server 2005 Express Edition Setup

Authentication Mode
The authentication mode specifies the security used when connecting to SQL Server.

Select the authentication mode to use for this installation.

○ Windows Authentication Mode

● Mixed Mode (Windows Authentication and SQL Server Authentication)

Specify the sa logon password below:

Enter password:

Confirm password:

In this window, it is necessary to select the authentication mode that will be used to open the DB. If the company has a domain and all the users will connect to the DB using the windows login, select the Windows Authentication.

On the other hand, if there isn’t any existing domain or if we want to connect to the DB using an SQL user, it will be necessary to select the Mixed Mode and place a password for the administrator (sa) user. The password will have to be secured;

The secured password cannot follow some conditions neither prohibited terms as follows;

a. NULL condition nor blank

b. "Password"

c. "Admin"

d. "Administrator"

e. "sa"

f. "sysadmin"

2. The secured passwords cannot contain the following terms related to the PC:

a. Name of the user used to log the actual session.

b. Name of the PC.

3. A secured password must be at least 6 characters long and comply with at least 3 of the 4 criteria.

a. Must contain uppercases.

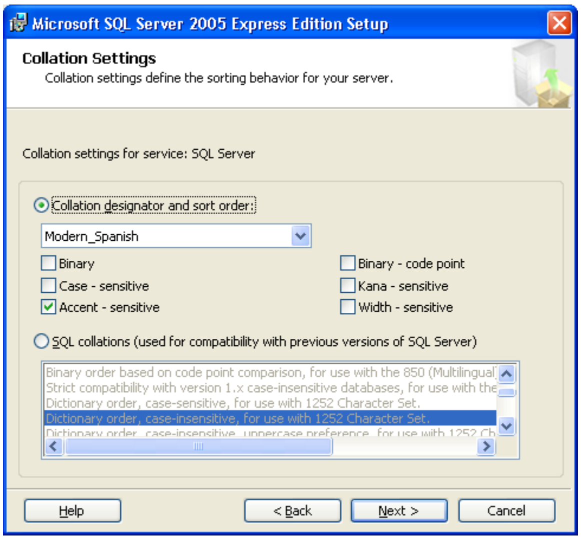
b. Must contain lowercases letters.

c. Must contain numbers.

d. Must contain alphanumeric characters as i.e., #, % or ^.

If the authentication mode to use is not known, we recommend to use the mixed mode, as this mode allows both authentication modes.

If only the windows authentication mode has been selected and the SQL authentication mode is needed, it will be necessary to install the Management Studio software in order to modify this option.



Microsoft SQL Server 2005 Express Edition Setup

Collation Settings

Collation settings define the sorting behavior for your server.

Collation settings for service: SQL Server

● Collation designator and sort order:

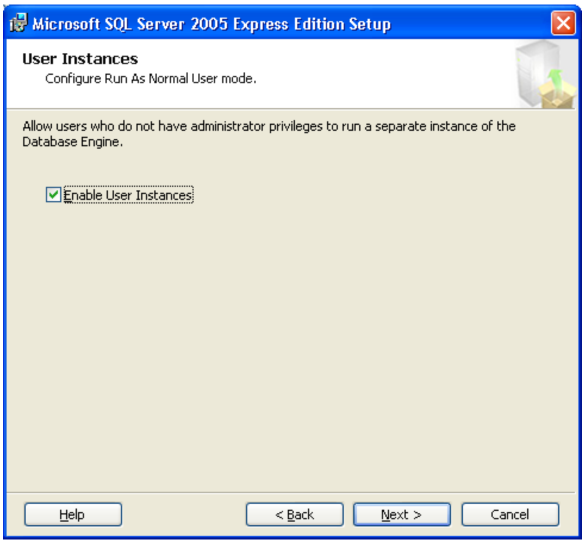
Modern_Spanish

□ Binary
□ Case - sensitive
☑ Accent - sensitive
□ Binary - code point
□ Kana - sensitive
□ Width - sensitive

○ SQL collations (used for compatibility with previous versions of SQL Server)

```
Binary order based on code point comparison, for use with the 850 (Multilingual)
Strict compatibility with version 1.x case-insensitive databases, for use with the
Dictionary order, case-sensitive, for use with 1252 Character Set.
Dictionary order, case-insensitive, for use with 1252 Character Set.
Dictionary order, case-insensitive, uppercase preference, for use with 1252 Ch
```

Select the option Accent-sensitive. Other options must be unchecked. Click next.



Microsoft SQL Server 2005 Express Edition Setup

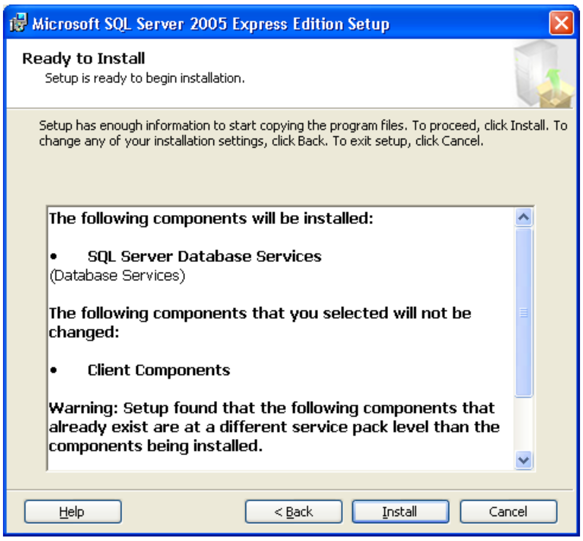
User Instances

Configure Run As Normal User mode.

Allow users who do not have administrator privileges to run a separate instance of the Database Engine.

☑ Enable User Instances

Leave it as by default and click next.



Microsoft SQL Server 2005 Express Edition Setup

Ready to Install

Setup is ready to begin installation.

Setup has enough information to start copying the program files. To proceed, click Install. To change any of your installation settings, click Back. To exit setup, click Cancel.

The following components will be installed:

- **SQL Server Database Services**

(Database Services)

The following components that you selected will not be changed:

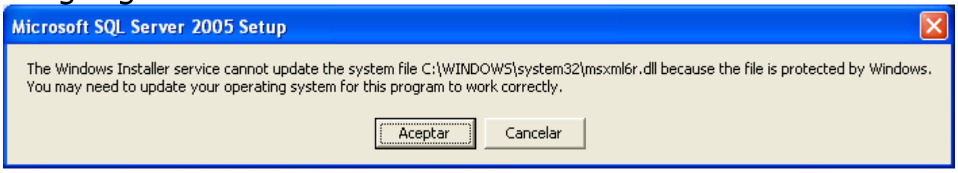
- **Client Components**

Warning: Setup found that the following components that already exist are at a different service pack level than the components being installed.

Finally, click "Install" to start.

During installation, it may happen that the following error would appear when trying to install a 2005 or 2008 SQL server English version on a non English language Windows XP SP3 operative system.

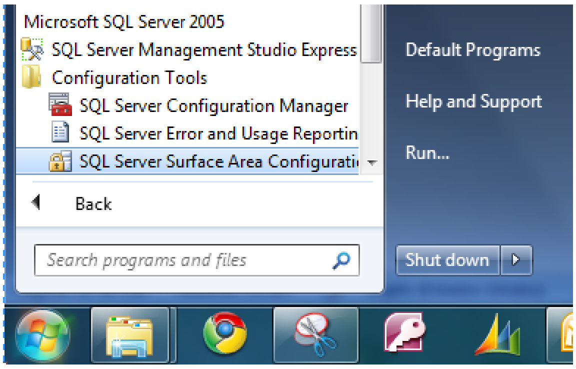
To fix this error, it will be necessary to download SQL Server Express installer with the operative system language from Microsoft web site.


Microsoft SQL Server 2005 Setup

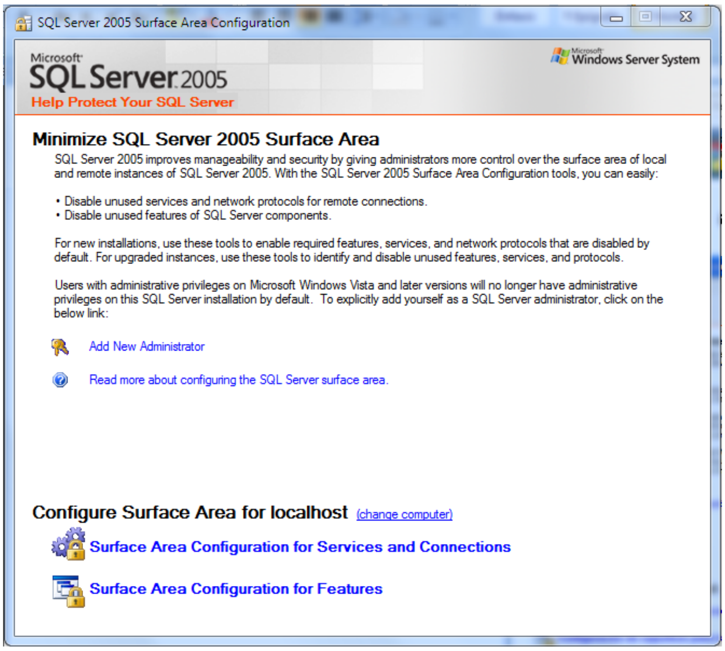
The Windows Installer service cannot update the system file C:\WINDOWS\system32\msxml6r.dll because the file is protected by Windows. You may need to update your operating system for this program to work correctly.

Remote conexions Service configurations

Now, we will use the **"SQL Server Surface Area Configuration"**


Microsoft SQL Server 2005
SQL Server Management Studio Express
Configuration Tools
SQL Server Configuration Manager
SQL Server Error and Usage Reportin
SQL Server Surface Area Configurati
Back
Search programs and files
Default Programs
Help and Support
Run...
Shut down

Now we go the "**Servicies and conexions area configurations**"



SQL Server 2005 Surface Area Configuration

Microsoft SQL Server 2005
Help Protect Your SQL Server

Microsoft Windows Server System

Minimize SQL Server 2005 Surface Area

SQL Server 2005 improves manageability and security by giving administrators more control over the surface area of local and remote instances of SQL Server 2005. With the SQL Server 2005 Surface Area Configuration tools, you can easily:

- Disable unused services and network protocols for remote connections.
- Disable unused features of SQL Server components.

For new installations, use these tools to enable required features, services, and network protocols that are disabled by default. For upgraded instances, use these tools to identify and disable unused features, services, and protocols.

Users with administrative privileges on Microsoft Windows Vista and later versions will no longer have administrative privileges on this SQL Server installation by default. To explicitly add yourself as a SQL Server administrator, click on the below link:

Add New Administrator

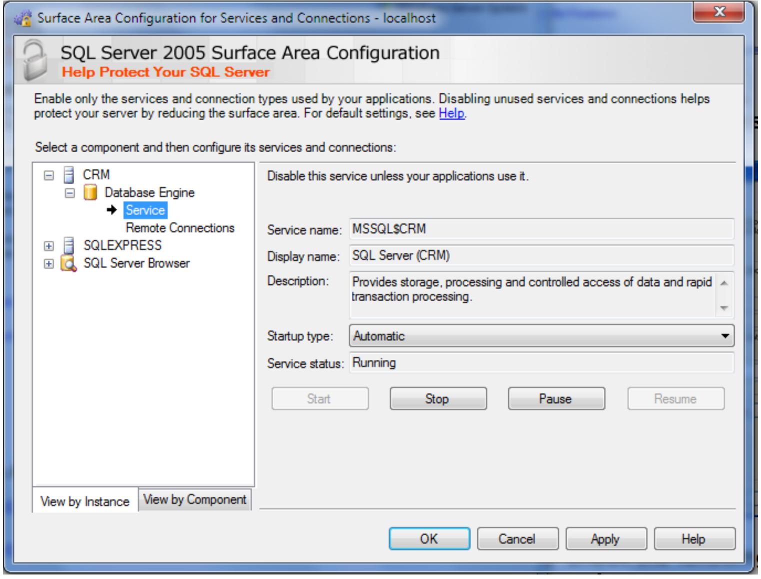
Read more about configuring the SQL Server surface area.

Configure Surface Area for localhost (change computer)

Surface Area Configuration for Services and Connections

Surface Area Configuration for Features

Select the “**Service**” for our SQL Server, (**“SQLEXPRESS”** as it is on the example**)** and make sure to set it as “**Automatic**”**.** Now, start the service.



Surface Area Configuration for Services and Connections - localhost

SQL Server 2005 Surface Area Configuration
Help Protect Your SQL Server

Enable only the services and connection types used by your applications. Disabling unused services and connections helps protect your server by reducing the surface area. For default settings, see Help.

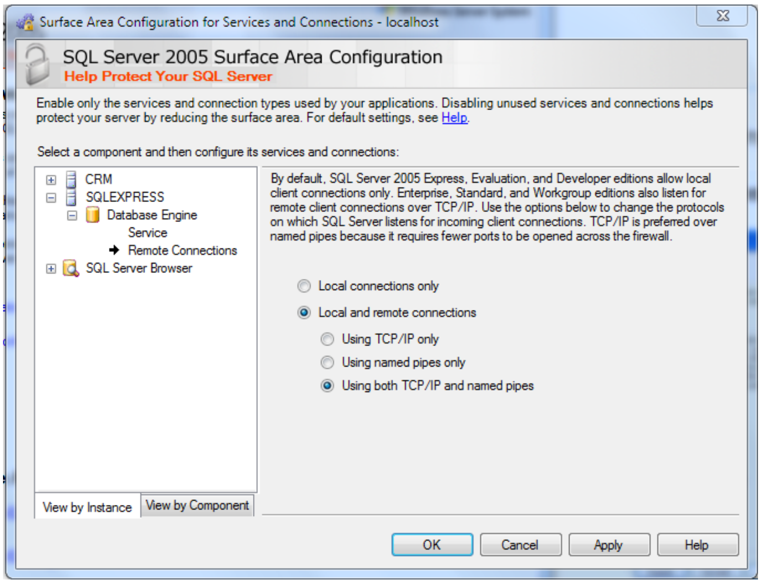
Select a component and then configure its services and connections:

Disable this service unless your applications use it.

Service name: MSSQL$CRM
Display name: SQL Server (CRM)
Description: Provides storage, processing and controlled access of data and rapid transaction processing.
Startup type: Automatic
Service status: Running

On the “**Remote conexions**” check the following options:

- **Local and Remote Conexions**
- **Use TCP/IP and named pipes conexions**



Surface Area Configuration for Services and Connections - localhost

SQL Server 2005 Surface Area Configuration
Help Protect Your SQL Server

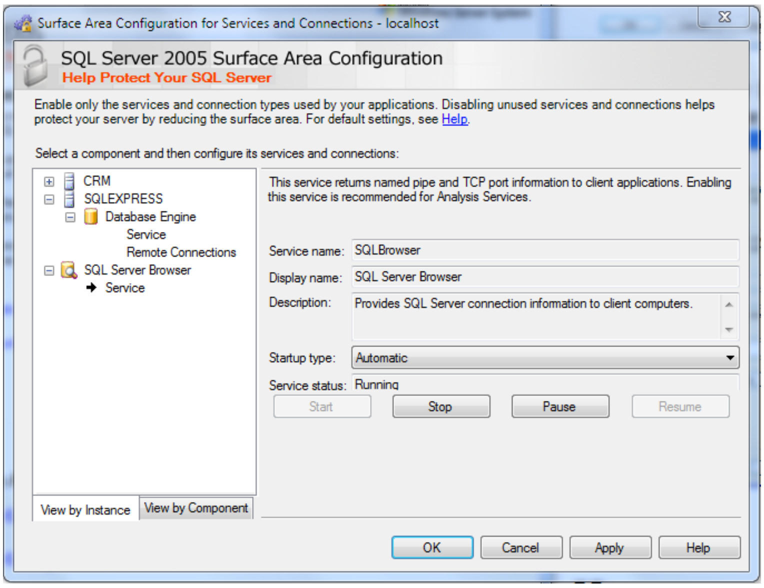
Enable only the services and connection types used by your applications. Disabling unused services and connections helps protect your server by reducing the surface area. For default settings, see Help.

Select a component and then configure its services and connections:

By default, SQL Server 2005 Express, Evaluation, and Developer editions allow local client connections only. Enterprise, Standard, and Workgroup editions also listen for remote client connections over TCP/IP. Use the options below to change the protocols on which SQL Server listens for incoming client connections. TCP/IP is preferred over named pipes because it requires fewer ports to be opened across the firewall.

○ Local connections only
● Local and remote connections
○ Using TCP/IP only
○ Using named pipes only
● Using both TCP/IP and named pipes

Now, select "**Service**" from the "**SQL Server Browser**", make sure that it is set as "**Automatic**" and start the service**.**



Surface Area Configuration for Services and Connections - localhost

SQL Server 2005 Surface Area Configuration
Help Protect Your SQL Server

Enable only the services and connection types used by your applications. Disabling unused services and connections helps protect your server by reducing the surface area. For default settings, see Help.

Select a component and then configure its services and connections:

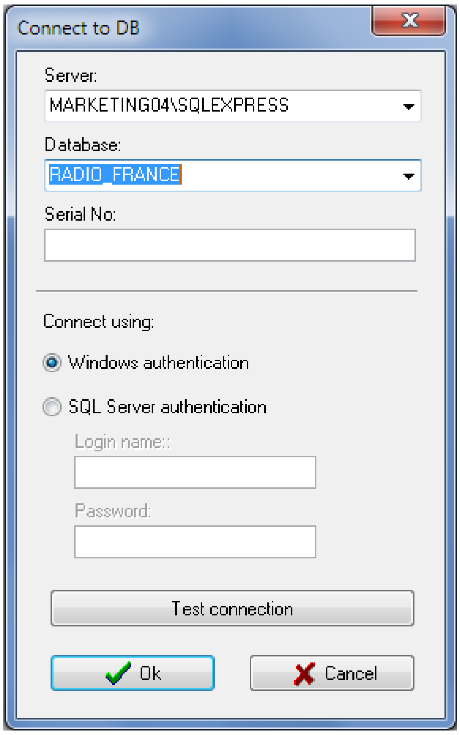
This service returns named pipe and TCP port information to client applications. Enabling this service is recommended for Analysis Services.

Service name: SQLBrowser
Display name: SQL Server Browser
Description: Provides SQL Server connection information to client computers.
Startup type: Automatic
Service status: Running

Opening the SQL DB

The next step is opening the DB.

Click "**File/ Open new DB**" and select the name of the server, the name of the service and below the name of the DB, ("SALTO_RW" by default) using the needed authentication mode.



Connect to DB

Server: MARKETING04\SQLEXPRESS

Database: RADIO_FRANCE

Serial No:

Connect using:

● Windows authentication

○ SQL Server authentication

Login name::

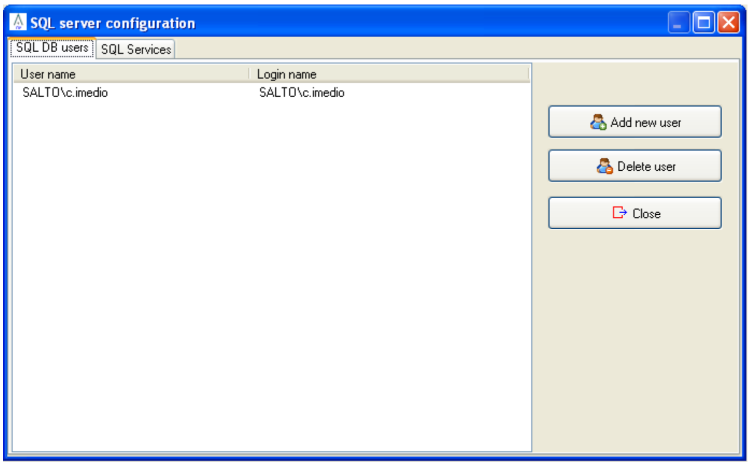
Password:

SQL Server Configuration

This option represents an alternative to the SQL data base management software in order to create logins.

Logins will permit to have access to the database from different PCs so it is possible to have a shared installation between different computers.

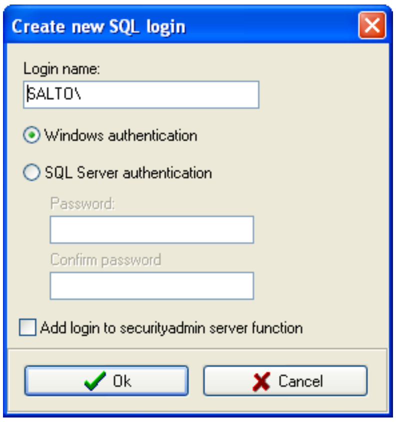
Tools/Configuration/SQL Server Configuration menu gives access to the following screen:



User name	Login name
SALTO\c.imedio	SALTO\c.imedio

This window manages the different logins to the SQL database.
"Add new user" creates a new login with the following options:

- Login name
  The format of this field depends on the authentication type (Windows or SQL)



Login name: SALTO\

● Windows authentication

○ SQL Server authentication

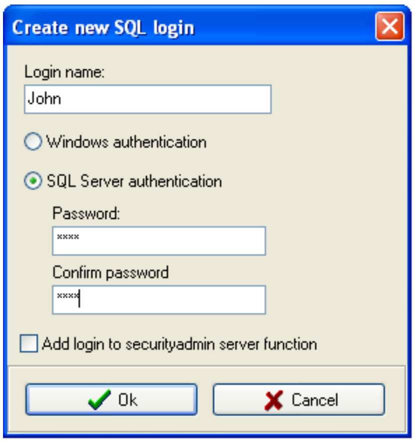
Password:

Confirm password

□ Add login to securityadmin server function

Windows authentication uses existing network users. By default, the field will show the actual Windows domain so it can be completed with the user information.
i.e. SALTO\c.imedio

SQL authentication permits to create new names that are independent from the actual network configuration.
i.e. John



Create new SQL login

Login name: John

○ Windows authentication

● SQL Server authentication

Password: ****

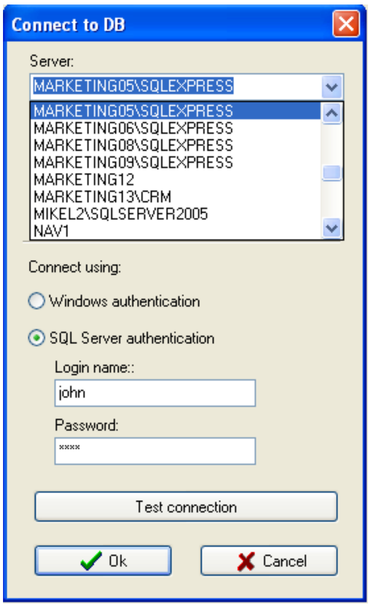
Confirm password ****

□ Add login to securityadmin server function

The password field is optional but may be used to improve the security level when connecting to the database.

This information will be used to connect to the database.

Caution!
It is important to choose correctly the SQL server. The list will display the different network servers. If SQL Express is used, the option xxx\SQLEXPRESS will be selected.
Xxx stands for the name of the machine (i.e. Marketing05).



Connect to DB

Server: MARKETING05\SQLEXPRESS

MARKETING05\SQLEXPRESS
MARKETING06\SQLEXPRESS
MARKETING08\SQLEXPRESS
MARKETING09\SQLEXPRESS
MARKETING12
MARKETING13\CRM
MIKEL2\SQLSERVER2005
NAV1

Connect using:

○ Windows authentication

● SQL Server authentication

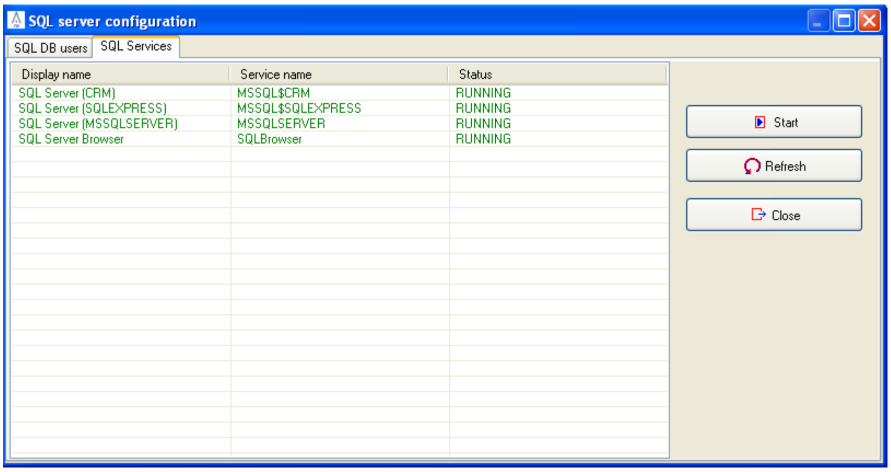
Login name:: john

Password: ****

Add login to securityadmin server function

This function allows to the created users to create new logins.

SQL Services tab shows the different SQL servers installed. The services are displayed with the possibility to start them.

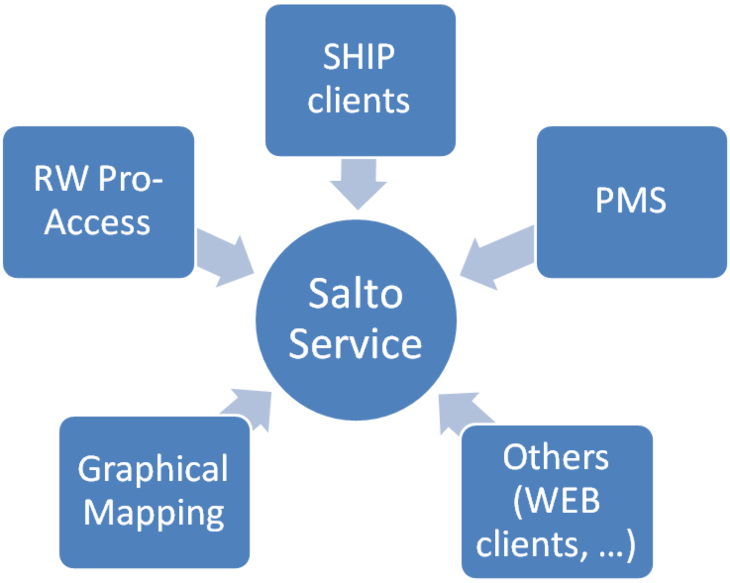


Display name	Service name	Status
SQL Server (CRM)	MSSQL$CRM	RUNNING
SQL Server (SQLEXPRESS)	MSSQL$SQLEXPRESS	RUNNING
SQL Server (MSSQLSERVER)	MSSQLSERVER	RUNNING
SQL Server Browser	SQLBrowser	RUNNING

3.SALTO Service RW

SALTO RW Pro-Access for Service is based on a Windows Service called SALTO Service RW that manages the communications with the on-line peripherals: CUs, encoders (the wireless locks are not included on this release).

This service is intended to be the core application of the SALTO software managing the different modules: Pro-Access, PMS,…



Hardware and System Requirements

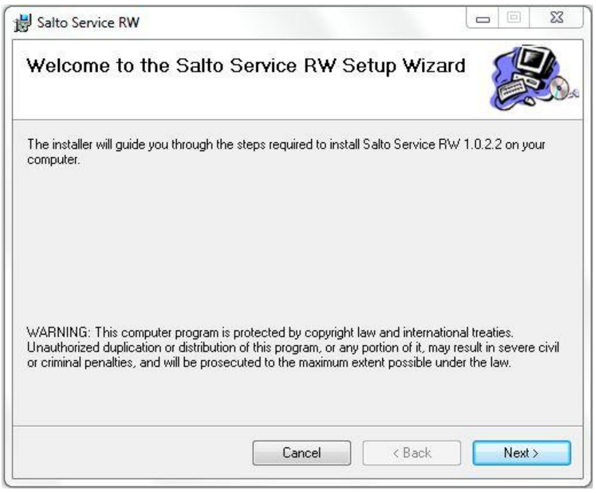
The hardware and system requirements for the Salto Service are as follows:

- Supported operative systems: Microsoft Windows XP (SP3), Vista, Server 2003, Server 2008 and W7. 32-bit or 64-bit. Server edition recommended, i.e., 2003 or 2008.
- Minimum hardware: 400 MHz CPU, 512 MB RAM, 800x600 256-color display.
- Recommended hardware: 1.0 GHz or higher CPU, 1 GB or more RAM, 1024x768 high-color 32-bit display.
- .NET framework 3.5 or higher.
- Up to 3 GB of hard disk space may be required, depending on the size of the locking plan.

- Microsoft SQL Server 2005 or 2008 (Express edition included). Important: if the Salto DB was originally created with version SQL Server 2000 and afterward migrated to an upper version, make sure that the compatibility level is set to 90 o higher.
- Machine name resolver: the Salto software DOES use machine names (rather than fixed IP addresses) for inter-machine communications. In this regards, a machine name resolver (such as a Domain Name System or DNS) is required to correctly resolve machine names into the corresponding IP address. If there is not a system for resolving machine names, certain Salto client applications may stop communicating correctly with the Salto service.
- Domain environment: though not strictly necessary, it is strongly recommended to use machines operating in a domain environment rather than in a workgroup arrangement, the main reason being that security and permission issues are greatly simplified, thus making Salto software configuration and setup less cumbersome and more secure.
- The Salto service installation program (setup.exe) requires MS-Windows Installer 3.1.

Installation

The installation is launched from the *SetupSALTOService.msi* file and installs, together with the service itself, a little application dedicated to do the setup of the RW Pro-Access for its optimum performance.

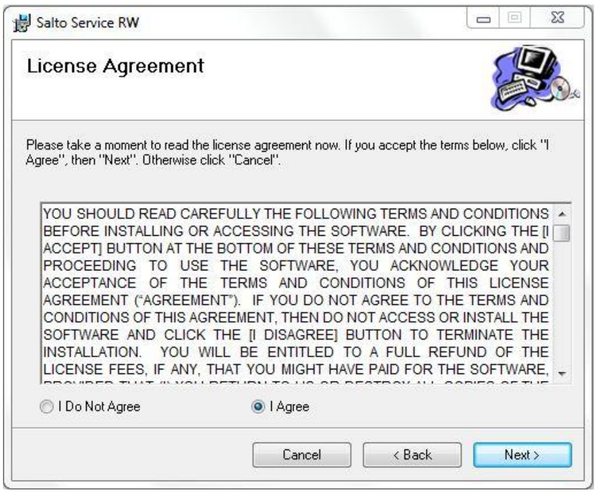


Salto Service RW

Welcome to the Salto Service RW Setup Wizard

The installer will guide you through the steps required to install Salto Service RW 1.0.2.2 on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.



Salto Service RW

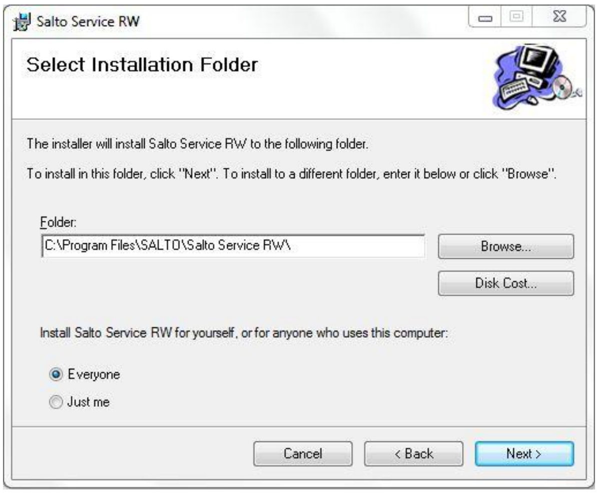
License Agreement

Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".

YOU SHOULD READ CAREFULLY THE FOLLOWING TERMS AND CONDITIONS BEFORE INSTALLING OR ACCESSING THE SOFTWARE. BY CLICKING THE [I ACCEPT] BUTTON AT THE BOTTOM OF THESE TERMS AND CONDITIONS AND PROCEEDING TO USE THE SOFTWARE, YOU ACKNOWLEDGE YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT ("AGREEMENT"). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN DO NOT ACCESS OR INSTALL THE SOFTWARE AND CLICK THE [I DISAGREE] BUTTON TO TERMINATE THE INSTALLATION. YOU WILL BE ENTITLED TO A FULL REFUND OF THE LICENSE FEES, IF ANY, THAT YOU MIGHT HAVE PAID FOR THE SOFTWARE,

○ I Do Not Agree ● I Agree

After accepting the license agreement, an installation folder must be selected and the "Next" button will be enabled to start with the installation.



Salto Service RW

Select Installation Folder

The installer will install Salto Service RW to the following folder.

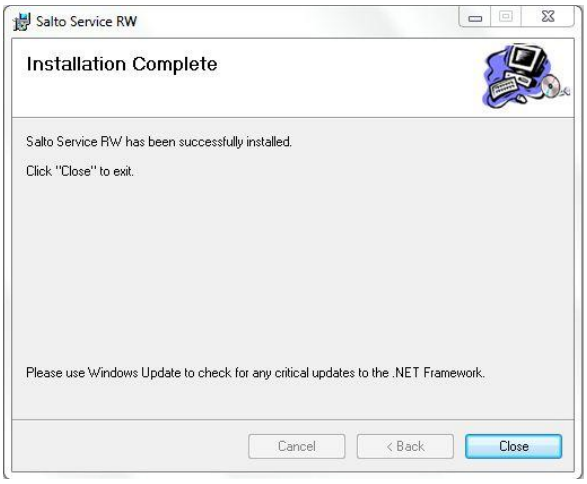
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\SALTO\Salto Service RW\

Install Salto Service RW for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

Once the process is finished, the "Close" button will end it and the service will be installed.



Salto Service RW

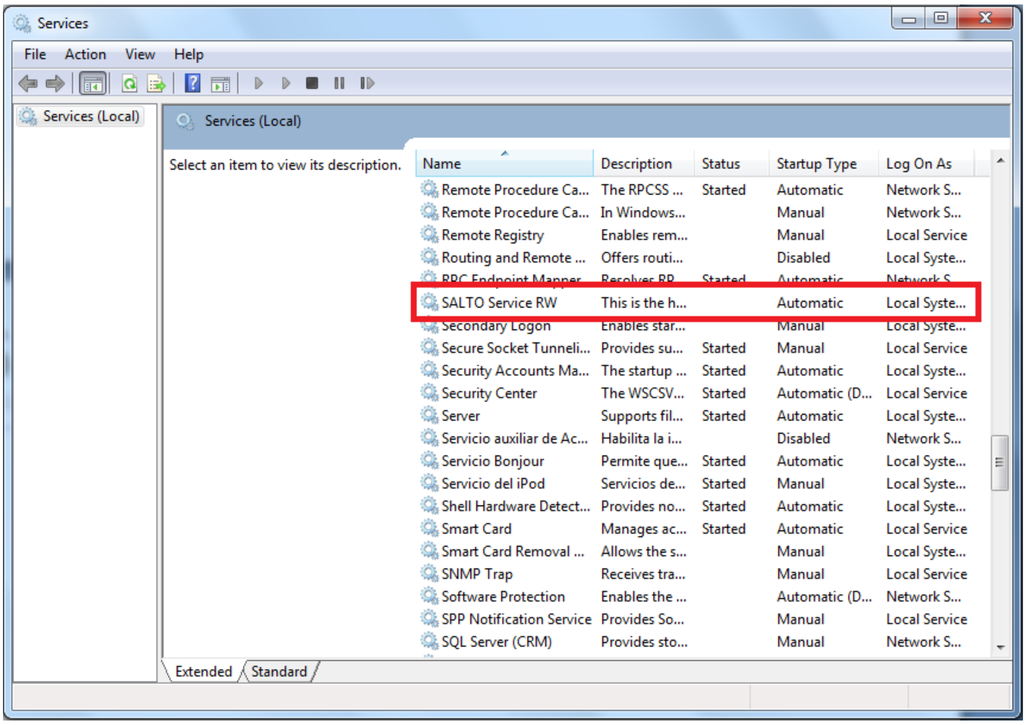
Installation Complete

Salto Service RW has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

The Windows services list will now show it with the name **SALTO Service RW.**



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Remote Procedure Ca...	The RPCSS ...	Started	Automatic	Network S...
Remote Procedure Ca...	In Windows...		Manual	Network S...
Remote Registry	Enables rem...		Manual	Local Service
Routing and Remote ...	Offers routi...		Disabled	Local Syste...
RPC Endpoint Mapper	Resolves RP...	Started	Automatic	Network S...
SALTO Service RW	This is the h...		Automatic	Local Syste...
Secondary Logon	Enables star...		Manual	Local Syste...
Secure Socket Tunneli...	Provides su...	Started	Manual	Local Service
Security Accounts Ma...	The startup ...	Started	Automatic	Local Syste...
Security Center	The WSCSV...	Started	Automatic (D...	Local Service
Server	Supports fil...	Started	Automatic	Local Syste...
Servicio auxiliar de Ac...	Habilita la i...		Disabled	Network S...
Servicio Bonjour	Permite que...	Started	Automatic	Local Syste...
Servicio del iPod	Servicios de...	Started	Manual	Local Syste...
Shell Hardware Detect...	Provides no...	Started	Automatic	Local Syste...
Smart Card	Manages ac...	Started	Automatic	Local Service
Smart Card Removal ...	Allows the s...		Manual	Local Syste...
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (D...	Network S...
SPP Notification Service	Provides So...		Manual	Local Service
SQL Server (CRM)	Provides sto...		Manual	Network S...

Service Configurator

Although the service configuration can be done with the operating system tools, the Configurator brings some more specific options for its management.

The Service Configurator is composed of three general tabs:

- Database
- Service ports
- Service properties

Database

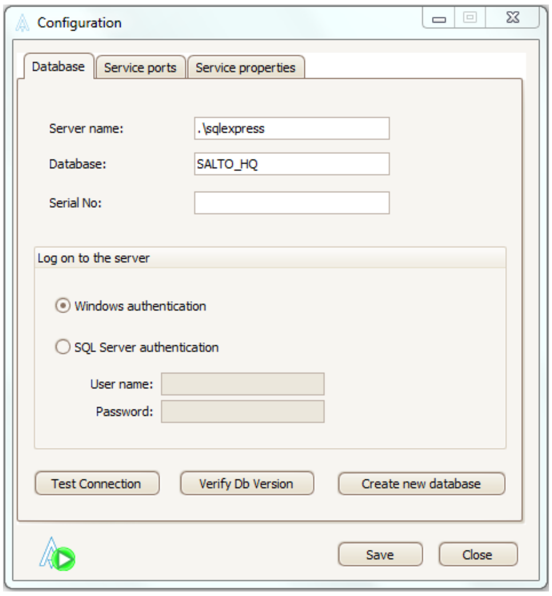
This tab contains information about the SQL database connection.

- Server name
  The name or IP address of the machine containing the database must be detailed on this field (NOTE: when using the "Express" SQL server versions, "\SQLEXPRESS" will have to added after the name of the PC).

- Database
  The database is target here.

- Serial No.
  Software license number (not mandatory field).

- Server authentication
  The authentication type can be selected between Windows or SQL (NOTE: The SQL authentication needs to have a valid SQL user created previously).



Configuration

Server name: .\sqlexpress

Database: SALTO_HQ

Serial No:

Log on to the server

● Windows authentication

○ SQL Server authentication

User name:

Password:

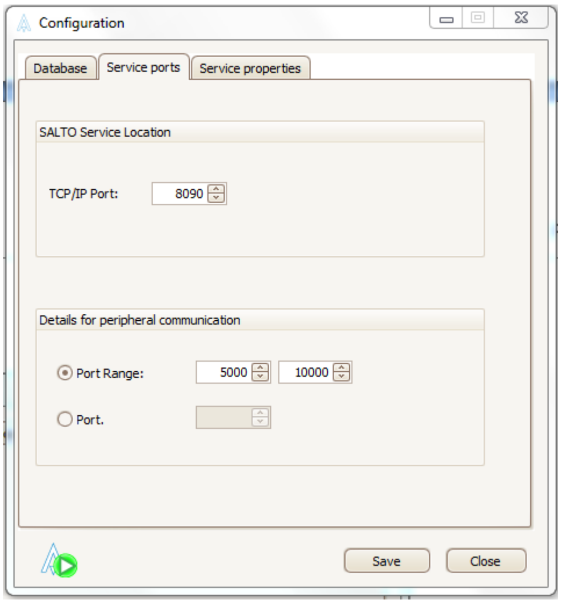
- Test Connection
  It is possible to check the connection with the SQL data base.

- Verify Db Version
  The SQL data base must be compatible with the service version.
  Older data bases require to be updated from the Pro-Access itself in order to make them service compatible.

- Create new database
  This option allows creating a new data base in order to be opened from the Pro-Access.

Service ports

The different ports are managed from this window.
The SALTO Service Location will open a socket to communicate with the different SALTO applications connected to it.
The bottom part is dedicated to open a port or a port range to communicate with the different peripherals.



SALTO Service Location

TCP/IP Port: 8090

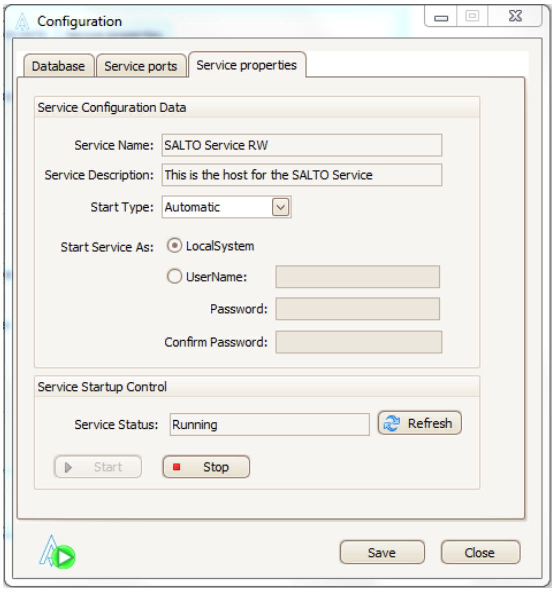
Details for peripheral communication

● Port Range: 5000 10000

○ Port.

Service properties

This screen is similar to the Windows one to manage the service properties.
The Start Type can be defined (Automatic, Manual, Disabled).
Start and Stop options are also available.
(*) LocalSystem option is recommended to start the Service.



Service Configuration Data

Service Name: SALTO Service RW

Service Description: This is the host for the SALTO Service

Start Type: Automatic

Start Service As: ● LocalSystem

○ UserName:

Password:

Confirm Password:

Service Startup Control

Service Status: Running

The following icon will indicate that the service is started and running (the same icon is shown under Pro-Access).

4.Software operators and competencies

Creating a new DB

RW program has two aspects, depending on the user name that begins the login session. (By default, the program has the user name: **ADMIN**. for the administrator)

The first time you login the program must be opened using the administrator login.

To open the program double click the shortcut icon on the desktop.

A window like Figure 1 with 2 fields will be displayed:

User name: type **admin..** in upper case.
Password: in your first login session is not necessary to choose one.

Validate both fields by clicking the "OK" box.

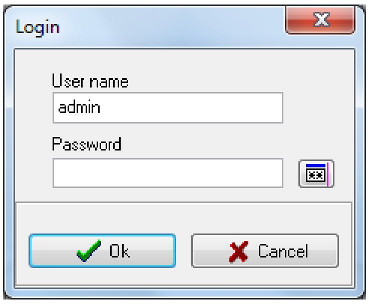


Figure.2

Since it is the first time that we have opened the program, Toolbar icons are disabled as "greyed out".

In order to activate the Toolbar, you need to name the data base that we will be using.

And assign a path and a directory in your computer.

- Click on the popup menu *FILE.*

- Select *NEW DB option* (Figure 3)
- A window like that of Figure 3 will display.

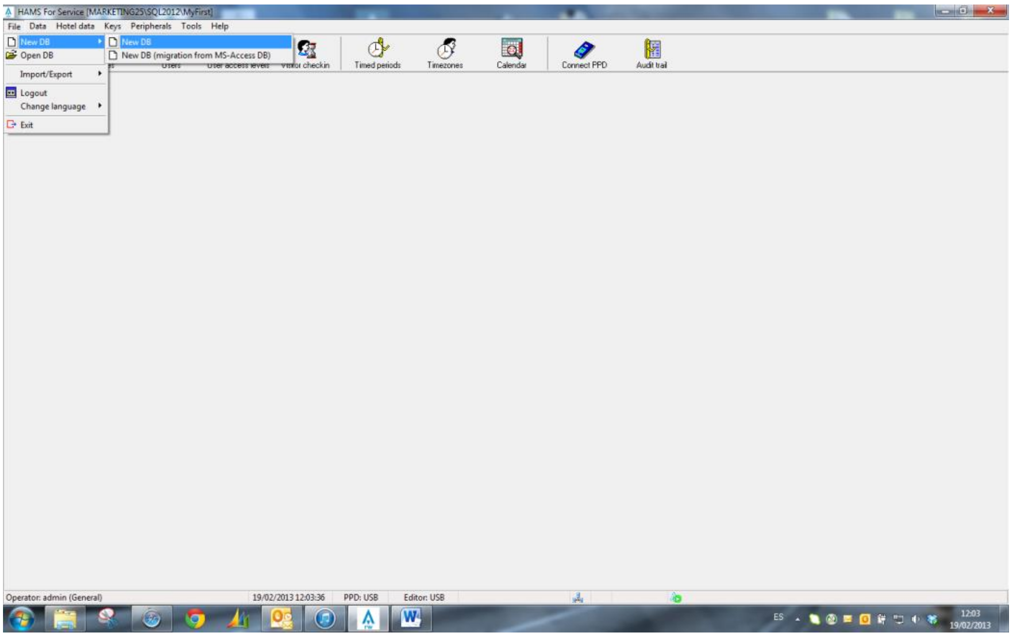
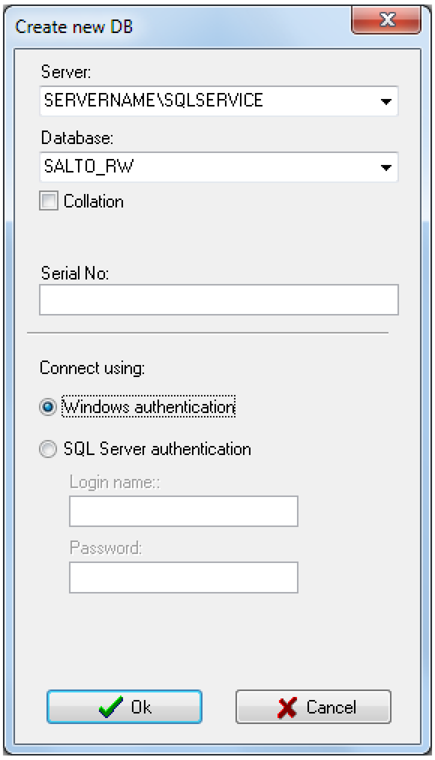


Figure 3

- To open or create a new data base through the PA RW SQL application Go to FILE/New Database. Then in the window write the name of the MS SQL Server program you want to work with. In the field below write the name of the data base you want to create
- You can write the software serial number in the matching field. This is a just informative purpose field.
- Validate data base name and SQL location (click "OK" button)
- Select the connect using: Windows or SQL authentication


Create new DB

Server:
SERVERNAME\SQLSERVICE

Database:
SALTO_RW

□ Collation

Serial No:

Connect using:

● Windows authentication

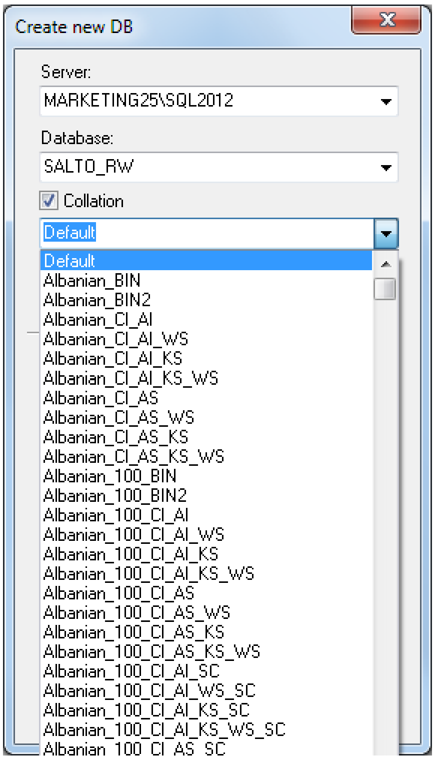
○ SQL Server authentication

Login name::

Password:

Figure 4

By default, the databases created by SALTO are CI (Case Insensitive). In case an SQL server is set as CS (Case Sensitive), when creating the new data base, it is possible to select what language and type of sensitivity is needed.


Create new DB

Server:
MARKETING25\SQL2012

Database:
SALTO_RW

☑ Collation

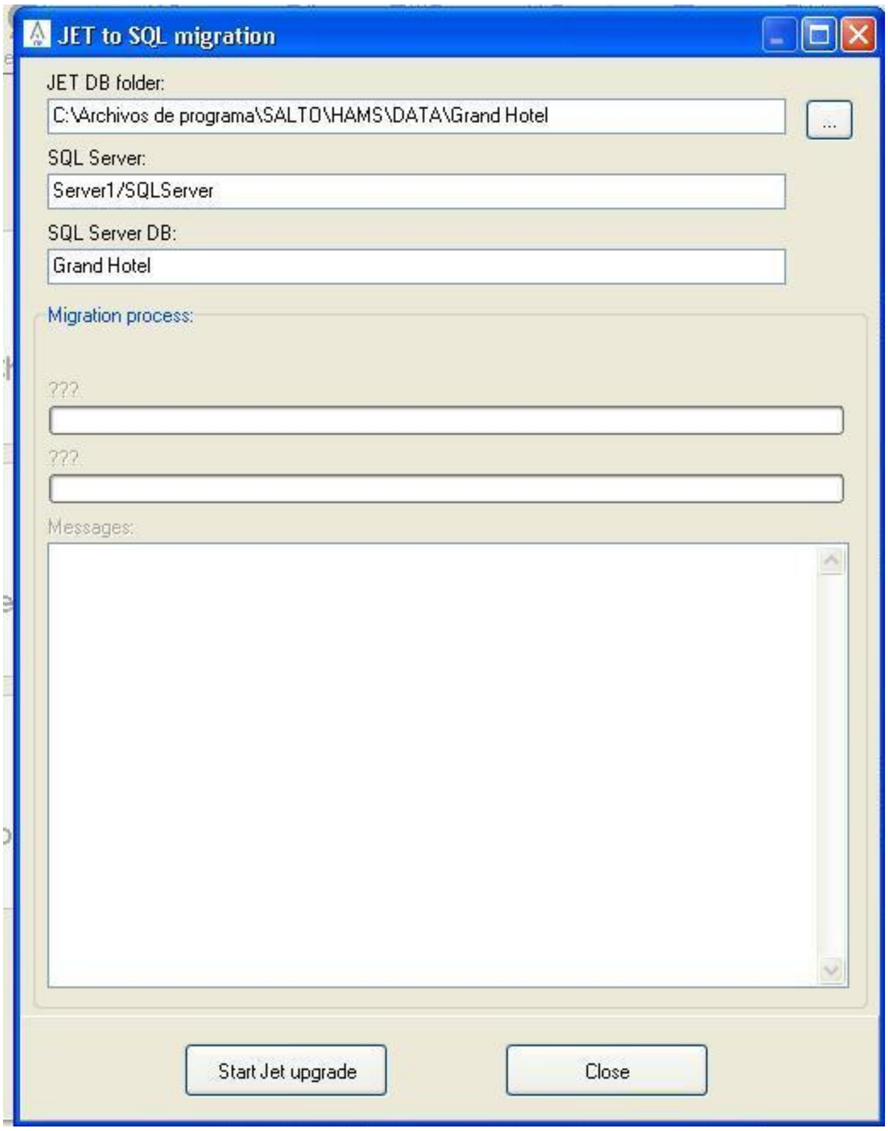
Default

Default
Albanian_BIN
Albanian_BIN2
Albanian_CI_AI
Albanian_CI_AI_WS
Albanian_CI_AI_KS
Albanian_CI_AI_KS_WS
Albanian_CI_AS
Albanian_CI_AS_WS
Albanian_CI_AS_KS
Albanian_CI_AS_KS_WS
Albanian_100_BIN
Albanian_100_BIN2
Albanian_100_CI_AI
Albanian_100_CI_AI_WS
Albanian_100_CI_AI_KS
Albanian_100_CI_AI_KS_WS
Albanian_100_CI_AS
Albanian_100_CI_AS_WS
Albanian_100_CI_AS_KS
Albanian_100_CI_AS_KS_WS
Albanian_100_CI_AI_SC
Albanian_100_CI_AI_WS_SC
Albanian_100_CI_AI_KS_SC
Albanian_100_CI_AI_KS_WS_SC
Albanian_100_CI_AS_SC

Migrating an existing MS-Access DB to a MS-SQLServer DB

In some occasions the customer may not want to create a new SQL DB from scratch but instead start from an already existing MS-Access DB. In this regard, the SALTO application offers the possibility of migrating an existing MS-Access DB to a brand new MS-SQLServer DB.

To migrate an Access DB the admin has to go to File/New DB/Migration from MS Access, where the following screen will be showed:



JET to SQL migration

JET DB folder: C:\Archivos de programa\SALTO\HAMS\DATA\Grand Hotel

SQL Server: Server1/SQLServer

SQL Server DB: Grand Hotel

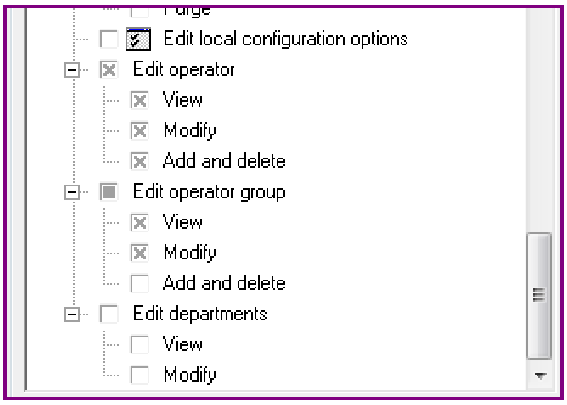
Then clicking on the right bottom we can find where the MS-Access DB is located. Then we will name the new SQL DB and we have to specify which is the SQL server program we want to work with. When all this has been specified we can click on the start upgrade, if everything has been properly configured the migration will be successfully done.

Operator competencies

The administrator must specify program operators and their competencies. In other words, which options of the main menu operators will be allowed to use.

The administrator could also define its own and front desk operators' program access passwords.

Moreover, the super administrator can concede rights to other group operators in order to let them create operators for their own group. But those won't be able to do so.



- □ Purge
- □ ☑ Edit local configuration options
- ⊟ ☒ Edit operator
  - ☒ View
  - ☒ Modify
  - ☒ Add and delete
- ⊟ ■ Edit operator group
  - ☒ View
  - ☒ Modify
  - □ Add and delete
- ⊟ □ Edit departments
  - □ View
  - □ Modify

Go to pop-up menu TOOLS/ OPERATORS AND PERMISSIONS/ OPERATORS, as is shown in the Figure.

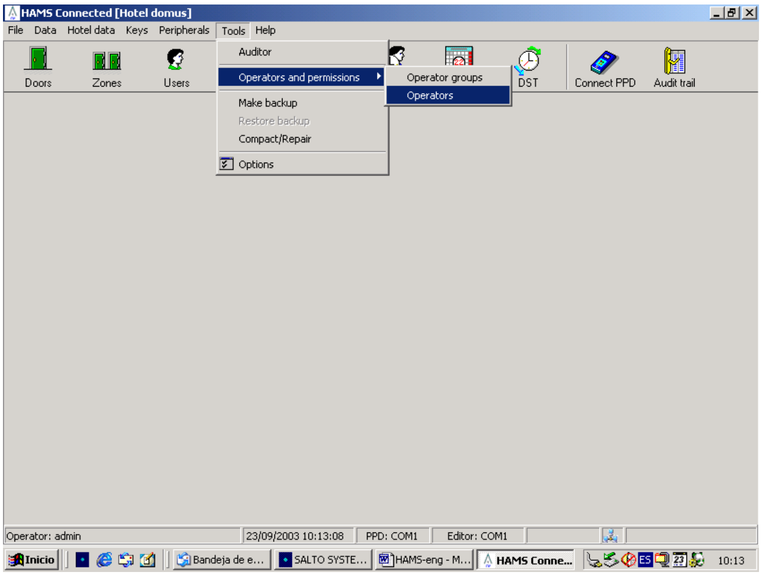
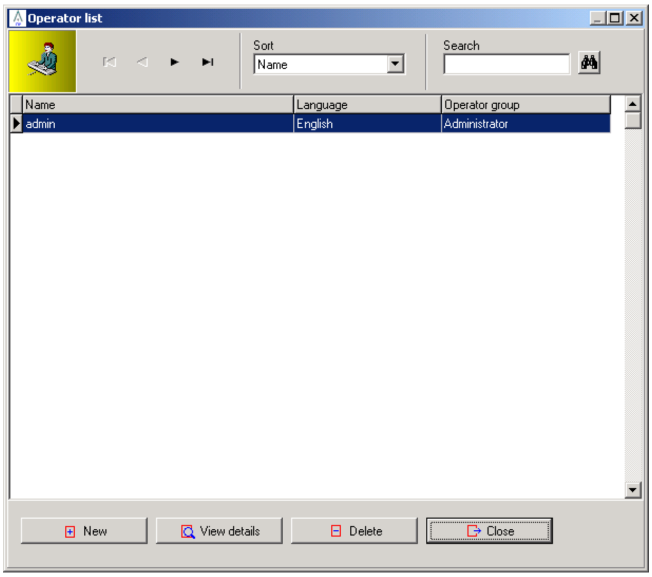


Figure 5

By default, the system offers one operator, ADMINISTRATOR.

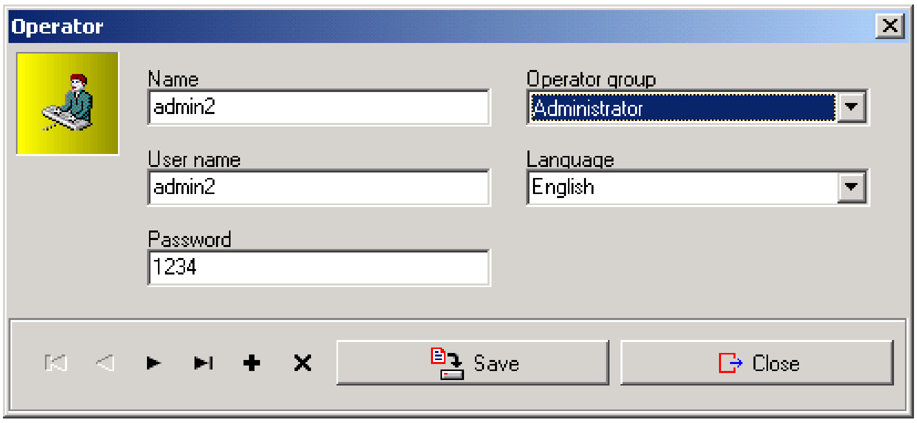


Name	Language	Operator group
admin	English	Administrator

Figure 6

You will probably be required to create further operators.

To create a new operator, click the NEW button on the bottom part of the window. A blank window will be displayed, as shown in the following Figure:


Operator

Name: admin2

User name: admin2

Password: 1234

Operator group: Administrator

Language: English

Figure 7

- You will have to write the operator's name, his user name (that is stored at the login), and a password.

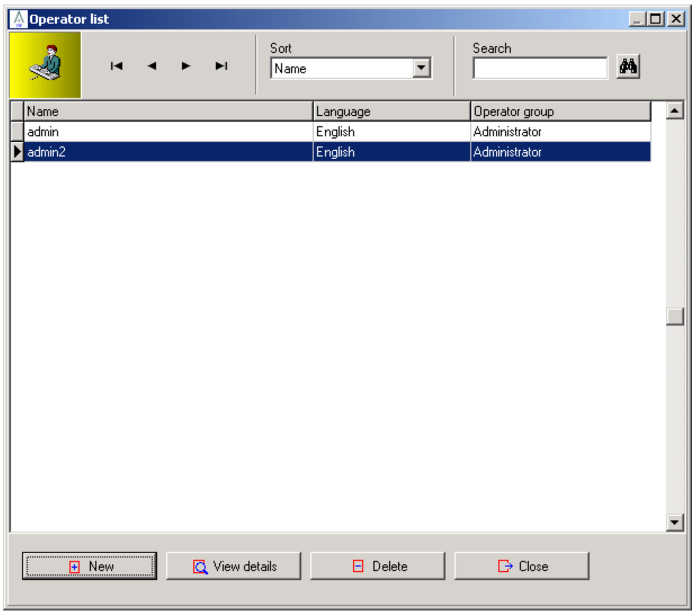
- The system brings, by default, 1 operator group: Administrator.

- Specify also the language this operator will use when running the application.

- Next, save changes and close the window.

- You must immediately inform the password you have just registered to the operator, since he will need it to access the application.

Follow this procedure as many times as new operator you want to create, and you will see how the operator list enlarges.



Operator list

Sort: Name

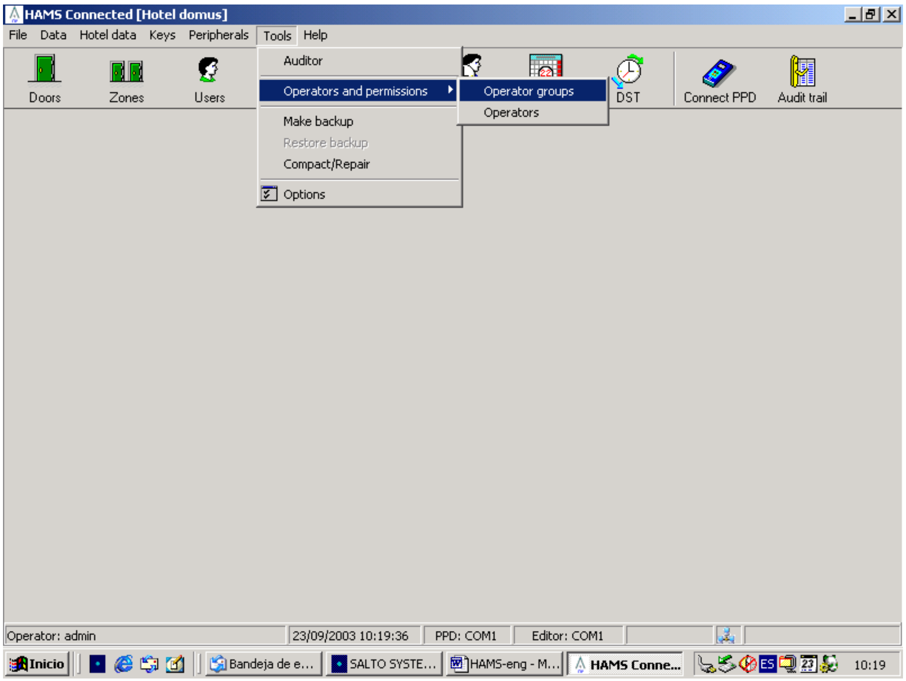
Search:

Name	Language	Operator group
admin	English	Administrator
admin2	English	Administrator

Figure 8

Once you have created the necessary new operators on your system, you may close this window and return to the TOOLS/ OPERATORS AND PERMISSIONS / OPERATORS GROUPS pull-up menu. Within this option operator competencies can be set.

.



HAMS Connected [Hotel domus]

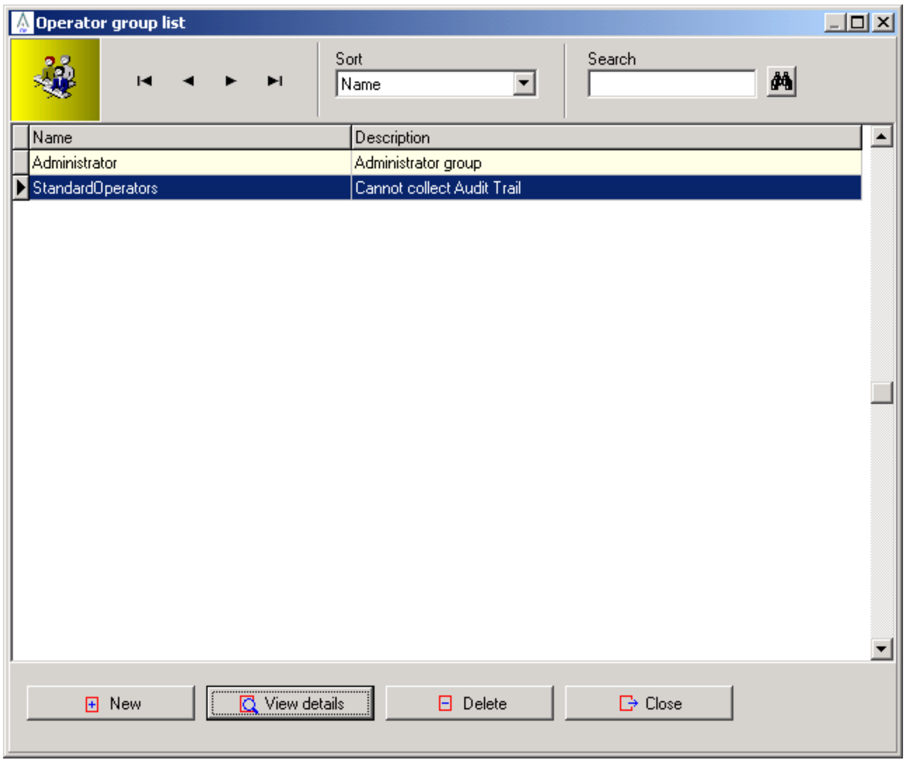
Operator: admin | 23/09/2003 10:19:36 | PPD: COM1 | Editor: COM1

Figure 9

Operators belonging to ADMINISTRATOR group may have access to full program menu functionality.

Administrator has the ability to create further operator groups, if he seems it convenient.

To create a new group, click the NEW button on the bottom part of this window.

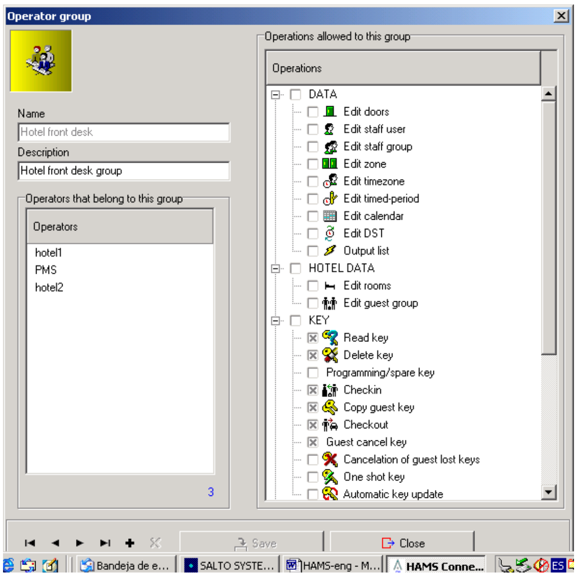


Name	Description
Administrator	Administrator group
StandardOperators	Cannot collect Audit Trail

Figure 10

In order to modify competencies of an existing group, you must highlight this group in the list (the line turns blue) and click the VIEW DETAILS button.

A window like that of the Figure 11 will be displayed.



Name: Hotel front desk

Description: Hotel front desk group

Operators that belong to this group

Operators
hotel1
PMS
hotel2

3

Operations allowed to this group

Operations

- □ DATA
  - □ Edit doors
  - □ Edit staff user
  - □ Edit staff group
  - □ Edit zone
  - □ Edit timezone
  - □ Edit timed-period
  - □ Edit calendar
  - □ Edit DST
  - □ Output list
- □ HOTEL DATA
  - □ Edit rooms
  - □ Edit guest group
- □ KEY
  - ☒ Read key
  - ☒ Delete key
  - □ Programming/spare key
  - ☒ Checkin
  - ☒ Copy guest key
  - ☒ Checkout
  - ☒ Guest cancel key
  - □ Cancelation of guest lost keys
  - □ One shot key
  - □ Automatic key update

Figure 11

- From this window, the operator may add or delete program functionality, by clicking with the mouse on the “check boxes” located on the left-hand side of every option. If the option is selected, this option will appear as an enabled option for the operator handling the program.

  Were the option is left blank; it will not appear as an enabled option for the operator within this group.

- The administrator should save changes when all modifications have been completed.

Import tool

Data type

The importable information is as follows:

- User list: title, first name, last name, general purpose field #1, #2 and #3.
- Door list: name and description.
- Zone list: name and description.
- Access level list: name and description.
- Access permissions between users and doors: user compound name and door name.
- Access permissions between users and zones: user compound name and zone name.
- Access permissions between access levels and doors: access level and door name.
- Access permissions between access levels and zones: access level and zone name.
- Relationships between doors and zones: door and zone name.

Note that the import process is not made on a transaction basis: this means that, if by any chance, errors occur in the middle of the process, the whole operation IS NOT rolled back or undone. Instead, errors are left aside and the import process continues until the end of file is reached.

Two file format are supported, namely, plain text (*.txt, *.csv, ...) and Excel file (*.xls).

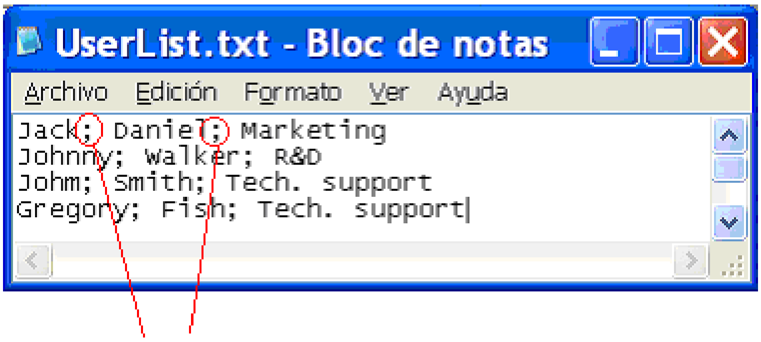
Text file

The file must contain just plain text. Any document file containing extra formatting data (such as MS-Word *.doc, Rich Text File *.rtf, etc ...) are not supported.

Additionally, each of the characters in the text file must occupy just 1 byte (like in the ASCII character set): if a given file contains characters with 2 or more bytes long (like in the UNICODE character set), then data is not correctly imported.

Each row in the file corresponds to a row in the SALTO DB. Within a row, fields (or columns) must be separated by a character of your choice (normally, ';').

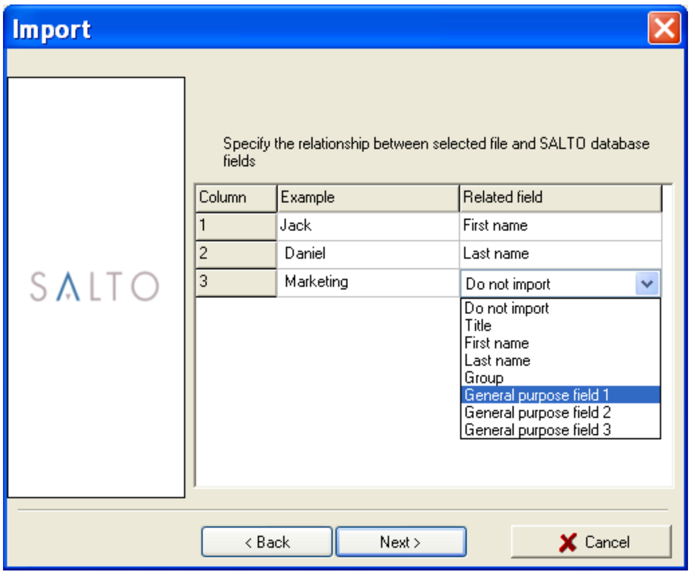
When importing, you must firstly specify the line at which data starts (zero-based) and the separator character. Afterwards, you must match each column in the text file with the corresponding SALTO field, as shown in the following picture:



```
Jack; Daniel; Marketing
Johnny; Walker; R&D
Johm; Smith; Tech. support
Gregory; Fish; Tech. support
```

Separator character

(Fig.1)



Specify the relationship between selected file and SALTO database fields

Column	Example	Related field
1	Jack	First name
2	Daniel	Last name
3	Marketing	Do not import

(Fig. 2)

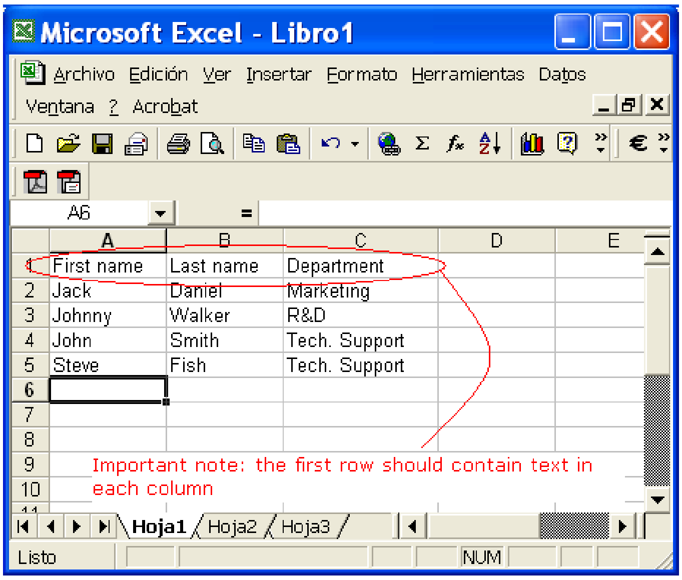
Excel file

All the data to be imported must be contained on one 'sheet'. It is strongly recommended for the excel file to include (within in the first positions) a row containing just text (for example, a header row containing titles for each column).

When importing data, the wizard asks you the name of the excel sheet at which data is located and the starting line (zero-based). As in the text format, you must also match each column in the excel sheet with the corresponding SALTO field.

Importing User List, Door List, Zone List and Access level List:

In the example below you will find the steps to import a User List from an Excel file. The procedure to import Door List, Zone List and Access level List is the same.

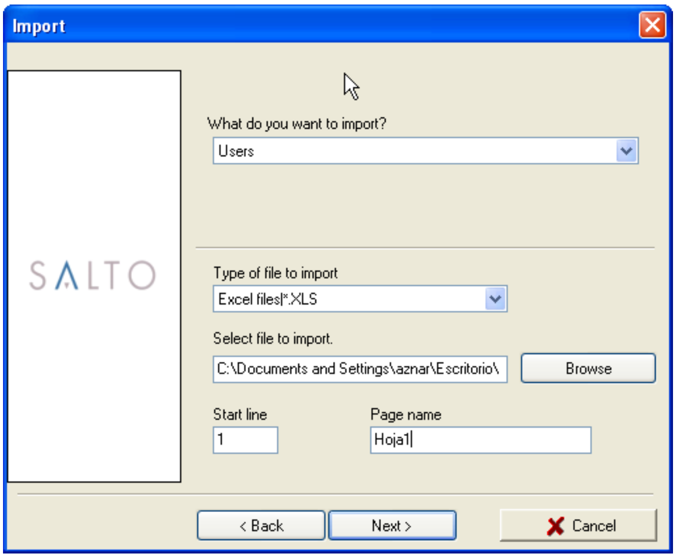


	A	B	C	D	E
1	First name	Last name	Department		
2	Jack	Daniel	Marketing		
3	Johnny	Walker	R&D		
4	John	Smith	Tech. Support		
5	Steve	Fish	Tech. Support		

Important note: the first row should contain text in each column

(Fig. 3)

Next step is to open the import tool and fill the fields:



What do you want to import? Users

Type of file to import: Excel files|*.XLS

Select file to import: C:\Documents and Settings\aznar\Escritorio\

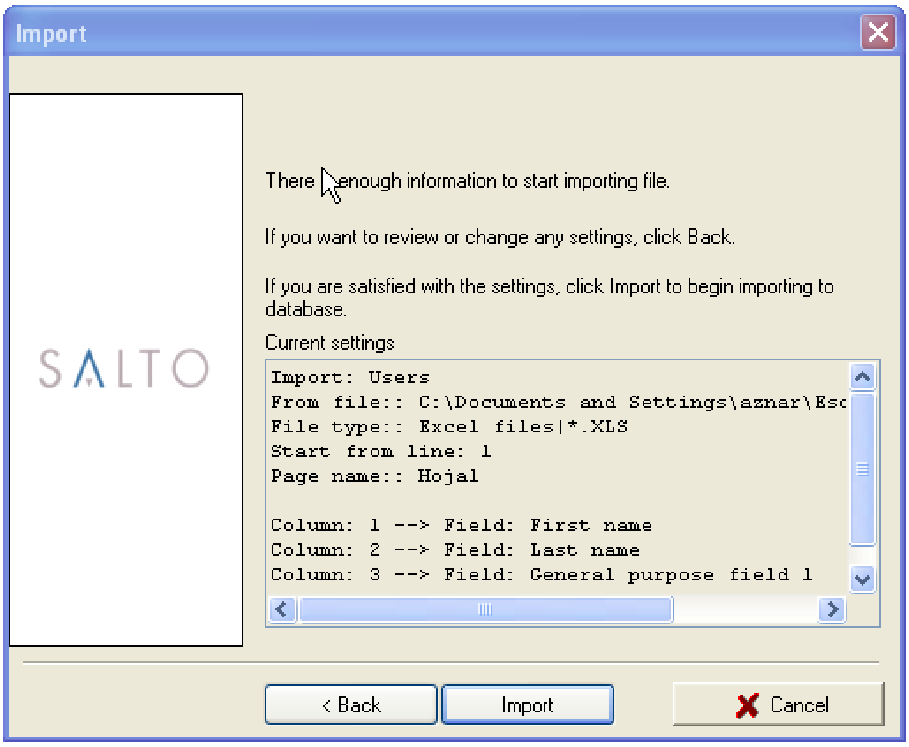
Start line: 1

Page name: Hoja1

(Fig. 4)

First of all delect what we want to import (users, doors, etc.) then select the type of file that we want to import. Next step is select the file we want to import, we have to use the browse button to find the file. After this we have to select the start line and finally the page name.

After this we will have to specify the relationship between selected file and SALTO database fields as shown in Fig. 2.The next screen will show a summary where we can see all selected options



There enough information to start importing file.

If you want to review or change any settings, click Back.

If you are satisfied with the settings, click Import to begin importing to database.

Current settings

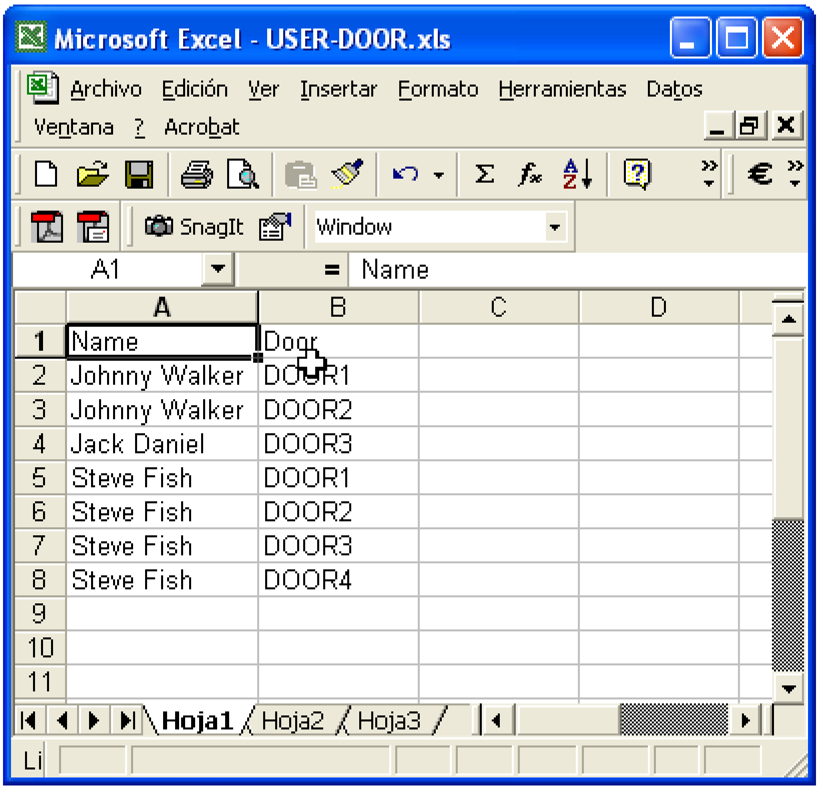
```
Import: Users
From file:: C:\Documents and Settings\aznar\Esc
File type:: Excel files|*.XLS
Start from line: 1
Page name:: Hoja1

Column: 1 --> Field: First name
Column: 2 --> Field: Last name
Column: 3 --> Field: General purpose field 1
```

(Fig. 5)

Finally a screen with the result of the import will be shown. If any error has happened during the process it will be shown in this window.

Importing Access permissions between Users and Doors, User and Zones, Access levels and Zones or Doors and Zones.

The procedure does not change much from importing users, the main difference is in the Excel File: We have to write the user´s complete name, as it is written in the “Name” field in the users profile. If we want to add more than one door to a user we have to make it in different lines as shown in (Fig. 6).



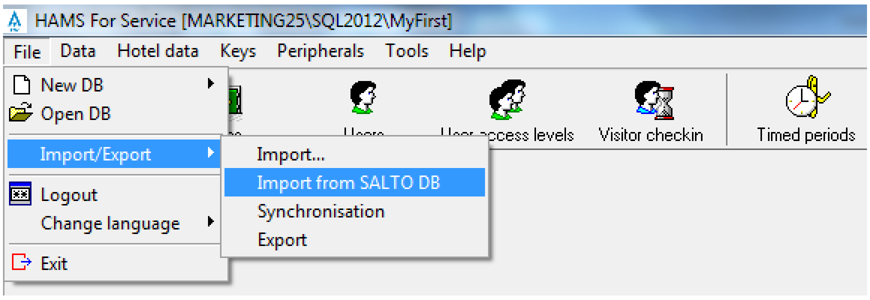
Microsoft Excel - USER-DOOR.xls
Archivo Edición Ver Insertar Formato Herramientas Datos
Ventana ? Acrobat
SnagIt
Window
A1
= Name
Hoja1
Hoja2
Hoja3
Li

	A	B	C	D
1	Name	Door		
2	Johnny Walker	DOOR1		
3	Johnny Walker	DOOR2		
4	Jack Daniel	DOOR3		
5	Steve Fish	DOOR1		
6	Steve Fish	DOOR2		
7	Steve Fish	DOOR3		
8	Steve Fish	DOOR4		
9				
10				
11				

(Fig. 6)

All the following steps are exactly the same as to import User List.

IMPORT FROM A SALTO DB (Merging)

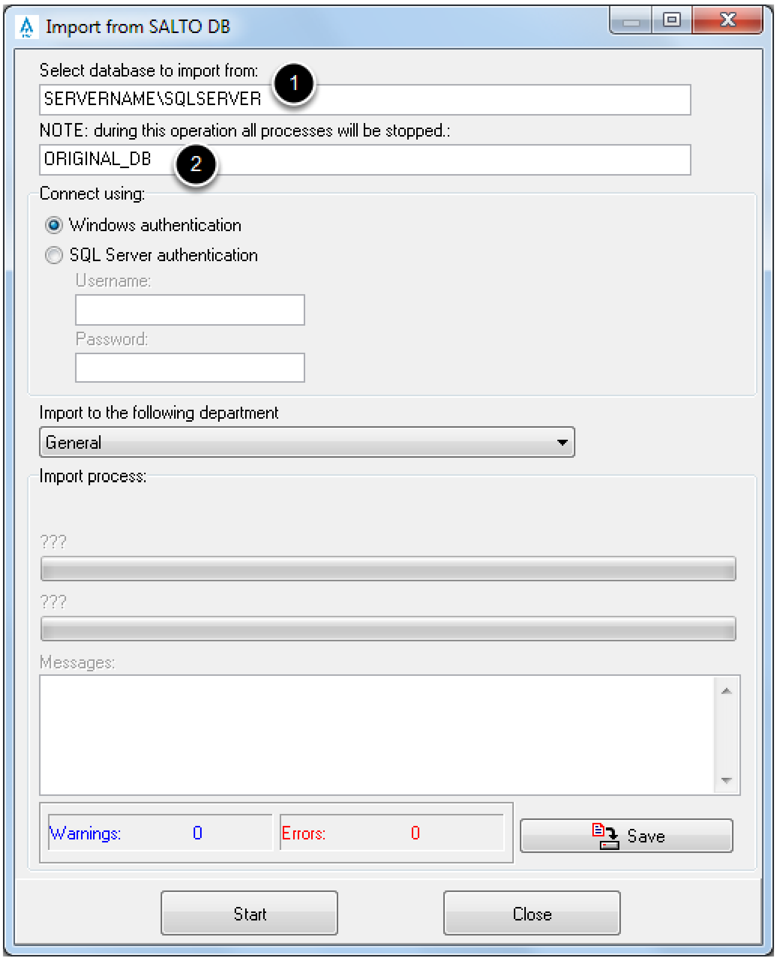


With the "Import from SALTO DB" tool it is possible to merge different DB in a single one.

The departmental option must be disabled from the ORIGINAL department and all the components must be into the general department.

The target DB can have one or various departments. When merging, it will be possible selecting to import to the general department or to a different one.

Origin of the DB



Import from SALTO DB

Select database to import from: 1

SERVERNAME\SQLSERVER

NOTE: during this operation all processes will be stopped.:

ORIGINAL_DB 2

Connect using:

● Windows authentication

○ SQL Server authentication

Username:

Password:

Import to the following department

General

Import process:

???

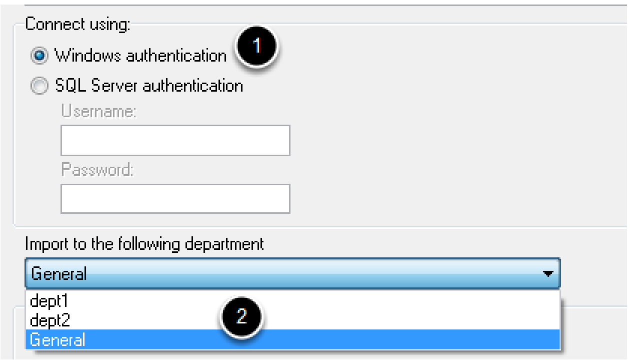
???

Messages:

Warnings: 0 Errors: 0

When clicking on "Import from SALTO DB", the window above will appear.

Fill where the ORIGINE DB is from (1) and its NAME (2).



Connect using:

● Windows authentication 1

○ SQL Server authentication

Username:

Password:

Import to the following department

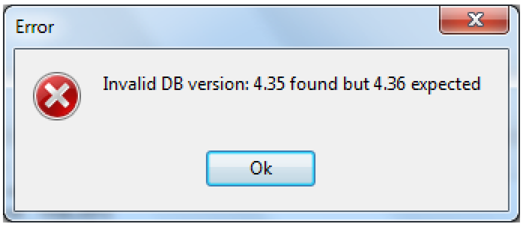
General

Select the type of authentication, Windows or SQL (1).

And finally select the department where the original data will be located. If the target DB has only one department, leave it in General.

After this, click Start.

Invalid DB version



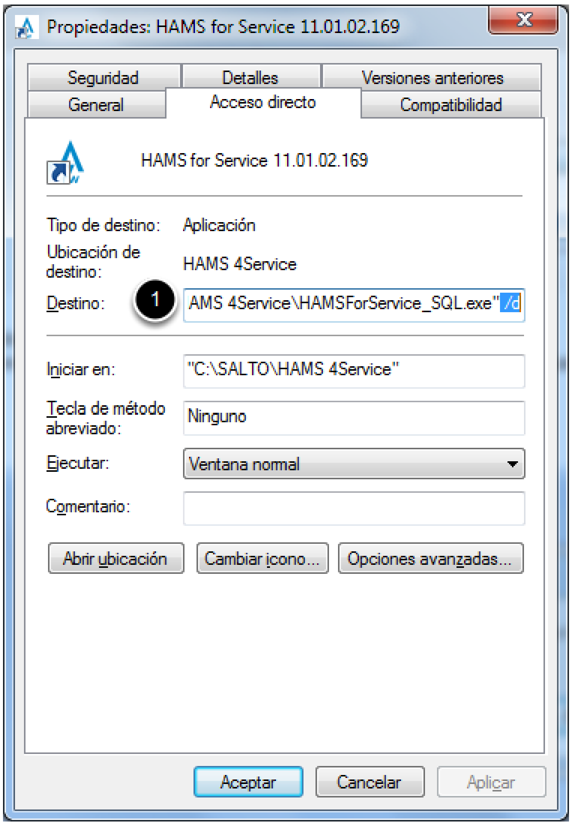
Error

Invalid DB version: 4.35 found but 4.36 expected

In case the DB does not have the same DB version, the message above will appear.

To solve it, first open the original DB with the same software version used with the target DB. Then repeat the process and click Start.

IMPORTANT notes



Propiedades: HAMS for Service 11.01.02.169

HAMS for Service 11.01.02.169

Tipo de destino: Aplicación

Ubicación de destino: HAMS 4Service

Destino: AMS 4Service\HAMSForService_SQL.exe" /d

Iniciar en: "C:\SALTO\HAMS 4Service"

Tecla de método abreviado: Ninguno

Ejecutar: Ventana normal

Comentario:

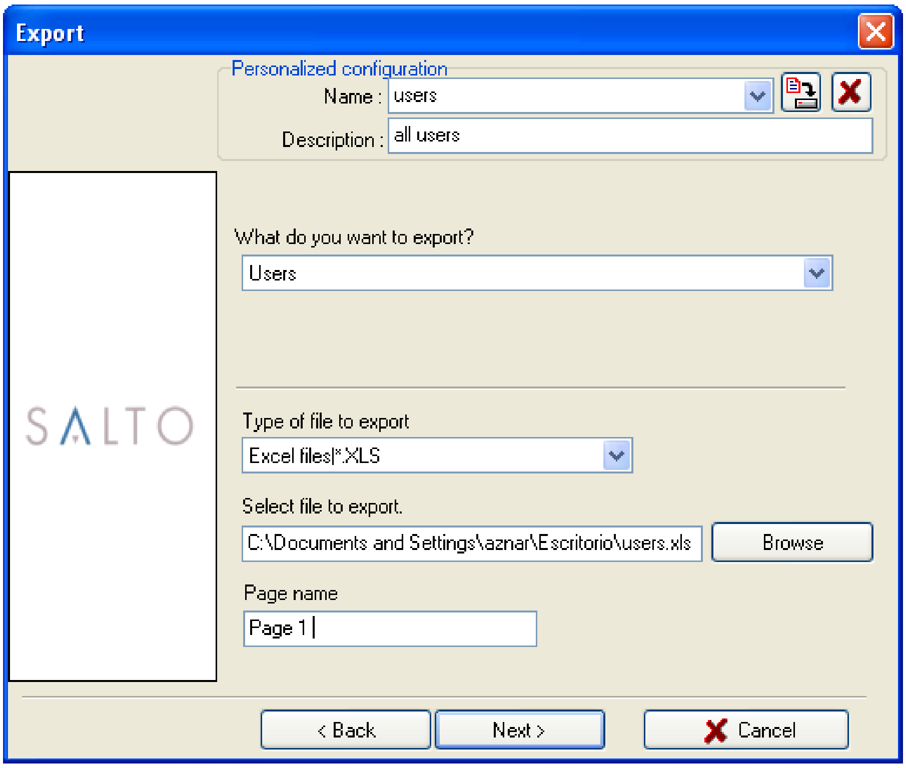
The SITE CODE of the original DB won't be maintained, the final DB will have the target DB site code. The doors belonging to the original DB will have to be re initialized and re encode the user keys.

This option will not be visible by default. In order to activate it, "_/d" will have to be written on the shortcut target as shown above (1) [**...HAMSForService_SQL.exe" /d**]

5.Export:

In order to export data from the database into a txt., xls. File we have to go to the menu FILE/ EXPORT/IMPORT/ EXPORT

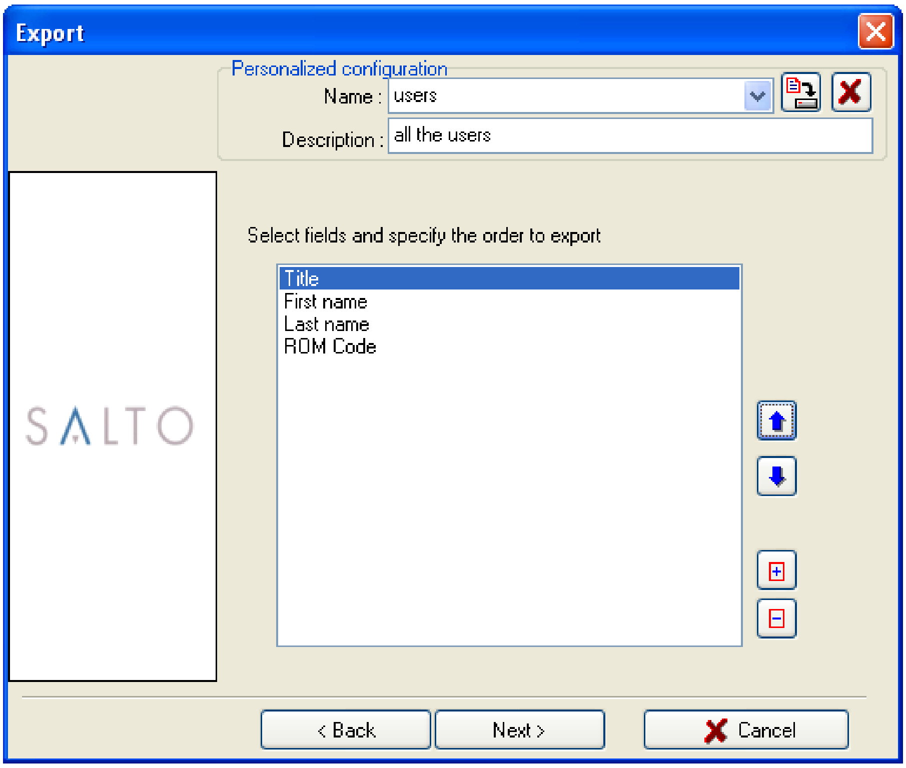
Once we have selected the option we will see a confirmation window, after pressing Next > we will find the following selection window (Fig. 1)



Personalized configuration
Name : users
Description : all users
What do you want to export?
Users
Type of file to export
Excel files|*.XLS
Select file to export.
C:\Documents and Settings\aznar\Escritorio\users.xls
Browse
Page name
Page 1

(Fig. 1)

We will start giving a name and description to the file, after that we select what do we want to export: Users, Doors, Access levels and or Zones. In the next field we have to select the type of file where we want to export the data: txt or xls. Once we have selected the type of file we will select the file where we want to export the data. Once we have filled up these fields we will press Next >. The following window will appear (Fig. 2)



Export

Personalized configuration

Name : users

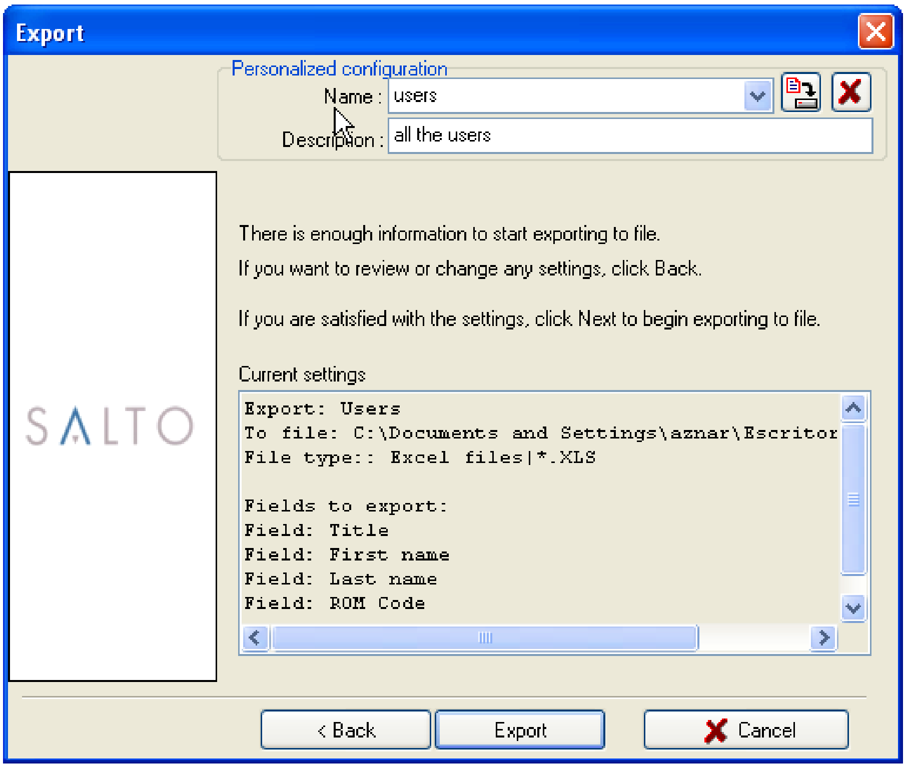
Description : all the users

Select fields and specify the order to export

Title
First name
Last name
ROM Code

(Fig. 2)

In this window we will have to select the fields that we want to export and the order by. We have to press ⊞ to add fields and ⊟ to remove the ones that we don´t want. We will use the arrows ⬆ and ⬇ to change the order of the fields. Once we have made the whole selection we press Next >. We will find the following confirmation window (Fig. 3)



There is enough information to start exporting to file.
If you want to review or change any settings, click Back.

If you are satisfied with the settings, click Next to begin exporting to file.

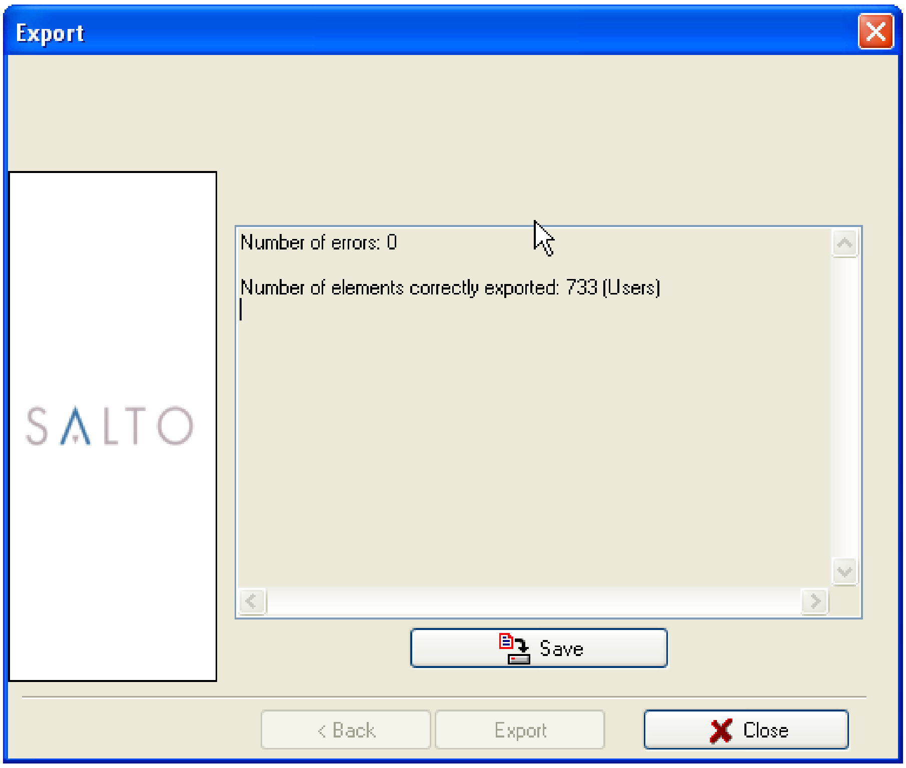
Current settings

```
Export: Users
To file: C:\Documents and Settings\aznar\Escritor
File type:: Excel files|*.XLS

Fields to export:
Field: Title
Field: First name
Field: Last name
Field: ROM Code
```

(Fig. 3)

Once we have confirmed all the data we press the Export button. We can save the export personal configuration for future applications by pressing .

Once we have completed the exportation, the software will show the following window: (Fig. 4).



Number of errors: 0

Number of elements correctly exported: 733 (Users)

(Fig. 4)

6. Administrator operator

The administrator (or administrators) is responsible to design the initial locking schedule of the building and facilities and editing cards that will allow employees access to the various zones and doors.

In this manual, with a view to explaining how this SALTO RW software is used, we have used a hypothetical locking schedule as a sample to illustrate the general procedure.

To begin with, it is important to note that almost every function of the software can be performed by clicking the icons on the Toolbar (except those related to the hotel exclusive data). Parameters can be defined along the way in any order, though it is advisable to follow the order given below:

0. **doors**
1. **zones**
2. **outputs**
3. **time zones**
4. **time periods**
5. **calendars**
6. **time change**
7. **user access levels**
8. **users and key assignment**
9. **PPD usage**

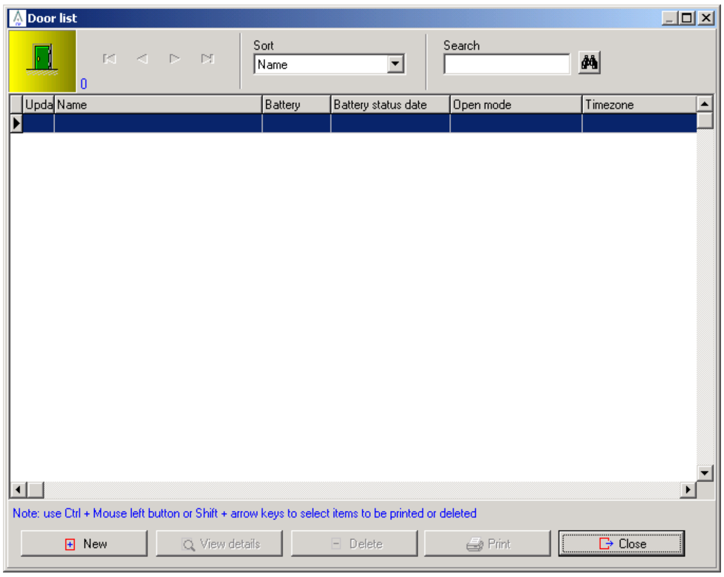
It is important to define time periods, time zones and calendars, before proceeding to PPD initiation of the doors (except for online doors, which can be initialized from the control PC straight).

Doors

Using this menu option we will create the access control for the users doors (electronic locks and wall readers alike), excluding the guests rooms.

Firstly, move the mouse over the Toolbar icon representing doors.

If it is the first time we open this option, the door list will be empty.



Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 22

- Click on the NEW button to add the first door to the list.

- In the pop-up window that will be displayed, we will view the fields we will fill in. (Except that of users, which cannot be specified as they have not been defined yet)

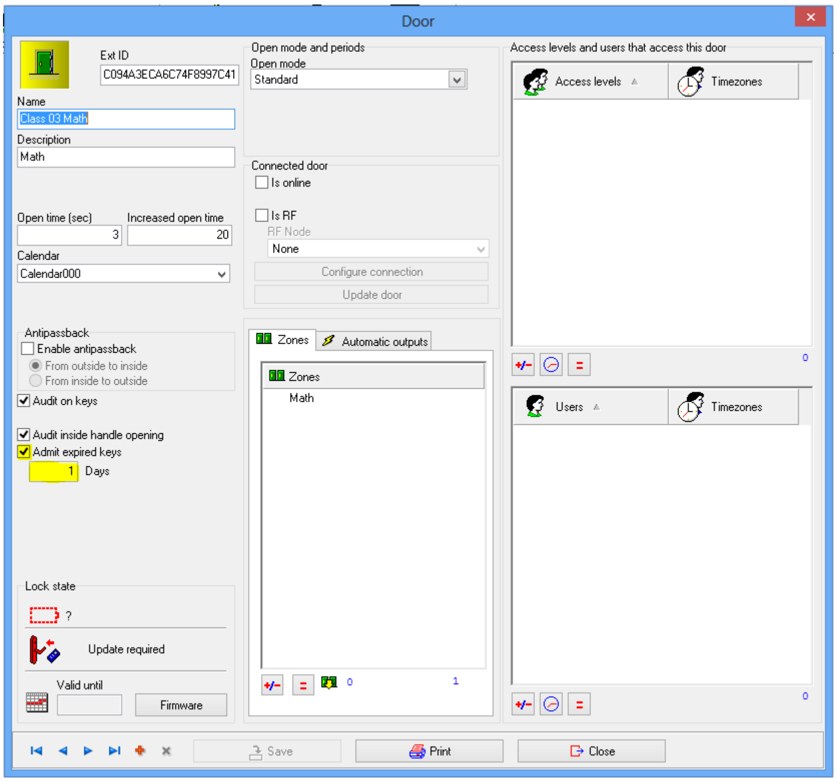
- Write the name of the first door.

- You can write a description for the door, if the name is no representative enough.

- ADMIT EXPIRED KEYS:

Door can be set up to admit cards already expired for a certain amount of days. This could be applied to low security offline doors located before an online hotspot, and in order to allow users get access to the hotspot to update their cards.
This time can be set up from 0 to 255 days.

Next, we set the characteristics for this door:



Door

Ext ID: C094A3ECA6C74F8997C41

Name: Class 03 Math

Description: Math

Open time (sec): 3

Increased open time: 20

Calendar: Calendar000

Antipassback

□ Enable antipassback

● From outside to inside

○ From inside to outside

☑ Audit on keys

☑ Audit inside handle opening

☑ Admit expired keys

1 Days

Lock state

?

Update required

Valid until

Open mode and periods

Open mode: Standard

Connected door

□ Is online

□ Is RF

RF Node: None

Zones: Math

Access levels and users that access this door

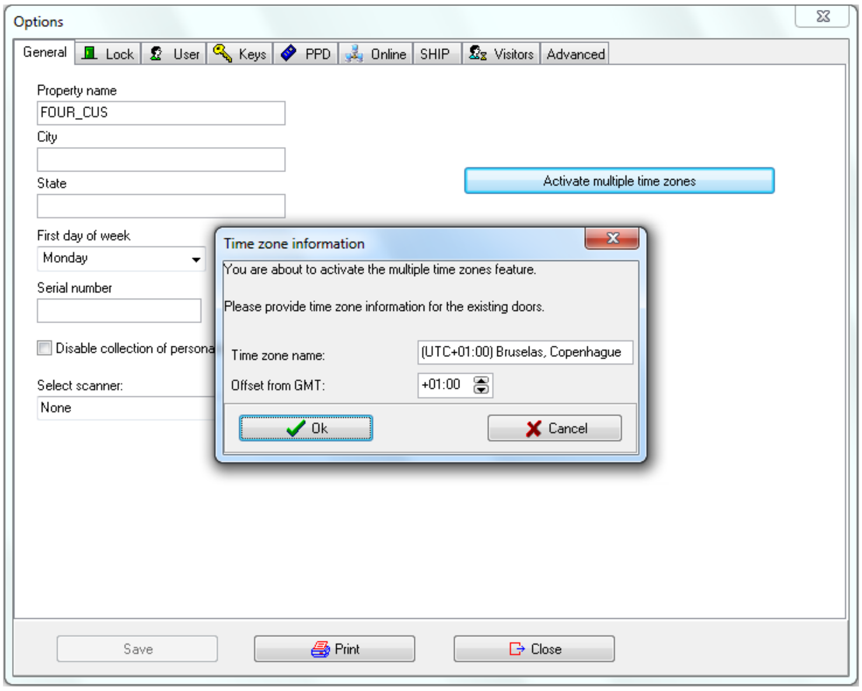
Figure 23

- The OPEN TIME field determines the time passed from the moment a user opens a door until the electronic system locks it again. By default, this time value is 10 seconds.

- The INCREASED OPEN TIME field determines an extended open time, especially designed for handicapped or "hands full" people. This time the value is 20 seconds, by default.

- Geographical Time Zones can be set up in the SALTO software to avoid time conflicts in installations with access points in different Geographical Time Zones sharing the same database. This could happen in installations within big countries like Canada, United States, Russia, and Australia, or access points from the same database in countries with different Time Zones, for instance, United Kingdom and Germany. This is important for the system to apply the different Timed Periods correctly to the access points in their specific geographical area or country, and also for the users in that area or country to have the correct access Timezones in regards to the same geographical area / time zone.

First of all, this feature has to be activated in the General option Menu, General tab, so the option is available in the software.



Property name: FOUR_CUS
City
State
First day of week: Monday
Serial number
□ Disable collection of persona
Select scanner: None

Time zone information

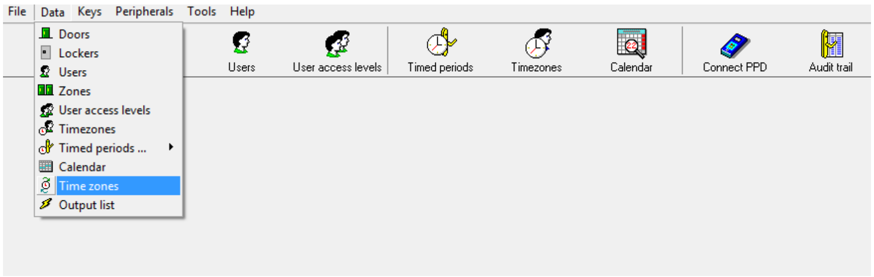
You are about to activate the multiple time zones feature.

Please provide time zone information for the existing doors.

Time zone name: (UTC+01:00) Bruselas, Copenhague
Offset from GMT: +01:00

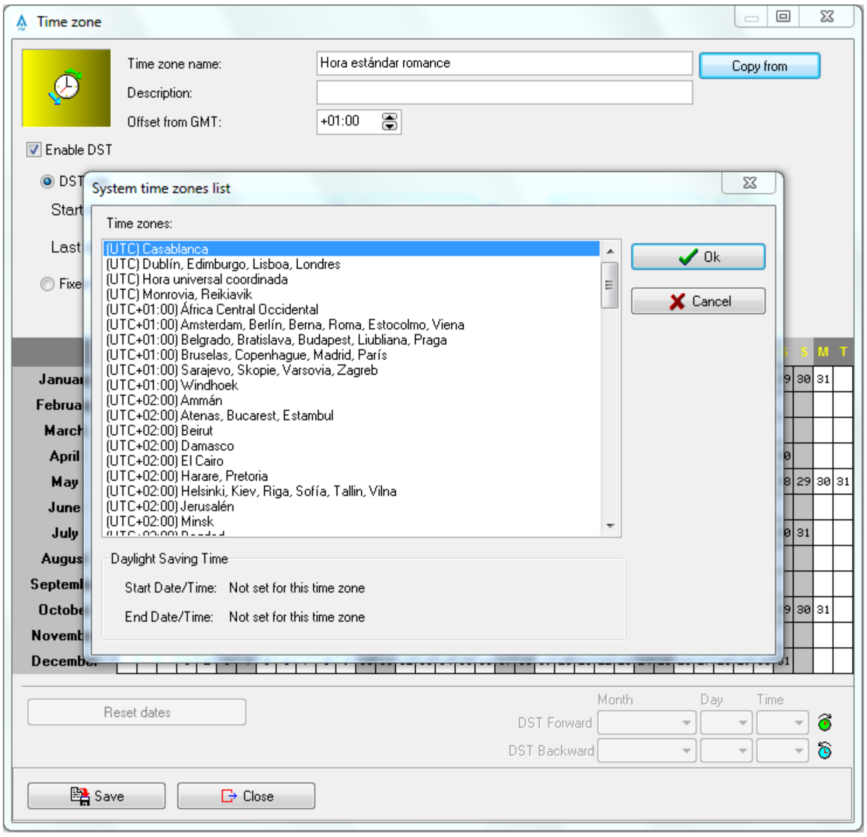
When activating the Time Zones, the Time Zone must be specified, as well as the offset from the GMT.

Different time zones can be created just by going to the Data menu and selecting the Time Zones option.



Just by clicking the New button, a new time zone can be created. The Time Zones in the list will be available later on to be assigned to the different access points, and avoid any time conflict with the time base at the database location, and the access points' location, as explained above.

Time Zones can be created from scratch, specifying the GMT and setting up the Daylight Saving time days manually, or the Official Time Zones can be used to set up the Time Zone, just by clicking the Copy From button, and selecting the Time Zone from the list that will pop up.



Time zone name: Hora estándar romance

Description:

Offset from GMT: +01:00

☑ Enable DST

Time zones:

(UTC) Casablanca
(UTC) Dublín, Edimburgo, Lisboa, Londres
(UTC) Hora universal coordinada
(UTC) Monrovia, Reikiavik
(UTC+01:00) África Central Occidental
(UTC+01:00) Amsterdam, Berlín, Berna, Roma, Estocolmo, Viena
(UTC+01:00) Belgrado, Bratislava, Budapest, Liubliana, Praga
(UTC+01:00) Bruselas, Copenhague, Madrid, París
(UTC+01:00) Sarajevo, Skopie, Varsovia, Zagreb
(UTC+01:00) Windhoek
(UTC+02:00) Ammán
(UTC+02:00) Atenas, Bucarest, Estambul
(UTC+02:00) Beirut
(UTC+02:00) Damasco
(UTC+02:00) El Cairo
(UTC+02:00) Harare, Pretoria
(UTC+02:00) Helsinki, Kiev, Riga, Sofía, Tallin, Vilna
(UTC+02:00) Jerusalén
(UTC+02:00) Minsk

Daylight Saving Time

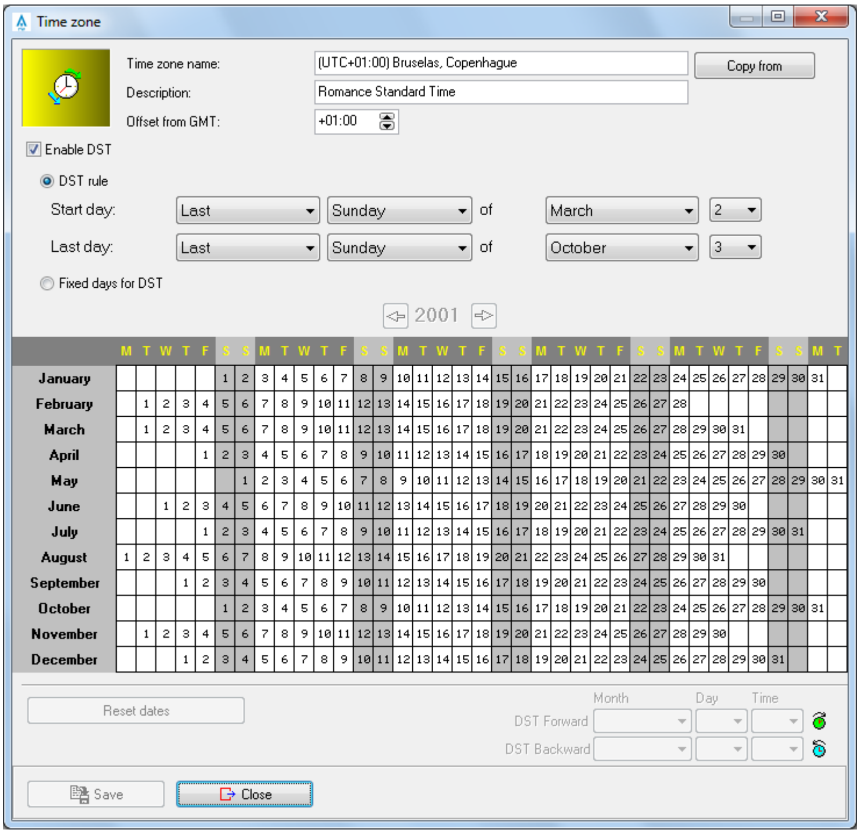
Start Date/Time: Not set for this time zone

End Date/Time: Not set for this time zone

Once the Time Zone is selected, the Daylight Saving Time (also called DST) days can be activated. Once active, there are two ways to configure these days:

-Selecting the Standard DST Rule.
-Fixed DST Days: Selecting two days in the calendar,

which always will be taken to make the time change.



Time zone

Time zone name: (UTC+01:00) Bruselas, Copenhague

Description: Romance Standard Time

Offset from GMT: +01:00

☑ Enable DST

● DST rule

Start day: Last | Sunday | of | March | 2

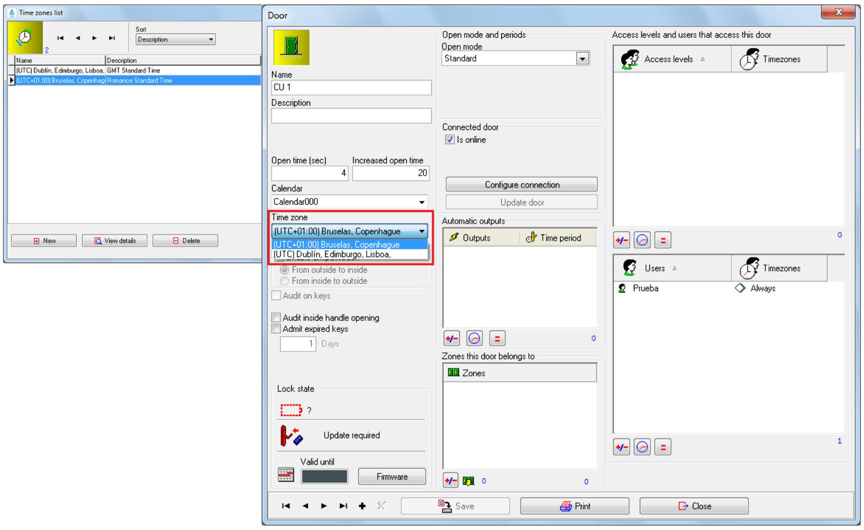
Last day: Last | Sunday | of | October | 3

○ Fixed days for DST

2001

	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T
January						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
February		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28								
March		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
April					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
May							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
June			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30					
July					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
August	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
September				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30				
October						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
November		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						
December				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			

Once different Time Zones have been created, access points located in different Geographical Time Zones can be set up to follow the time and Daylight Saving Times at that location.



Time zones list

Sort: Description

Name	Description
(UTC) Dublín, Edimburgo, Lisboa,	GMT Standard Time
(UTC+01:00) Bruselas, Copenhagı	Romance Standard Time

Door

Name: CU 1

Description:

Open time (sec): 4

Increased open time: 20

Calendar: Calendar000

Time zone: (UTC+01:00) Bruselas, Copenhague
(UTC+01:00) Bruselas, Copenhague
(UTC) Dublín, Edimburgo, Lisboa,

● From outside to inside
○ From inside to outside
□ Audit on keys
□ Audit inside handle opening
□ Admit expired keys
1 Days

Lock state: ?
Update required
Valid until

Open mode and periods
Open mode: Standard

Connected door
☑ Is online

Users	Timezones
Prueba	Always

- The OPEN MODE field determines the electronic locks working mode. It can be chosen from the several available:

1. **Standard mode:** the lock will only open if you use an authorized card, within its allowed time zones.

2. **Office mode:** the lock will be opened for any user who wishes to gain access. It is not essential to have an authorized card key. In order to enable this operation mode, it is necessary to insert an authorized key card on the slot while we keep the inner handle pressed down. If you want to disable the office mode, repeat this procedure.

3. **Timed office mode:** It is the same as the operation mode in the previous example, except for a difference that lies in the fact that the office mode can only be enabled within a given time framework, called a PERIOD. Note that the lock will automatically revert to the Standard mode at the end time period. If you choose this mode, you will need to assign one of the opening periods available. Next, you will have to define a period, using the PERIOD tool, from the Toolbar. (As detailed later).

4. **Automatic opening mode:** Quite similar to the previous mode, but the door can switch to and from office mode automatically, without any manual user operation. In this mode it is also necessary to set a time period (defined with the PERIOD tool).

5. **Toggle:** In this mode, presenting a valid user key will set the door in office mode, without needing to hold down the inner handle. The next valid key presented will cancel office mode. This will continue "toggling" the office setting on presentation of each valid user key.

6. **Timed toggle:** This mode works in the same way as Toggle above, with the difference that, you can only toggle the door within a set TIME PERIOD.

7. **Automatic opening + office:** The same as "automatic opening "mode except for the fact that out of the opening periods, the escutcheon can be

left in office mode by a user with this attribute enabled.

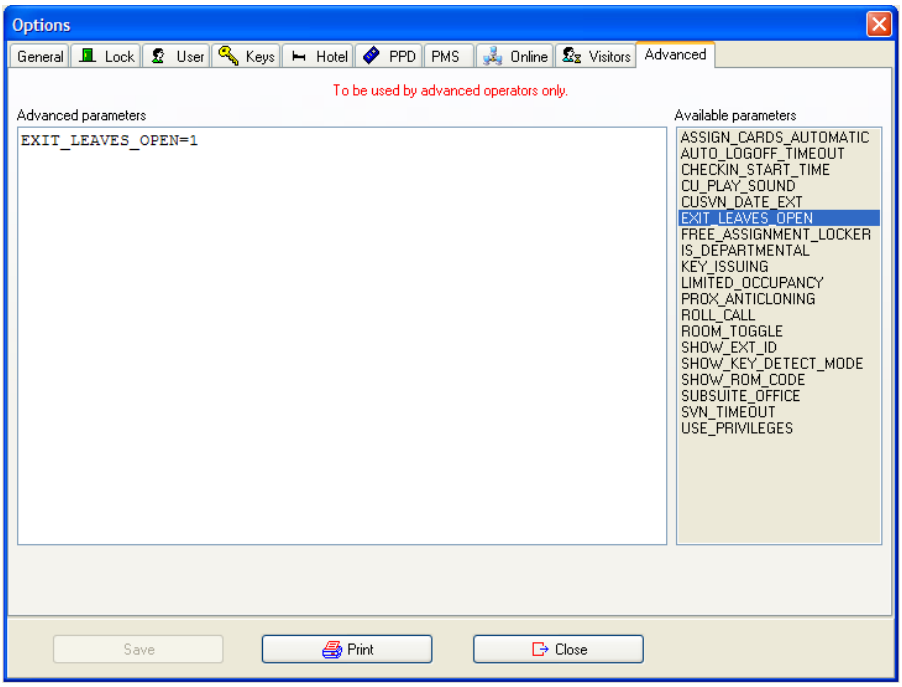
8. **Keypad only:** The door can be opened by just typing a valid code on its keypad, at any time. This code is defined in the door detail window.

9. **Timed keypad:** same as the previous mode except that the code is only used into a specific time interval (period). Out of the period, we can open the door with the key.

10. **Key + PIN:** The door demands 2 conditions in order to open: a valid key and a valid PIN typed in the keypad. This PIN is defined in the user detail window (later).

11. **Key + timed PIN:** same as the previous mode except that the keypad is only active during a specific time interval (period). Out of the period, it is enough with using the key to open the door.

12. Exit leaves open (requires to be activated in General Options): The lock remains open when the inner lever is used.



To be used by advanced operators only.

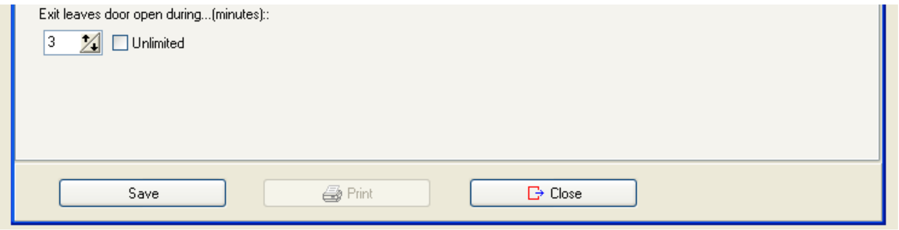
Advanced parameters

```
EXIT_LEAVES_OPEN=1
```

Available parameters

ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CHECKIN_START_TIME
CU_PLAY_SOUND
CUSVN_DATE_EXT
EXIT_LEAVES_OPEN
FREE_ASSIGNMENT_LOCKER
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
PROX_ANTICLONING
ROLL_CALL
ROOM_TOGGLE
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SUBSUITE_OFFICE
SVN_TIMEOUT
USE_PRIVILEGES

- The door stays opened endless by default. This can be temporized in minutes in "lock" tab option (Tools/Configuration/General options).


Exit leaves door open during...(minutes)::

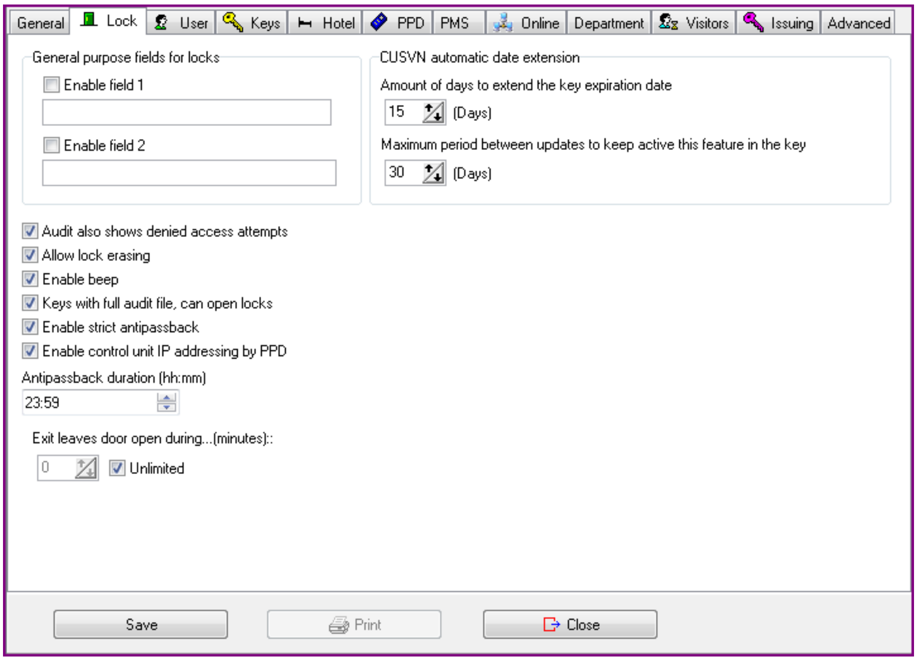
3 □ Unlimited

13. Toggle + Exit leaves open: it is a combination of the two modes. The entrance with a valid ID works in Toggle (alternate opening and closing) mode while the inner handle will activate the Exit leaves open.

- The box called ZONES shows the door access level that the door we are currently defining belongs to. This box will remain blank until the zones are defined.
- ANTIPASSBACK: Anti pass back is the fact that a user is not able to enter again through the same door twice until he has gone out by the exit. (Or until a specific delay time has gone by). This is a protection against different people try to enter with the same user key.
- In the Salto access control it is also possible to get the anti-pass back feature with off line doors. The anti-pass back feature is something that is written in the user card.
- The anti-pass back check box has to be marked if we want anti pass back control on this door. If the door is an online one, it is supposed that there are an entrance wall reader and an exit wall reader. But if the door is not on line, then it is necessary to select the direction of the anti-pass back control – from outside to inside – or from inside to outside-.
- In order to get the anti-pass back function working, it is also necessary to select this option for the user, in the user access profile. (User list). We can define

the anti-pass back delay time in TOOLS/OPTIONS/LOCK.

- If you need to control the entry and the exit then a "Strict" anti-pass back is needed. This means that a user won't be able to go out if he hasn't come in first. In order to activate the "Strict" anti-pass back, go to "Tools/ Advanced Options and on Locks Tab" as you can see in the next picture, and check the "Enable strict anti-pass back" check box.



General purpose fields for locks

□ Enable field 1

□ Enable field 2

CUSVN automatic date extension

Amount of days to extend the key expiration date

15 (Days)

Maximum period between updates to keep active this feature in the key

30 (Days)

☑ Audit also shows denied access attempts

☑ Allow lock erasing

☑ Enable beep

☑ Keys with full audit file, can open locks

☑ Enable strict antipassback

☑ Enable control unit IP addressing by PPD

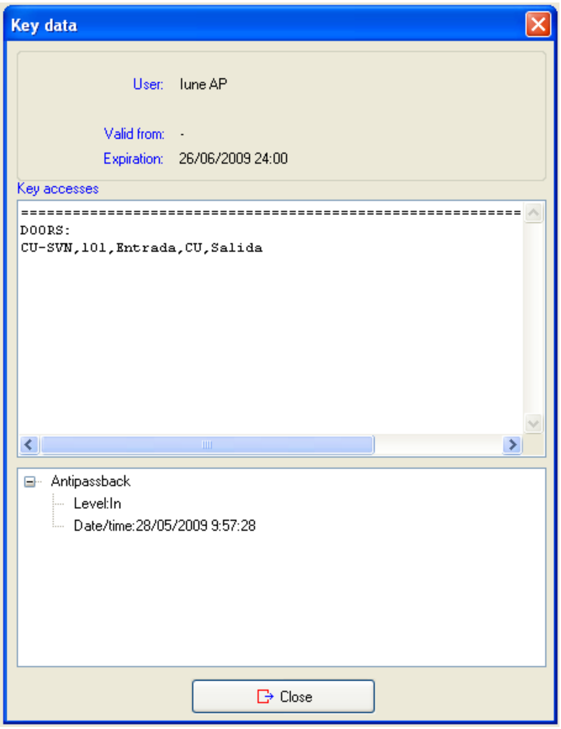
Antipassback duration (hh:mm)

23:59

Exit leaves door open during...(minutes)::

0 ☑ Unlimited

When reading the card and clicking on the "Content>>" button we´ll get the following information.



User: Iune AP

Valid from: -

Expiration: 26/06/2009 24:00

Key accesses

```
==========================================================
DOORS:
CU-SVN,101,Entrada,CU,Salida
```

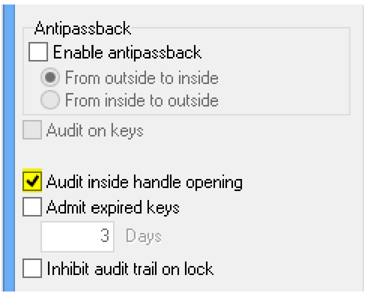
⊟ Antipassback
- Level:In
- Date/time:28/05/2009 9:57:28

If the Anti-pass back option is being used, this window will show the information present on the card ("In" access in the example) with the date and time the card was presented on it.

- The AUDIT ON KEYS check box can be marked if we want the escutcheon to record the opening events on the staff keys. You need to enable this feature on both, escutcheons and keys (users).

- On CALENDAR it can be selected one of the calendar configuration created. This is useful when we have doors in different geographical areas with different calendars configuration.

- Audit inside handle opening is used to audit the exit of the user through the use of the inner lever.



Antipassback

☐ Enable antipassback

● From outside to inside

○ From inside to outside

☐ Audit on keys

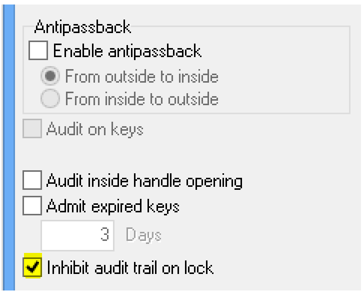
☑ Audit inside handle opening

☐ Admit expired keys

3 Days

☐ Inhibit audit trail on lock

- INHIBIT AUDIT TRAIL ON LOCK will disable the audits collection on this specific door, meaning that NO audit trail will be stored into the door memory. Once this option is enabled, the door must be updated with the PPD.



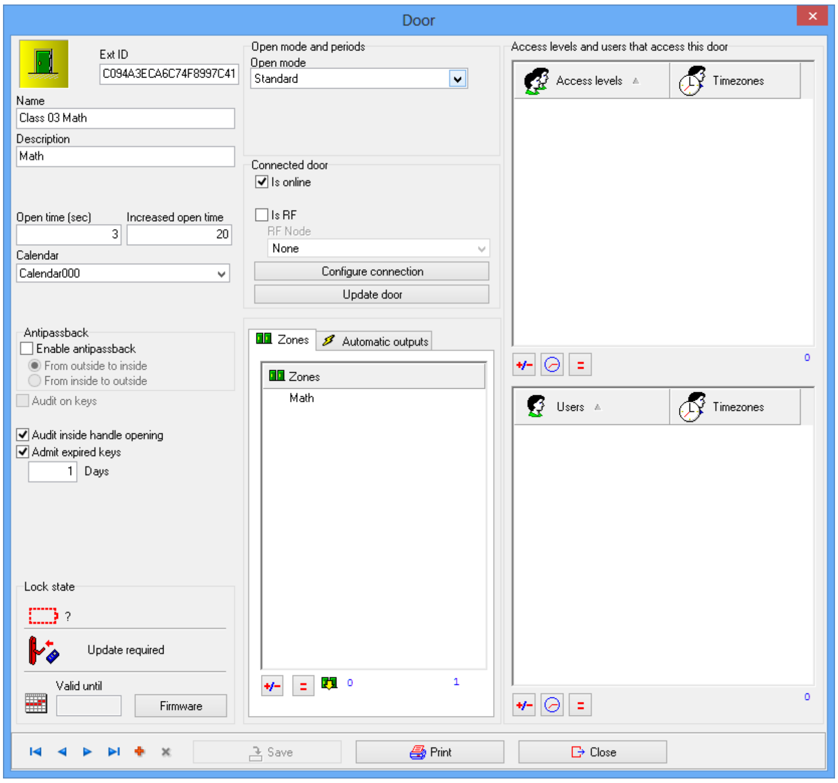
Antipassback
☐ Enable antipassback
● From outside to inside
○ From inside to outside
☐ Audit on keys
☐ Audit inside handle opening
☐ Admit expired keys
3 Days
☑ Inhibit audit trail on lock

In order to see this function in the door list, it is necessary to enable "ALLOW INHIBITION OF AUDIT TRAIL" in general option, lock tab.

- On line features are only available in the PA software connected. Not in the standard PA software.

1. If the door is a wall reader with online control unit (CU50EN, CU50ENSVN) then, you have to mark the check box IS ON LINE. The CONFIGURE CONNECTION BUTTON is used to assign an IP address to this device and initialize it at the same time.

2. The UPDATE DOOR button can be used to transmit new information to this online door when changes are made.



Door

Ext ID: C094A3ECA6C74F8997C41

Name: Class 03 Math

Description: Math

Open time (sec): 3

Increased open time: 20

Calendar: Calendar000

Antipassback

☐ Enable antipassback

● From outside to inside

○ From inside to outside

☐ Audit on keys

☑ Audit inside handle opening

☑ Admit expired keys

1 Days

Lock state

?

Update required

Valid until

Open mode and periods

Open mode: Standard

Connected door

☑ Is online

☐ Is RF

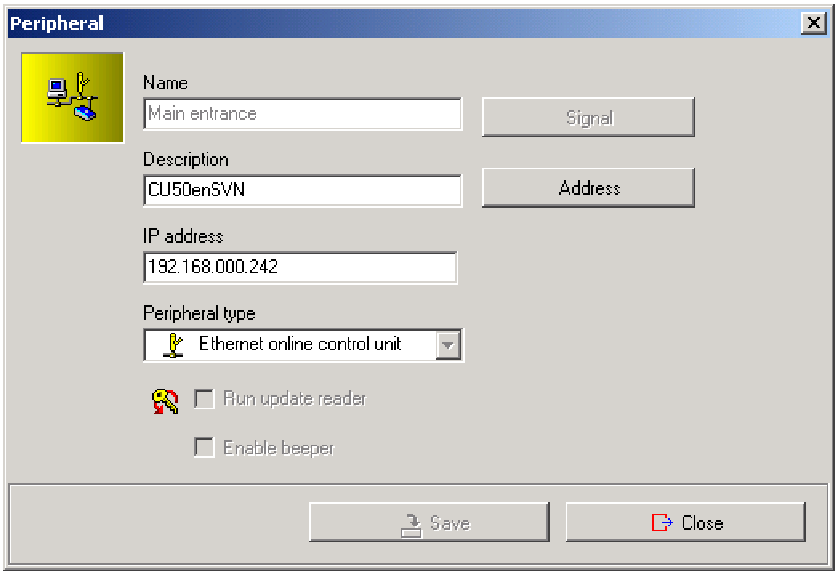
RF Node: None

Zones: Math

Access levels and users that access this door

The CONFIGURE CONNECTION button and the UPDATE DOOR button won´t be enabled until you save the changes for this window. Now, we are going to initialize this door as it is an online one:

- Press the CONFIGURE CONNECTION BUTTON.
- You will get a window like the following:



Peripheral

Name: Main entrance

Description: CU50enSVN

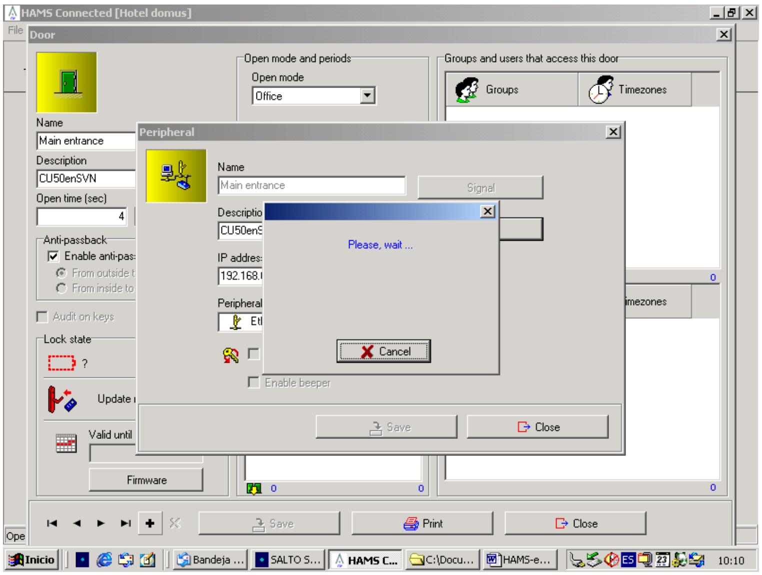
IP address: 192.168.000.242

Peripheral type: Ethernet online control unit

□ Run update reader

□ Enable beeper

- It is necessary to write the IP address we are going to assign to this device in our local area network. Then save the changes.



HAMS Connected [Hotel domus]

Door

Name: Main entrance

Description: CU50enSVN

Open time (sec): 4

Anti-passback: ☑ Enable anti-pas

Open mode and periods — Open mode: Office

Groups and users that access this door

Peripheral

Name: Main entrance

Description: CU50enS

IP address: 192.168.

Please, wait ...

- Consult your LAN administrator if you are not sure about which is the IP address we should give to this control unit. Then someone has to press the CLR button in the control unit circuit during several seconds until the LED starts blinking in the CU. In that moment, you have to press the ADDRESS button in the software.

- If you do not get an error message, it is assumed that the IP address has been assigned properly. Also, the device has been initialized at the same time.

- The SIGNAL button can be used with Ethernet encoders but not with wall readers. It makes the encoder to beep and blink for a while.

- On line devices can be created from the door list or from the PERIPHERAL LIST, the result is the same for wall readers. (Ethernet encoders can only be created from PERIPHERAL LIST).

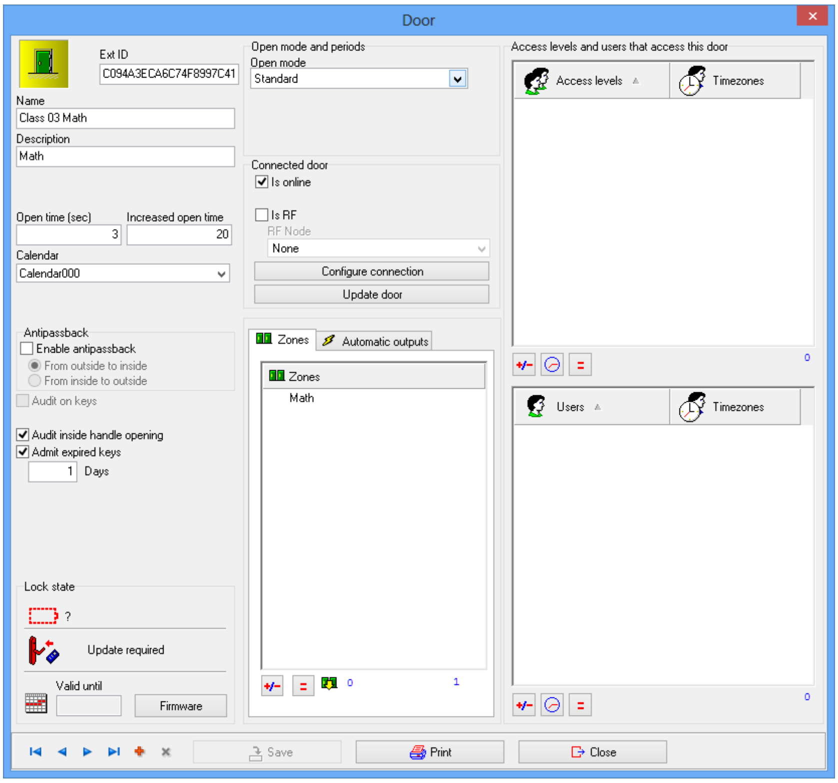
- We can go creating more doors for the DOOR LIST, no matters if they are online doors or off line devices.

- In the bottom left-hand side of the window there are some scroll arrows that will pass us from the previous door to the door immediately after (< >) or rather, move to the first or last door of the list.

- On the right-hand side of the window there is a box called THIS DOOR IS BEING ACCESSED BY... USERS. Here there will appear those users with access rights to this door, after we have set the users.

- The box called THIS DOOR IS BEING ACCESSED BY... ACCESS LEVELS will also present the user access levels with access rights to this door, once the user access levels have been defined (Later in this manual).

- Once we have completed the door definition, we can save the changes and define the rest of the doors the button +.



Ext ID: C094A3ECA6C74F8997C41

Name: Class 03 Math

Description: Math

Open time (sec): 3

Increased open time: 20

Calendar: Calendar000

Antipassback
☐ Enable antipassback
● From outside to inside
○ From inside to outside
☐ Audit on keys

☑ Audit inside handle opening
☑ Admit expired keys
1 Days

Lock state
?
Update required
Valid until

Open mode and periods
Open mode: Standard

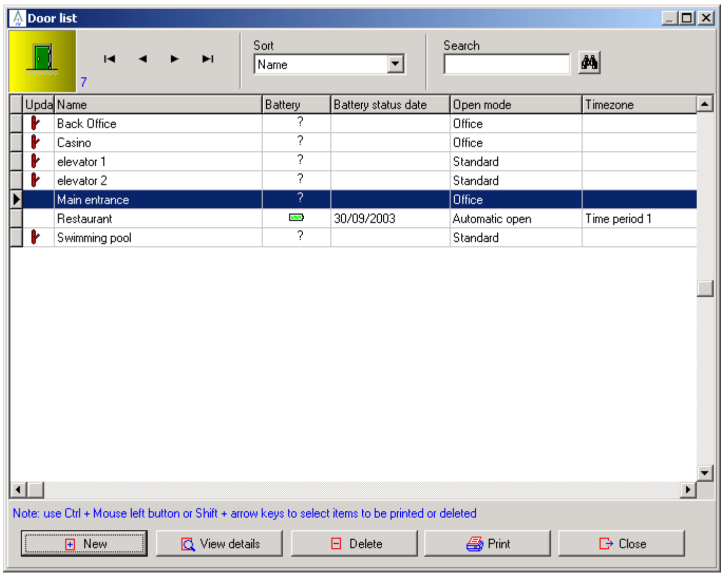
Connected door
☑ Is online
☐ Is RF
RF Node: None

Zones
Math

Access levels and users that access this door

Figure 24

When you complete the door definition, you can obtain a door list like the following:



Upda	Name	Battery	Battery status date	Open mode	Timezone
	Back Office	?		Office	
	Casino	?		Office	
	elevator 1	?		Standard	
	elevator 2	?		Standard	
	Main entrance	?		Office	
	Restaurant		30/09/2003	Automatic open	Time period 1
	Swimming pool	?		Standard	

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 25

- When we have this window active, and want to view the characteristics of a particular door, we just have to select this door in the list and click on the *VIEW DETAILS* button*.*

- If, by mistake, we have written a door in the list that should not appear, we must simply select it and click on the *DELETE* button*.*

- The field BATTERY shows the battery level, once the PPD has been connected back to the PC after the first initializing procedure. Now, this information is not available yet.

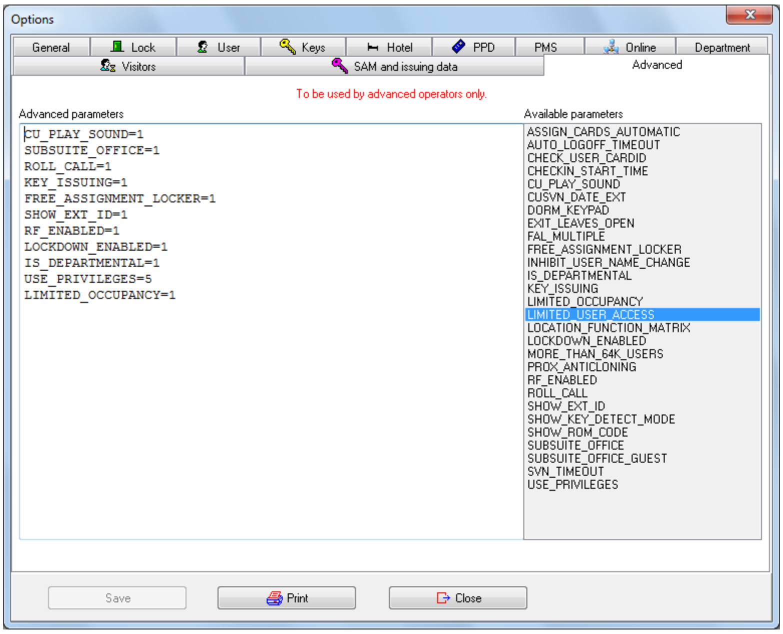
- The field BATTERY STATUS DATE shows the date of the last PPD connection which supplied this information to the PC. So, the battery level shown is only real when this date is recent.

- A box on the upper part of the list called SORT can be used to re sort the list order. If you click here, you can change the order in which the doors will appear, so that they appear in order by name or by battery status, or by open mode.

- The PRINT button can be used to obtain a hardcopy report from the door list. You can select between printing all of the door list or just the details that relate to one particular door.

Limited User Access

The SALTO software allows defining a maximum quantity of individual users allowed to open a certain door.
In order to do this, the Advanced Parameter LIMITED_USER_ACCESS must be activated:



Options

To be used by advanced operators only.

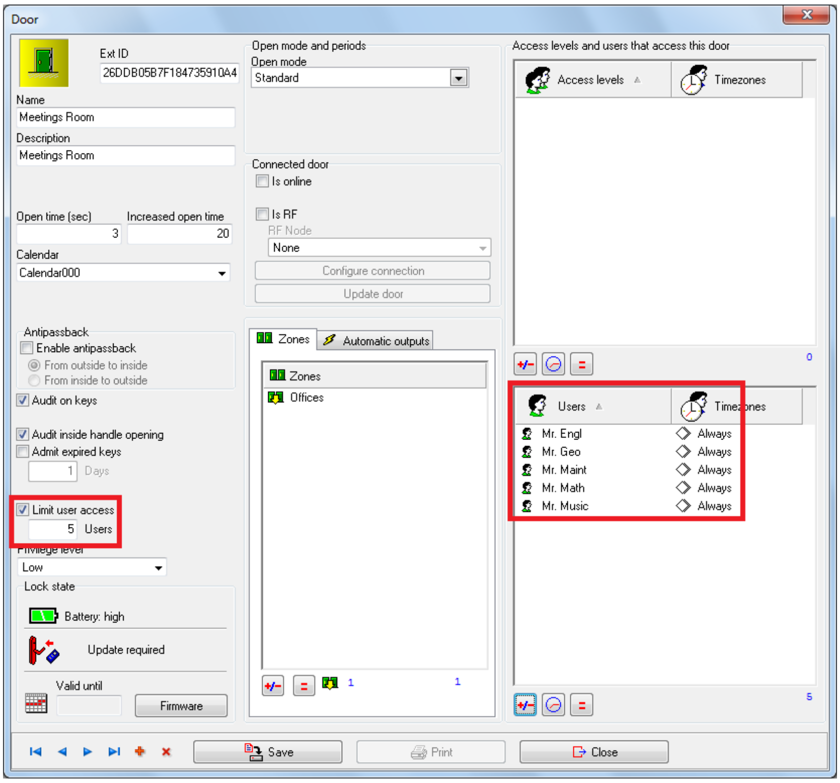
Advanced parameters

```
CU_PLAY_SOUND=1
SUBSUITE_OFFICE=1
ROLL_CALL=1
KEY_ISSUING=1
FREE_ASSIGNMENT_LOCKER=1
SHOW_EXT_ID=1
RF_ENABLED=1
LOCKDOWN_ENABLED=1
IS_DEPARTMENTAL=1
USE_PRIVILEGES=5
LIMITED_OCCUPANCY=1
```

Available parameters

```
ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CHECK_USER_CARDID
CHECKIN_START_TIME
CU_PLAY_SOUND
CUSVN_DATE_EXT
DORM_KEYPAD
EXIT_LEAVES_OPEN
FAL_MULTIPLE
FREE_ASSIGNMENT_LOCKER
INHIBIT_USER_NAME_CHANGE
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
LIMITED_USER_ACCESS
LOCATION_FUNCTION_MATRIX
LOCKDOWN_ENABLED
MORE_THAN_64K_USERS
PROX_ANTICLONING
RF_ENABLED
ROLL_CALL
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SUBSUITE_OFFICE
SUBSUITE_OFFICE_GUEST
SVN_TIMEOUT
USE_PRIVILEGES
```

This Advanced Parameter will enable a new option on the Doors configuration window, which will allow the system operator define how many users could be individually assigned to open the door:



Door

Ext ID: 26DDB05B7F184735910A4

Name: Meetings Room

Description: Meetings Room

Open time (sec): 3

Increased open time: 20

Calendar: Calendar000

Antipassback

□ Enable antipassback

○ From outside to inside

○ From inside to outside

☑ Audit on keys

☑ Audit inside handle opening

□ Admit expired keys

1 Days

☑ Limit user access

5 Users

Privilege level: Low

Lock state

Battery: high

Update required

Valid until

Open mode and periods

Open mode: Standard

Connected door

□ Is online

□ Is RF

RF Node: None

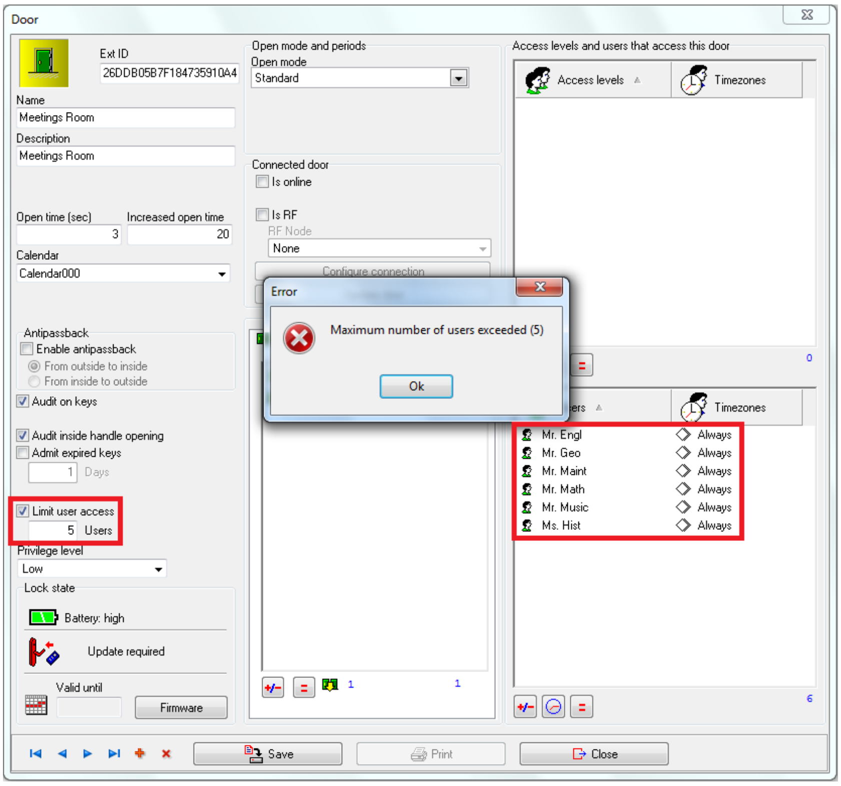
Zones

Offices

Access levels and users that access this door

Users	Timezones
Mr. Engl	Always
Mr. Geo	Always
Mr. Maint	Always
Mr. Math	Always
Mr. Music	Always

In case the system operator exceeds the specified number of users, the software will warn about it when the changes are to be saved:



Door

Ext ID: 26DDB05B7F184735910A4

Name: Meetings Room

Description: Meetings Room

Open time (sec): 3
Increased open time: 20

Calendar: Calendar000

Antipassback
□ Enable antipassback
● From outside to inside
○ From inside to outside

☑ Audit on keys
☑ Audit inside handle opening
□ Admit expired keys
1 Days

☑ Limit user access
5 Users

Privilege level: Low

Lock state
Battery: high
Update required
Valid until

Open mode and periods
Open mode: Standard

Connected door
□ Is online
□ Is RF
RF Node: None

Error
Maximum number of users exceeded (5)

Access levels and users that access this door

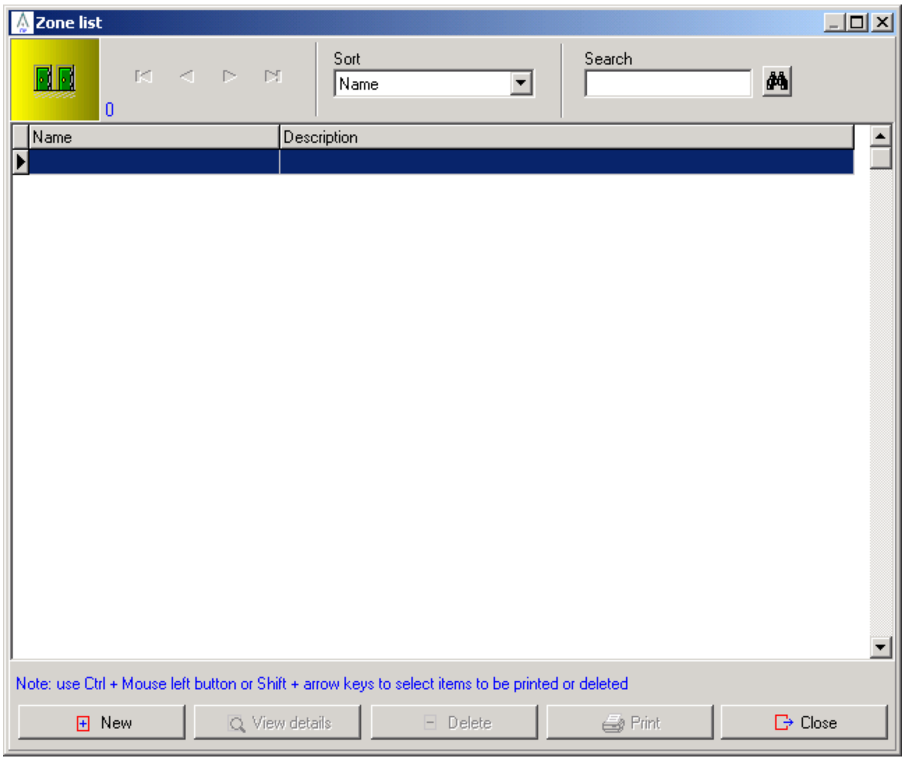
Users	Timezones
Mr. Engl	Always
Mr. Geo	Always
Mr. Maint	Always
Mr. Math	Always
Mr. Music	Always
Ms. Hist	Always

IMPORTANT NOTE: This feature only limits the quantity of users that could be individually assigned on the door configuration window, but does not limit the real quantity of users that could get access to this same door due to the fact that they have access to a zone that includes this door, or they belong to an access level that can open this door.

Zones

In this section we will explain how to use the zone list. Zones being defined as an access level of doors that have been grouped for reasons of practicality, for instance, the doors located on the first floor, on the second floor, etc.

On the Toolbar, click on the *ZONES* icon and you will be shown a window like the one below:



Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 26

- Click on the *NEW* button in order to create the first zone of the list.

- A blank window like this will be displayed:

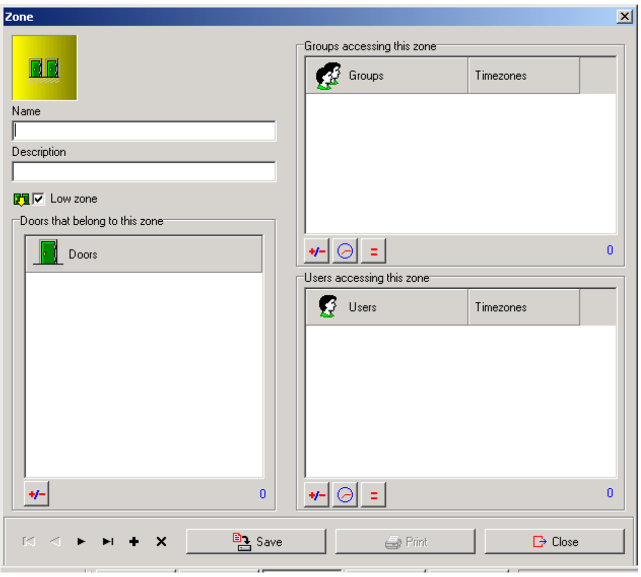

Zone
Name
Description
☑ Low zone
Doors that belong to this zone
Doors
0
Groups accessing this zone
Groups
Timezones
0
Users accessing this zone
Users
Timezones
0
Save
Print
Close

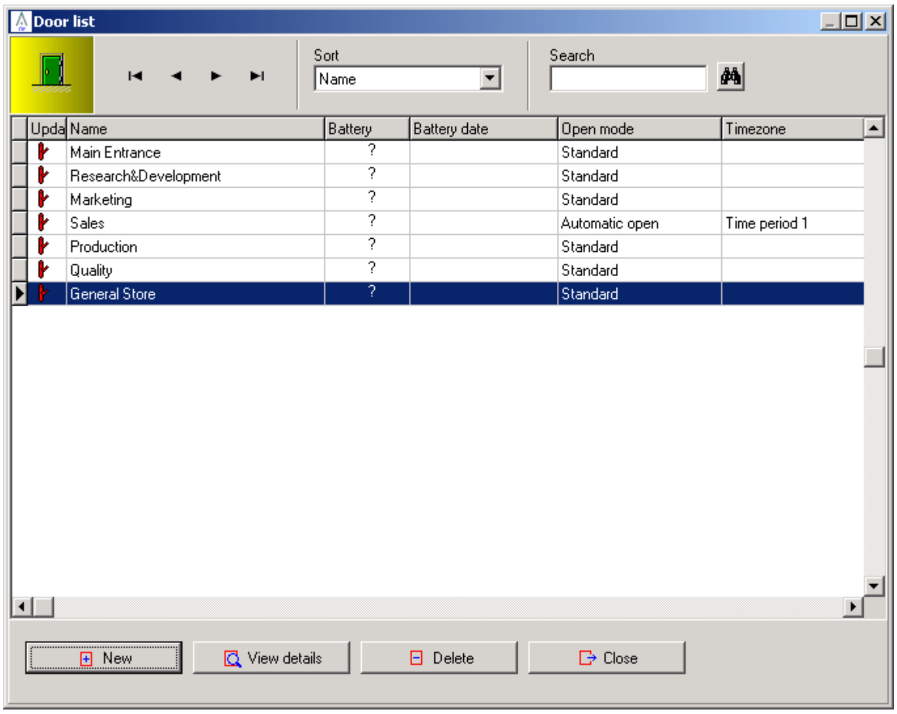
Figure 27

- Firstly, type a zone name.

- In the field DESCRIPTION you may type an explanation on what basis you have gathered together these doors.

- The check box LOW ZONE should not be modified unless our locking plan needs more than 96 different zones. Zones are classified as low or high according to the way zone information is stored on escutcheons. You are allowed to create up to 96 low zones and 928 high zones. Once this check box has been modified and changes saved, it is not possible to modify it again. From the escutcheon point of view, you can make a given door belong to a maximum number of 96 low zones, but only 20 of high zones.

- The box called DOORS BELONGING TO THIS ZONE is used to list all doors within the zone. Move the mouse over the +/- button to view the doors list and pick up those that you want to belong to this zone.



Sort: Name

Upda	Name	Battery	Battery date	Open mode	Timezone
	Main Entrance	?		Standard	
	Research&Development	?		Standard	
	Marketing	?		Standard	
	Sales	?		Automatic open	Time period 1
	Production	?		Standard	
	Quality	?		Standard	
	General Store	?		Standard	

Figure 28

- Move the mouse over the door you want to select to include in this zone group, and then, click on the yellow arrow these points at the right column.

- The door selected will appear on the right-hand side column as an integral part of the zone.

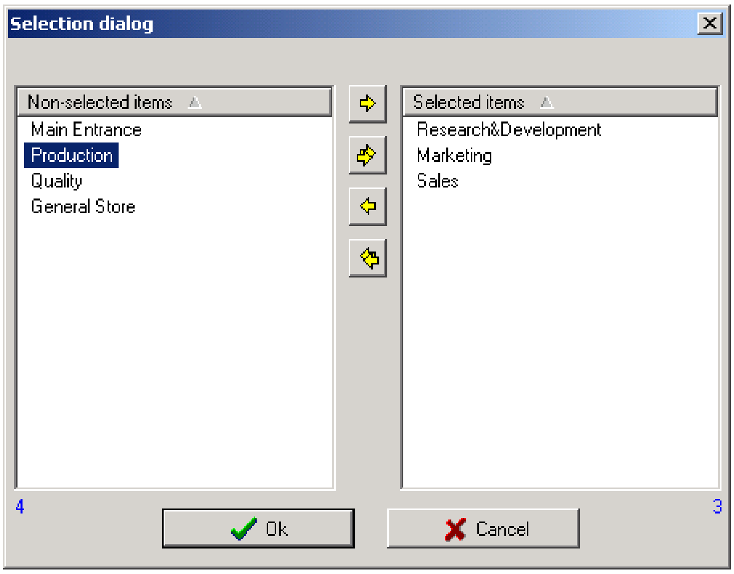


Figure 29

- Repeat this operation as many times as doors you want to incorporate to this zone.

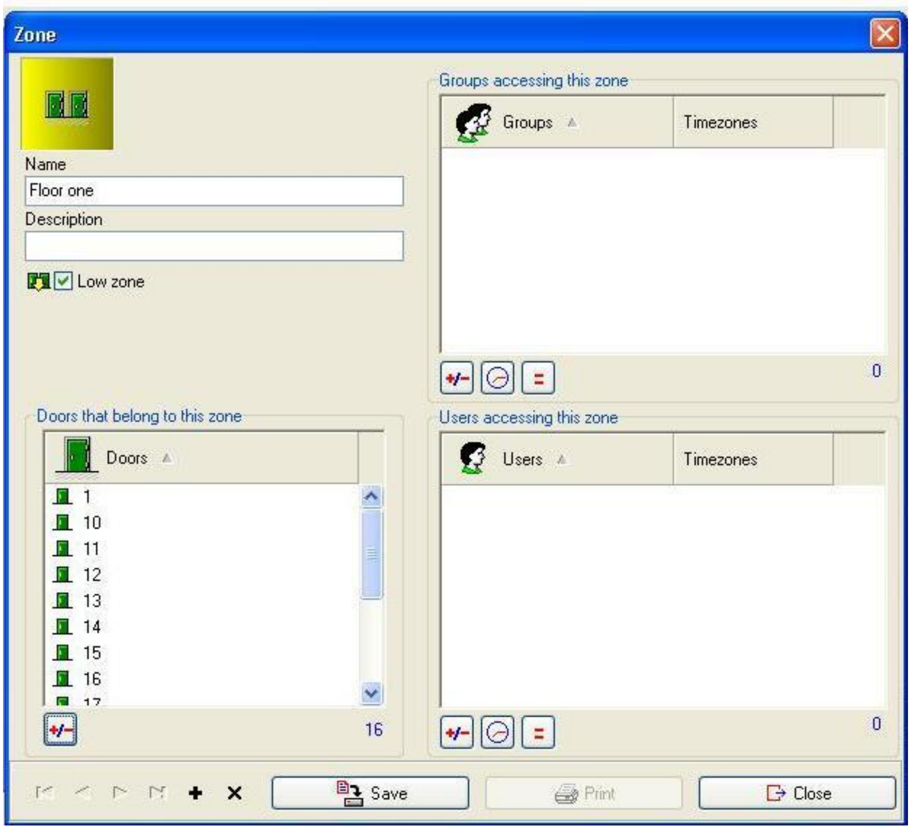
- When you fill up the right-hand side column with the doors required in this zone, click on the OK button.

- At this point, the doors belonging to this zone will be shown in the bottom left-hand side box, within the zone detail window.

- The tag called ACESSED BY... USERS is left blank since we have not yet defined users. Once we have defined them, we would use this box to specify which users will have access to this zone (and on what time zone basis)

- The tag called ACCESSED BY... ACCESS LEVELS works similarly to users, except for the fact that instead of assigning accesses to the zone individually, accesses are assigned collectively, as a access level. This saves time.

- When you have filled in all the fields of this zone detail window, save the changes.



Zone
Groups accessing this zone
Groups
Timezones
0
Doors that belong to this zone
Doors
Users accessing this zone
Users
Timezones
0
+/-
Save
Print
Close

Name: Floor one

Description:

☑ Low zone

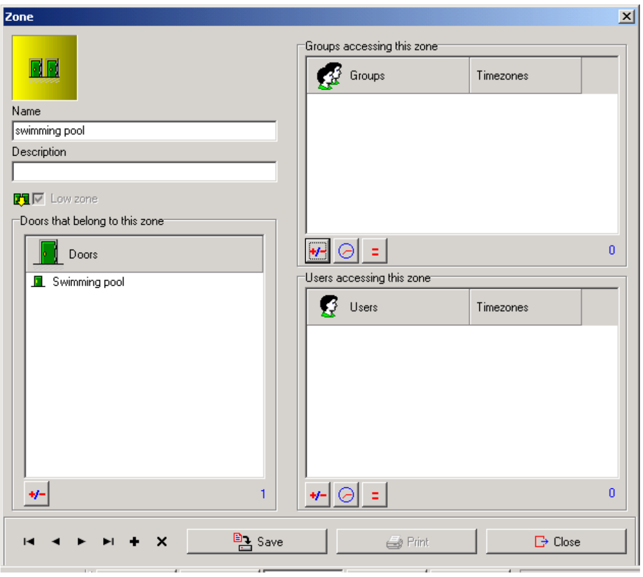
Doors
1
10
11
12
13
14
15
16
17

16

Figure 30

- If you click on the + button, you go on to the next detail window, and thus, you can define the whole set of zones for our installation.

In the following example, a zone comprises of 1 door that gives access to the swimming pool.



Name: swimming pool

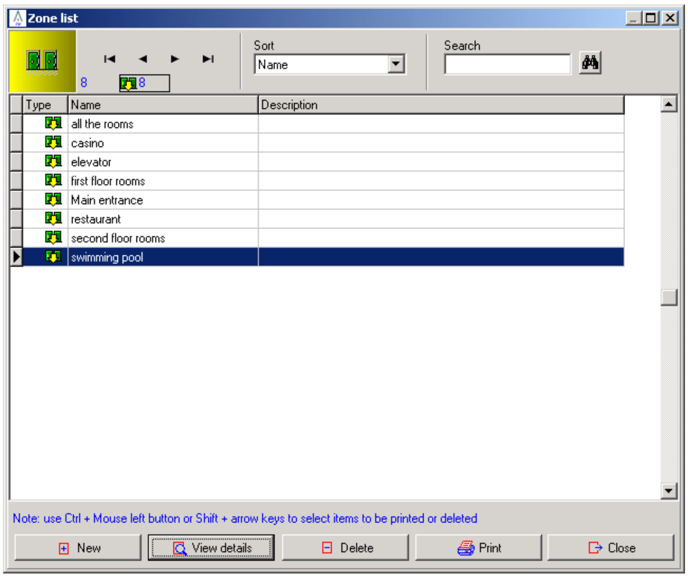
Description:

☑ Low zone

Doors that belong to this zone: Swimming pool

Figure 31

- Finally, we would have a zone list like the one shown below:



Sort: Name

Type	Name	Description
🟩	all the rooms	
🟩	casino	
🟩	elevator	
🟩	first floor rooms	
🟩	Main entrance	
🟩	restaurant	
🟩	second floor rooms	
🟩	swimming pool	

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 32

- Should we have created a zone by mistake, you will only have to select it with the mouse and click on the DELETE button.

- If, after we have saved changes, we want to view a zone details from the list, you only have to select it with the mouse and click on the VIEW DETAILS button.

- Should we want to select a zone from the list without the mouse, we can also use the scroll arrows located on the upper right-hand side of this window <> , to move forward to the next element of the list, to move back, or also, to go directly to the first or to the last elements of the list.

- The box called SORT BY is used to sort the zones list alphabetically, by zone name, or by zone description.

- The PRINT button can be used to obtain a hardcopy report from the zone list. You can select between printing all of the zone list or only the details that relate to one particular zone.

Outputs

It is possible that one control unit is connected to a relay extension board, so one allowed user will be able to activate only one or several relays, for example, in an elevator. In our example, guests in second floor will be able to go to second floor using the elevator (and also ground level) but they won´t be able to go to first floor using the elevator.

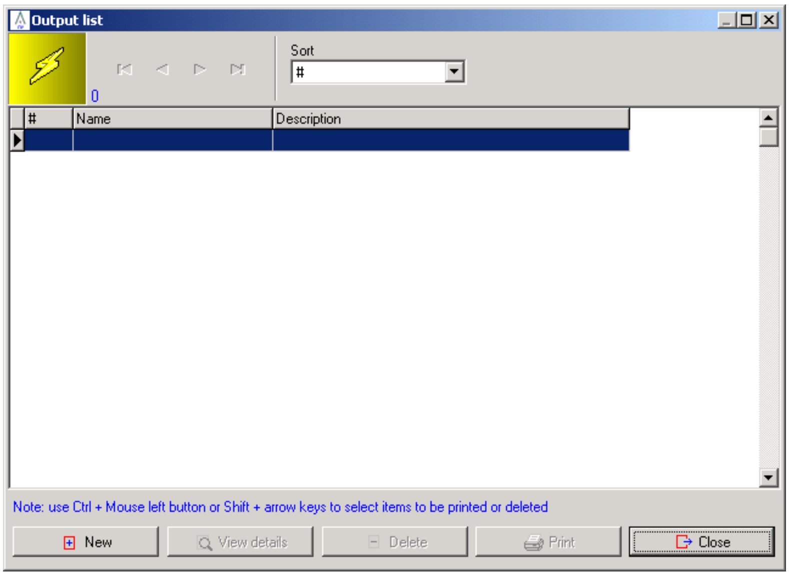
In our example, we have also 2 elevators, but they give access to the same areas, so the outputs relating every elevator, are the same, Output 1= first floor, Output 2= second floor. Output 3= ground level.

We have to create so many outputs as relays the extension board is going to control, and then these outputs can be assigned to users and guest access levels, in the same way zones are assigned. It is very important to have into account the fact that in order a user is able to activate one relay, he needs to activate first the wall reader which is linked to this relay extension board.

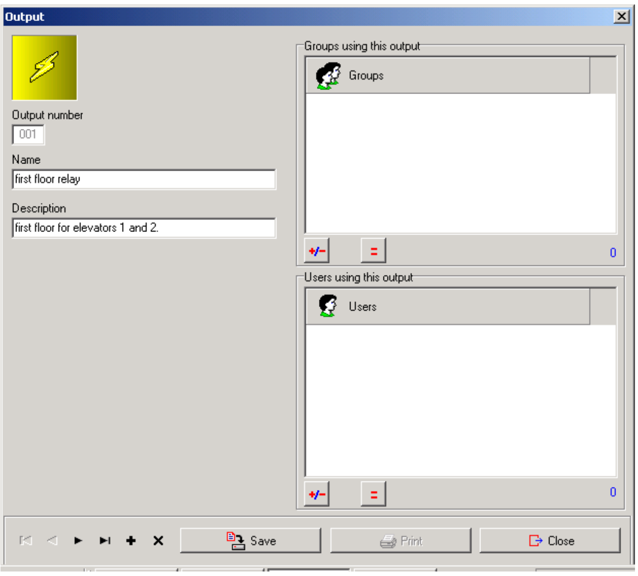
In our example, we are going to create 3 outputs, for the relay extension board.

The first output will be the first floor (for elevators 1 and 2) and the second output will be the second floor (for elevators 1 and 2). There is a wall reader mounted into every elevator cabin.

So, let´s go to DATA/OUTPUT LIST:


Output list
0
Sort
#
#
Name
Description
Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted
New
View details
Delete
Print
Close

Here, we can define the different relays in the relay extension board and explain the use of that relay.



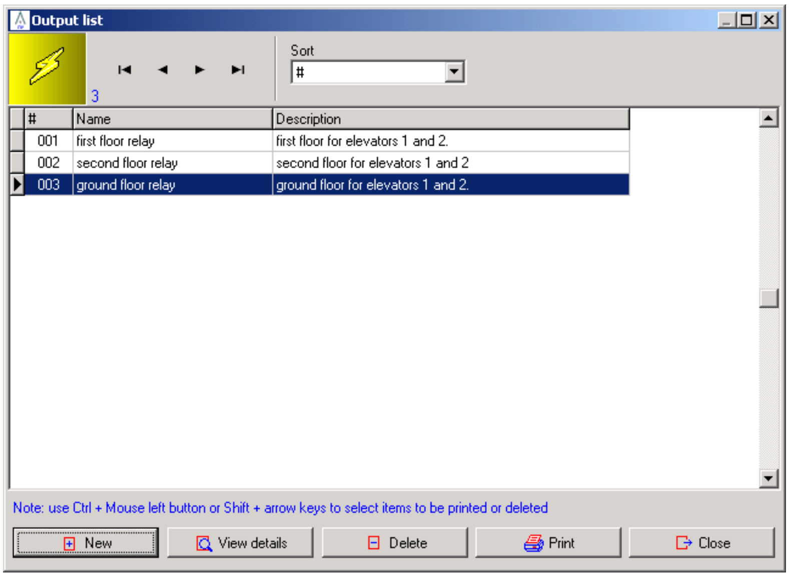
Output number
001

Name
first floor relay

Description
first floor for elevators 1 and 2.

It is very important to remember the numbers assigned to every relay, as the number (output number 1) matches physically the first relay, in the relay extension board. We can write the name and description, and then save changes.

We can go creating outputs until the output list is complete.



Sort: #

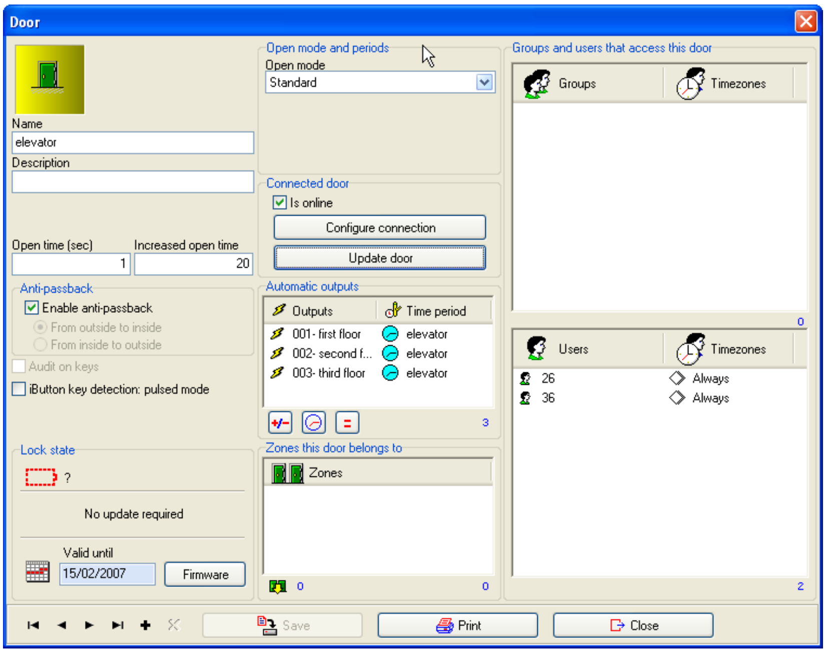
#	Name	Description
001	first floor relay	first floor for elevators 1 and 2.
002	second floor relay	second floor for elevators 1 and 2
003	ground floor relay	ground floor for elevators 1 and 2.

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Then, these outputs will be assigned to users and guest access levels in the same way we can assign zones. It is very important not to forget to assign to these users, the elevator wall readers, as a door. So, they will be able to command the outputs linked to these wall readers.

Automatic Outputs:

If we want some of the outputs from a door to work on an automatic opening mode on a specific time period we will need to assign this time period to the outputs in each door. Go to the door/room details:



Name: elevator

Description:

Open time (sec): 1

Increased open time: 20

Anti-passback

☑ Enable anti-passback

○ From outside to inside

○ From inside to outside

□ Audit on keys

□ iButton key detection: pulsed mode

Lock state

?

No update required

Valid until: 15/02/2007

Open mode and periods

Open mode: Standard

Connected door

☑ Is online

Automatic outputs

Outputs	Time period
001- first floor	elevator
002- second f...	elevator
003- third floor	elevator

3

Zones this door belongs to

Zones

0 0

Groups and users that access this door

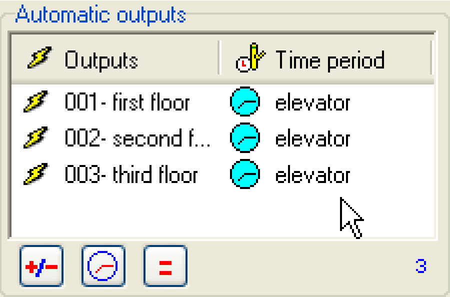
Groups	Timezones

0

Users	Timezones
26	Always
36	Always

2

In the following window:


Automatic outputs

Outputs	Time period
001- first floor	elevator
002- second f...	elevator
003- third floor	elevator

3

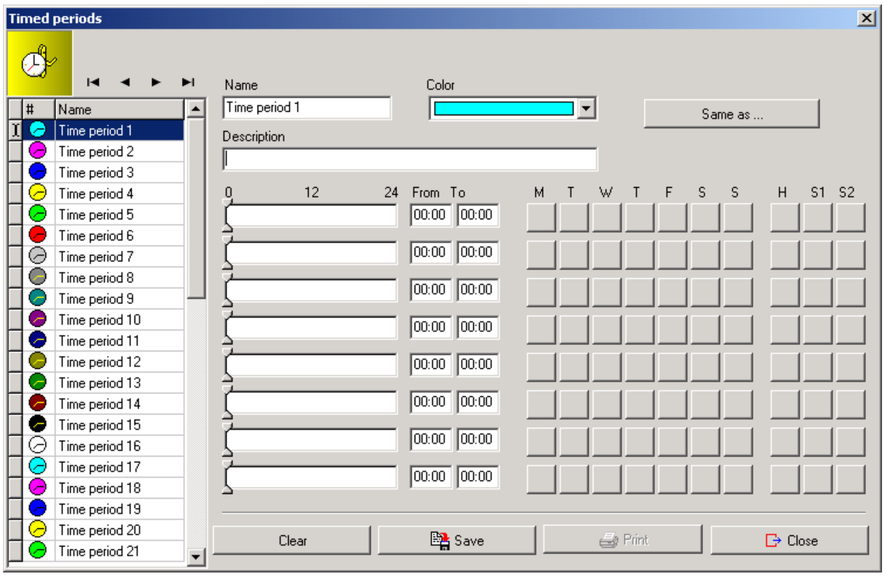
Just add the outputs and the selected time period.

NOTE: The maximum number of timed outputs is 4.

Time periods

Time periods are time intervals associated to the electronic locks (unlike time zones that are associated to people). A time period determines the time intervals at which a lock will operate in a special mode – timed office mode, automatic opening mode-.

If at the time you performed the door definitions, you selected a timed operating mode for any of these doors, you will have to use time periods to define the period assigned to that door.



Name: Time period 1

#	Name
	Time period 1
	Time period 2
	Time period 3
	Time period 4
	Time period 5
	Time period 6
	Time period 7
	Time period 8
	Time period 9
	Time period 10
	Time period 11
	Time period 12
	Time period 13
	Time period 14
	Time period 15
	Time period 16
	Time period 17
	Time period 18
	Time period 19
	Time period 20
	Time period 21

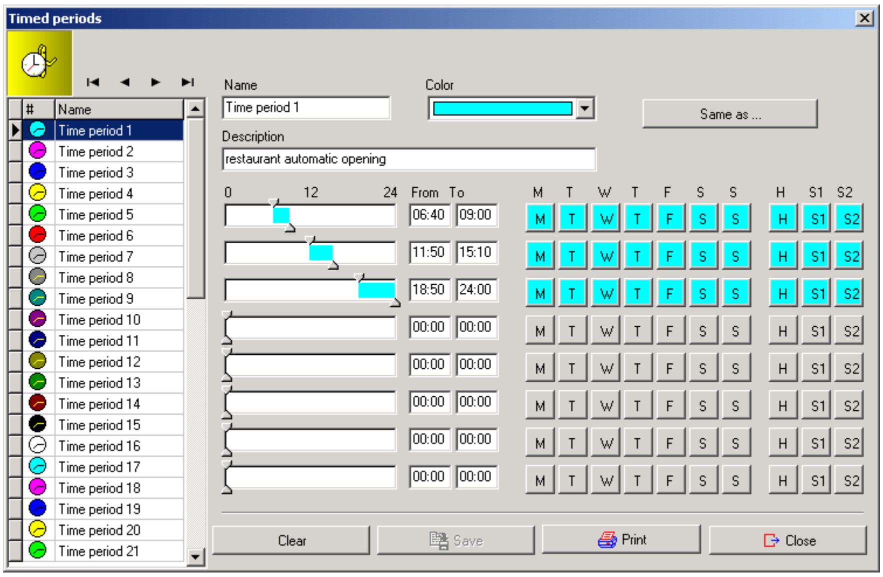
From	To
00:00	00:00
00:00	00:00
00:00	00:00
00:00	00:00
00:00	00:00
00:00	00:00
00:00	00:00
00:00	00:00

Figure 33

- Click on the time period icon on the Toolbar. A window like the one shown in the previous figure will be displayed.

- Name the Time period and assign it a distinctive colour.

- Within the description field, it is rather useful to describe the doors that belong to the time period we are about to define.



#	Name
▶	Time period 1
	Time period 2
	Time period 3
	Time period 4
	Time period 5
	Time period 6
	Time period 7
	Time period 8
	Time period 9
	Time period 10
	Time period 11
	Time period 12
	Time period 13
	Time period 14
	Time period 15
	Time period 16
	Time period 17
	Time period 18
	Time period 19
	Time period 20
	Time period 21

Name: Time period 1

Color

Same as ...

Description: restaurant automatic opening

From	To	M	T	W	T	F	S	S	H	S1	S2
06:40	09:00	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
11:50	15:10	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
18:50	24:00	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
00:00	00:00	□	□	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□	□	□

Figure 34

- The time period is defined using the mouse. Click with the mouse on the upper triangular slider and drag it to the desired interval beginning time.

- Click with the mouse over the lower slider to set the time interval end. Maximum time accuracy is 10 minutes.

- Afterwards, you will have to specify on which week days this period is going to be applicable. You can also adjust if it is to operate on public holidays or special holidays (these buttons relate to calendar 0, as this is where public holidays and special holidays for time periods are defined)

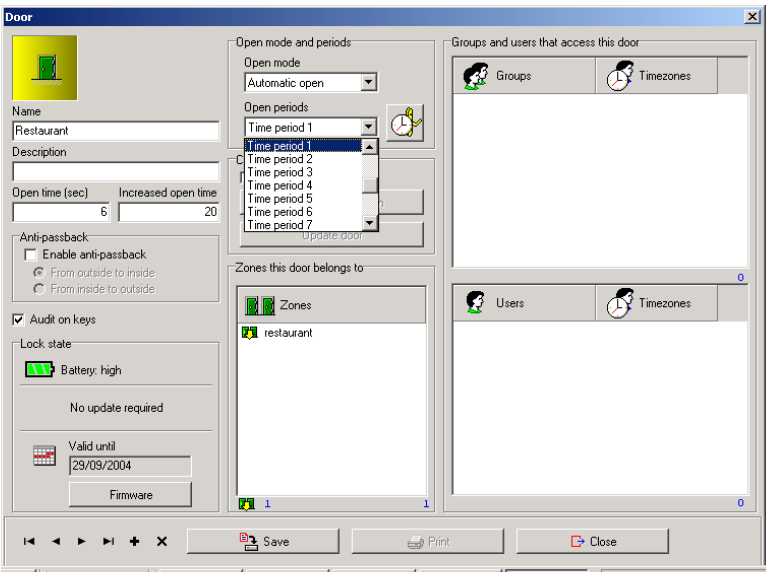
- The system applies the period to every weekday, by default.

- If the time period we are defining contains several time subintervals, we will use the number of lines necessary to define it.

- When you have finished defining a time period, save changes and you can then go on to define more periods for the system.

- The PRINT button can be used to obtain a hardcopy report for the time period list. You can select between printing all of the list or only the details that relate to one particular period.

- Do not forget to assign the time period to its corresponding door, if you have not assigned it previously. In order to do so, go to DOORS and choose the door that requires a time period. Click on the VIEW DETAILS button and you will see the list of periods that you previously defined. Select the time period applicable to this door and save changes.



Door

Name: Restaurant

Description:

Open time (sec): 6

Increased open time: 20

Anti-passback

□ Enable anti-passback

● From outside to inside

○ From inside to outside

☑ Audit on keys

Lock state

Battery: high

No update required

Valid until: 29/09/2004

Open mode and periods

Open mode: Automatic open

Open periods: Time period 1

Time period 1
Time period 2
Time period 3
Time period 4
Time period 5
Time period 6
Time period 7

Zones this door belongs to

Zones: restaurant

Groups and users that access this door

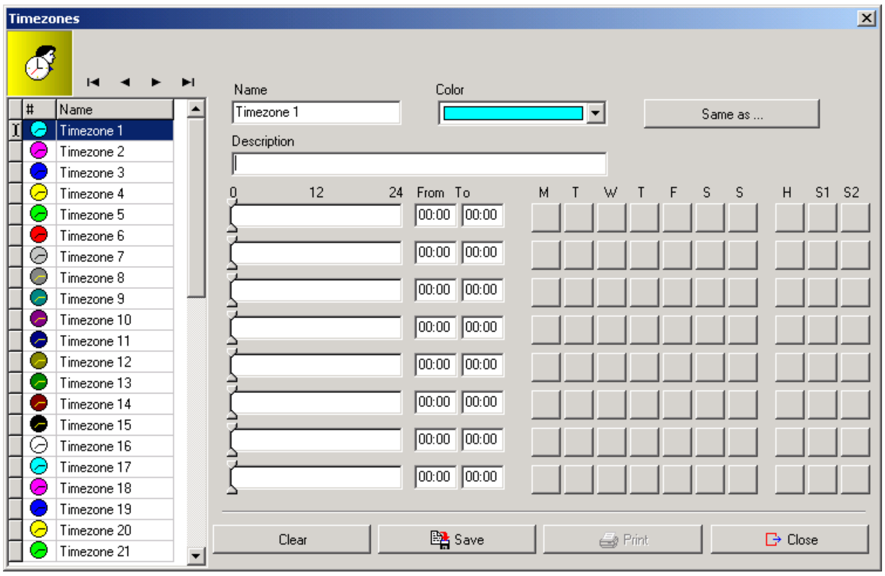
Figure 35

Time zones.

Time zones are time intervals to which people belong (unlike time periods that belong to doors). A Time zone is the interval of time in which a user has access to a particular door or zone.

- To define time zones, click on the TIME ZONE icon on the Toolbar.

- A blank window like the one below will be displayed.



Name: Timezone 1

From 00:00 To 00:00

Figure 36

- Type the first time zone name and assign it a color.

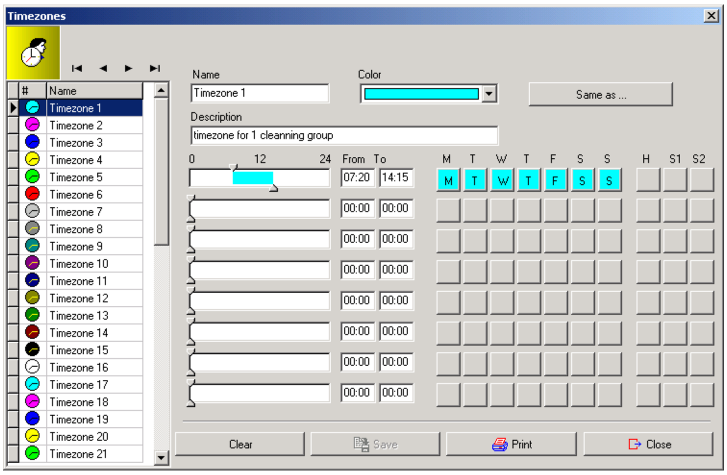
- Within the description field, it is very useful to type the name or names of people that this time zone belongs to.

- In order to define this time zone, we must follow the same procedure as in time periods, as explained in the preceding section.

- Remember to specify on which week days the time zone will be effective, as well as whether that time zone will be effective on public holidays or special holidays. You just have to highlight off the corresponding check boxes with the mouse, if you do not want the time zone to be operative on that day.

- Once time zone definition is completed, save changes and go on to define further time zones for other users or user access levels.

- You can use the PRINT button to obtain a hardcopy report from the timezone list. You can select between printing all of the timezone list or only the details that relate to one particular timezone.



Name: Timezone 1

Color

Description: timezone for 1 cleanning group

From	To	M	T	W	T	F	S	S	H	S1	S2
07:20	14:15	M	T	W	T	F	S	S			
00:00	00:00										
00:00	00:00										
00:00	00:00										
00:00	00:00										
00:00	00:00										
00:00	00:00										
00:00	00:00										

#	Name
●	Timezone 1
●	Timezone 2
●	Timezone 3
●	Timezone 4
●	Timezone 5
●	Timezone 6
●	Timezone 7
●	Timezone 8
●	Timezone 9
●	Timezone 10
●	Timezone 11
●	Timezone 12
●	Timezone 13
●	Timezone 14
●	Timezone 15
●	Timezone 16
●	Timezone 17
●	Timezone 18
●	Timezone 19
●	Timezone 20
●	Timezone 21

Figure 37

- Remember to assign the time zones to users or users access level, as is detailed later in the user and users access levels definition section.

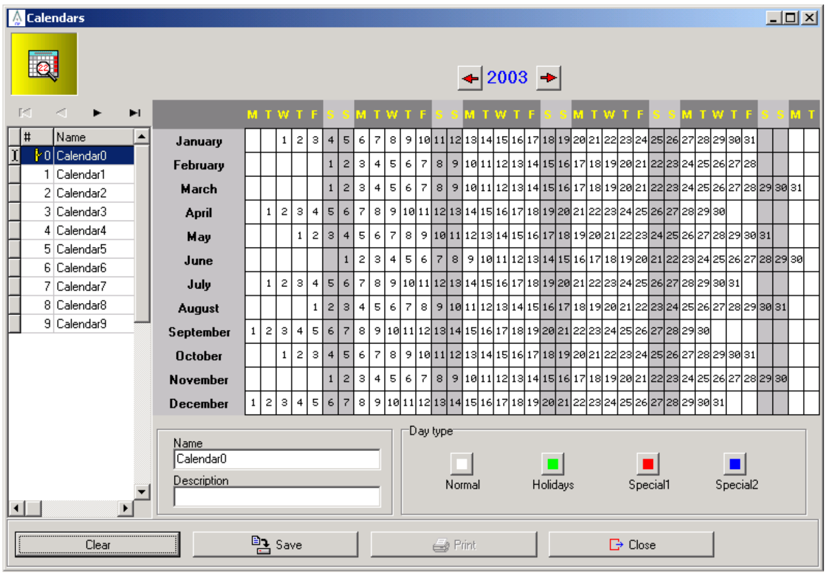
Calendars

- It is essential to define calendars within our locking schedule for two main reasons:

- The calendars range available is from 0 to 255. And each of them can be selected for the escutcheons and for the users as well.
- For the escutcheons the calendars are used when they operate in timed mode(timed office mode, automatic opening mode) so as to define on which days their periods are to be applied. This is also the calendar assigned to users without expiration date in their keys.

- Concerning the users, to define on which days their access time zones are applicable.

To define our calendars, you just have to click on the calendar icon on the Toolbar.



#	Name
0	Calendar0
1	Calendar1
2	Calendar2
3	Calendar3
4	Calendar4
5	Calendar5
6	Calendar6
7	Calendar7
8	Calendar8
9	Calendar9

	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T
January			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
February						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28				
March						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
April		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						
May				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
June							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
July		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
August					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
September	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30							
October			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
November						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
December	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						

Name: Calendar0

Description:

Figure 38

- A window like the one above will be displayed. We can name our first calendar and provide it with a relevant description.

- It is advisable to define the calendar for the current year and for the following year, if possible. To go to the next year you have just to click on the red scroll arrow on the upper part of the window.

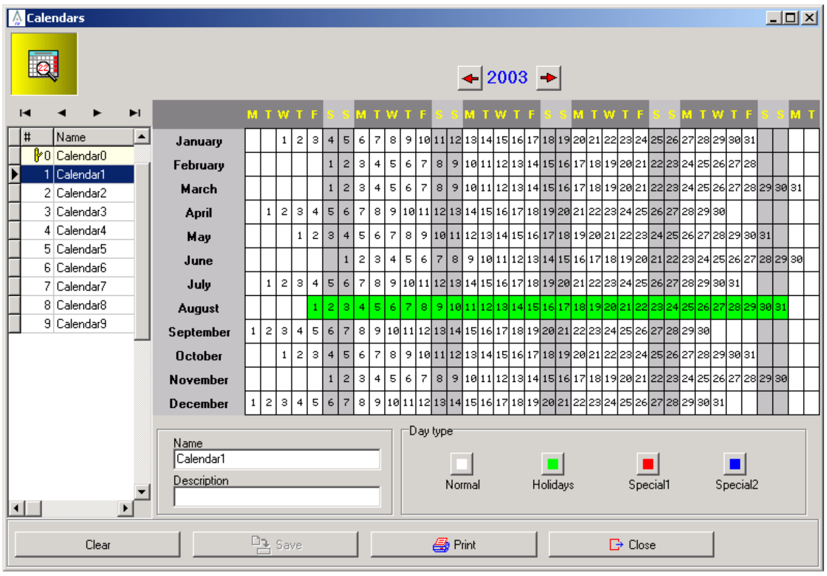
- There are four categories for each day: Normal, Holidays, Special 1 and Special 2 and 9 calendars for users.

- Using the mouse you can tick off a group of days in the calendar. Drag the mouse whilst you keep the right mouse button pressed down.

- Next, you must click on the box in the lower part of the screen which corresponds to the day category you want to assign to this group of days, and you will see how the days selected change colour according to their type selection.

- It is important to bear in mind that if a user has access to a door on public holidays, it does not depend only on the calendar but also on that users time zone being enabled for holidays or special days.

- When you have completed calendar definition, you will obtain something similar to the figure below.



#	Name
0	Calendar0
1	Calendar1
2	Calendar2
3	Calendar3
4	Calendar4
5	Calendar5
6	Calendar6
7	Calendar7
8	Calendar8
9	Calendar9

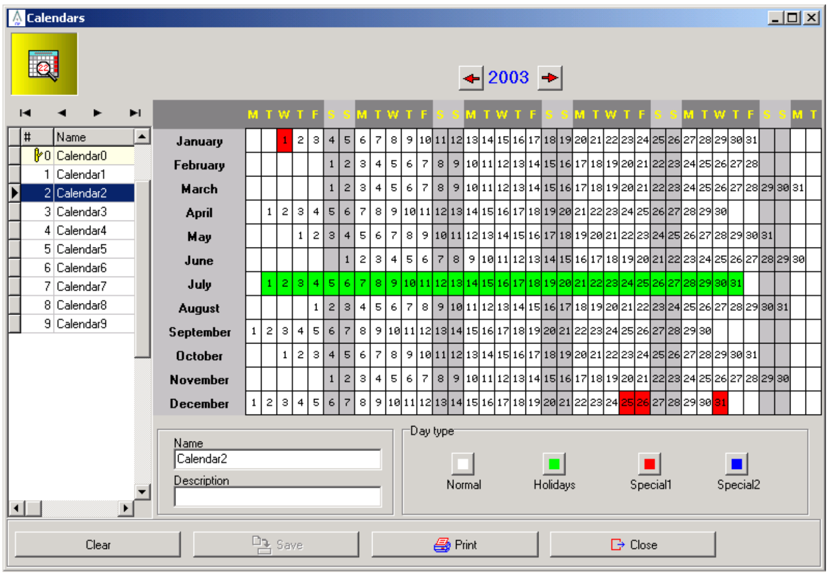
	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T
January			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
February						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28				
March						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
April		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						
May				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
June							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
July		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
August					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
September	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30							
October			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
November						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
December	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						

Name: Calendar1
Description:

Figure 39

- Save changes when calendar definition is finished and continue to define the next calendar, if your installation requires it.

- The PRINT button can be used to obtain a hardcopy report for the calendar list. You can select between printing all of the calendars or only the details that relate to one particular calendar. The types of day will be recognised by a letter, H for Holiday, S for special day, N for normal day.



#	Name
0	Calendar0
1	Calendar1
2	Calendar2
3	Calendar3
4	Calendar4
5	Calendar5
6	Calendar6
7	Calendar7
8	Calendar8
9	Calendar9

	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T
January			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
February						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28				
March						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
April		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						
May				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
June							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
July		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
August					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
September	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30							
October			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
November						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
December	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						

Name: Calendar2
Description:

Figure 40

- Remember to assign the different calendars (1 and 2) to the different users and user access levels, as is later detailed in the user and users access levels definition section.
- The same for the escutcheons.

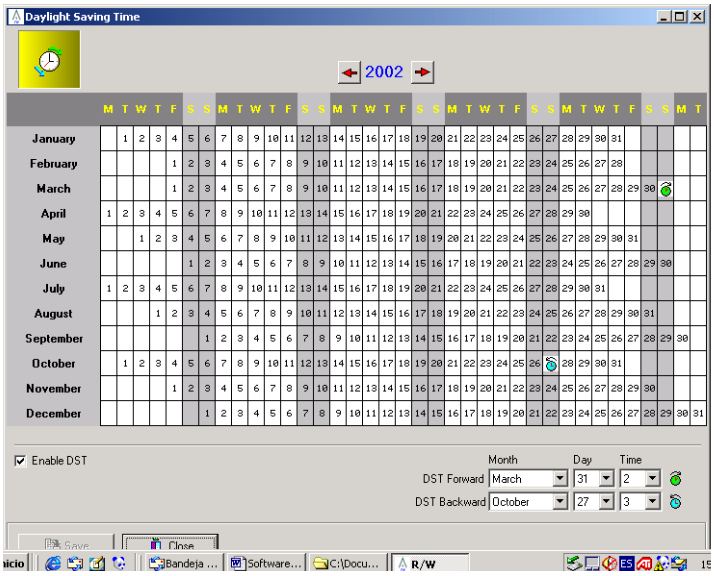
Time change

DST stands for the English Daylight Saving Time, that is to say, the time change that takes place with a view to saving power by means of daylight optimisation.

This time change is generally made shortly after vernal equinox and autumnal equinox, putting time forward in the former and putting time backward in the latter.

Salto electronic locks perform time change automatically, if it is set up in the software.

Click on the DST icon on the Toolbar and you will get a window similar to this:



	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T
January		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
February					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28					
March					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	●		
April	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30							
May			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
June						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
July	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
August				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
September							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
October		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	○	28	29	30	31					
November					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
December							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

☑ Enable DST

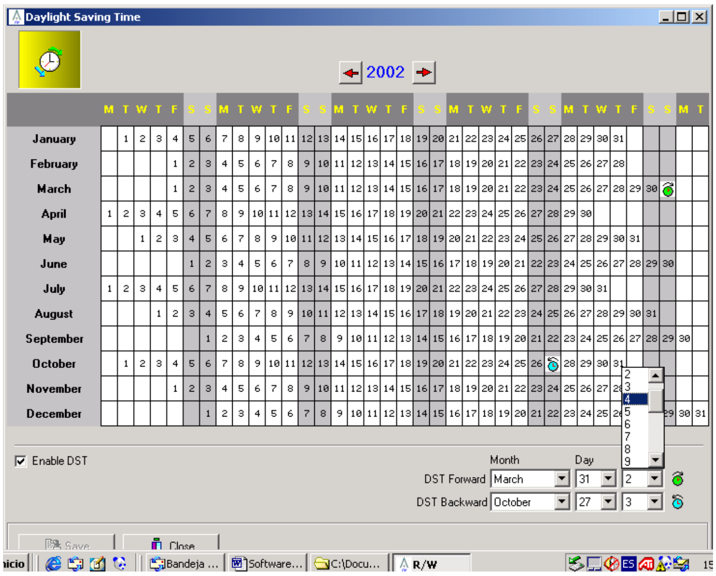
	Month	Day	Time
DST Forward	March	31	2
DST Backward	October	27	3

Figure 41

- You can either enable (or not) time change by ticking off the ENABLE DTS check box that is located on the bottom left-hand side of the window.

- You may also change the time at which the time change DAY and HOUR takes place, using the bottom right-hand side arrows of the window.

- If you modify time change day, the symbol that embodies it will be moved in the calendar accordingly.



	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T
January		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
February					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28					
March					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	●		
April	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30							
May			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
June						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
July	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
August				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
September							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
October		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	○	28	29	30	31					
November					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	2					
December							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	2			9	30	31

☑ Enable DST

	Month	Day	Time
DST Forward	March	31	2
DST Backward	October	27	3

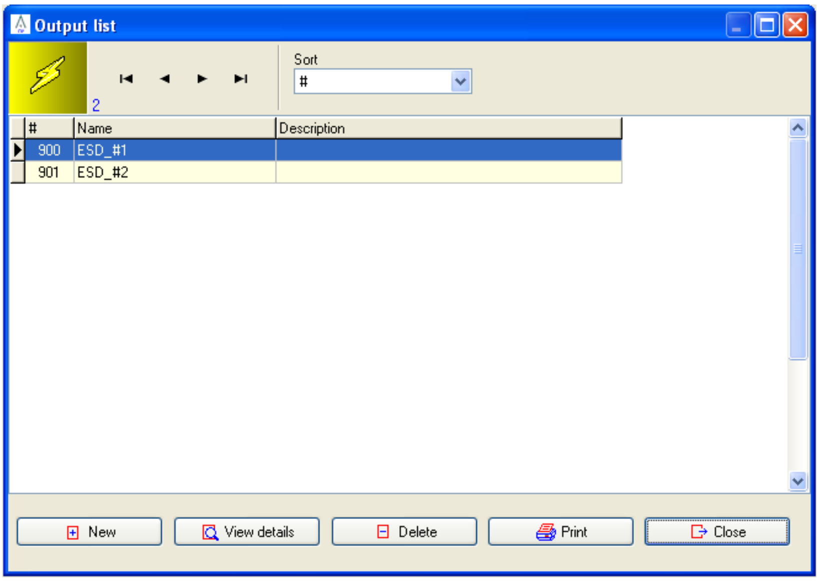
- You can also set the time change for next year, if you wish. Click on the red arrow (right) of the window upper part, to move on to the next year.

- Save changes when you have finished establishing appropriate parameters for time change.

- It is recommended to enable automatic time change, since if it is not software enabled, you will have to update every door in your hotel using the PPD, on the scheduled date of the change.

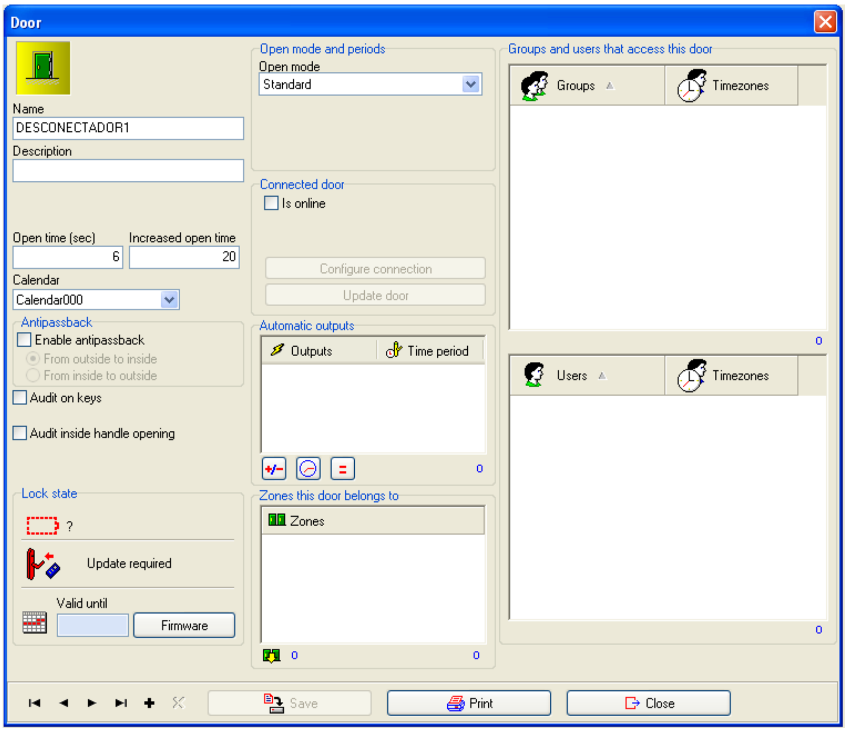
Output List for Electronic Saving Devices (ESD)

It is possible to use ESD under Salto ProAccess using the outputs option.
The selected user must have access to one of the two outputs (or both) available under Output list menu. Output 900 will activate relay1 and output 901 relay2.



#	Name	Description
900	ESD_#1	
901	ESD_#2	

The ESD is created from Doors menu the same way as a normal lock. The only information to use is the name (the rest of params won´t be sent to the ESD).



Name: DESCONECTADOR1

Description:

Open time (sec): 6

Increased open time: 20

Calendar: Calendar000

□ Enable antipassback

○ From outside to inside

○ From inside to outside

□ Audit on keys

□ Audit inside handle opening

Lock state: ?

Update required

Valid until:

Open mode: Standard

□ Is online

Automatic changes

Starting from version 6, the RW software supports automatic changes. This is a new open mode for CUs. Unlike the open modes we have known so far (for example, OFFICE), automatic changes allow CUs to vary their open mode along different time intervals. For example, from 00:00H to 08:00H -> OFFICE mode, from 08:00H to 18:00H -> AUTOMATIC OPENING and from 18:00H to 24:00H -> STANDARD mode.

More specifically, an automatic change is a time interval in which the CU works in a defined opening mode. Thus, three parameters define an automatic change: start time, end time and opening mode. For a given day type (normal day of week, holiday, special 1 and special 2), up to 8 automatic changes may be declared. In order to allow different combinations, the RW software groups different day types (and their associated automatic changes) into 256 tables.

In summary, the SALTO DB includes 256 automatic change tables, where each table contains the 10 day types (Monday to Sunday, Holiday, Special1 and Special2) and each day type, in turn, may contains up to 8 automatic changes.

As for the graphic interface, the ‘DATA\TIME PERIODS…’ menu option now shows two more sub-options, namely, Time Periods and Automatic Changes, as shown in the picture below.

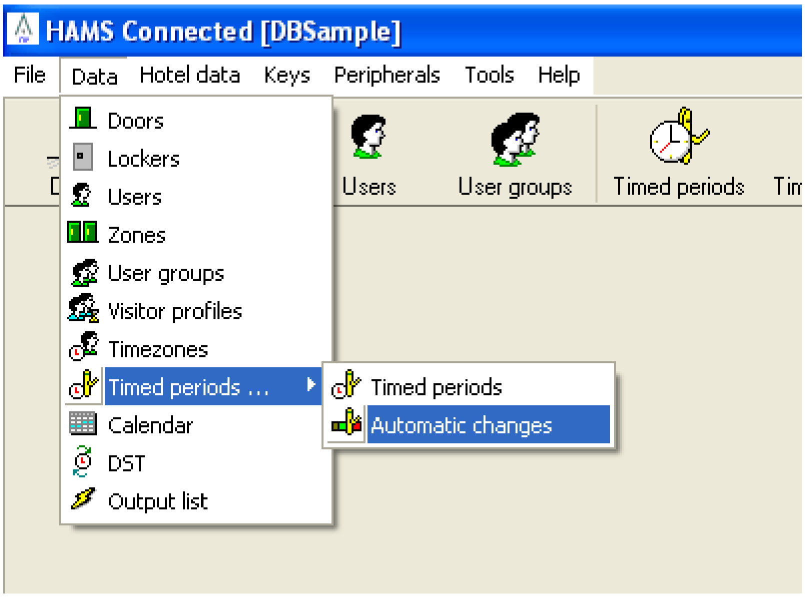
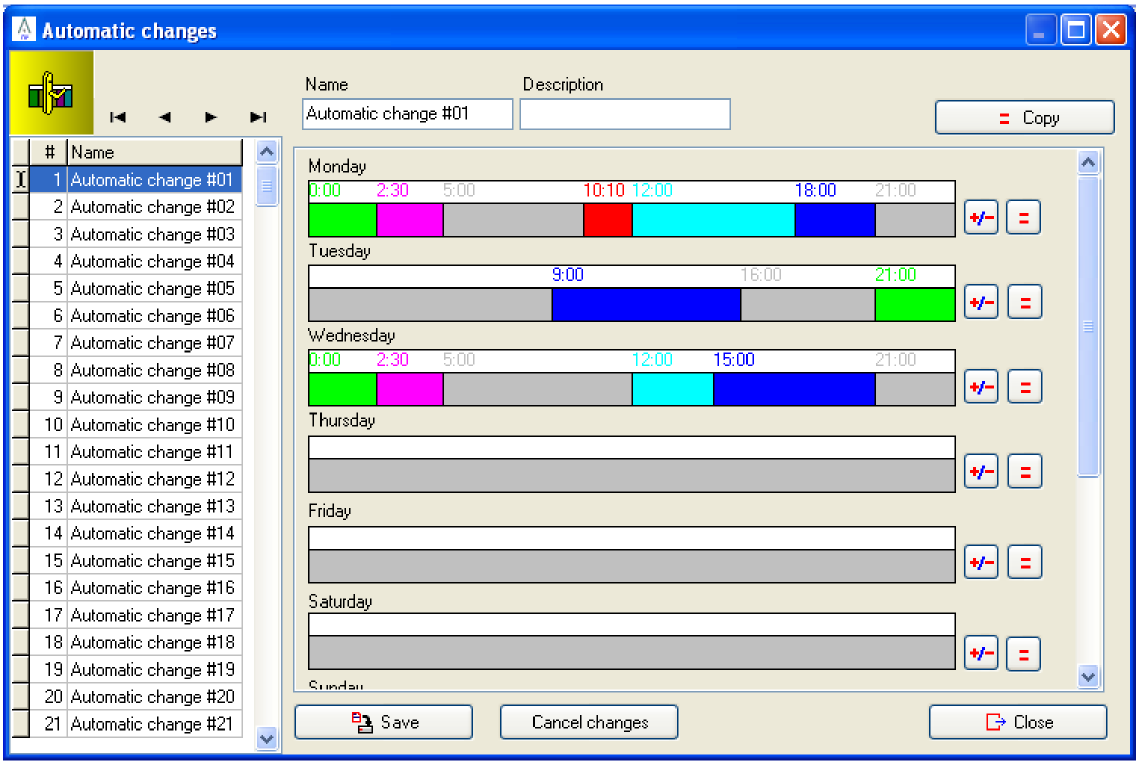


Figure 1

The picture below (figure 2) shows the window that allows setting up automatic changes. Within this window you may modify the automatic changes of a given table and day type (through the corresponding '+/-' button) as shown in figure 3. You may also copy automatic changes from one day type to another (through the '=' button) as shown in figure 4 or even copy a whole table into another (through the '= Copy' button) as shown in figure 5. Finally, you may make a given CU works in automatic change mode as shown in figure 6.

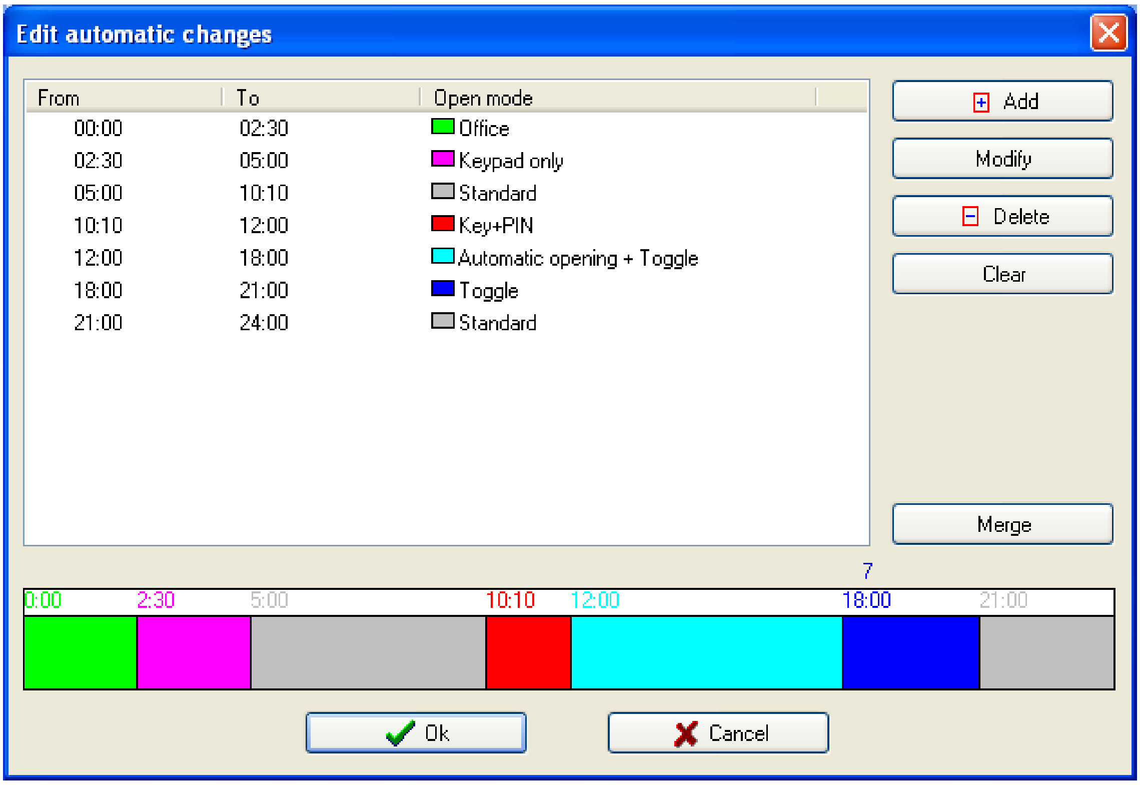


Name: Automatic change #01

Description:

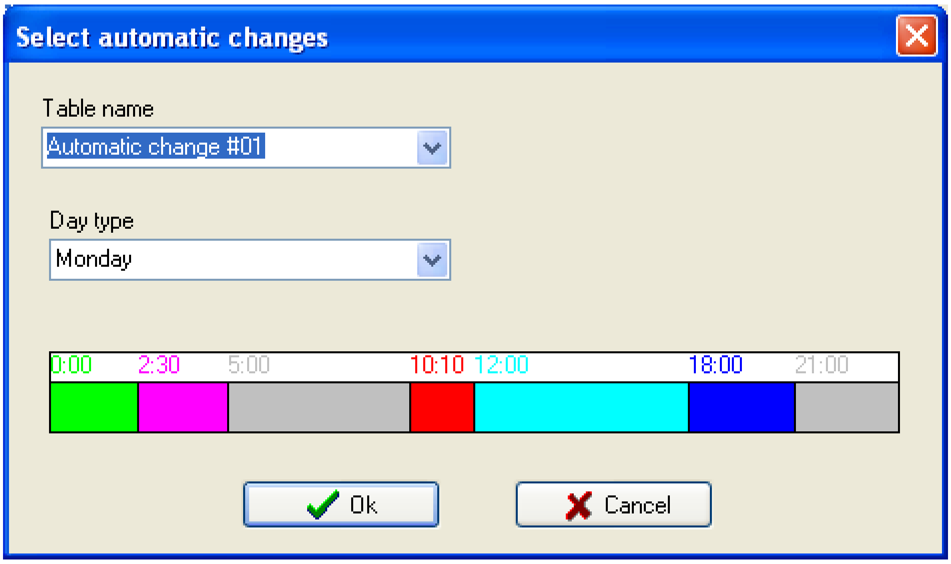
#	Name
1	Automatic change #01
2	Automatic change #02
3	Automatic change #03
4	Automatic change #04
5	Automatic change #05
6	Automatic change #06
7	Automatic change #07
8	Automatic change #08
9	Automatic change #09
10	Automatic change #10
11	Automatic change #11
12	Automatic change #12
13	Automatic change #13
14	Automatic change #14
15	Automatic change #15
16	Automatic change #16
17	Automatic change #17
18	Automatic change #18
19	Automatic change #19
20	Automatic change #20
21	Automatic change #21

Figure 2: automatic changes window.



From	To	Open mode
00:00	02:30	🟩 Office
02:30	05:00	🟪 Keypad only
05:00	10:10	⬜ Standard
10:10	12:00	🟥 Key+PIN
12:00	18:00	🟦 Automatic opening + Toggle
18:00	21:00	🟦 Toggle
21:00	24:00	⬜ Standard

Figure 3: modifying automatic changes of a given table and day type (button '+/-').

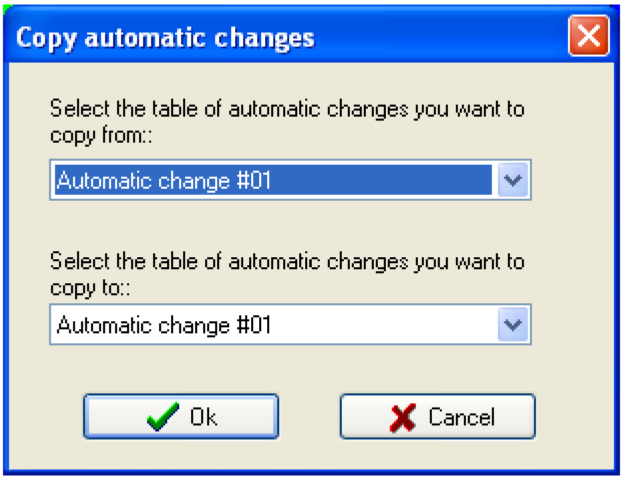


Select automatic changes

Table name: Automatic change #01

Day type: Monday

Figure 4: specifying the table and day type from which you want automatic changes to be copied (button '=').

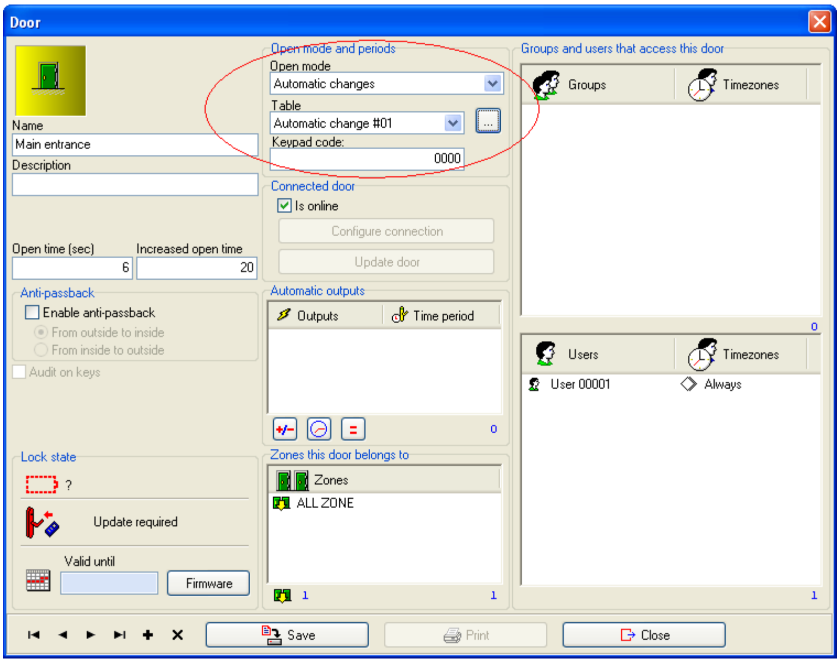


Copy automatic changes

Select the table of automatic changes you want to copy from:: Automatic change #01

Select the table of automatic changes you want to copy to:: Automatic change #01

Figure 5: specifying the source table and the destination table for automatic changes to be copied (button '= Copy').



Door

Name: Main entrance
Description:
Open time (sec): 6
Increased open time: 20

Anti-passback
- ☐ Enable anti-passback
- ● From outside to inside
- ○ From inside to outside
- ☐ Audit on keys

Lock state: ?
Update required
Valid until

Open mode and periods
Open mode: Automatic changes
Table: Automatic change #01
Keypad code: 0000

Connected door
- ☑ Is online

Automatic outputs

Zones this door belongs to: ALL ZONE

Groups and users that access this door

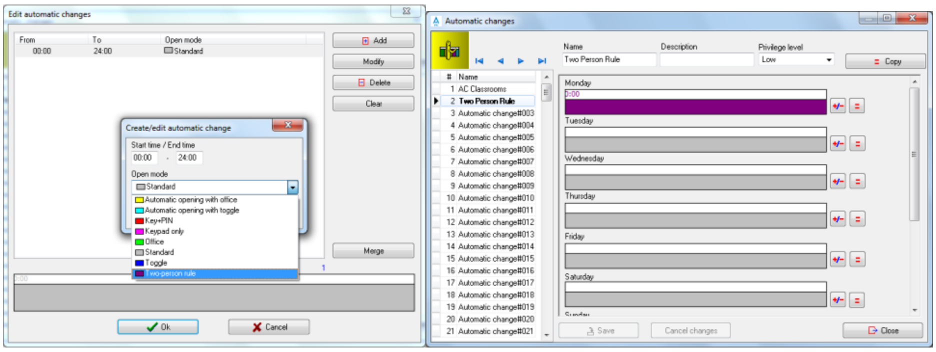
Users	Timezones
User 00001	Always

Figure 6: making a CU work in automatic change mode.

The Automatic Changes also include a special locks working mode that can be only activated in the Automatic Changes modes menu, called Two-Person Rule. This mode requires two of the users to be presenting their valid cards into SALTO hardware controlling the access point to be able to open the door.

This mode can be only activated then when the locks are configured to be working with the Automatic Changes working mode.

As can be seen in the picture below, the Two-Person Rule is included in the working modes of the Automatic Changes drop down list:



Edit automatic changes

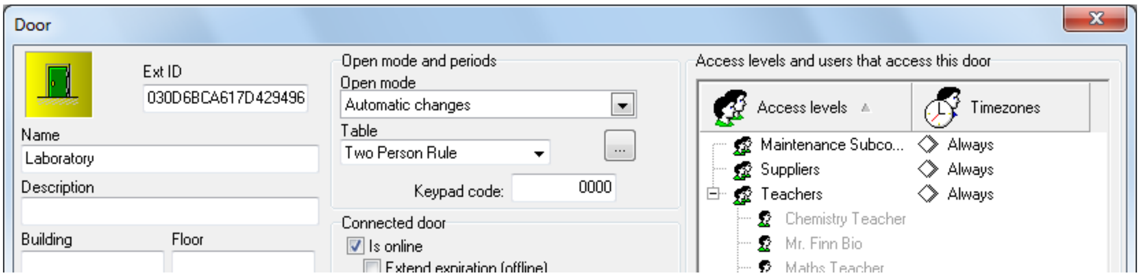
From	To	Open mode
00:00	24:00	Standard

Create/edit automatic change
Start time / End time: 00:00 - 24:00
Open mode: Standard
- Automatic opening with office
- Automatic opening with toggle
- Key+PIN
- Keypad only
- Office
- Standard
- Toggle
- Two-person rule

Automatic changes
Name: Two Person Rule
Description:
Privilege level: Low

#	Name
1	AC Classrooms
2	Two Person Rule
3	Automatic change#003
4	Automatic change#004
5	Automatic change#005
6	Automatic change#006
7	Automatic change#007
8	Automatic change#008
9	Automatic change#009
10	Automatic change#010
11	Automatic change#011
12	Automatic change#012
13	Automatic change#013
14	Automatic change#014
15	Automatic change#015
16	Automatic change#016
17	Automatic change#017
18	Automatic change#018
19	Automatic change#019
20	Automatic change#020
21	Automatic change#021

Once the selected Automatic Change is prepared to be working in the Two-Person Rule mode, The Automatic Change and the related Table must be selected in the Door’s configuration:


Door

Ext ID: 030D6BCA617D429496

Name: Laboratory

Description:

Building:

Floor:

Open mode and periods

Open mode: Automatic changes

Table: Two Person Rule

Keypad code: 0000

Connected door

☑ Is online

□ Extend expiration (offline)

Access levels and users that access this door

Access levels	Timezones
Maintenance Subco...	Always
Suppliers	Always
Teachers	Always
Chemistry Teacher	
Mr. Finn Bio	
Maths Teacher	

NOTE: This working mode must be also available in the firmware of the device to be programmed with this working mode. Please check compatibility with your usual SALTO contact person.

Users access levels

It is advisable to take heed of the fact that users are hotel personnel (staff) members, but *never* guests.

Users access levels are definable groups of users, that share a common feature: For instance, we can group together users by job type or department, like cleaners etc tend to share time zones and accesses.

Click on the USERS ACCESS LEVEL icon on the Toolbar:

A window like this will be displayed:

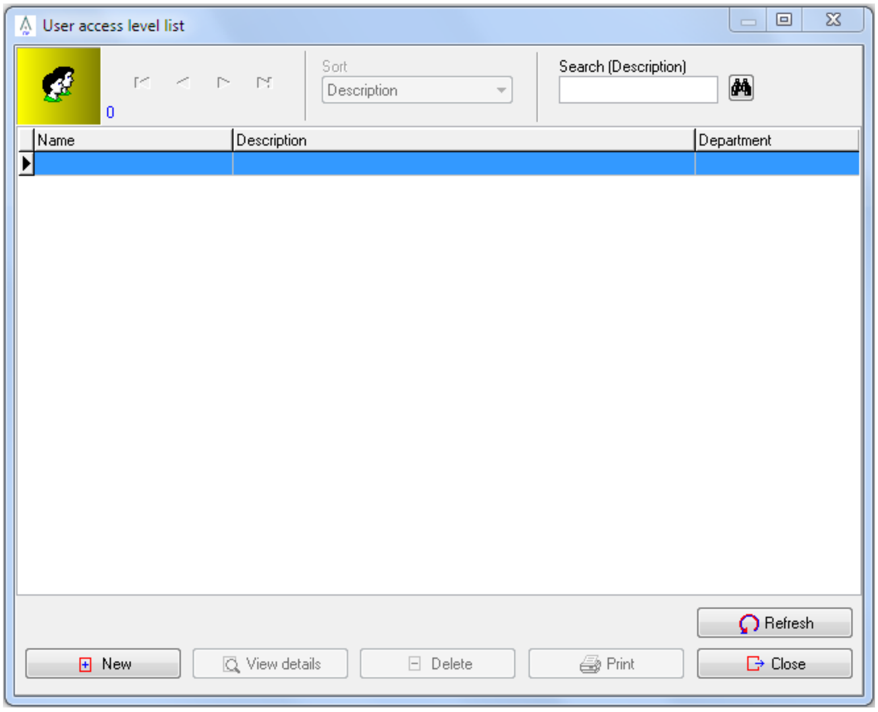


Figure 42

- Since we have not created any user access levels yet, the list will be empty.
- To create the first users access level, click on the NEW button.
- A window like the one below will be displayed:

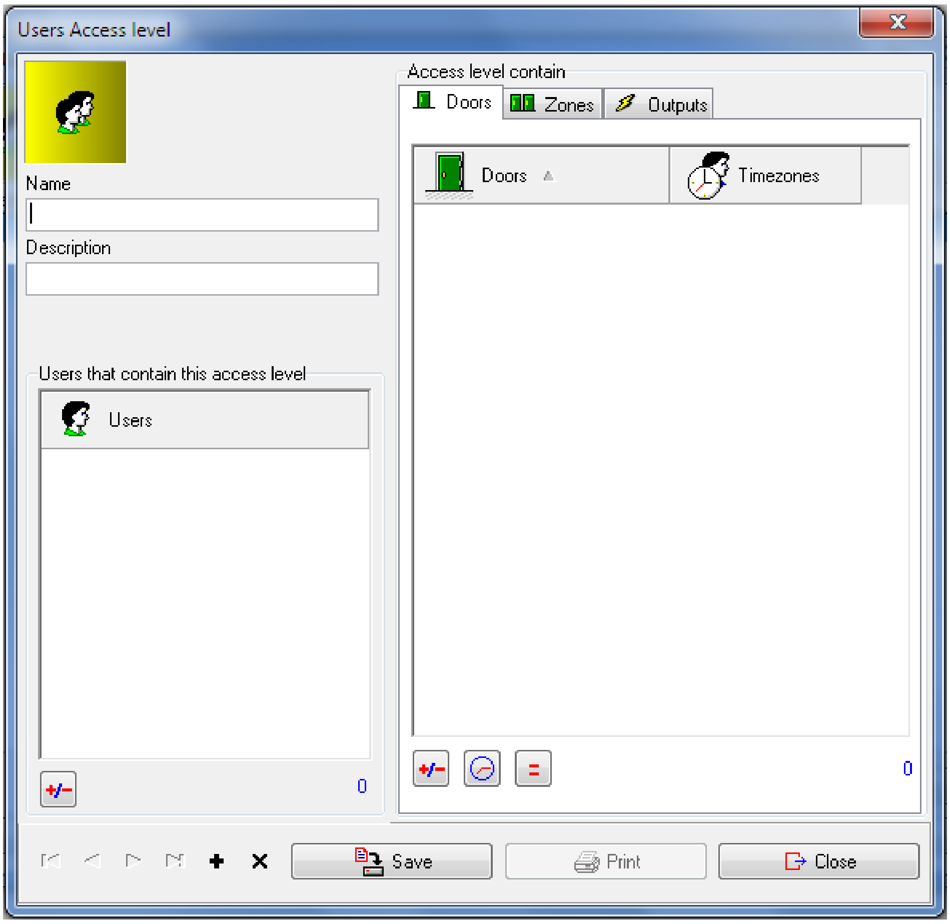


Figure 43

- Firstly, type this user access levels name, and below, a description detailing the main characteristic that best defines the access level.

- Given that we have not defined users yet, we cannot specify the users that belong to the access level, though we can establish access level accesses.

- In the tag called ZONES BEING ACCESSED, click on the +/- button to assign door zones to the access level.

- If a user must belong to different access levels there are two ways to do it,

  1/ into the Access lever window, as shown in Figure 44, we add users into the list using button +/-, for each of the access levels where we want the user to belong to.

2/ in the user accesses, located into the user list, we can add the previously created Access levels as shown on Figure 44b.
On the other hand, the user can also have Accesses to separate doors.

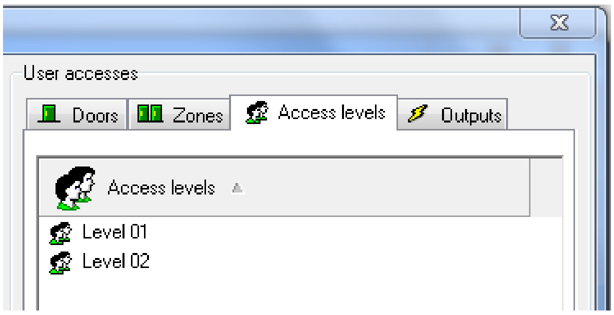


Figure 44

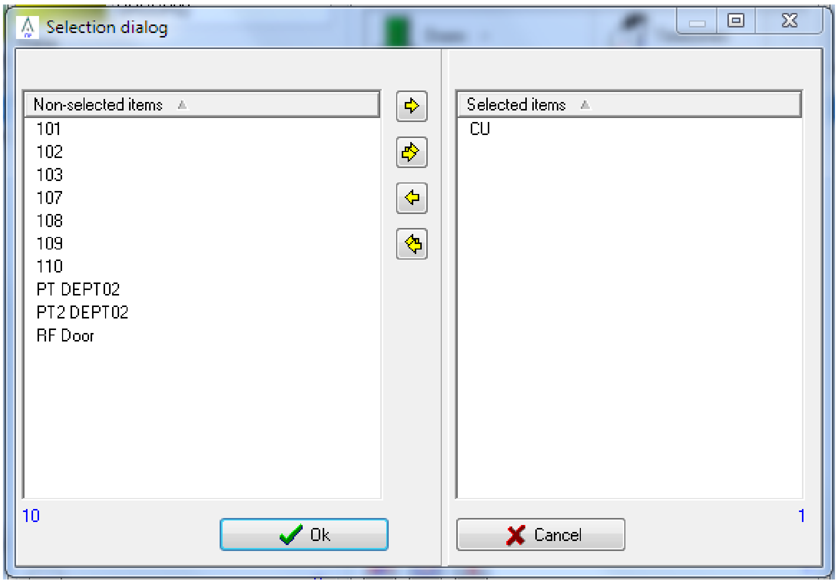


Figure 44b

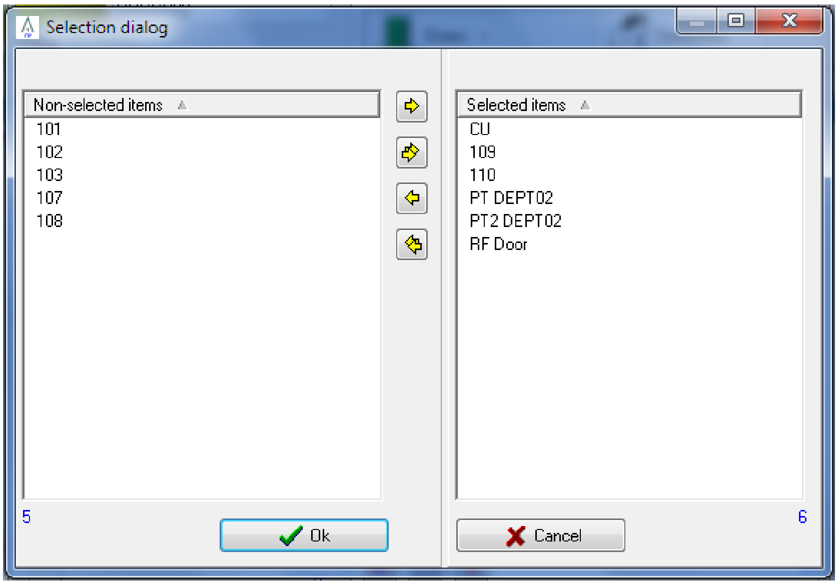
- We have to move from left-hand side to the right-hand side column, the zones that are going to be accessed by this group of users.

- If we have included a zone by mistake, highlight it in blue color, and click on the yellow arrow pointing left, to put it back to the left column.

- Yellow double-arrow performs the same function as single arrow, but instead of moving an individual zone, they move all zones from source to target column.

- In this window, we can specify to which zones the access level is allowed access, (clicking on the +/- button), and we can also determine group time zones, (clicking on the hourglass symbol).

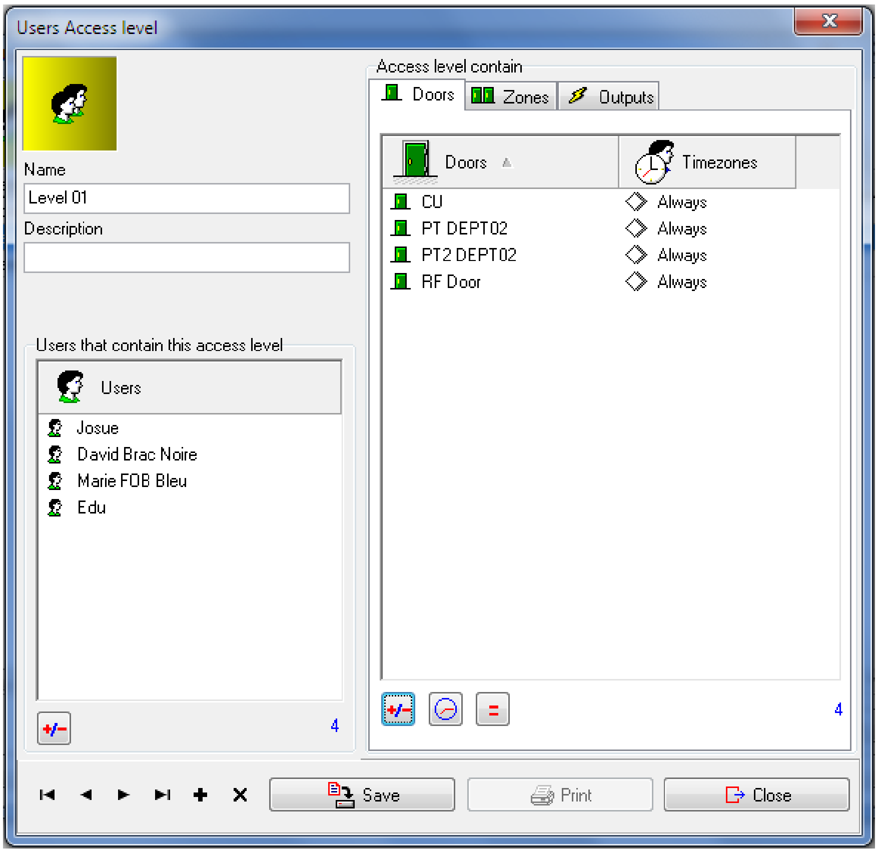
- **Authorizing an access level access into a zone implies that all the users who belong to that access level, may enter every door of the zone**.



Non-selected items	Selected items
101	CU
102	109
103	110
107	PT DEPT02
108	PT2 DEPT02
	RF Door
5	6

In the access level details window there is a tag titled DOORS BEING ACCESSED. The procedure for completing this box is similar to that of the ZONES BEING ACCESSED box, the only difference is that instead of assigning accesses by zones, they are assigned by individual doors. This option may be used for a single door, but access by door zones management is generally recommended, as this saves time and chip (key) memory.

It is also necessary to assign outputs to this user access level, if necessary. The tag OUTPUTS works in the same way as zones or doors, and here we can select the relays that are going to be commanded by this user access level.



Name: Level 01

Description:

Users that contain this access level

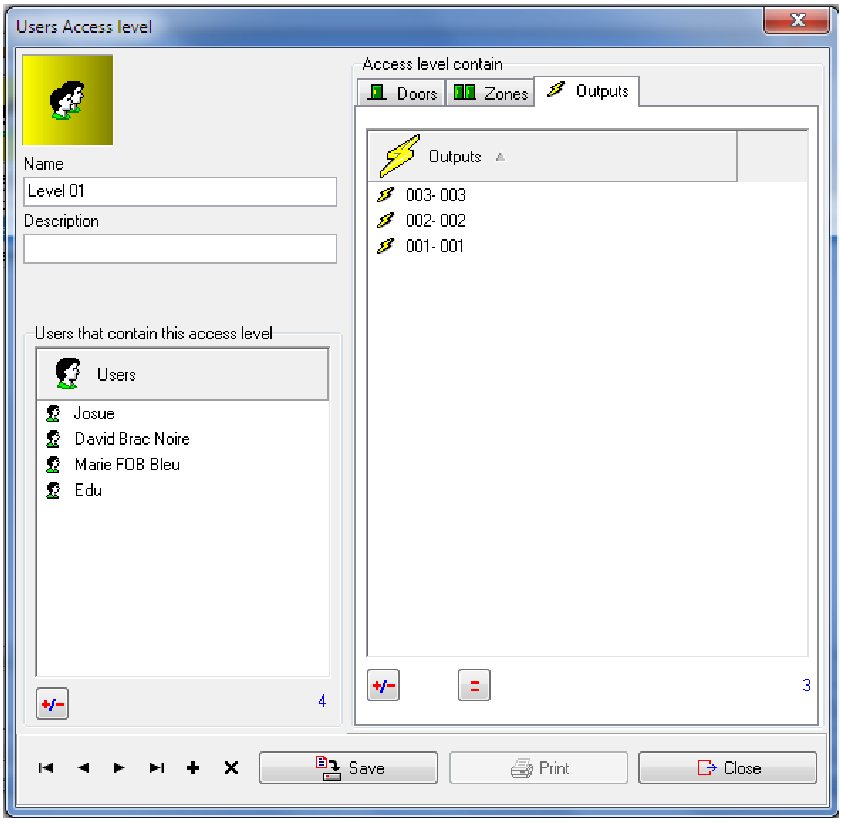
Users
Josue
David Brac Noire
Marie FOB Bleu
Edu

4

Doors	Timezones
CU	Always
PT DEPT02	Always
PT2 DEPT02	Always
RF Door	Always

4

This way the complete access profile for this user access level is designed.



Name: Level 01

Description:

Users that contain this access level

Users
Josue
David Brac Noire
Marie FOB Bleu
Edu

4

Outputs
003- 003
002- 002
001- 001

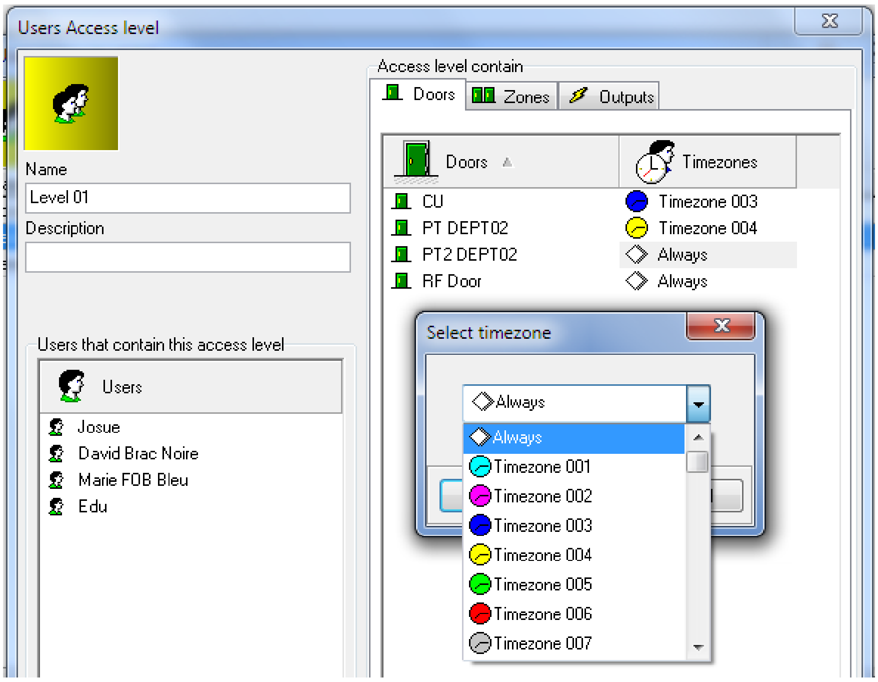
3

Figure 45

- When you have specified every single characteristic of this user access level, save the changes and go on to define next access level by clicking on + button.

- In the example here, a time zone for cleaning personnel has been set up. Assigning accesses to the *cleaners* group, we can also assign them time zones using the hourglass symbol.

- If no time zone is assigned to a door or zone of doors, by default, the system sets a 24 hour access to the access level.



Name: Level 01

Description:

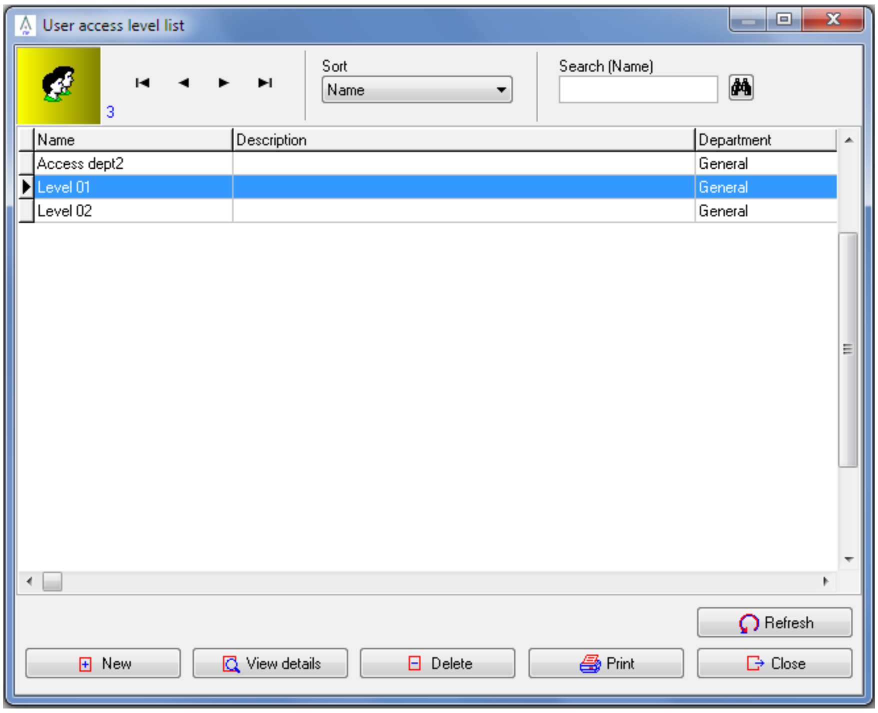
Doors	Timezones
CU	Timezone 003
PT DEPT02	Timezone 004
PT2 DEPT02	Always
RF Door	Always

Users
Josue
David Brac Noire
Marie FOB Bleu
Edu

Select timezone: Always

- Always
- Timezone 001
- Timezone 002
- Timezone 003
- Timezone 004
- Timezone 005
- Timezone 006
- Timezone 007

- Finally, the user access levels list will look like this below:



Sort: Name

Name	Description	Department
Access dept2		General
Level 01		General
Level 02		General

Figure 46

- If we have created an access level by mistake, just select it in blue color and click on the DELETE button.

- If at a given point, we want to view the details of an access level of the list, simply select that access level and click on the VIEW DETAILS button.

- Another way of selecting an access level from the list is with the |< < > >| scroll arrows that are located on the upper left-hand side of the window, instead of using the mouse.

- The box on the upper part titled SORT BY is used to sort user's access levels list in alphabetical order, by name or by description.

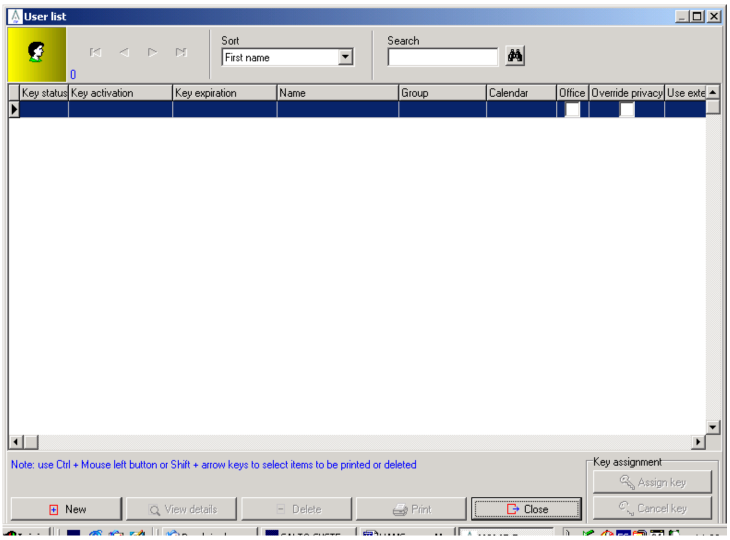
- The PRINT button can be used to obtain a hardcopy report from the user access level list. You can select between printing all of the user access level lists or only the details that relate to one particular user access level.

Users List

In this section we will define the users characteristics.

Click with the mouse on the USERS icon on the Toolbar.

A window like this one will be displayed:



User list

Sort: First name

Search:

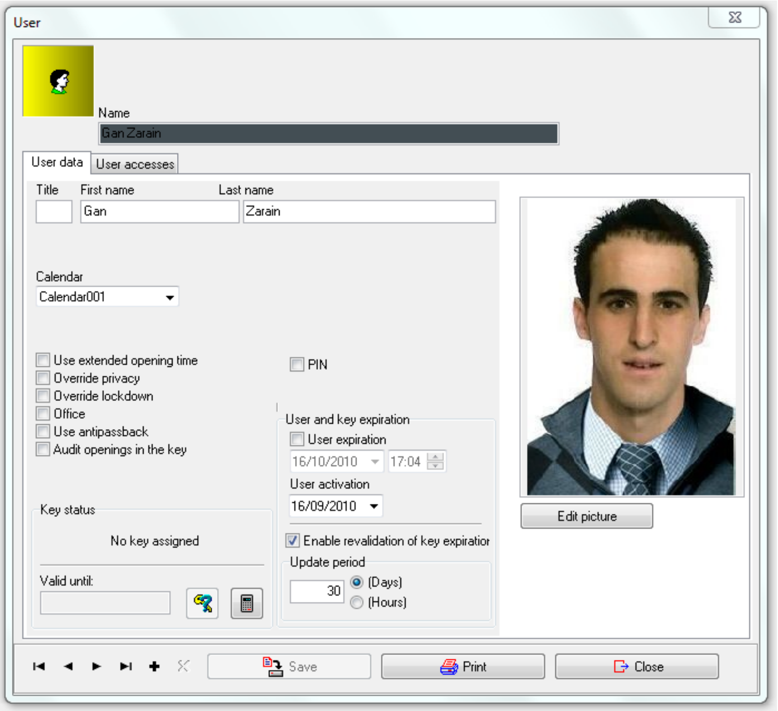
0

Key status	Key activation	Key expiration	Name	Group	Calendar	Office	Override privacy	Use exte

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 47

- Given that it is the first time we have opened the users list, the list is empty.
- Click on the NEW button to create the first user.
- A window like this one will be displayed:



User

Name: Gan Zarain

User data | User accesses

Title:

First name: Gan

Last name: Zarain

Calendar: Calendar001

□ Use extended opening time
□ Override privacy
□ Override lockdown
□ Office
□ Use antipassback
□ Audit openings in the key

□ PIN

User and key expiration
□ User expiration
16/10/2010 17:04
User activation
16/09/2010

☑ Enable revalidation of key expiratior

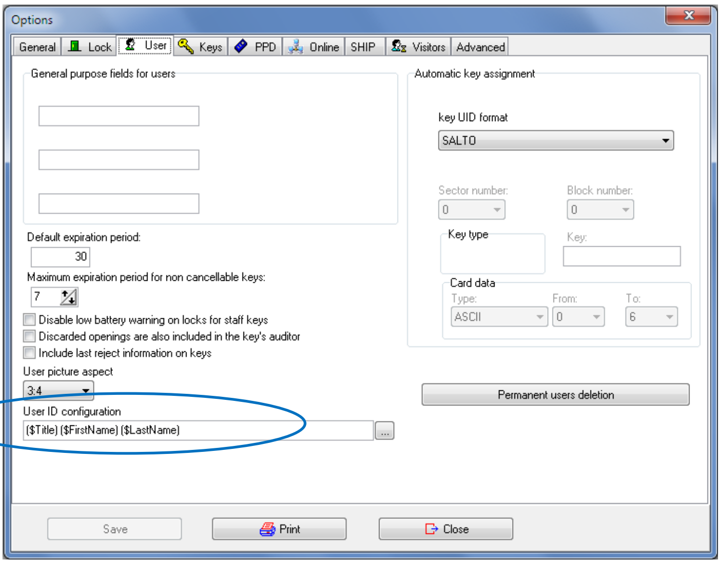
Update period
30 ● (Days) ○ (Hours)

Key status
No key assigned

Valid until:

Figure 48

- Type our first user name and surname.
  In the situation where more than one person has the same name, it will be necessary to define the users ID composition. To do so, go to Tools/ Configuration/ General options and users tab, as shown below;



General purpose fields for users

Default expiration period: 30

Maximum expiration period for non cancellable keys: 7

□ Disable low battery warning on locks for staff keys
□ Discarded openings are also included in the key's auditor
□ Include last reject information on keys

User picture aspect: 3:4

User ID configuration: ($Title) ($FirstName) ($LastName)

Automatic key assignment

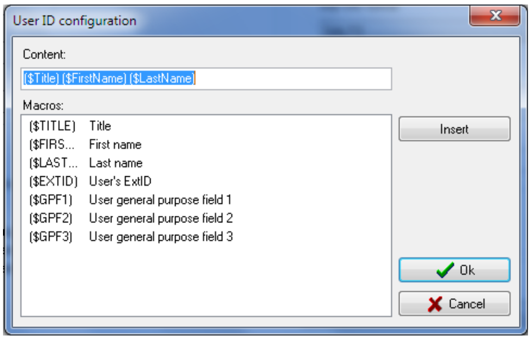
key UID format: SALTO

Sector number: 0 Block number: 0

Key type

Key:

Card data
Type: ASCII From: 0 To: 6



Content: ($Title) ($FirstName) ($LastName)

Macros:

($TITLE)	Title
($FIRS...	First name
($LAST...	Last name
($EXTID)	User's ExtID
($GPF1)	User general purpose field 1
($GPF2)	User general purpose field 2
($GPF3)	User general purpose field 3

As you can see on the previous image, the user ID can be set up with the information contained on various fields as;

1/ TITLE
2/ FIRST NAME
3/ LAST NAME
4/ GPF1
5/ GPF2
6/ GPF3
7/ EXT USER ID
I.E. User ID= GPF1 or User ID= GPF1+LAST NAME+EXT USER ID.

- The parameter INHIBIT_USER_NAME_CHANGE=1 will prevent a system operator from changing a user's name once a key has been assigned to that user. This will avoid false audit trail names. If a user requires a name change, the existing user will have to be deleted and new key will need to be assigned, thus, keeping the consistency of the audit trail.

- We have the ability to assign a calendar to our first user, according to the calendar settings we have previously defined.

- We have to specify which user access level this person belongs to. As we have already created users access levels, then we must select one for this user.

- We get a check box titled USE EXTENDED OPENING TIME. Tick this check box if our user is a handicapped person.

- The OVERRIDE PRIVACY check box must only be ticked when we want a user to have the privilege of accessing a guest room even when the door has been locked from the inside.

- The SET IN OFFICE check box may be ticked to allow users who are responsible for setting doors into office mode to do so.

- The USE ANTIPASS BACK check box may be ticked off to allow this special access mode for users who must have it, in the doors where this access mode has been selected. The anti-pass back time can be selected in TOOLS/OPTION/LOCK, in hours and minutes.

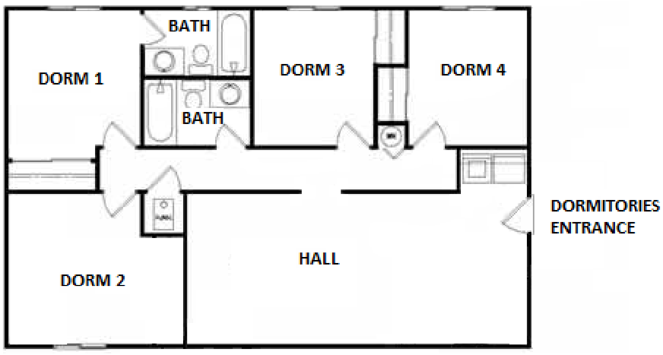
- If a user has not got the ANTIPASS BACK check box ticked off, this user will have a standard access, so he won´t have any restriction to enter twice by the same door.

- The check box AUDIT OPENINGS IN THE KEY can be marked if we want this user to have his personal audit trail on his key (recorded by doors).

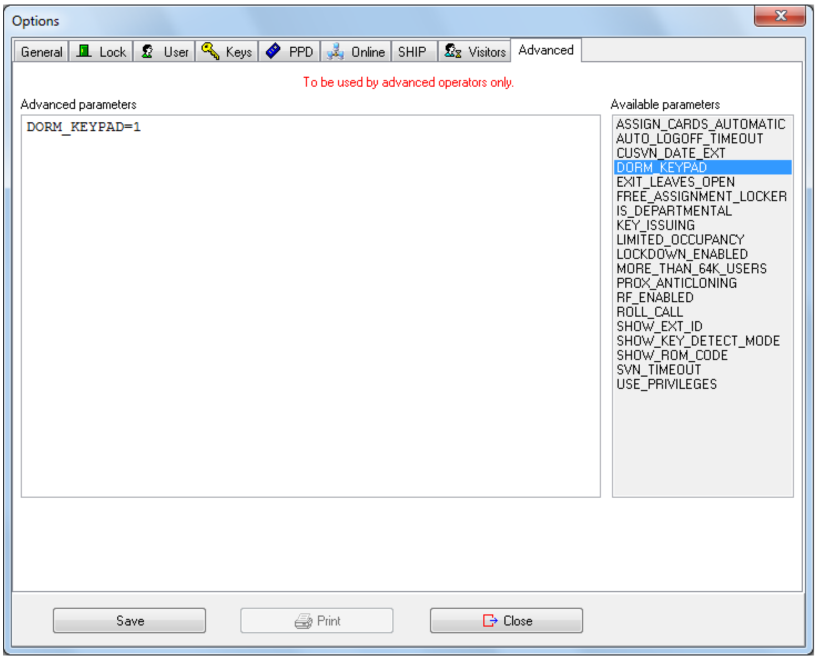
- In the lower left-hand side you find a box titled KEY STATUS. In this box will appear the characteristics of the card assigned to this user, when user keys have been assigned.

- The box titled KEY UPDATING displays information about the key updating procedure.

- Doors working in Keypad Only mode could have their Code changed by one of the users that have got access through it.
  This option is normally useful in Dormitory Entrances, where the dormitories users' turnover requires a code change from time to time, in order to avoid security issues.



In order to activate this function, the DORM_KEYPAD=1 parameter has to be added to the Advanced options, in the General Options menu. <u>This is only available in Pro Access For Service.</u>



To be used by advanced operators only.

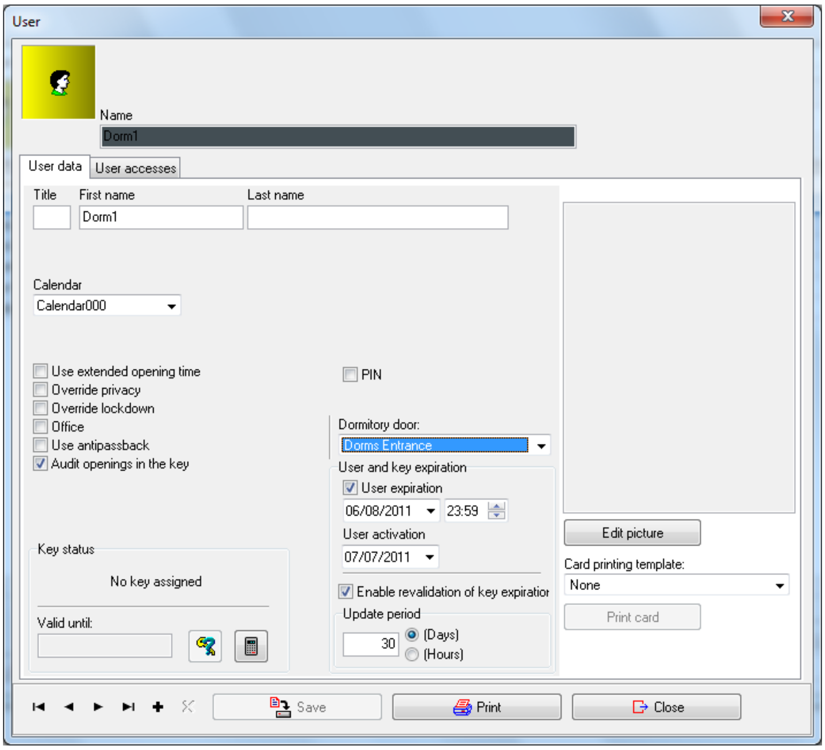
Advanced parameters

```
DORM_KEYPAD=1
```

Available parameters

ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CUSVN_DATE_EXT
DORM_KEYPAD
EXIT_LEAVES_OPEN
FREE_ASSIGNMENT_LOCKER
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
LOCKDOWN_ENABLED
MORE_THAN_64K_USERS
PROX_ANTICLONING
RF_ENABLED
ROLL_CALL
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SVN_TIMEOUT
USE_PRIVILEGES

This option will activate the “Dormitory Door” option in the User set up window. When a dormitory door is selected, the user (or users) will be able to change the keypad code in that dormitory door.



Name: Dorm1

Title:
First name: Dorm1
Last name:

Calendar: Calendar000

□ Use extended opening time
□ Override privacy
□ Override lockdown
□ Office
□ Use antipassback
☑ Audit openings in the key

□ PIN

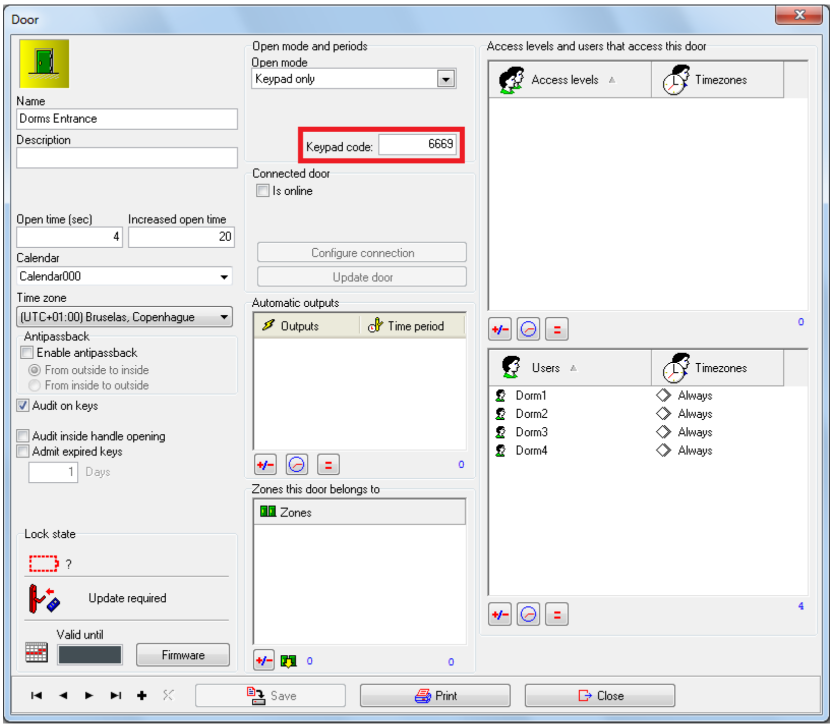
Dormitory door: Dorms Entrance

User and key expiration
☑ User expiration
06/08/2011 23:59
User activation
07/07/2011
☑ Enable revalidation of key expiratior
Update period
30 ● (Days) ○ (Hours)

Key status
No key assigned
Valid until:

Card printing template: None

The door’s code has to be changed in the Door set up window, changing the original code in the Keypad code field.



Name: Dorms Entrance

Description:

Open time (sec): 4

Increased open time: 20

Calendar: Calendar000

Time zone: (UTC+01:00) Bruselas, Copenhague

Antipassback

□ Enable antipassback

○ From outside to inside

○ From inside to outside

☑ Audit on keys

□ Audit inside handle opening

□ Admit expired keys

1 Days

Lock state: ?

Update required

Valid until

Open mode and periods

Open mode: Keypad only

Keypad code: 6669

Connected door

□ Is online

Automatic outputs: 0

Zones this door belongs to: 0 0

Access levels and users that access this door

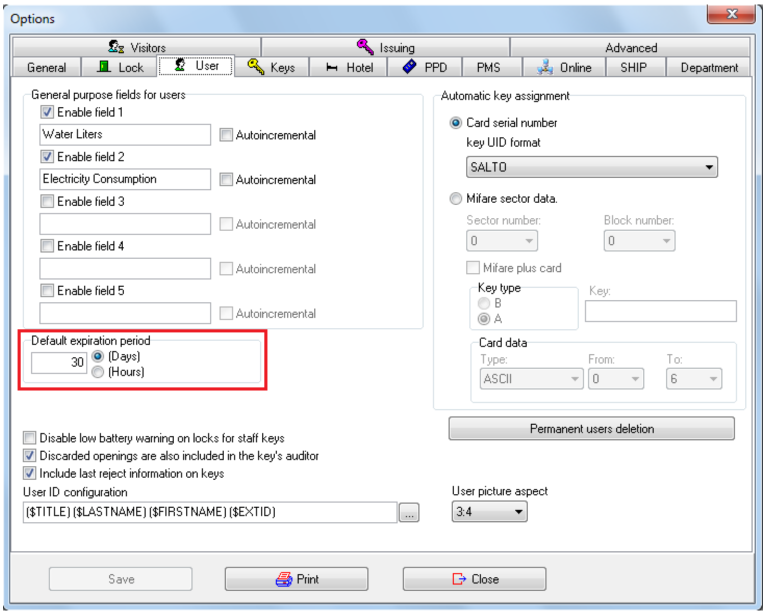
Access levels: 0

Users	Timezones
Dorm1	Always
Dorm2	Always
Dorm3	Always
Dorm4	Always

4

Once the code is changed, the user will have the new Keypad code written on its card when the card is presented at a SVN hotspot. As soon as the card is presented in the Dormitory door, the Keypad code will be updated, invalidating the previous one.

- The check box “ENABLE REVALIDATION OF KEY EXPIRATION” should be marked if we want this key to be updated with a particular frequency, on SVN wall readers. If this option is not checked, it is assumed that there is SVN and no key update (except through encoder)
  A default expiration period can be set in general options/ Users tab, “DEFAULT EXPIRATION PERIOD” in days and hours.
  In case of DAYS EXPIRATION TIME is selected, bear in mind that the last day of the expiration date would have to pass in order for the card to get expired. For instance, if a card is encoded on Monday at 08:00, and the Default Expiration Period is set up to 2 days, the card will expire on Wednesday at 24:00.
  In case HOURS EXPIRATION TIME is selected, the expiration would be precise, that is to say, if a card is encoded at 16:06 hours, and the Default Expiration Period is set up to 4 hours, the card will get expired at 20:06.



General purpose fields for users

☑ Enable field 1
Water Liters □ Autoincremental
☑ Enable field 2
Electricity Consumption □ Autoincremental
□ Enable field 3
□ Autoincremental
□ Enable field 4
□ Autoincremental
□ Enable field 5
□ Autoincremental

Default expiration period
30 ● (Days) ○ (Hours)

Automatic key assignment
● Card serial number
key UID format: SALTO
○ Mifare sector data.
Sector number: 0 Block number: 0
□ Mifare plus card
Key type: ○ B ● A Key:
Card data: Type: ASCII From: 0 To: 6

□ Disable low battery warning on locks for staff keys
☑ Discarded openings are also included in the key's auditor
☑ Include last reject information on keys

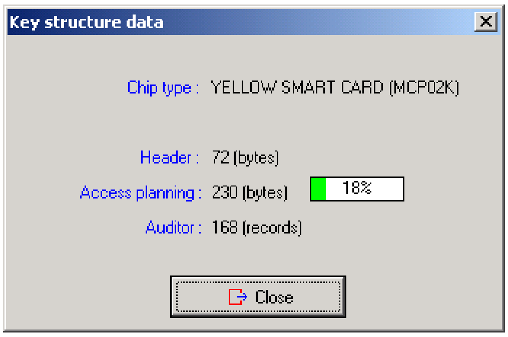
User ID configuration: ($TITLE) ($LASTNAME) ($FIRSTNAME) ($EXTID)

User picture aspect: 3:4

- Users without expiration date are only allowed to use calendar 0.

- The check box LAST UPDATE DATE means the end of updating procedure for this key. After this date, the key won´t be updated any longer. It is not mandatory to establish a last update date for a key.

- KEY WITH A QUESTION MARK BUTTON: this is a tool to show the key structure data. (such as header size, number of auditor records, consumed memory percentage, etc…)



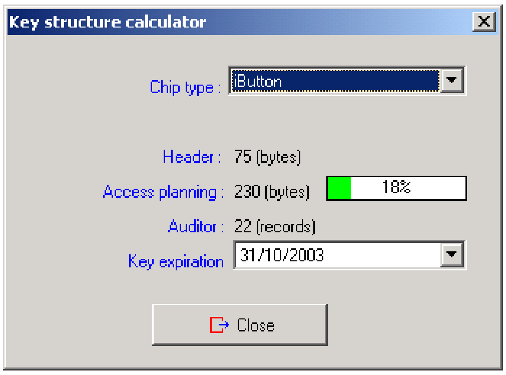
Chip type : YELLOW SMART CARD (MCP02K)

Header : 72 (bytes)

Access planning : 230 (bytes) 18%

Auditor : 168 (records)

- KEY CALCULATOR BUTTON: this tool can be used as a preview for the key structure information and memory consumption before any actual encoding is done. This tool works as a simulator for different technologies (smart. IButton, proximity).



Key structure calculator

Chip type : iButton

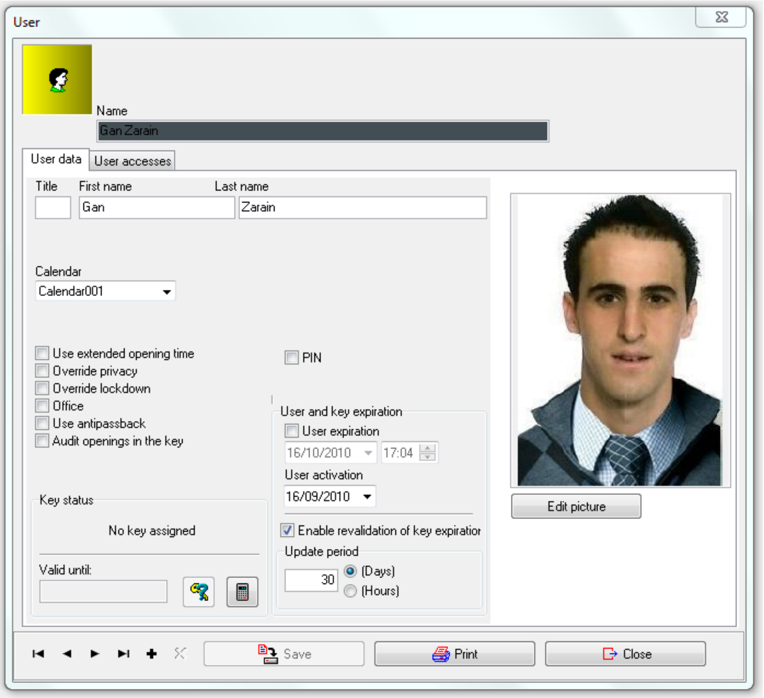
Header : 75 (bytes)

Access planning : 230 (bytes) 18%

Auditor : 22 (records)

Key expiration 31/10/2003

- It is not essential to define user accesses when this user belongs to an access level, since the user will have access level accesses as previously defined.
- Only when the user is not included in any access level, would you assign accesses at this point.
- It is not compulsory to assign the same time zone to different zones.



User

Name: Gan Zarain

User data | User accesses

Title:
First name: Gan
Last name: Zarain

Calendar: Calendar001

□ Use extended opening time
□ Override privacy
□ Override lockdown
□ Office
□ Use antipassback
□ Audit openings in the key

□ PIN

User and key expiration
□ User expiration
16/10/2010 17:04
User activation
16/09/2010

☑ Enable revalidation of key expiratior
Update period
30 ● (Days) ○ (Hours)

Key status
No key assigned
Valid until:

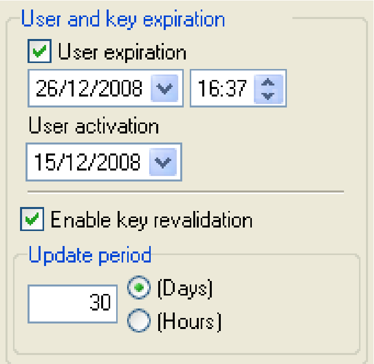
Figure 49

- Assigning a door zone to a user, will grant the user access to every door that is included in that zone.

- When we have a user that does not belong to any access level, we can assign his accesses from this window by following the procedure explained in the USERS ACCESS LEVELS section of this manual.

- The user and card expiration are managed from the following options

    - **User expiration** sets the maximum user validity
    - **User activation** sets the date since the card will be functional
    - **Enable key revalidation** sets the period the card will be updated for (in days or hours)



User and key expiration

☑ User expiration

26/12/2008 16:37

User activation

15/12/2008

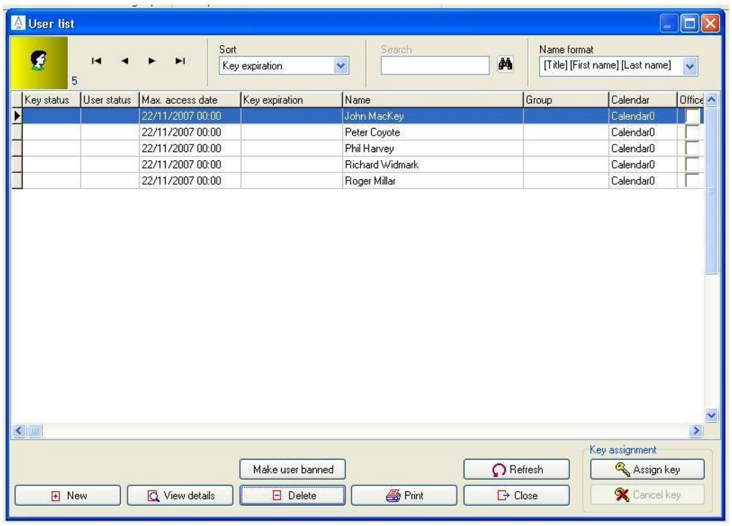
☑ Enable key revalidation

Update period

30 ● (Days) ○ (Hours)

- Once we have finished defining user characteristics, save the changes and click on the + button to go on to the next user in the list.

- When we have all the users (staff) defined, we will obtain a list that should look like the following:



Sort: Key expiration

Search:

Name format: [Title] [First name] [Last name]

	Key status	User status	Max. access date	Key expiration	Name	Group	Calendar	Office
▶			22/11/2007 00:00		John MacKey		Calendar0	□
			22/11/2007 00:00		Peter Coyote		Calendar0	□
			22/11/2007 00:00		Phil Harvey		Calendar0	□
			22/11/2007 00:00		Richard Widmark		Calendar0	□
			22/11/2007 00:00		Roger Millar		Calendar0	□

Figure 51

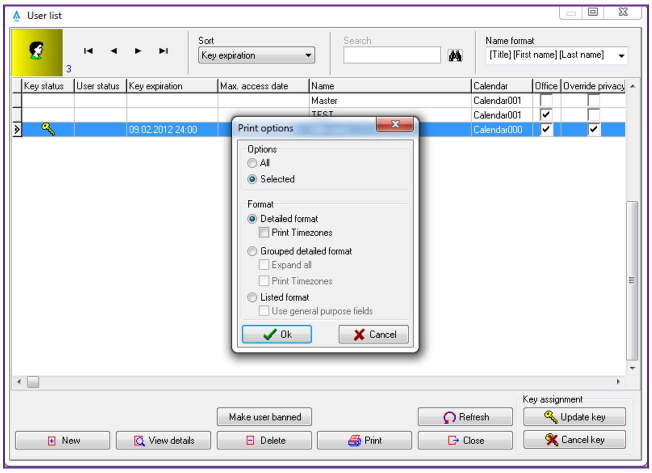
- If we have inserted a user by mistake, we can delete it selecting it first and then, clicking on the DELETE button.

- To view the details window of a given user, select the user and click on the VIEW DETAILS button.

- We can also use the scroll arrows on the left-hand corner to select a user from the list, instead of using the mouse to do so. With these scroll arrows <>, we pass to the user immediately after or before, and with these arrows |< >|, to the first or last users of the list.

- The box called SORT BY is used to sort users list according to the most convenient criteria, by name, by surname, by calendar, by access level, by expiration date…

- The PRINT button can be used to obtain a hardcopy report for the user list. It is possible to use user reports with some information from the user, i.e. to confirm a key delivery to a user or other reasons where a place is reserved for the date and signature. To use this document, go to the user list and click "Print"



User list

Sort: Key expiration
Search:
Name format: [Title] [First name] [Last name]

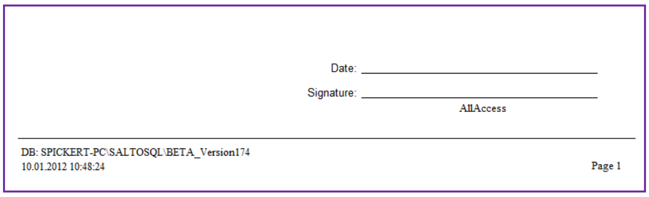
Key status	User status	Key expiration	Max. access date	Name	Calendar	Office	Override privacy
				Master	Calendar001	□	□
				TEST	Calendar001	☑	□
		09.02.2012 24:00			Calendar000	☑	☑

Print options

Options
○ All
● Selected

Format
● Detailed format
□ Print Timezones
○ Grouped detailed format
□ Expand all
□ Print Timezones
○ Listed format
□ Use general purpose fields

Here chose “Selected” and “Detailed format”. If the user’s timezone, must be shown, click the check box. When ready click “Ok” and a preview of the report will appear. In the bottom of the document a place is reserved to date and sign.



Date: ____________________

Signature: ____________________

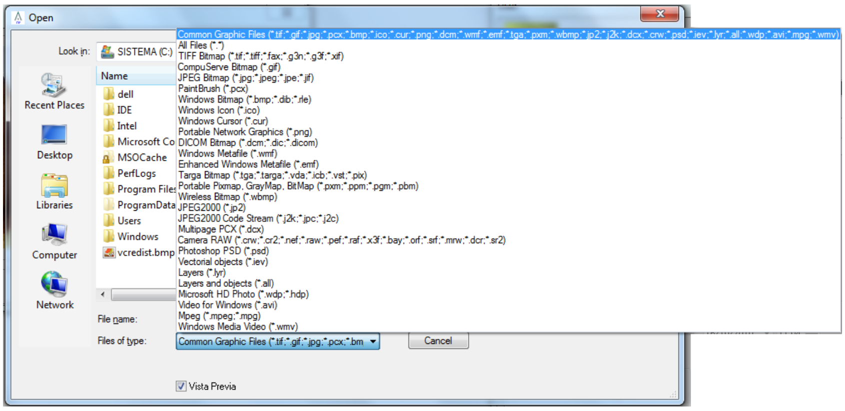
AllAccess

DB: SPICKERT-PC\SALTOSQL\BETA_Version174
10.01.2012 10:48:24

Page 1

- The Make user banned is an option to block a user. So any change or modification can be done on him. It can be configured on the operators and permissions the operator who will have the privilege to make banned a user. When a user has been banned and he presents the card to the CU the access plan is going to be erased and that user won’t be able to access to any part of that installation. As soon as the same user has been disbanned and presents his card to the CU will be again updated with his access plan.

- Picture. A picture can be added to identify the user. The photo can be imported from any storage device (hard disk, USB pendrive, memory card,…) or directly from a connected camera device.
  Many picture formats are compatible (jpeg, bmp, tif, gif,…).


Open
Look in: SISTEMA (C:)
Recent Places
Desktop
Libraries
Computer
Network
Name
dell
IDE
Intel
Microsoft Co
MSOCache
PerfLogs
Program Files
ProgramData
Users
Windows
vcredist.bmp
Common Graphic Files (*.tif;*.gif;*.jpg;*.pcx;*.bmp;*.ico;*.cur;*.png;*.dcm;*.wmf;*.emf;*.tga;*.pxm;*.wbmp;*.jp2;*.j2k;*.dcx;*.crw;*.psd;*.iev;*.lyr;*.all;*.wdp;*.avi;*.mpg;*.wmv)
All Files (*.*)
TIFF Bitmap (*.tif;*.tiff;*.fax;*.g3n;*.g3f;*.xif)
CompuServe Bitmap (*.gif)
JPEG Bitmap (*.jpg;*.jpeg;*.jpe;*.jif)
PaintBrush (*.pcx)
Windows Bitmap (*.bmp;*.dib;*.rle)
Windows Icon (*.ico)
Windows Cursor (*.cur)
Portable Network Graphics (*.png)
DICOM Bitmap (*.dcm;*.dic;*.dicom)
Windows Metafile (*.wmf)
Enhanced Windows Metafile (*.emf)
Targa Bitmap (*.tga;*.targa;*.vda;*.icb;*.vst;*.pix)
Portable Pixmap, GrayMap, BitMap (*.pxm;*.ppm;*.pgm;*.pbm)
Wireless Bitmap (*.wbmp)
JPEG2000 (*.jp2)
JPEG2000 Code Stream (*.j2k;*.jpc;*.j2c)
Multipage PCX (*.dcx)
Camera RAW (*.crw;*.cr2;*.nef;*.raw;*.pef;*.raf;*.x3f;*.bay;*.orf;*.srf;*.mrw;*.dcr;*.sr2)
Photoshop PSD (*.psd)
Vectorial objects (*.iev)
Layers (*.lyr)
Layers and objects (*.all)
Microsoft HD Photo (*.wdp;*.hdp)
Video for Windows (*.avi)
Mpeg (*.mpeg;*.mpg)
Windows Media Video (*.wmv)
Cancel

File name:

Files of type: Common Graphic Files (*.tif;*.gif;*.jpg;*.pcx;*.bm

☑ Vista Previa

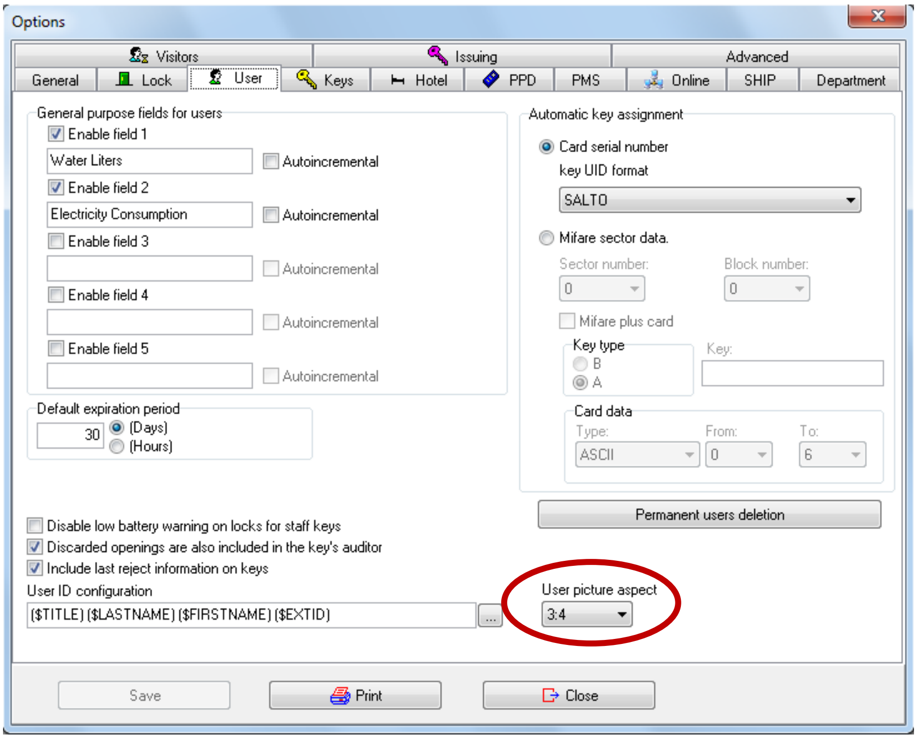
Picture aspect

The picture aspect can be predefined from the General Options menu, user tab. The options are:

3:4

2:3

1:1



General purpose fields for users

☑ Enable field 1

Water Liters □ Autoincremental

☑ Enable field 2

Electricity Consumption □ Autoincremental

□ Enable field 3

□ Autoincremental

□ Enable field 4

□ Autoincremental

□ Enable field 5

□ Autoincremental

Default expiration period

30 ● (Days) ○ (Hours)

Automatic key assignment

● Card serial number

key UID format: SALTO

○ Mifare sector data.

Sector number: 0 Block number: 0

□ Mifare plus card

Key type: ○ B ● A

Key:

Card data

Type: ASCII From: 0 To: 6

Permanent users deletion

□ Disable low battery warning on locks for staff keys

☑ Discarded openings are also included in the key's auditor

☑ Include last reject information on keys

User ID configuration

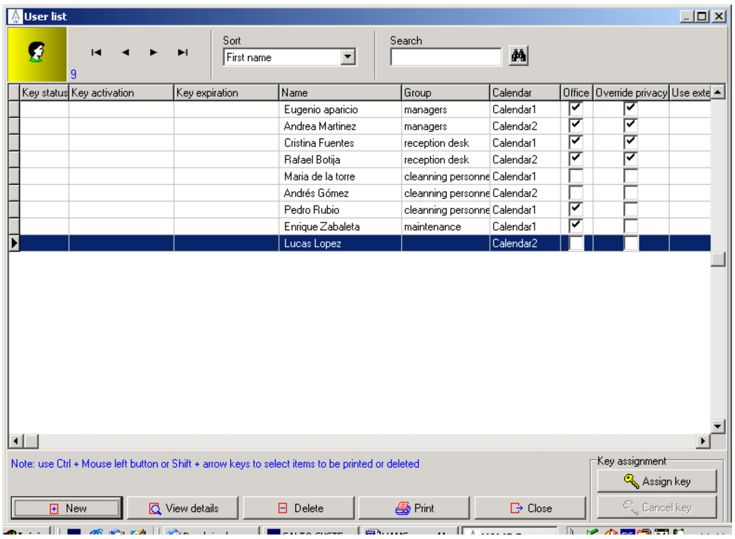
($TITLE) ($LASTNAME) ($FIRSTNAME) ($EXTID)

User picture aspect: 3:4

User key assignment

Once you have completed user list definition, we can then proceed to assign each user their key (Smart Card, iButtton, proximity.) In order to do so, you must connect the ENCODER to the serial port of your computer. You must also supply power to the ENCODER plugging the feeder provided to a 220-240 V. AC, 50 Hz socket and inserting the respective jack into the ENCODER.

To assign user keys, follow the steps detailed below:



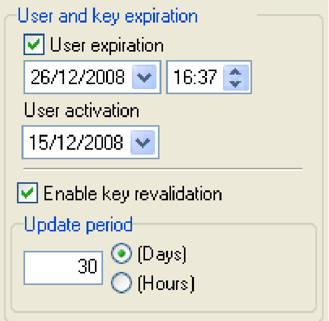
Sort: First name

Key status	Key activation	Key expiration	Name	Group	Calendar	Office	Override privacy	Use exte
			Eugenio aparicio	managers	Calendar1	☑	☑	
			Andrea Martinez	managers	Calendar2	☑	☑	
			Cristina Fuentes	reception desk	Calendar1	☑	☑	
			Rafael Botija	reception desk	Calendar2	☑	☑	
			Maria de la torre	cleanning personne	Calendar1	□	□	
			Andrés Gómez	cleanning personne	Calendar2	□	□	
			Pedro Rubio	cleanning personne	Calendar1	☑	□	
			Enrique Zabaleta	maintenance	Calendar1	☑	□	
			Lucas Lopez		Calendar2	□	□	

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 52

- From the user list, highlight a user with the mouse. Then, click on the ASSIGN KEY button that can be found on the lower right-hand side corner of the window.


User and key expiration

☑ User expiration

26/12/2008 16:37

User activation

15/12/2008

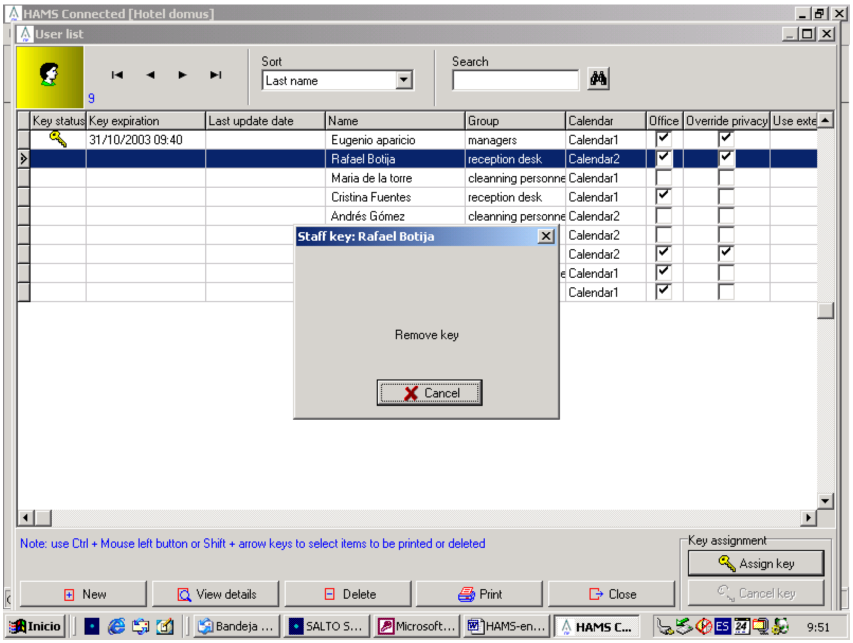
☑ Enable key revalidation

Update period

30 ● (Days) ○ (Hours)

Figure 53

- The system will prompt a message window requesting you to insert a card into the ENCODER.


HAMS Connected [Hotel domus]

User list

Sort: Last name

Search:

9

	Key status	Key expiration	Last update date	Name	Group	Calendar	Office	Override privacy	Use exte
	🔑	31/10/2003 09:40		Eugenio aparicio	managers	Calendar1	☑	☑	
>				Rafael Botija	reception desk	Calendar2	☑	☑	
				Maria de la torre	cleanning personne	Calendar1	☐	☐	
				Cristina Fuentes	reception desk	Calendar1	☑	☐	
				Andrés Gómez	cleanning personne	Calendar2	☐	☐	
						Calendar2	☐	☐	
						Calendar2	☑	☑	
					e	Calendar1	☑	☐	
						Calendar1	☑	☐	

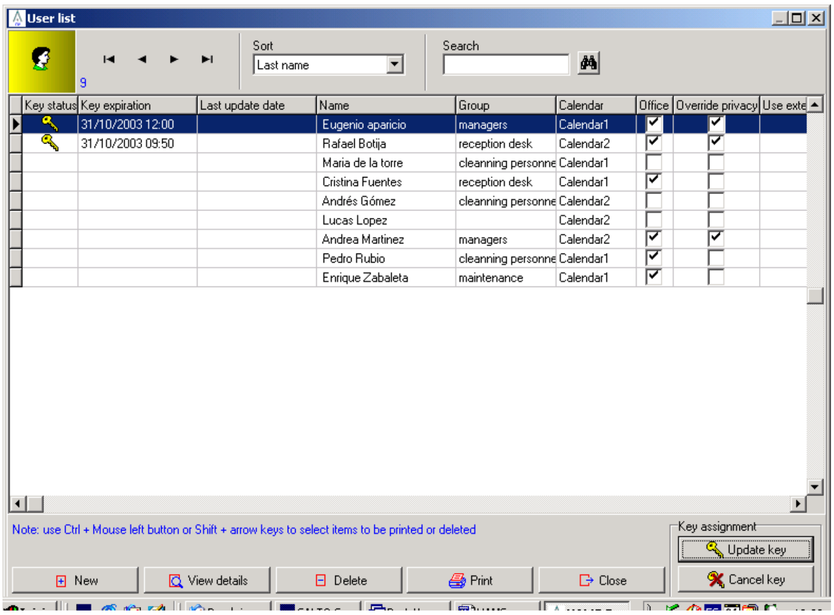
Staff key: Rafael Botija

Remove key

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 54

- Encoding process is very swift. The system will tell you to withdraw the card almost straightaway.
- Now, you will check that a yellow key icon appears next to the user name to which key has been assigned.


User list

Sort: Last name

Search:

9

	Key status	Key expiration	Last update date	Name	Group	Calendar	Office	Override privacy	Use exte
▶	🔑	31/10/2003 12:00		Eugenio aparicio	managers	Calendar1	☑	☑	
	🔑	31/10/2003 09:50		Rafael Botija	reception desk	Calendar2	☑	☑	
				Maria de la torre	cleanning personne	Calendar1	☐	☐	
				Cristina Fuentes	reception desk	Calendar1	☑	☐	
				Andrés Gómez	cleanning personne	Calendar2	☐	☐	
				Lucas Lopez		Calendar2	☐	☐	
				Andrea Martinez	managers	Calendar2	☑	☑	
				Pedro Rubio	cleanning personne	Calendar1	☑	☐	
				Enrique Zabaleta	maintenance	Calendar1	☑	☐	

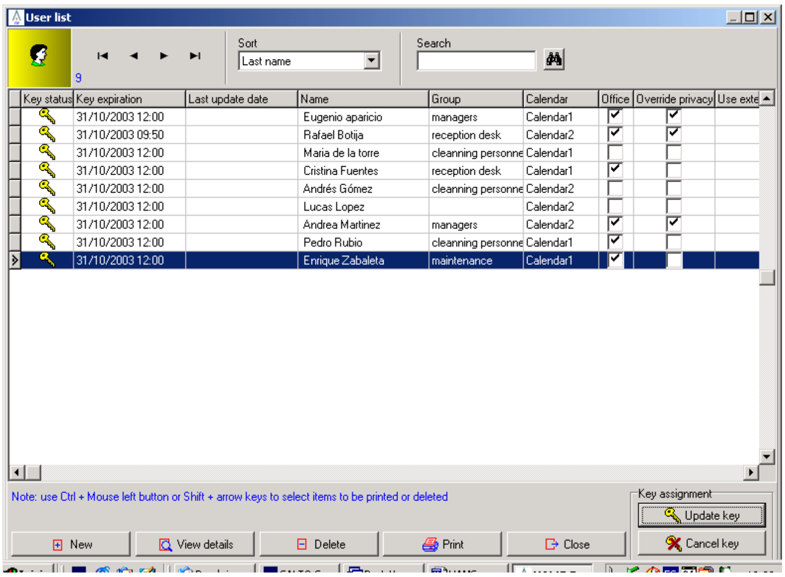
Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 55

- You are encouraged to hand the keys over to respective users without any delay.

- To further assign the keys to other users, follow the same procedure.

- Finally, you will obtain a user list with their key assigned, as shown in the following figure:



	Key status	Key expiration	Last update date	Name	Group	Calendar	Office	Override privacy	Use exte
		31/10/2003 12:00		Eugenio aparicio	managers	Calendar1	☑	☑	
		31/10/2003 09:50		Rafael Botija	reception desk	Calendar2	☑	☑	
		31/10/2003 12:00		Maria de la torre	cleanning personne	Calendar1	□	□	
		31/10/2003 12:00		Cristina Fuentes	reception desk	Calendar1	☑	□	
		31/10/2003 12:00		Andrés Gómez	cleanning personne	Calendar2	□	□	
		31/10/2003 12:00		Lucas Lopez		Calendar2	□	□	
		31/10/2003 12:00		Andrea Martinez	managers	Calendar2	☑	☑	
		31/10/2003 12:00		Pedro Rubio	cleanning personne	Calendar1	☑	□	
▶		31/10/2003 12:00		Enrique Zabaleta	maintenance	Calendar1	☑	□	

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 56

- If a user loses a key, you must immediately cancel it in the user list. To do so, highlight the user that has lost their card, and click on CANCEL KEY button.

- Afterwards, a new card for this user has to be edited, following the same procedure as previously detailed. From now on, the user will have a new card. However, should for any reason whatsoever the lost key turn up, this will no longer open any of the doors where the new key has been used.

- If we modify any users access rights, we will have also to update the users key. To accomplish this task, you should ask the user for their key so as to allow you to update it on the ENCODER.

- The colour of the icon of the key denotes its status. Thus, a red key means that it has changes to be updated; a blue key means that its expiration date is approaching and a yellow key with an hourglass means that it has already expired.

- There are 2 reasons for a key appearing in blue colour: 1. The key is going to expire in the next 15 days but it was edited more than 15 days ago. 2. The key is going to expire in the next 7 days but it was edited more than 7 days ago.

- Once the key has been assigned to the user, any change made in the user access profile will imply the key turns red colour. This changes can be updated in the SVN wall readers but there are 2 specific changes that imply "key re-edition" or "key re-encoding". These are ANTIPASSBACK and AUDIT ON KEY option. (for users).

- When one of these changes is made, the key will appear in red color with a cog symbol, to remember you need to update the key in the serial encoder – "re-edition". See image below.

- The fact of changing the antipass back time, TOOLS/OPTIONS/LOCK also implies re-edition for the user cards , although the cog symbol will not appear next to the key symbol, in the user list.

If there is any doubt about the need of re-edit the user cards, this can be cleared by the light signals given by the Salto Virtual net wall reader.

The light signals are different depending on the technology:

- Smart card: orange flashing light (key is being updated) followed by a fix light red or green (door close, door open). This is the standard sequence. If after that there is a fixed orange light, then this means that the key needs re-edition.

- I button and proximity cards: blue flashing light (key is being updated) followed by a fixed light red or green (door close, door open). This is the standard sequence. IF after that there is a fixed blue light, this means that the key needs re-edition.

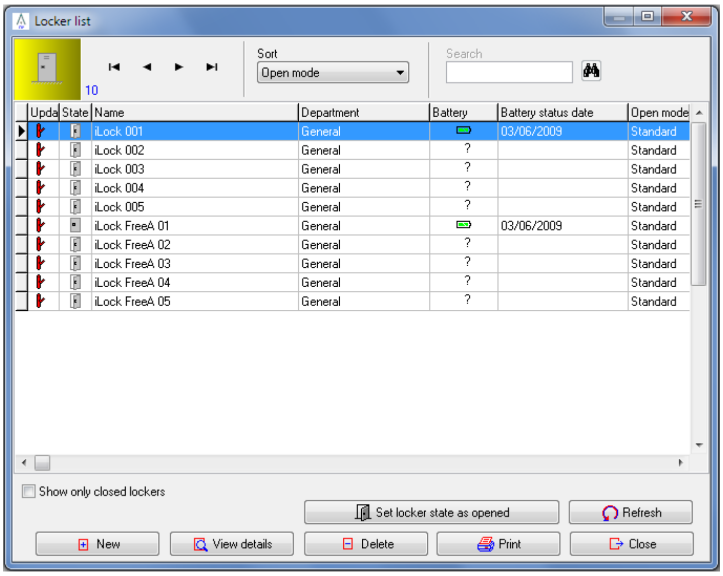
Lockers

SALTO includes in his software the option to manage as web the Lockers. The configuration and use of them is very intuitive and similar to our escutcheons and permits us as well obtain the same info as we get from our escutcheons (Openings, rejects, etc.)

Define Lockers:

First of all we have to include the Lockers in the software. To do this we have to go to the menu DATA/ LOCKERS. The following window will be shown (Fig 1). In this window we will see the Locker list, the status (open/close), Name, Battery Status, Date, Opening Mode and Time Zone.

In the bottom part there is a check box “Show only closed Lockers”. If you enable this option only the closed Lockers will be shown in the screen. There is another button “Set Locker state as opened”. This option is very helpful when a user has left the Locker closed and we open it with a master key. In this way we can change the state manually.



Sort: Open mode

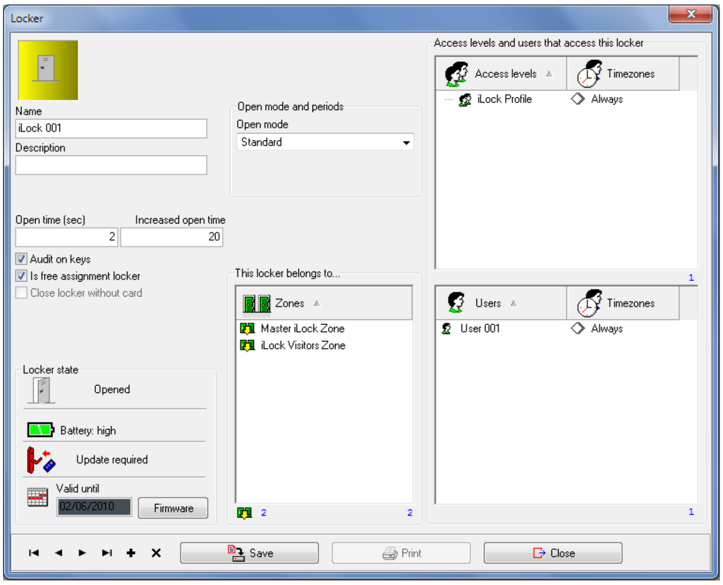
10

Upda	State	Name	Department	Battery	Battery status date	Open mode
		iLock 001	General	🟩	03/06/2009	Standard
		iLock 002	General	?		Standard
		iLock 003	General	?		Standard
		iLock 004	General	?		Standard
		iLock 005	General	?		Standard
		iLock FreeA 01	General	🟩	03/06/2009	Standard
		iLock FreeA 02	General	?		Standard
		iLock FreeA 03	General	?		Standard
		iLock FreeA 04	General	?		Standard
		iLock FreeA 05	General	?		Standard

☐ Show only closed lockers

(Fig. 1)

Next step will be to press the “New” button and start defining the Lockers profile. The procedure is similar to create a new door. (Fig 2)



Name: iLock 001

Description:

Open mode and periods

Open mode: Standard

Open time (sec): 2

Increased open time: 20

☑ Audit on keys

☑ Is free assignment locker

☐ Close locker without card

Locker state: Opened

Battery: high

Update required

Valid until: 02/06/2010

Access levels and users that access this locker

Access levels	Timezones
iLock Profile	Always

1

This locker belongs to...

Zones
Master iLock Zone
iLock Visitors Zone

2 2

Users	Timezones
User 001	Always

1

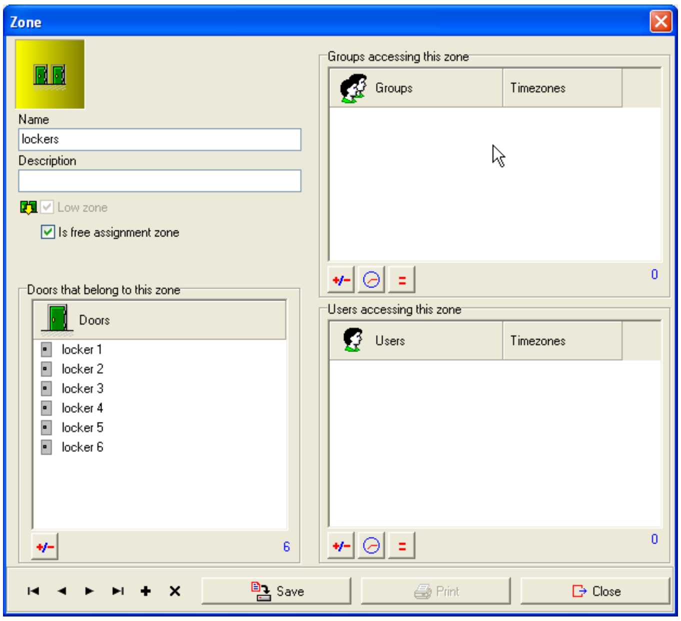
(Fig. 2)

We have to define the profile:

Select opening mode (Standard or Automatic Opening). If the Locker is going to be included in a “Free assignment Zone” it is very important to enable the checkbox “Is free assignment locker”

Define Free Assignment Zones:

To enable this option we have to go to the menu: TOOLS/ CONFIGURATION/ GENERAL OPTIONS/ ADVANCE and enable the option “Free assignment Locker”


Zone
Groups accessing this zone
Groups
Timezones
Users accessing this zone
Users
Timezones
Doors that belong to this zone
Doors
Save
Print
Close

Name: lockers

Description:

☑ Low zone

☑ Is free assignment zone

Doors that belong to this zone: locker 1, locker 2, locker 3, locker 4, locker 5, locker 6 — 6

Groups accessing this zone: 0

Users accessing this zone: 0

(Fig. 4)

In this case we have to enable the checkbox “Is free assignment zone”. **It is very important that we have defined the Lockers as “Free assignment Locker” otherwise the software will show us an error message.**

Free Assignment Zone:

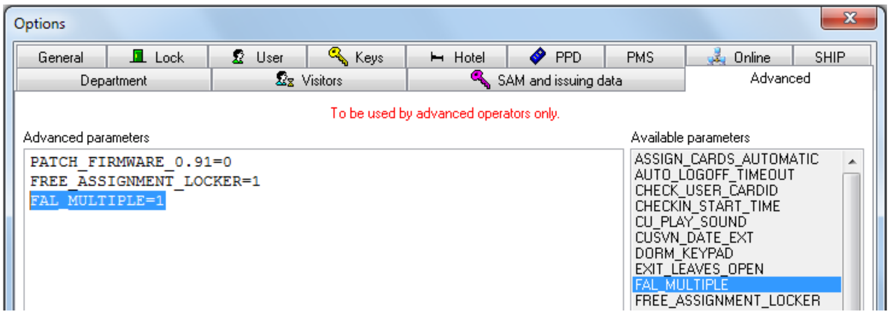
We can either assign a Locker directly to a User (like with the escutcheons) or there is another option where the user can choose freely the Locker that he wants to use.

In these cases we have to create a Zone including all the Lockers where users will choose a free one. The procedure to create this Zone is similar to create a Door Zone.

Multiple Free Assignment Zones:

The FAL_MULTIPLE advanced parameter allows creating two additional locker zones, in order to allow a System user capture more than one locker with a single card, as long as they belong to a different free assignment group.

In order to activate this function, the FAL_MULTIPLE advanced parameter must be added to the list of active advanced parameters in the software, as can be seen in the picture below:



To be used by advanced operators only.

Advanced parameters

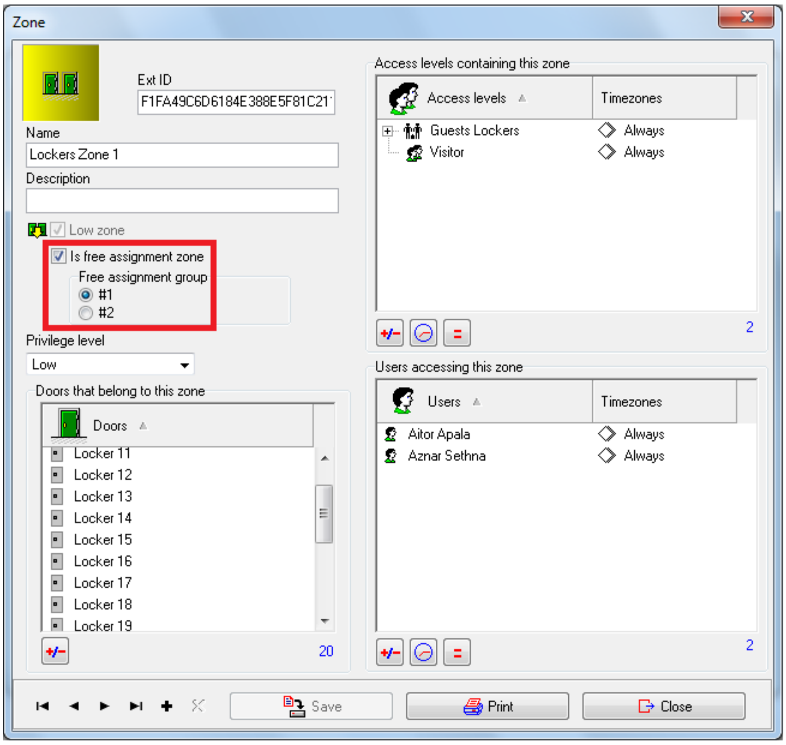
```
PATCH_FIRMWARE_0.91=0
FREE_ASSIGNMENT_LOCKER=1
FAL_MULTIPLE=1
```

Available parameters

```
ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CHECK_USER_CARDID
CHECKIN_START_TIME
CU_PLAY_SOUND
CUSVN_DATE_EXT
DORM_KEYPAD
EXIT_LEAVES_OPEN
FAL_MULTIPLE
FREE_ASSIGNMENT_LOCKER
```

Once the function is active, the following option will be added to the zones configuration window:

- Free assignment group #1.
- Free assignment group #2.



Ext ID: F1FA49C6D6184E388E5F81C21'

Name: Lockers Zone 1

Description:

☑ Low zone

☑ Is free assignment zone

Free assignment group
● #1
○ #2

Privilege level: Low

Doors that belong to this zone

Doors
Locker 11
Locker 12
Locker 13
Locker 14
Locker 15
Locker 16
Locker 17
Locker 18
Locker 19

20

Access levels containing this zone

Access levels	Timezones
Guests Lockers	Always
Visitor	Always

2

Users accessing this zone

Users	Timezones
Aitor Apala	Always
Aznar Sethna	Always

2

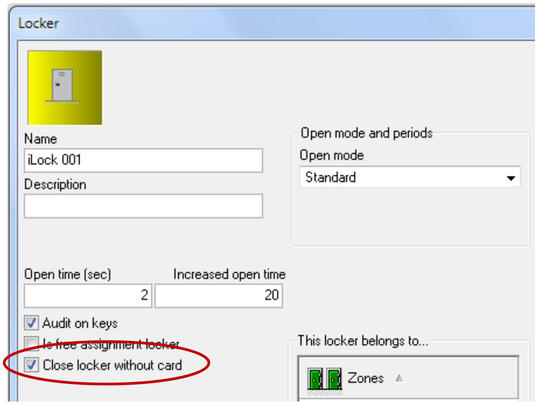
These mentioned options will be only selectable when the zone is defined as a free assignment zone.

When activated, lockers could be assigned to one of the free assignment groups. This group identification will be written on the card when the user captures a locker from one of the free assignment groups, not allowing this same user capturing a locker from the same free assignment group, but allowing capturing a locker from the other free assignment group.

IMPORTANT NOTE: A single locker cannot be included in both free assignment groups.

Free Closing:

The free closing option will allow a user or a group of users to close the locker without the need to present a key. The thumb turn stays closable every time it is opened. The keys will have to be configured as Static keys. In example, this configuration could be used for common lockers used by a few users for medicines or some components in a store.



Locker

Name: iLock 001

Description:

Open mode and periods

Open mode: Standard

Open time (sec): 2

Increased open time: 20

☑ Audit on keys

□ Is free assignment locker

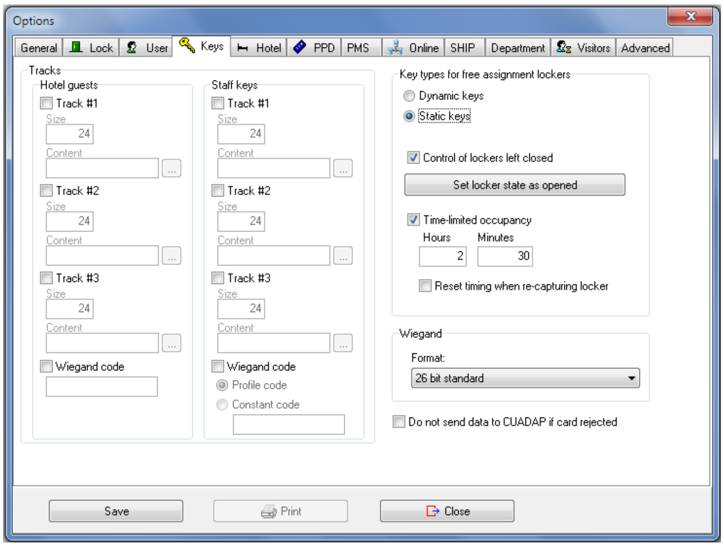
☑ Close locker without card

This locker belongs to...

Zones

Types of Keys:

If we go to the menu TOOLS/ CONFIGURATION/ GENERAL OPTIONS/ KEYS we will be able to select different types of keys that we want to use in this zone.



Tracks

Hotel guests

- □ Track #1 — Size: 24 — Content:
- □ Track #2 — Size: 24 — Content:
- □ Track #3 — Size: 24 — Content:
- □ Wiegand code

Staff keys

- □ Track #1 — Size: 24 — Content:
- □ Track #2 — Size: 24 — Content:
- □ Track #3 — Size: 24 — Content:
- □ Wiegand code
- ● Profile code
- ○ Constant code

Key types for free assignment lockers

- ○ Dynamic keys
- ● Static keys

☑ Control of lockers left closed

Set locker state as opened

☑ Time-limited occupancy — Hours: 2 — Minutes: 30

□ Reset timing when re-capturing locker

Wiegand — Format: 26 bit standard

□ Do not send data to CUADAP if card rejected

(Fig. 3)

- **Dynamic Keys:** This type of key allows users capture any Locker from a Free assignment Zone and after he has leave it empty can capture again another different one from the same Zone.

- **Static Keys:** In this case the user can firstly close any locker from the Free assignment zone. However, after he has empty it he can only capture the same one.

- **Set locker state as opened** this function is the same one as we can find in the "Locker List"

Time-limited Occupancy:

This option limits the occupancy of a locker. We have to fill the boxes and give the time in hours and Minutes.

Note: If this time expires ONLY a master key will be able to open the locker.

Reset timing when re-capturing locker: This option allows reset the timing of a Locker.

Lockers & Visitors:

In the menu: TOOLS/ CONFIGURATION/ GENERAL OPTIONS and in the Key tag there is a checkbox "Control of lockers left closed". This option will show if the Visitor has left the locker opened or closed (Not allowing other users use this locker) when we make the Visitors Checkout.

Locker Initialization:

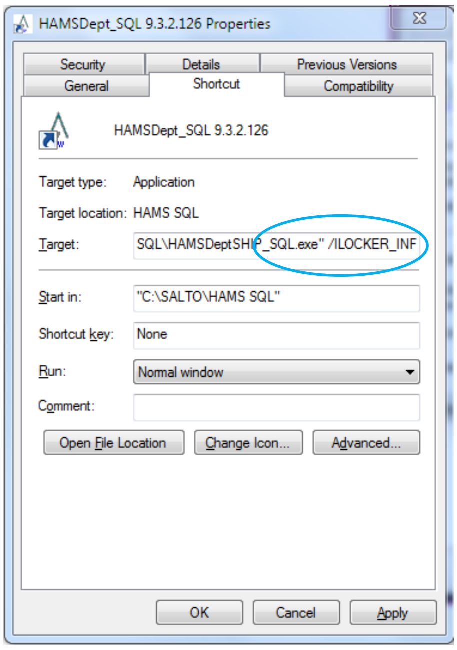
To initialize the Lockers we have to follow the normal procedure. We select the lockers that we want to initialize and load them to the ppd. Once we have initialized them we have to download again this information to the software.

Locker number information:

It exist the possibility to obtain information about which Locker has been captured by a user with the key.

In order to do so, it is necessary to have a dedicated PC with its own screen and a Salto key encoder.

In the Salto application shortcut properties, it is need to write after the default target "…exe" **/ILOCKER_INF** at the end of the line.



HAMSDept_SQL 9.3.2.126 Properties

HAMSDept_SQL 9.3.2.126

Target type: Application

Target location: HAMS SQL

Target: SQL\HAMSDeptSHIP_SQL.exe" /ILOCKER_INF

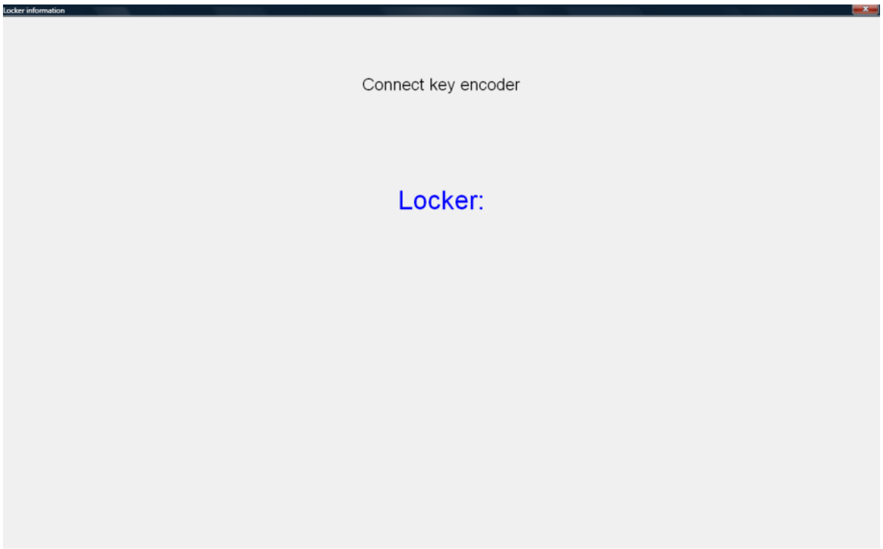
Start in: "C:\SALTO\HAMS SQL"

Shortcut key: None

Run: Normal window

Comment:

Then you will see a window as shown below, which indicate what Locker has been captured with the key just by showing the key to the encoder.



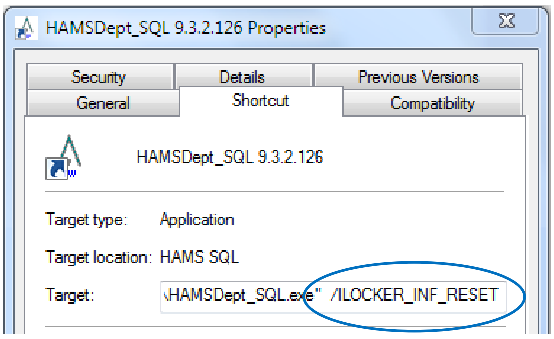
Locker information

Connect key encoder

Locker:

On the other hand, well as display the name of the locker, it is possible to reset the key counter in case that it is corrupted or cannot open the locker.

To do so, it is necessary to write the following text on the Salto software shortcut properties; "…exe" **/ILOCKER_INF_RESET** as shown below.



HAMSDept_SQL 9.3.2.126 Properties

HAMSDept_SQL 9.3.2.126

Target type: Application

Target location: HAMS SQL

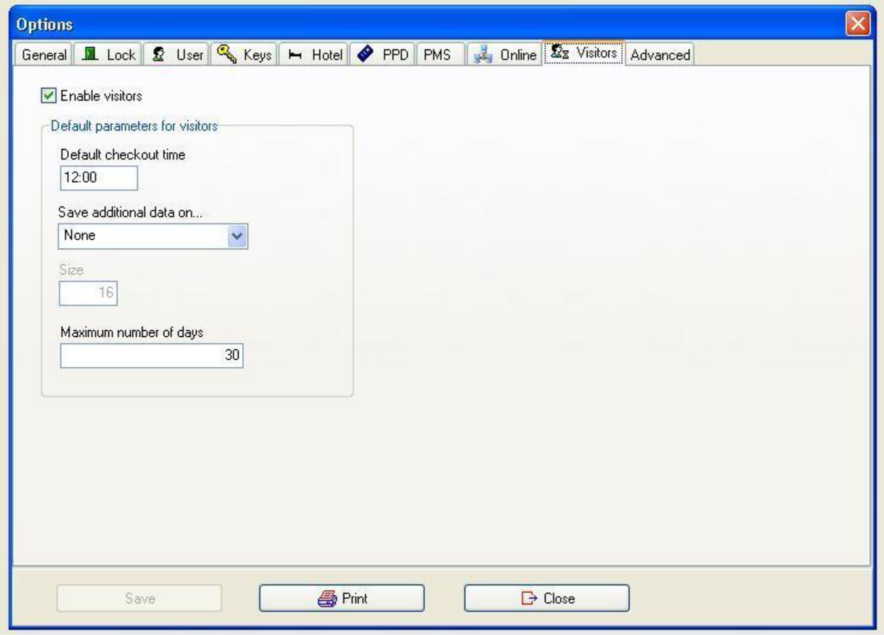
Target: \HAMSDept_SQL.exe" /ILOCKER_INF_RESET

After the reset, the user will be able to open his locker but also any other free locker.

WARNING; In case the user captures another locker, it won't be possible to capture again the locker captured before the reset. On the other hand, the user will only be able to read what locker is captured once, because after the reset, this information will disappear.

Visits:

The software allows as well Visitors managing, we define as Visitors, those people not included in our database and that are going to have temporal accesses to the system due to different reasons. In order to activate the Visitors features we have to go to: TOOLS/ CONFIGURATION/ GENERAL OPTIONS and then click on the **Visitors** tag. (Fig 1)



☑ Enable visitors

Default parameters for visitors

Default checkout time: 12:00

Save additional data on...: None

Size: 16

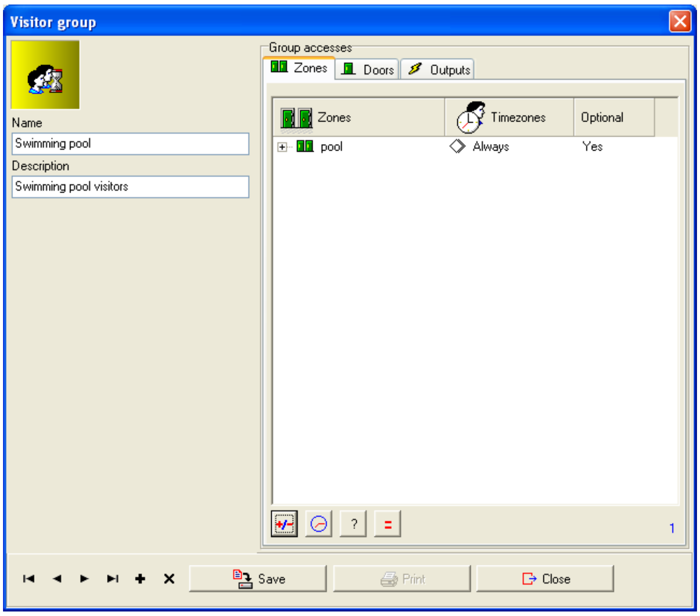
Maximum number of days: 30

(Fig 1)

We have to enable the checkbox "Enable Visitors". The next box will show us the default checkout time. This time can be modified when we make a visit check in. The second box enables the track (track 1, track2, track 3) if we want to write extra information in the card. In this case we have to determine the character size for this option. On the last box we can delimit the maximum number of days for each visit. That parameter will delimit the expiration date checking out the visit.

Once we have enabled Visitors, we have to define the Visitors profile. To do this we have to go the menu DATA and select VISITORS PROFILES. A Visitor Group List window will appear, we have to create a new group. The method is similar to create a new User access level, we have to define the accesses and timezones as well as if these accesses are optional. This is important as if we make them optional they will appear as such when we make a check in. (Fig. 2)

Please bear in mind that the maximum number of doors that could be assigned to a card will be 96 doors, but this does not limit the quantity of optional doors that could be assigned to the visitors group (there is no limit in that sense).



Name: Swimming pool

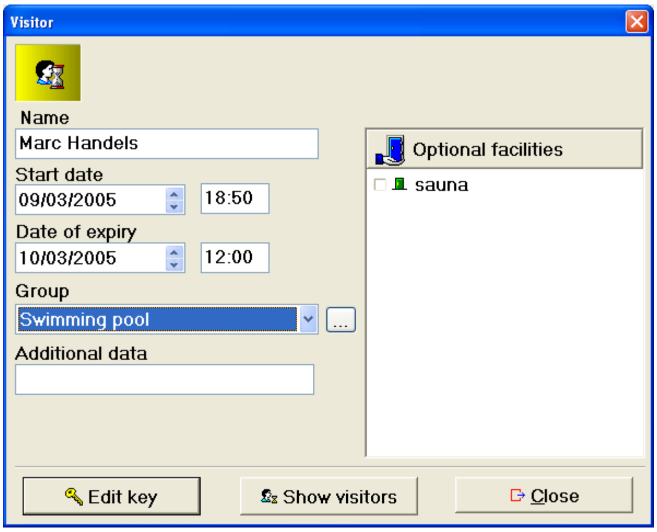
Description: Swimming pool visitors

Zones	Timezones	Optional
pool	Always	Yes

(Figure 2)

Vistors Checkin :

To make a Visitors checkin we have to go to the menu Keys and select « Visitors Checkin » or press F10. (Fig 3)



Name: Marc Handels

Start date: 09/03/2005 18:50

Date of expiry: 10/03/2005 12:00

Group: Swimming pool

Additional data:

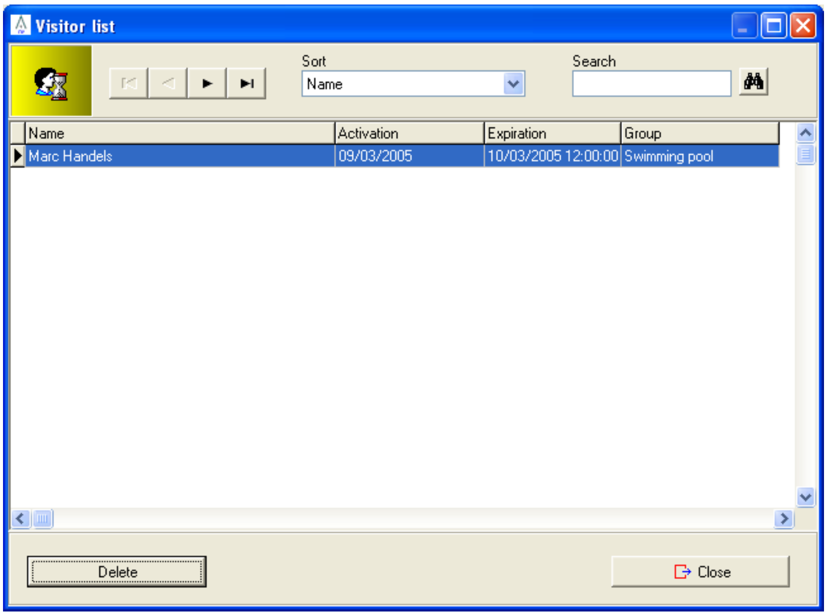
□ sauna

(Figure 3)

We have to fill the following fields:

- Name
- Start date and time
- Expiry date and time , the maximum date available will depend on the number written on the maximum number days on the visit general configuration.
- Access level
- Give any optional facility and Additional data
- Finally Edit the key.

In this window there is a button "Show Visitors". This option will allow us to see all active visits that we have (Fig. 4)



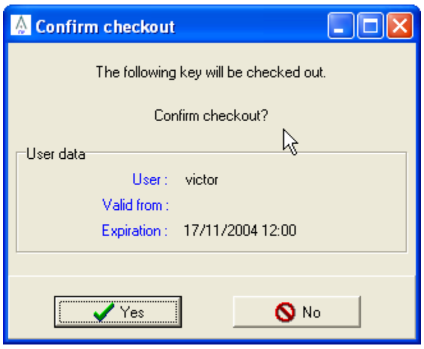
Sort: Name

Name	Activation	Expiration	Group
Marc Handels	09/03/2005	10/03/2005 12:00:00	Swimming pool

(Figura 4)

Checkout visitors:

To make a checkout we have to go to the menu Keys and press Visitors checkout or press F11.



The following key will be checked out.

Confirm checkout?

User data

User : victor

Valid from :

Expiration : 17/11/2004 12:00

Blacklist

The blacklist is a virtual list where are placed canceled user keys IDs. Once a key has been canceled, the ID is sent through our virtual network called SVN. Every online SVN wall reader will update the users’ keys with the blacklist information. At the same time all updated keys will update the offline escutcheons and wall readers, this way, the information concerning the canceled key will be spread by the keys containing the blacklist information.

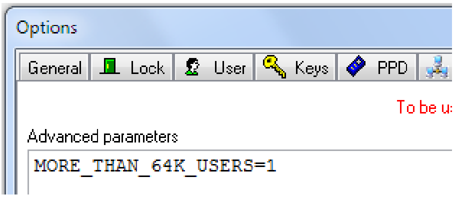
Blacklist Configuration

The software allows the creation of an unlimited quantity of users, 4 million user keys but only maximum of 64000 keys will be able to be cancelled through blacklist.

Once the blacklist arrives to its maximum, 64000 canceled keys, the blacklist won’t be sent through the SVN virtual network to the keys; this is why it is IMPORTANT to understand this concept in order to manage it the best way.

By default, all the users are sent to blacklist when canceled, therefore the software allows to select what users will be sent or not to the blacklist when canceled.

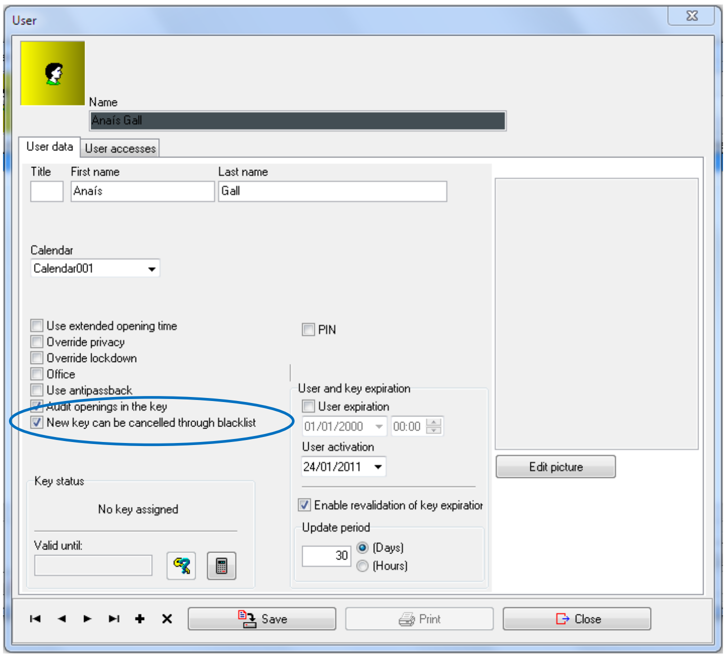
To do so, select the advanced parameter into the general options, advanced tab; MORE_THAN_64K_USERS=1, as shown on the image below;



Advanced parameters

```
MORE_THAN_64K_USERS=1
```

Once this parameter is saved, a new option will be shown on the user list to select what users can be canceled through blacklist.



User

Name: Anaís Gall

Title:
First name: Anaís
Last name: Gall

Calendar: Calendar001

□ Use extended opening time
□ Override privacy
□ Override lockdown
□ Office
□ Use antipassback
☑ Audit openings in the key
☑ New key can be cancelled through blacklist

□ PIN

User and key expiration
□ User expiration 01/01/2000 00:00
User activation 24/01/2011

Key status
No key assigned
Valid until:

☑ Enable revalidation of key expiratior
Update period
30 ● (Days) ○ (Hours)

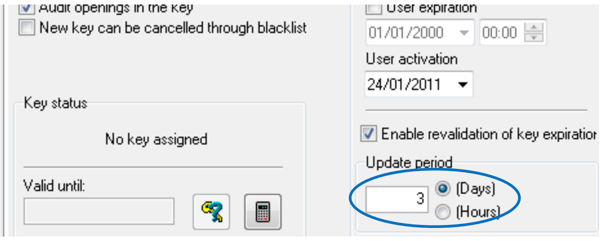
If the option is selected, a canceled user will be sent to blacklist and the information will be spread to all the units through SVN.

In case it is NOT selected, the canceled key won’t be sent to blacklist. It is important to know that in this case there is only 2 ways to invalidate this canceled key;

1/ the canceled key is presented to an SVN online wall reader. The wall reader will DELETE the key immediately; this will avoid the key to open any door, online as offline.

Therefore, the wall reader won’t update other users’ keys with the information of the blacklist for them to spread it.

2/ the key expire. For this reason, when un checking the “cancel key through blacklist” option, the revalidation period will have to be changed to a maximum of 7 days.



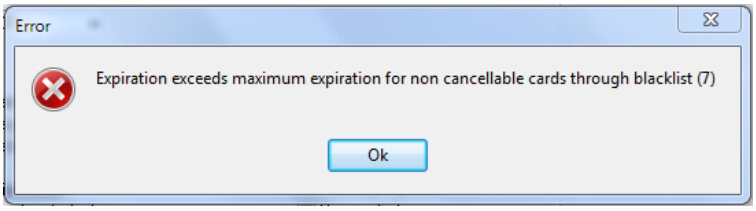
☑ Audit openings in the key
□ New key can be cancelled through blacklist

□ User expiration 01/01/2000 00:00
User activation 24/01/2011

Key status
No key assigned
Valid until:

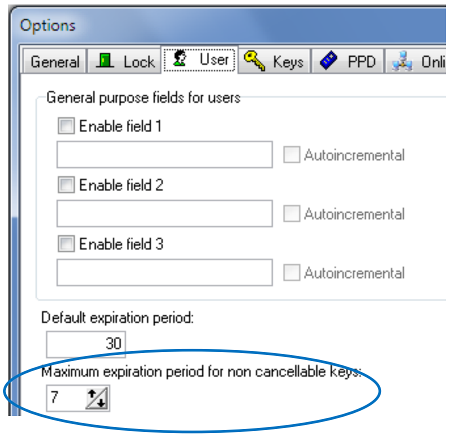
☑ Enable revalidation of key expiratior
Update period
3 ● (Days) ○ (Hours)

If the revalidation period is higher than the planned, by default 3 days, the following message will appear.



Expiration exceeds maximum expiration for non cancellable cards through blacklist (7)

In this case, the maximum expiration period allowed is 7 days, as shown below, therefore, by default it is configured to 3 days because of the fact that as lower is the period of expiration as higher will be the security, if the key expires as soon as possible.



General purpose fields for users

□ Enable field 1 □ Autoincremental

□ Enable field 2 □ Autoincremental

□ Enable field 3 □ Autoincremental

Default expiration period: 30

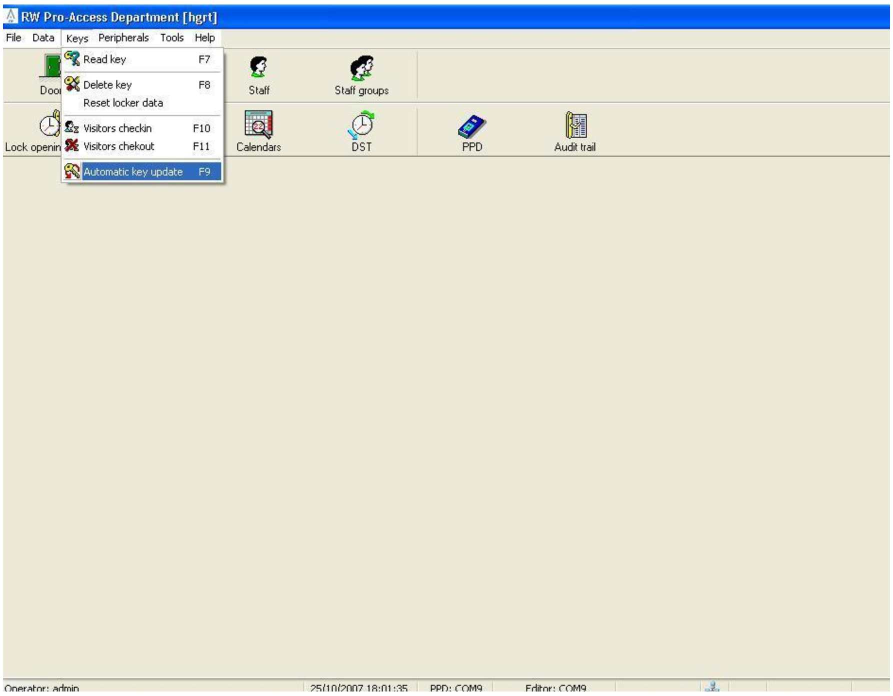
Maximum expiration period for non cancellable keys: 7

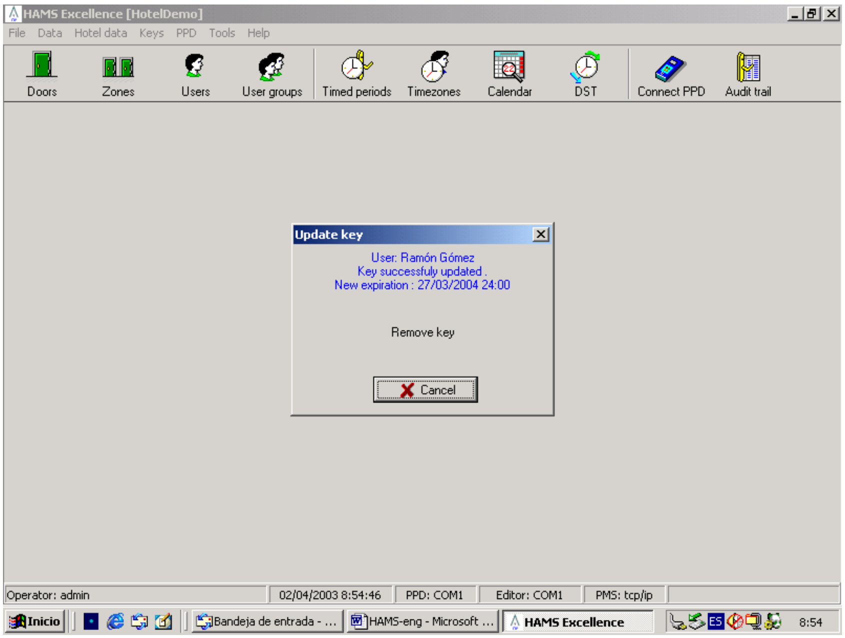
Automatic key up date

There is an option in the KEYS menu, called AUTOMATIC KEY UP DATE, which allows you to update the user cards without needing to go to the user list and select the required user.

This function leaves the encoder in the requesting key status, and it will automatically update user access profiles, (new and eliminated user cards), on every user card inserted. It does not matter in which order the user cards are inserted. The expiration date given to these cards will be the same for all users, and it is the value stated at TOOLS/OPTIONS/USER, in days.

This function allows the system administrator to make the changes in the user profiles, without needing to manually up date the cards one by one.





User: Ramón Gómez
Key successfuly updated .
New expiration : 27/03/2004 24:00

Remove key

Using PPD. Initialization

The PPD is a Portable Programming Device used to communicate with the locks and transfer data from the PC on the locking schedule we have designed. Should you have any doubts on this device usage, please, refer to the PPD Smart User´s Manual that you will find included in the RW software CD-ROM.

Main menu:

Below, you can review a diagram of PPD menu options. It is important to note that all these options will not always be present, depending on their being enabled or not from the management computer. As default value, DIAGNOSTIC and COLLECT OPENINGS options will be present, although we have not enabled them on the computer.

Initializing doors:

When we have our locking schedule finished on our computer, we must transfer all the data from our computer to the portable programming device.

We will initialize every door granting it a name that will be definitive from now onwards.

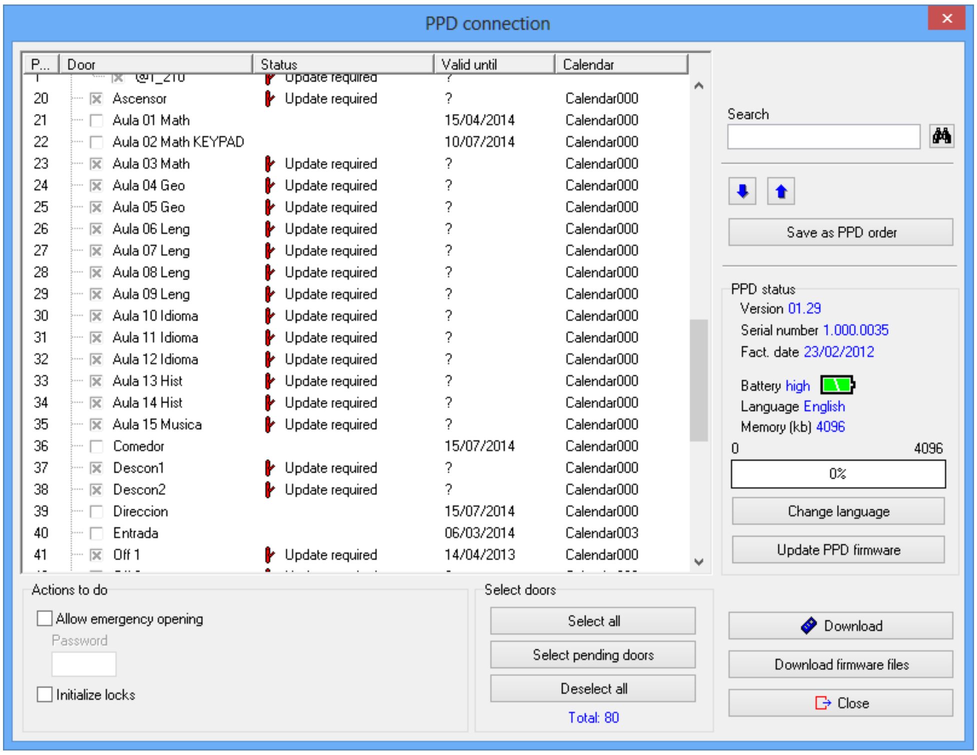
Ensure that your computer clock time (on the PC that you are running the SALTO Software) is correctly adjusted to show the correct time, as it will determine the time on which the electronic locks operation will be based.

- To download all our locking schedule data on the portable programming device, connect the device to our computer by means of a serial cable, and go to program main menu. Click on the *PPD* icon*.*

- If it is the first time you use the PPD to download a locking schedule, you may be prompted with an error message window. Click on the *YES* button to confirm that, from now on, your PPD will be exclusively devoted to your installation.

- A window like the one below will be displayed. In this window we see all doors pending initialization are selected.

- It is not compulsory to initialize all of them simultaneously, though it is highly recommended not to leave any pending door.



PPD connection

P...	Door	Status	Valid until	Calendar
1	☒ @I_210	Update required	?	
20	☒ Ascensor	Update required	?	Calendar000
21	□ Aula 01 Math		15/04/2014	Calendar000
22	□ Aula 02 Math KEYPAD		10/07/2014	Calendar000
23	☒ Aula 03 Math	Update required	?	Calendar000
24	☒ Aula 04 Geo	Update required	?	Calendar000
25	☒ Aula 05 Geo	Update required	?	Calendar000
26	☒ Aula 06 Leng	Update required	?	Calendar000
27	☒ Aula 07 Leng	Update required	?	Calendar000
28	☒ Aula 08 Leng	Update required	?	Calendar000
29	☒ Aula 09 Leng	Update required	?	Calendar000
30	☒ Aula 10 Idioma	Update required	?	Calendar000
31	☒ Aula 11 Idioma	Update required	?	Calendar000
32	☒ Aula 12 Idioma	Update required	?	Calendar000
33	☒ Aula 13 Hist	Update required	?	Calendar000
34	☒ Aula 14 Hist	Update required	?	Calendar000
35	☒ Aula 15 Musica	Update required	?	Calendar000
36	□ Comedor		15/07/2014	Calendar000
37	☒ Descon1	Update required	?	Calendar000
38	☒ Descon2	Update required	?	Calendar000
39	□ Direccion		15/07/2014	Calendar000
40	□ Entrada		06/03/2014	Calendar003
41	☒ Off 1	Update required	14/04/2013	Calendar000

Actions to do
□ Allow emergency opening
Password
□ Initialize locks

Select doors
Total: 80

PPD status
Version 01.29
Serial number 1.000.0035
Fact. date 23/02/2012
Battery high
Language English
Memory (kb) 4096
0 4096
0%

Figure 63

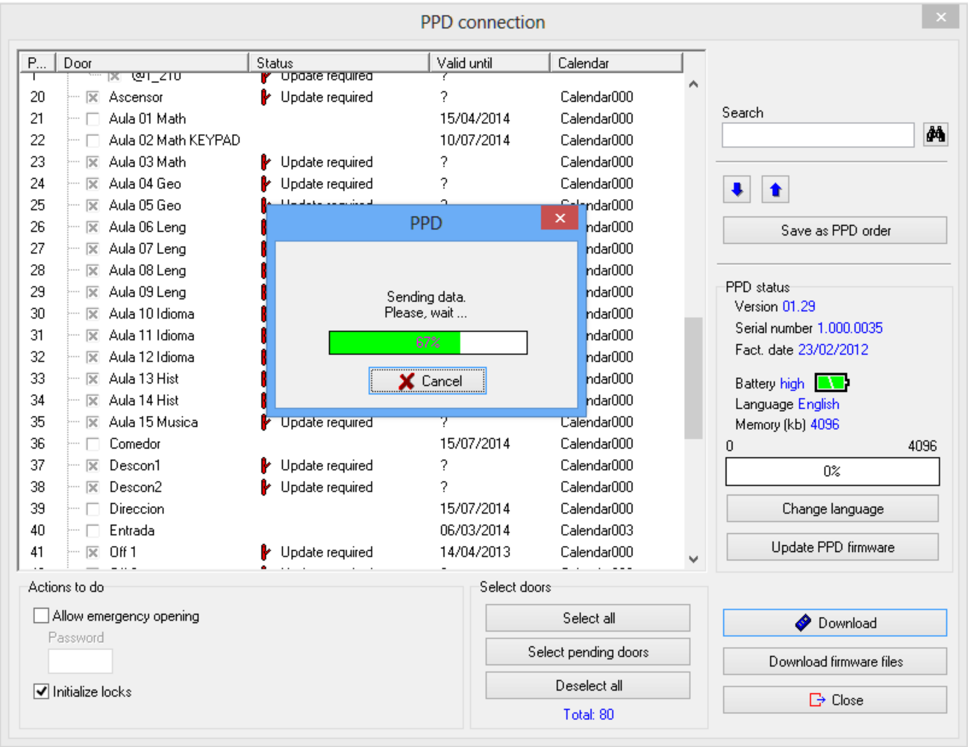
On the lower left-hand side corner we find a box called *ACTIONS TO DO.* In this box we will tick off those actions to be done with PPD.

1. If we tick off *ALLOW EMERGENCY OPENING*, this option will later be shown on the PPD menu.

2. **If we tick off *INITIALIZE LOCKS*, this option will later be shown on the PPD menu. We will now perform this action.**

To tick off these two possible options, bear in mind that it is not enough to tick off the action to do, but also to mark with a cross the door or doors on which you want to do the action.

- If we do not tick off any of these two options, the only option available in the PPD will be: Update locks.
- We can change the language of PPD display messages. In order to do that, click on the *CHANGE LANGUAGE* option*.*
- When we get all doors arranged in order, click on the DOWN*LOAD TO PPD* option*.*
- Data transfer from computer to PPD will last a few seconds. Watch the computer screen and when you see the progress bar of the active window reaches 100%, you will know the transfer is over.



PPD connection

P...	Door	Status	Valid until	Calendar
20	☒ Ascensor	Update required	?	Calendar000
21	□ Aula 01 Math		15/04/2014	Calendar000
22	□ Aula 02 Math KEYPAD		10/07/2014	Calendar000
23	☒ Aula 03 Math	Update required	?	Calendar000
24	☒ Aula 04 Geo	Update required	?	Calendar000
25	☒ Aula 05 Geo			Calendar000
26	☒ Aula 06 Leng			ndar000
27	☒ Aula 07 Leng			ndar000
28	☒ Aula 08 Leng			ndar000
29	☒ Aula 09 Leng			ndar000
30	☒ Aula 10 Idioma			ndar000
31	☒ Aula 11 Idioma			ndar000
32	☒ Aula 12 Idioma			ndar000
33	☒ Aula 13 Hist			ndar000
34	☒ Aula 14 Hist			ndar000
35	☒ Aula 15 Musica	Update required	?	Calendar000
36	□ Comedor		15/07/2014	Calendar000
37	☒ Descon1	Update required	?	Calendar000
38	☒ Descon2	Update required	?	Calendar000
39	□ Direccion		15/07/2014	Calendar000
40	□ Entrada		06/03/2014	Calendar003
41	☒ Off 1	Update required	14/04/2013	Calendar000

PPD

Sending data.
Please, wait ...

67%

Cancel

Search

Save as PPD order

PPD status
Version 01.29
Serial number 1.000.0035
Fact. date 23/02/2012

Battery high
Language English
Memory (kb) 4096

0 4096

0%

Change language

Update PPD firmware

Actions to do

□ Allow emergency opening
Password

☑ Initialize locks

Select doors

Select all

Select pending doors

Deselect all

Total: 80

Download

Download firmware files

Close

Figure 64

- Now you can disconnect serial cable, and go to every door to initialize them.

- Connect to the PPD the cable connected to a special card with 3 conductors (on the opposite end you will have a RJ11 phone connector).

- Approach to the first door of your system, plug in the special cable and turn the PPD on.

- From the main menu window, select *INITIALIZE* option. You will get the door list. Now choose the door that you want to initialize. Be especially careful when performing this step, since the door name is limited.

- When you view on screen the name of the door to be initialized, click on the OK button of the PPD, and the device will request that you connect it to the lock.

- You will get on the PPD screen a *CONNECT TO LOCK* message*.* Insert in the lock reader the card cable and watch the PPD screen. You will get a progress bar and a sharp beep sound emitted, that means that data transfer is in progress.

- If, by mistake, this communication is interrupted for longer than three seconds, you will have to repeat the communication.

- Repeat these steps with every door within your facilities. Take into account that door names will not disappear from the door list contained in the INITIALIZE option, by having simply initialized a door. This will allow you to reinitialize a door if you have given it a wrong name.

- When you have completed the initialization process, reconnect the PPD to your computer through the serial cable, and click on CONNECT PPD icon. This will update software data comparing it with actual battery status values, as well as pending updates. At this point, INITIALIZE LOCKS menu option will not appear on your PPD main menu.

7. Advanced options

In this section some features will be described which, on some occasions are not essential, but they prove to be very important to designing the locking schedule.

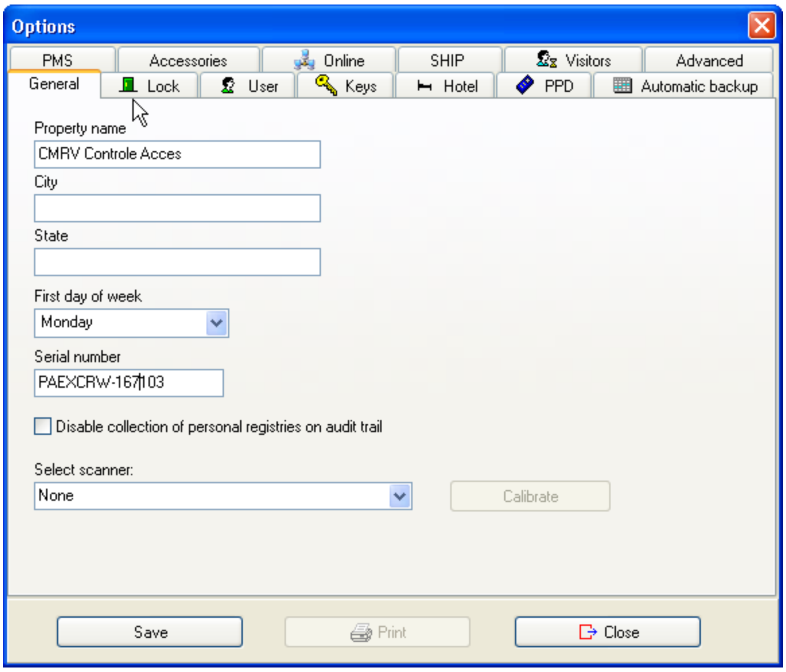
General info

Go to the *TOOLS pop-up* menu and click on *GENERAL OPTIONS* option*.*

- The first tag we obtain, displays in the PROPERTY NAME. This is the name we gave to the data base at the start.

- We will also have more boxes, CITY and STATE/COUNTRY. Please, fill in these fields according to your facilities address.

- It is also important to fill in the FIRST DAY OF THE WEEK field, since this piece of information has an effect on calendar structure.



Property name
CMRV Controle Acces

City

State

First day of week
Monday

Serial number
PAEXCRW-167103

□ Disable collection of personal registries on audit trail

Select scanner:
None

Figure 65

- The serial number field shows the serial number of the software which was written when creating the data base for the first time.

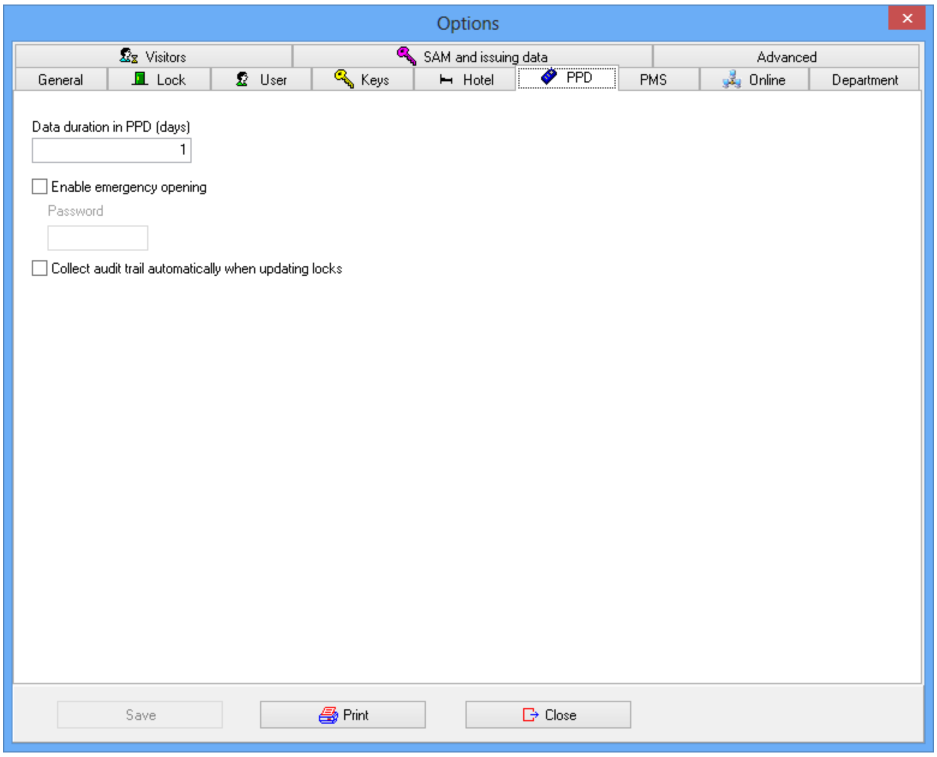
- The check box DISABLE COLLECTION OF PERSONAL REGISTERS ON AUDIT TRAIL can be marked if we want to filter the information kept in the audit trail , so software operators can only view the events regarding lock updates or key updates (not openings or rejections).

- The print option can be used to obtain a hardcopy report from all the tags in OPTIONS. It is better to use this option when the data base is completely desiged, so we can see all of the fields filled out in these tags.

- Save changes before proceeding to the following tags.

PPD status

Go to the *TOOLS* pull up menu and click on the *GENERAL OPTIONS* option*.* On this occasion, we will choose the PPD tag.



Data duration in PPD (days)
1

□ Enable emergency opening

Password

□ Collect audit trail automatically when updating locks

Figure 66

- The first field refers to the length of time the downloaded data will reside in the PPDs memory. As a default value, the system sets a day, though you are allowed to increase this duration. Below, you view two optional fields, that can be selected if you want to customize the PPD default set up.

- If you tick the ENABLE EMERGENCY OPENING option, it will also be present on PPD main menu, even after data expiration.

NOTE: be careful with this option, since if you enable permanently the emergency opening option, the PPD turns into a master key that opens all your facilities doors, and could be misused if in the possession of an unauthorized person.

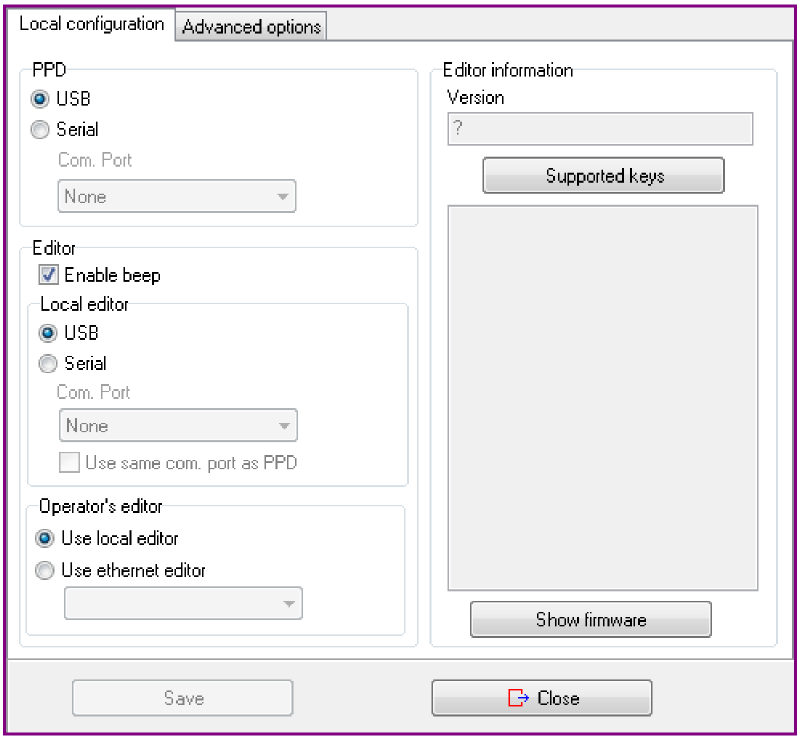
- If you tick COLLECT AUDIT TRAIL AUTOMATICALLY WHEN UPDATING LOCKS, the PPD will also collect the audit trails of every door, each time you update that door.

- The box COMMUNICATION PORT allows you to set which serial port you are using in the computer to communicate with the PPD.

- SALTO PA software allows you to use different com. Ports for the PPD and the encoder. You can select between using the same com. Port for both or a different com. Port for each one. The encoder com. Port is set in the EDITOR tag.

Local Options

By selecting the LOCAL OPTIONS, located in the TOOL menu, a window like the following will appear:



PPD
● USB
○ Serial
Com. Port
None

Editor
☑ Enable beep
Local editor
● USB
○ Serial
Com. Port
None
□ Use same com. port as PPD

Operator's editor
● Use local editor
○ Use ethernet editor

Editor information
Version
?

Picture 67

You can select to communicate with the PPD through a **USB** port. The drivers will installed by installing the Software and any other configuration will be necessary.

On COM PORT field, you can select the PC’s port through which you want to communicate with the PPD.

It is also possible to use a SERIAL port to communicate with your encoder and a different one for the PPD. By the same way, you can also use a USB port to communicate your USB encoder.

Encoder status

From the TOOLS/ LOCAL OPTIONS pop-up menu, choose EDITOR tag. A window like Picture 67 will display:

- In this window, you will view the version number of the card editor, when it is connected to your computer serial port.

- In this window, you will view the version number of the card editor, when it is connected to your computer serial port.

- This also shows the card types that are compatible with the editor if you click on the CARDS SUPPORTED button.

- The ENABLE BEEP check box can be ticked, if you want the editor to make a noise.

- The check box SAME COM. PORT AS PPD is used to say whether we are going to use the same com. port for the PPD and encoder or whether we are going to use different com. Ports. To work with multiple com. Ports, it is necessary to have at least 2 serial com. Ports available in the computer.

- It is important to fully understand the following two key concepts to avoid confusion: the 'local serial encoder' and the 'operator's encoder'. The 'operator's encoder' refers to the actual encoder to be used by any SALTO operator that logs on locally in the SALTO software. It may be any encoder that has been setup within the system, be it serial or Ethernet. If you select Ethernet as the type of encoder, you must also choose one among all the available Ethernet encoders.

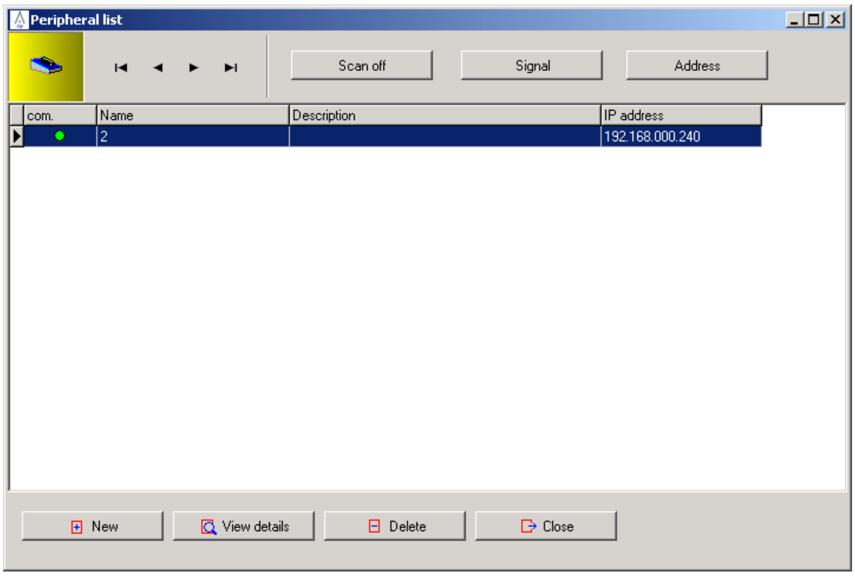
- On the other hand, the 'local serial encoder' refers to the actual encoder connected to the machine through a serial port (or USB-to-serial adaptor). This encoder may be used by the SALTO PMS server or the SALTO SHIP server when requested to issue keys in the local encoder. Likewise, this local encoder may also be used by any SALTO operator logged on provided that the 'operator's encoder' parameter has been set to use the 'local serial encoder'.

Configuration of Ethernet encoders

To configure Ethernet encoders, the peripheral list window must be opened (*tools/peripheral list*). This window contains a list of all the peripherals set up for the installation.

Two fundamental parameters are required for each encoder: an identity number and an IP address. For the ID number, it is advisable to start from #2 since number one (#1) is normally assigned to the local serial encoder. As for the IP address, you need to obtain them from the administrator of the network. You need to make sure that the IP address is a valid one that is not already in use by any other device. IP address conflicts may lead to communication problems.

Ethernet encoder configuration can be carried out by opening the *Peripheral List* window (*Tools/Peripheral list*) as shown in the following picture;



com.	Name	Description	IP address
●	2		192.168.000.240

As usual, the buttons at the bottom of the window can be used for adding, removing and editing peripheral parameters.

On the top of the window, the following buttons can be found:

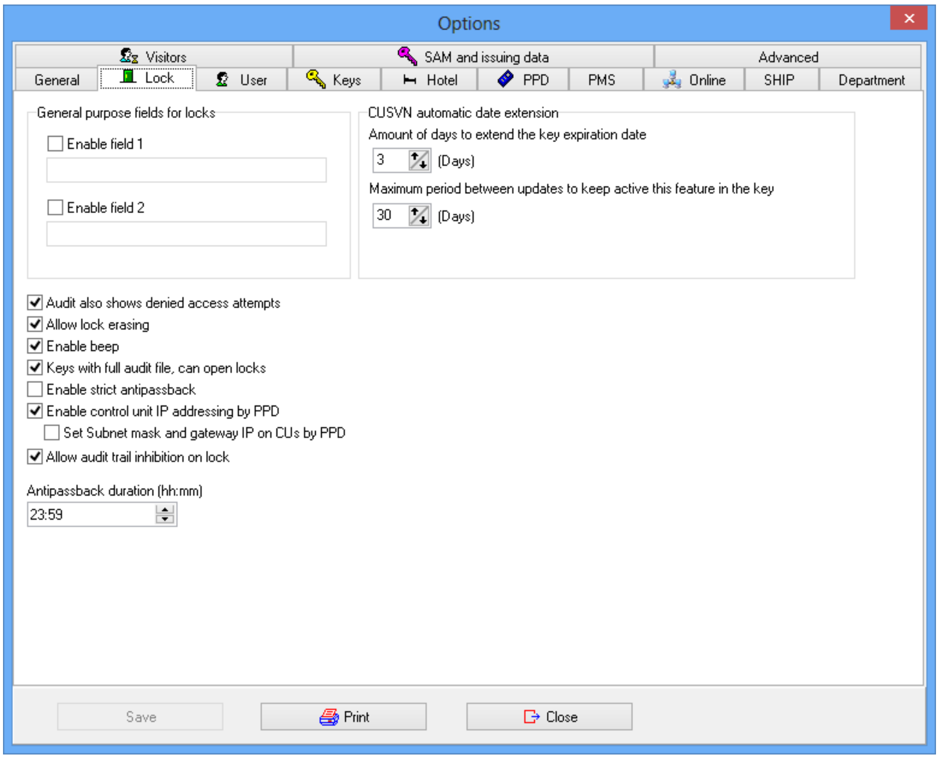
- **SCAN ON/OFF:** when clicking this button, the application will check whether all peripherals in the list are connected to the machine: a green icon indicates that the corresponding peripheral is communicating whereas a red icon represents no communication.

- **SIGNAL:** this function is provided for making the LED of a particular peripheral blink and beep for a while. In this way, we can identify the location of the peripheral as well as whether the communication is OK.

- **ADDRESS:** this function is used for giving a new IP address to a peripheral. Firstly, we must press the button on the back of the encoder so that the green led starts blinking. Then, we must select a peripheral from the list and click the 'ADDRESS' button. If no error message is shown, then it is assumed that the peripheral contains the new IP address. Use 'SIGNAL' or 'SCAN ON/OFF' to check communication.

Lock status.

In this window we will specify some operating features of the electronic locks.



General purpose fields for locks

☐ Enable field 1

☐ Enable field 2

CUSVN automatic date extension

Amount of days to extend the key expiration date: 3 (Days)

Maximum period between updates to keep active this feature in the key: 30 (Days)

☑ Audit also shows denied access attempts
☑ Allow lock erasing
☑ Enable beep
☑ Keys with full audit file, can open locks
☐ Enable strict antipassback
☑ Enable control unit IP addressing by PPD
☐ Set Subnet mask and gateway IP on CUs by PPD
☑ Allow audit trail inhibition on lock

Antipassback duration (hh:mm): 23:59

- You can activate the AUDIT ALSO SHOWS DENIED ACCESS ATTEMPTS check box if you want the Audit Trail to show failed door access attempts.

- ALLOW LOCK ERASING: if you enable this option, it is possible to reset any of the locks in the system. We do not recommend this option is enabled for security reasons (unless you are certain that the electronic locks may be used in more than just one locking schedule). This option can always be changed at a later date.

- **Note:** if, at a given point, you want to enable erasing of a particular lock, you will have to initialize the lock you want to reset. Updating would not be enough.

- You can tick the ENABLE BEEP check box if you want the electronic locks to beep on operation.

- The check box KEYS WITH FULL AUDIT TRAIL CAN OPEN LOCKS comes enabled by default. We can disable it if we want to make the user notice that his personal audit trail on key is full.

- ENABLE STRICT ANTI-PASS BACK

- CU IP ADDRESSING BY PPD. By checking this option, the PPD will assign the IP address to the CU during the initialization. This option is very useful when the CU is part of a network with a different range from the one where the peripheral manager is located.

- ALLOW INHIBITION OF AUDIT TRAIL will only add a new option on the door list. Enabling this option, in the door list, will avoid the creation of the audit trail on that specific lock's memory, meaning that no audit trail will be collectable even using the PPD.

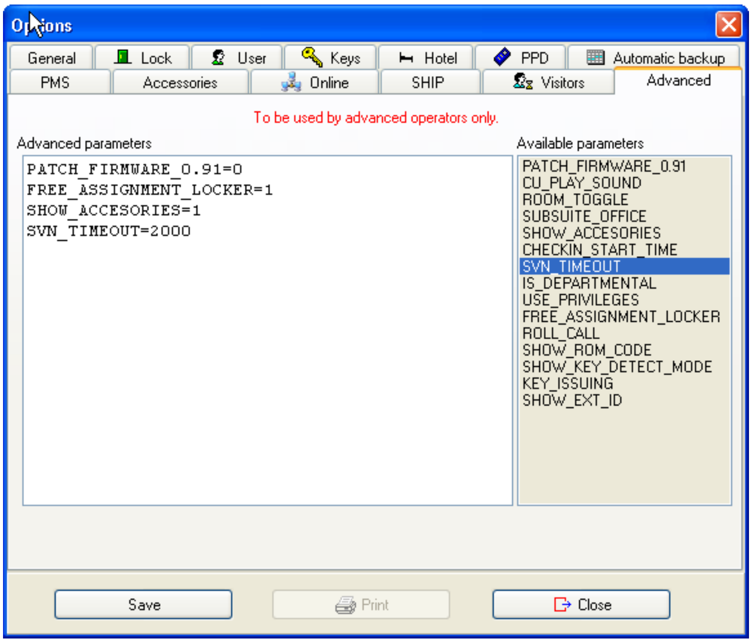
- CUSVN AUTOMATIC DATE EXTENSION. This feature regulates the operation of a SVN reader when, for some reason, it is working off-line. This way, the updater will continue revalidating cards following the parameters below:

- Days to increment: number of days to revalidate.
- Valid refresh interval: maximum revalidation delay (in days) since last on-line update.

- If this field shows the value 00:00, then the anti-pass back time is unlimited, therefore the user has to go out by the exit in order to be able to enter again by the entrance.

Advanced parameters

This window is for future development. It will allow program features to be modified by the administrator. For instance, maximum number of doors which can be defined etc



To be used by advanced operators only.

Advanced parameters

```
PATCH_FIRMWARE_0.91=0
FREE_ASSIGNMENT_LOCKER=1
SHOW_ACCESORIES=1
SVN_TIMEOUT=2000
```

Available parameters

PATCH_FIRMWARE_0.91
CU_PLAY_SOUND
ROOM_TOGGLE
SUBSUITE_OFFICE
SHOW_ACCESORIES
CHECKIN_START_TIME
SVN_TIMEOUT
IS_DEPARTMENTAL
USE_PRIVILEGES
FREE_ASSIGNMENT_LOCKER
ROLL_CALL
SHOW_ROM_CODE
SHOW_KEY_DETECT_MODE
KEY_ISSUING
SHOW_EXT_ID

It is necessary to double click the text SHOW ACCESSORIES when designing the data base for the first time if you want the ACCESSORIES tag to appear among the OPTIONS tags. If safes and energy saving devices are not going to be used in the hotel, then this step is not necessary.

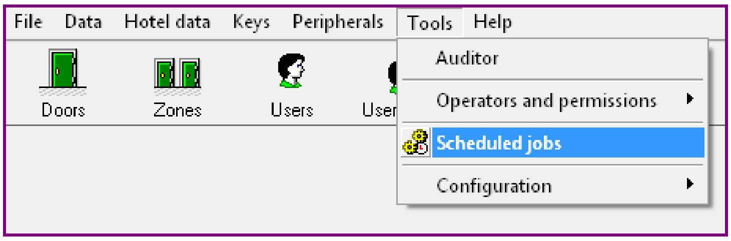
If you have acquired the locks after May 2002, we recommend to set PATCH FIRMWARE = 0 in order to improve the system performance.

- CHECK-IN START TIME: by double clicking this sentence, it will be possible to state the start time for a guest (a time different from the edition time). This can be interesting when we do not want the guest card working until 20:00, for example.

- SVN TIMEOUT: by double clicking this sentence, it is possible to define the time since a key is presented to the SVN control unit until the control unit receives the information from the master computer, to update that key. This time is expressed in milliseconds. This is useful for environments having long delays (slow stations, narrow bandwidth network), anyway the majority of systems will work OK with the standard timeout delay, 2000 milliseconds. If the network is very slow, a good value would be 4000 or 6000 milliseconds.

Automatic Purge

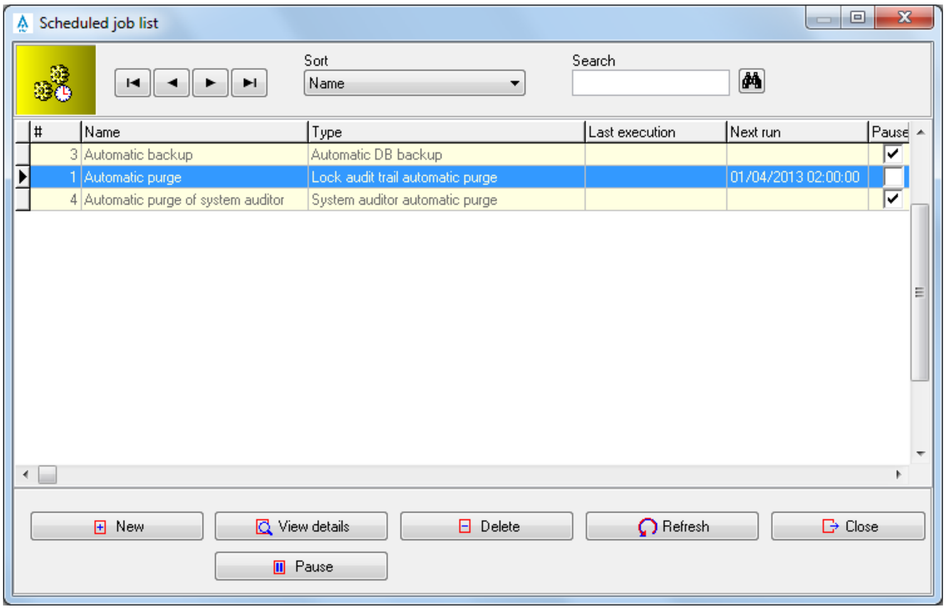
With the option shown below it is possible to have a programmed automatic purge for the audit trail or the system auditor.



The purged events will be saved to a TXT file for further consultation.

As shown in the next pictures, there are a few options to take into account like, amount of events, % of events to purge, frequency and location.

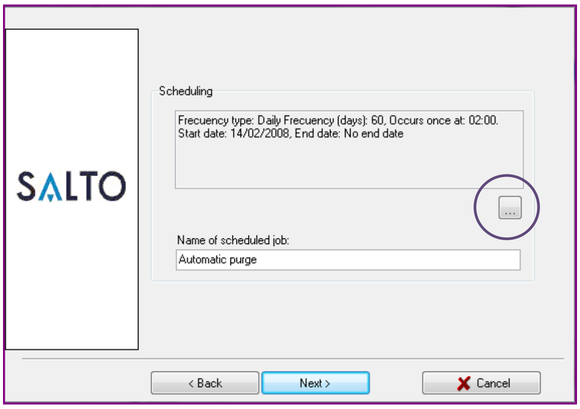
The next window shows the pre-defined purge lines to be edited.



Sort: Name

#	Name	Type	Last execution	Next run	Pause
3	Automatic backup	Automatic DB backup			☑
1	Automatic purge	Lock audit trail automatic purge		01/04/2013 02:00:00	□
4	Automatic purge of system auditor	System auditor automatic purge			☑

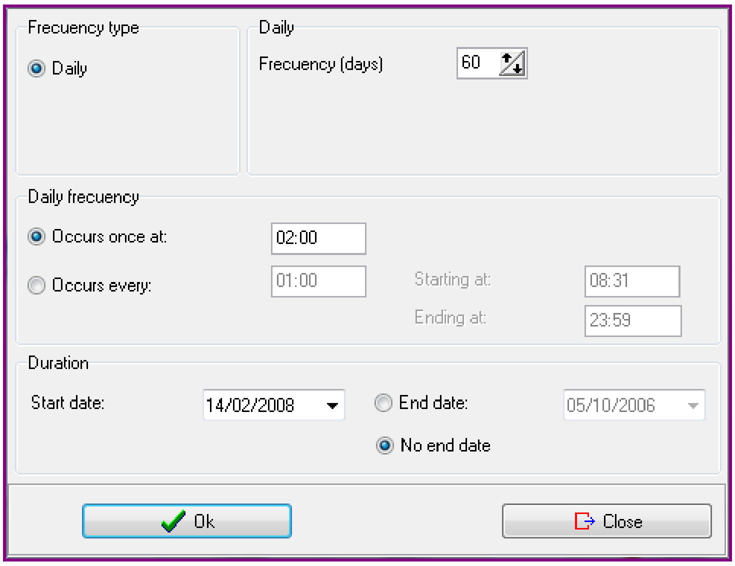
Doble clic on the “Automatic purge” or “Automatic purge of system auditor” row.



Frecuency type: Daily Frecuency (days): 60, Occurs once at: 02:00.
Start date: 14/02/2008, End date: No end date

Name of scheduled job: Automatic purge

The next window shows the frequency base.



Frecuency type

● Daily

Daily

Frecuency (days) 60

Daily frecuency

● Occurs once at: 02:00

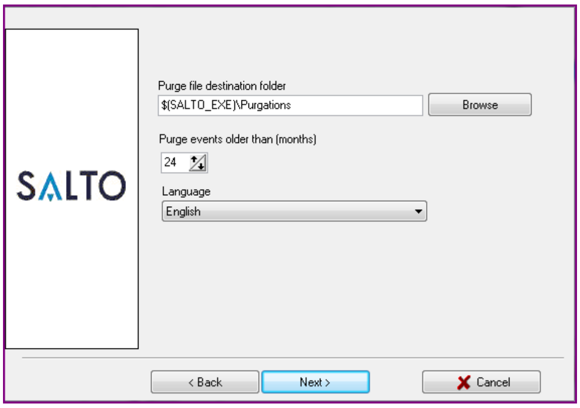
○ Occurs every: 01:00 Starting at: 08:31

Ending at: 23:59

Duration

Start date: 14/02/2008 ○ End date: 05/10/2006

● No end date



Purge file destination folder

$(SALTO_EXE)\Purgations

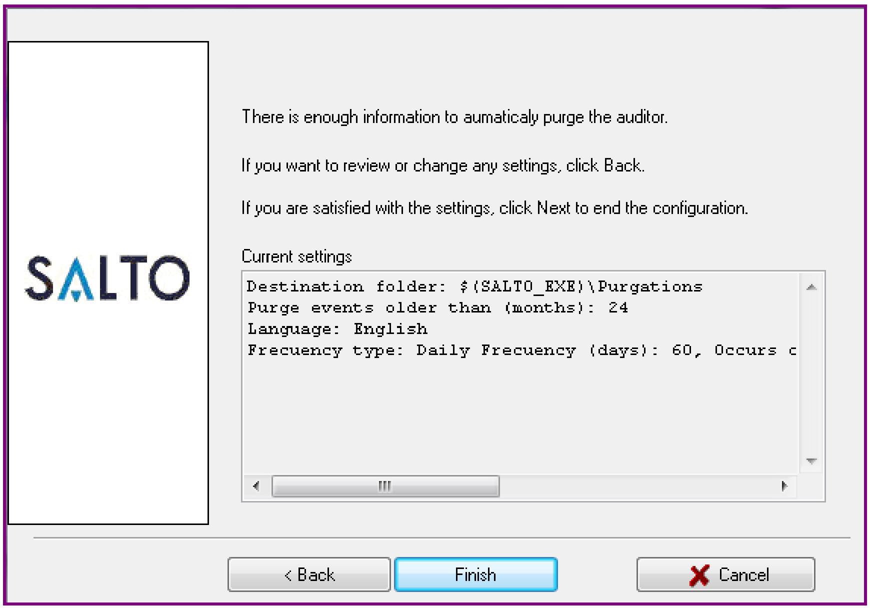
Purge events older than (months)

24

Language

English

Press on “Next”.



There is enough information to aumaticaly purge the auditor.

If you want to review or change any settings, click Back.

If you are satisfied with the settings, click Next to end the configuration.

Current settings

```
Destination folder: $(SALTO_EXE)\Purgations
Purge events older than (months): 24
Language: English
Frecuency type: Daily Frecuency (days): 60, Occurs c
```

IMPORTANT!
The “Automatic purge of system auditor” is available only in the SERVICE software.

User

The GENERAL PURPOSE FIELD FOR USERS can be enabled if we want an additional field to appear in the user detail window. This field can be used to insert some special information or number, for example, the passport number.

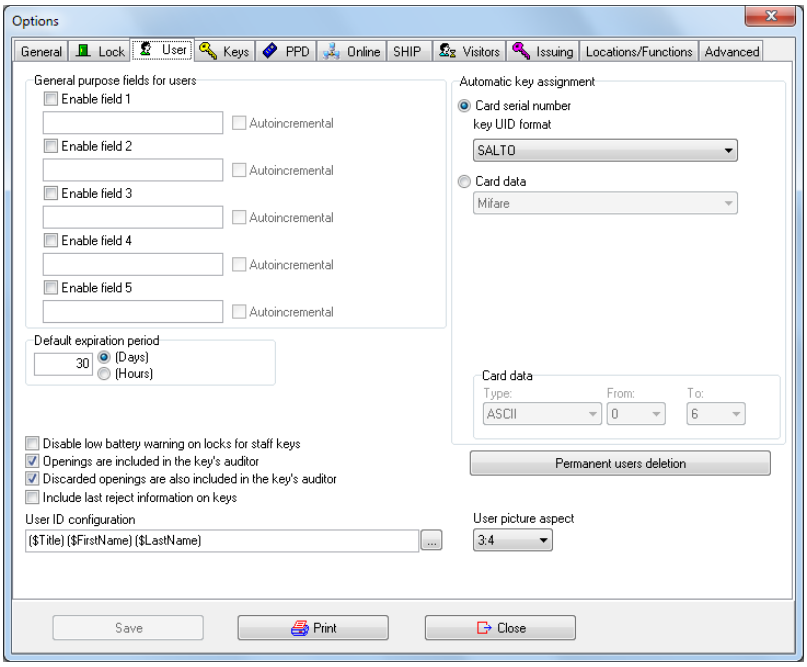
The check box AUTOINCREMENTAL should be marked if we want the number to increase automatically when creating a new user.

- The DEFAULT EXPIRATION PERIOD is the expiration time given to the users, by default, in the user detail window. This time is shown in days.

- The check box DISABLE LOW BATTERY WARNING TO THE USER can be marked if we want the locks not to give this acoustic warning , because we can be informed about this through the “on key” audit trail.

- The check box REJECTED OPENINGS ARE ALSO INCLUDED IN THE KEY´S AUDITOR. Can be used to obtain an “on key audit trail”, but not only for the door openings but also the denied access attempts.

- The check box INCLUDE LAST REJECT INFORMATION ON KEYS can be enabled if we want to know why a given key cannot open a door. You can read the last reject information by reading the key and clicking the CONTENT button.
  It is possible to select if the successful opening of lock is to be included or not in the key audit trail as well as discarded openings. This function is enabled by default.
  To enable or disable this function go to **TOOLS / CONFIGURATION / GENERAL OPTIONS / USER TAB**



Options

General purpose fields for users

- □ Enable field 1 — □ Autoincremental
- □ Enable field 2 — □ Autoincremental
- □ Enable field 3 — □ Autoincremental
- □ Enable field 4 — □ Autoincremental
- □ Enable field 5 — □ Autoincremental

Default expiration period: 30 ● (Days) ○ (Hours)

- □ Disable low battery warning on locks for staff keys
- ☑ Openings are included in the key's auditor
- ☑ Discarded openings are also included in the key's auditor
- □ Include last reject information on keys

User ID configuration: ($Title) ($FirstName) ($LastName)

Automatic key assignment

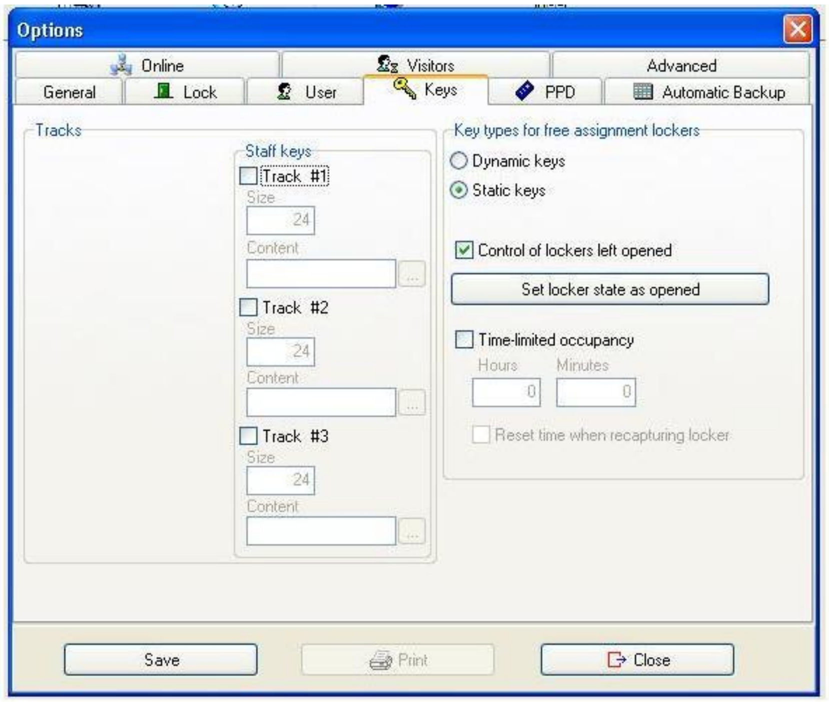
- ● Card serial number — key UID format: SALTO
- ○ Card data — Mifare

Card data — Type: ASCII, From: 0, To: 6

User picture aspect: 3:4

Writing extra info on track 1, 2 or 3 for staff keys

To enable the space to write on the tracks first of all we have to go to the menu: TOOLS/ CONFIGURATIONS/ GENERAL OPTIONS and in the key tag we will see the checkboxes to enable the tracks where we want to write in and the character size that we want to assign. (Fig 1)



Options

Tracks

Staff keys

- □ Track #1 — Size: 24 — Content:
- □ Track #2 — Size: 24 — Content:
- □ Track #3 — Size: 24 — Content:

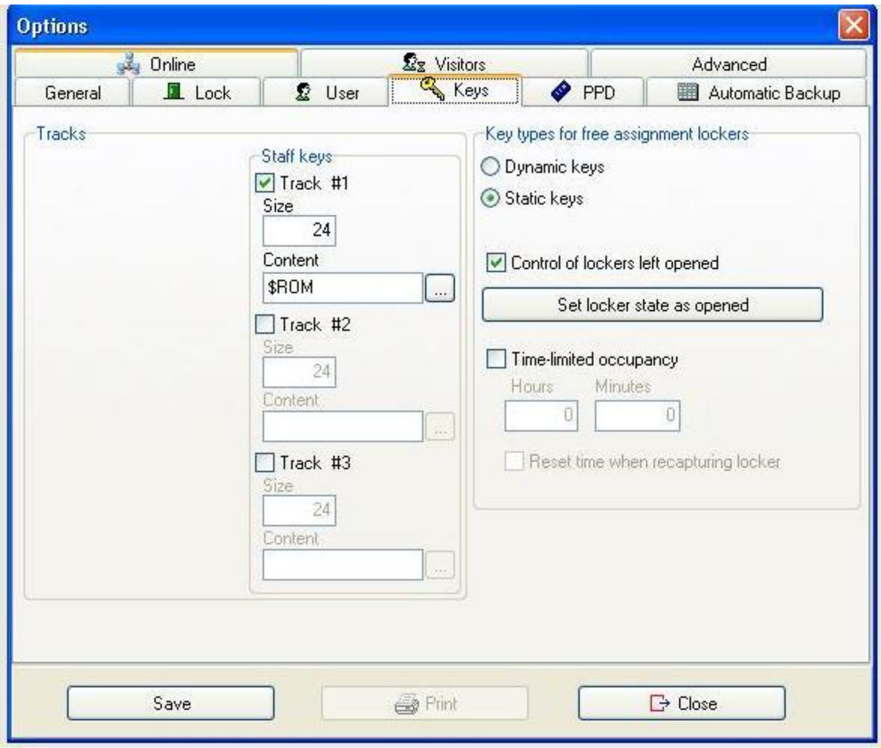
Key types for free assignment lockers

- ○ Dynamic keys
- ● Static keys
- ☑ Control of lockers left opened

- □ Time-limited occupancy — Hours: 0, Minutes: 0
- □ Reset time when recapturing locker

Writting extra info in users cards:

To write information in any of the tracks of the cards we have to go to the menu TOOLS/ CONFIGURATION/ GENERAL OPTIONS/ KEYS. We will find the following window (Fig. 1)



Tracks

Staff keys

☑ Track #1
Size: 24
Content: $ROM

□ Track #2
Size: 24
Content:

□ Track #3
Size: 24
Content:

Key types for free assignment lockers

○ Dynamic keys
● Static keys

☑ Control of lockers left opened

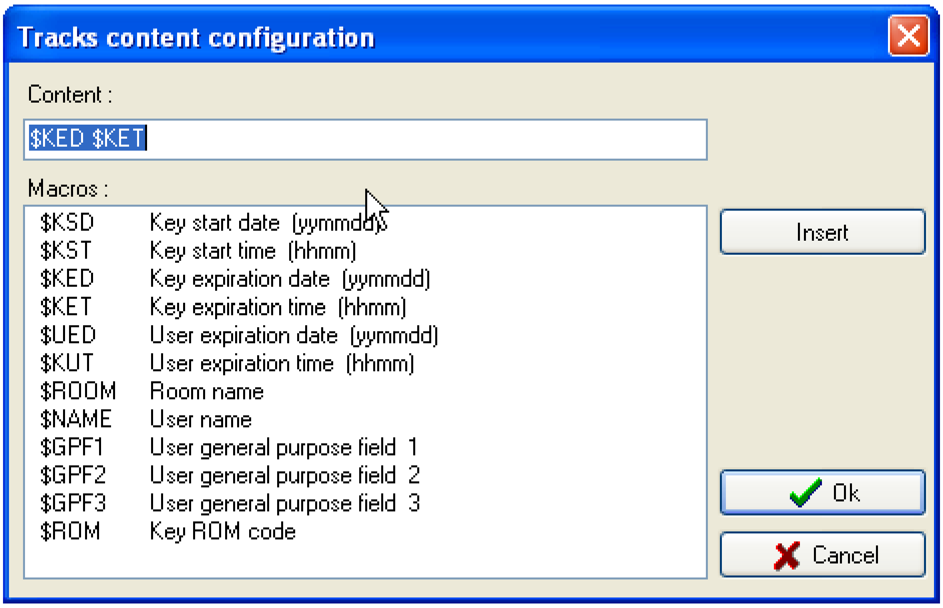
□ Time-limited occupancy
Hours: 0 Minutes: 0

□ Reset time when recapturing locker

(Fig. 1)

In this window we can select the track in which we want to write, the size as well as if we want to write the info in the users keys. In addition, we have to define the size (number of bytes) that we want to reserve for each track.

The next step will be to select what we want to write in the track. To do this we have to press the ... button. We will see the following window (Fig. 2)



Tracks content configuration

Content : $KED $KET

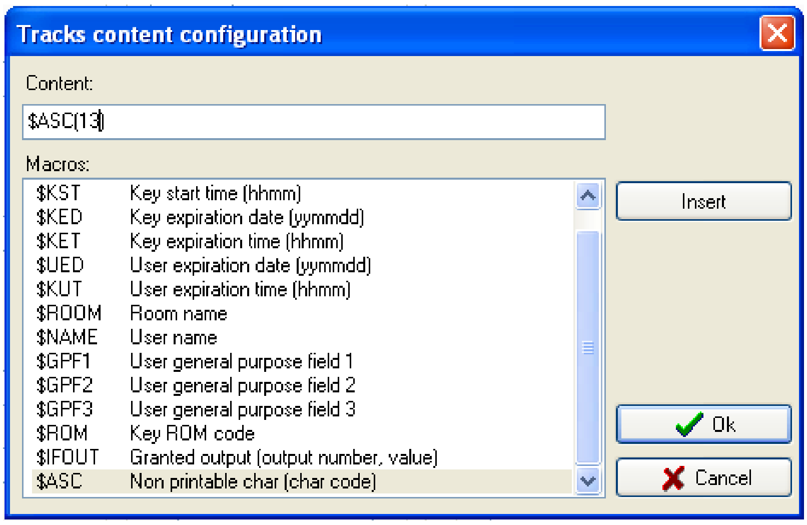
Macros :

$KSD	Key start date (yymmdd)
$KST	Key start time (hhmm)
$KED	Key expiration date (yymmdd)
$KET	Key expiration time (hhmm)
$UED	User expiration date (yymmdd)
$KUT	User expiration time (hhmm)
$ROOM	Room name
$NAME	User name
$GPF1	User general purpose field 1
$GPF2	User general purpose field 2
$GPF3	User general purpose field 3
$ROM	Key ROM code

(Fig. 2)

In this screen we will select the macro or macros that we want to be written by default each time we encode a new key. The software allows us to write as well a constant value before or after each macro. To do this we will write it before or after the macro in the content window.

A new macro has been integrated in order to send ASCII characters such as the "ENTER"



Tracks content configuration

Content: $ASC(13)

Macros:

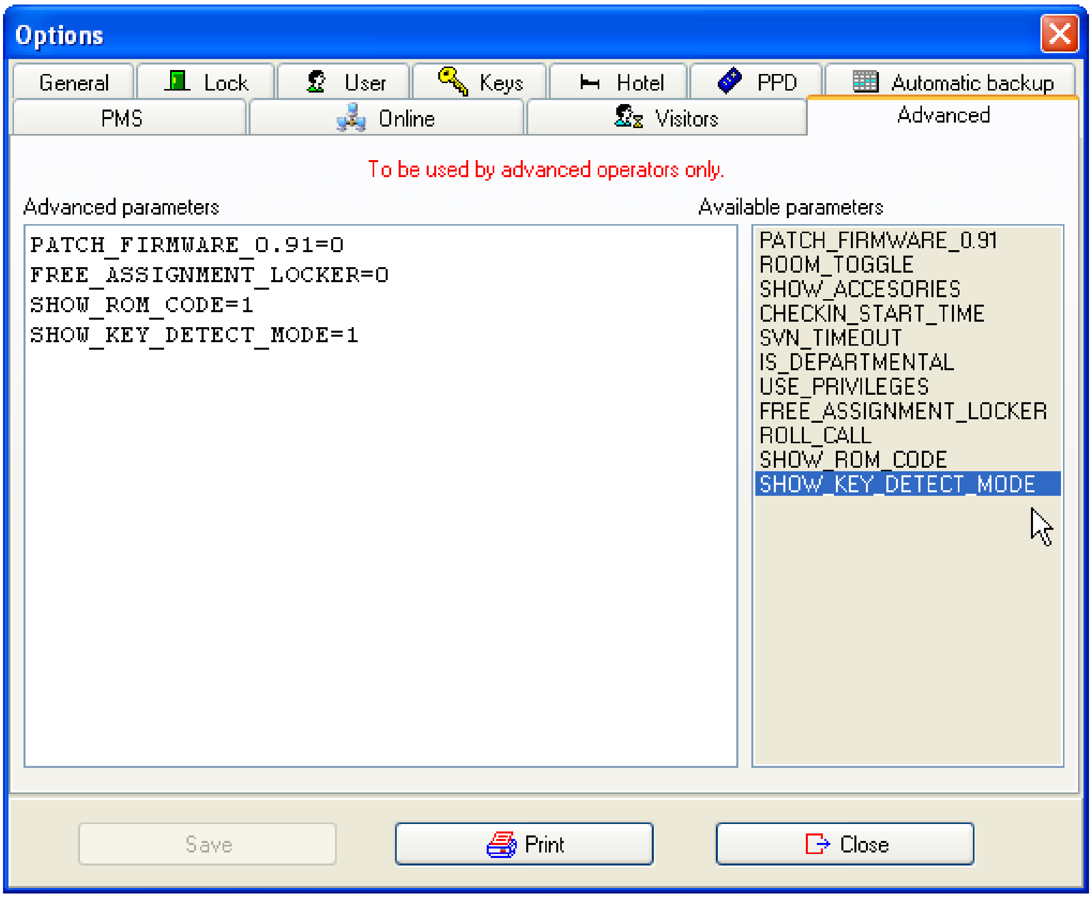
$KST	Key start time (hhmm)
$KED	Key expiration date (yymmdd)
$KET	Key expiration time (hhmm)
$UED	User expiration date (yymmdd)
$KUT	User expiration time (hhmm)
$ROOM	Room name
$NAME	User name
$GPF1	User general purpose field 1
$GPF2	User general purpose field 2
$GPF3	User general purpose field 3
$ROM	Key ROM code
$IFOUT	Granted output (output number, value)
$ASC	Non printable char (char code)

Finally we will press the ✓ OK button. As from this moment each time we issue a key this fields will be written in the selected tracks.

Show Key detect mode:

NOTE: THIS OPTION IS ONLY COMPATIBLE WITH THE FOLLOWING FIRMWARE VERSIONS. ALL PPD WITH FIRMWARE VERSIONS V.1.0.2 OR INFERIOR ARE NOT COMPATIBLE WITH THIS OPTION.

In order to activate this option is the software, we have to go to the menu: TOOLS/ CONFIGURATION/ GENERAL OPTIONS and press the "ADVANCED" tab. (Fig. 1)



To be used by advanced operators only.

Advanced parameters

```
PATCH_FIRMWARE_0.91=0
FREE_ASSIGNMENT_LOCKER=0
SHOW_ROM_CODE=1
SHOW_KEY_DETECT_MODE=1
```

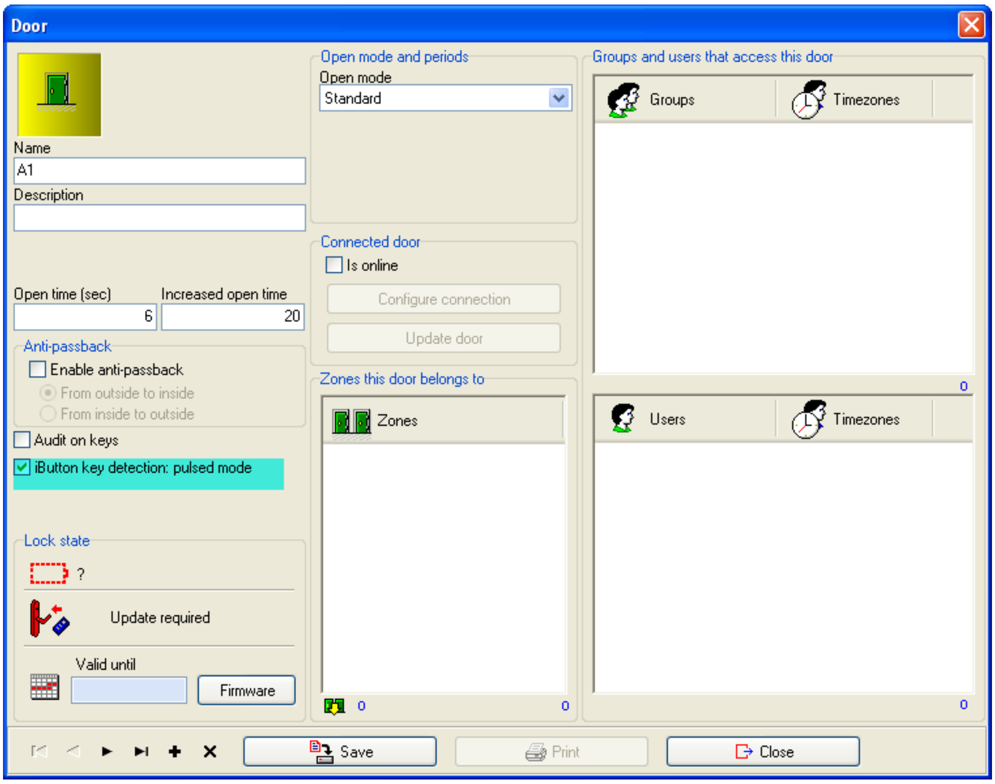
Available parameters

```
PATCH_FIRMWARE_0.91
ROOM_TOGGLE
SHOW_ACCESORIES
CHECKIN_START_TIME
SVN_TIMEOUT
IS_DEPARTMENTAL
USE_PRIVILEGES
FREE_ASSIGNMENT_LOCKER
ROLL_CALL
SHOW_ROM_CODE
SHOW_KEY_DETECT_MODE
```

(Fig. 1)

We have to pass to the advanced parameters window the option "SHOW_KEY_DETECT_MODE"

After this we will have to go to each Door, Room, iLocker and or Associated Door where we want to enable this option and enable the checkbox "ibutton key detection: Pulse mode". (Fig. 2)



Door

Name: A1

Description:

Open time (sec): 6

Increased open time: 20

Anti-passback

□ Enable anti-passback

● From outside to inside

○ From inside to outside

□ Audit on keys

☑ iButton key detection: pulsed mode

Lock state

?

Update required

Valid until

Open mode and periods

Open mode: Standard

Connected door

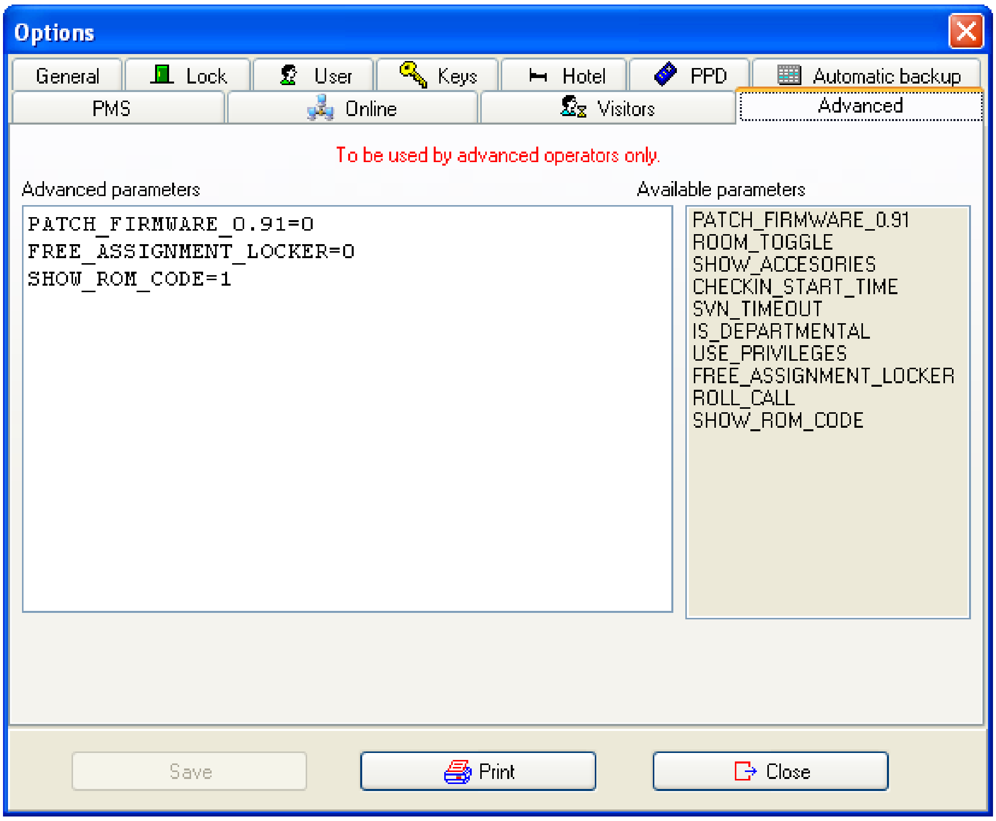
□ Is online

(Fig. 2)

After finishing with the selection, we will need to update all the doors, rooms, ilockers or associated doors that we have modified.

Show ROM code:

In order to activate this option is the software, we have to go to the menu: TOOLS/ CONFIGURATION/ GENERAL OPTIONS and press the "ADVANCED" tab. (Fig. 1)



To be used by advanced operators only.

Advanced parameters

```
PATCH_FIRMWARE_0.91=0
FREE_ASSIGNMENT_LOCKER=0
SHOW_ROM_CODE=1
```

Available parameters

```
PATCH_FIRMWARE_0.91
ROOM_TOGGLE
SHOW_ACCESORIES
CHECKIN_START_TIME
SVN_TIMEOUT
IS_DEPARTMENTAL
USE_PRIVILEGES
FREE_ASSIGNMENT_LOCKER
ROLL_CALL
SHOW_ROM_CODE
```

(Fig. 1)

We have to pass to the advanced parameters window the option "SHOW_ROM_CODE"

The ROM code will be shown when we read a key inside the content of it.

The ROM code will be shown each time we export users and each time we export the Audit Trail.

Wiegand Code:

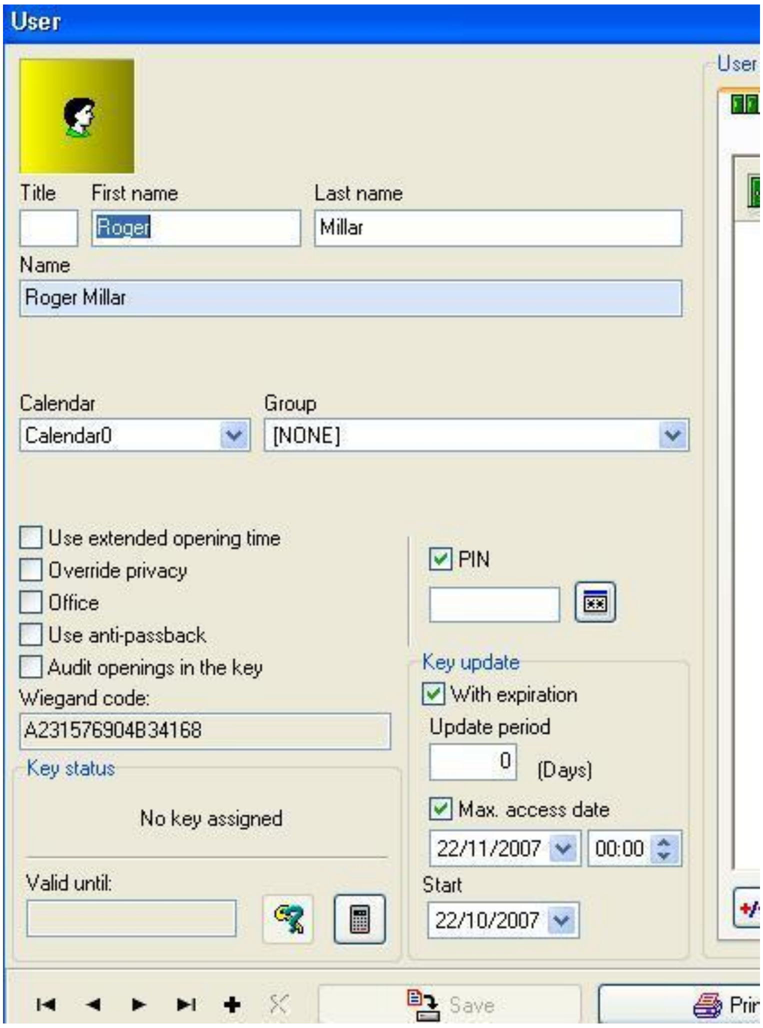
For some external application as T&A, POS… could be interesting or necessary to send the Wiegand code of the user. In some occasions that external application needs that code to identify each of the users.

Through that tool we are going to be able to write that code on the card so can be sent to other application through the WRAdaptor, CUAdaptor or DR.

The enabling of that option has to be done on tools/general options/keys there the Wiegand option. When this is enabled on the user list can be seen the new option activated. It is important to know that the Wiegand code cannot be written directly on this field. The Wiegand code can be written on the DB through the synchronization tool. There is a column on the table to be synchronized that assign the

Wiegand code to each of the users. (See Synchronization document)

When the code has been downloaded on the DB can be written on the user card and be read and sent to other application.



User

Title:
First name: Roger
Last name: Millar
Name: Roger Millar

Calendar: Calendar0
Group: [NONE]

□ Use extended opening time
□ Override privacy
□ Office
□ Use anti-passback
□ Audit openings in the key

Wiegand code: A231576904B34168

Key status: No key assigned

Valid until:

☑ PIN

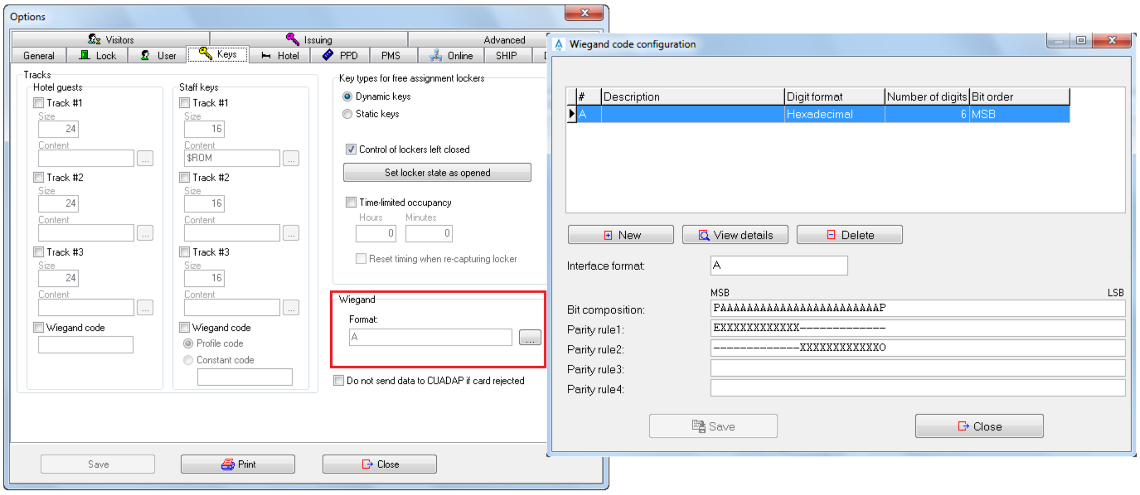
Key update
☑ With expiration
Update period: 0 (Days)
☑ Max. access date: 22/11/2007 00:00
Start: 22/10/2007

In the above window can be see the Wiegand code of this particular user.

FLEXIBLE WIEGAND FORMAT GENERATOR.

Keys tab in the Advanced Options allows the Wiegand cards to be encoded with different formats. This option allows the software to adapt to the Corporate 1000 format from HID or any other formats different from the classical Wiegand 26 bits format.

As can be seen in the picture below, the software will allow defining the bits composition of the Wiegand code, as well as the data format.



Tracks

Hotel guests

- ☐ Track #1, Size: 24, Content:
- ☐ Track #2, Size: 24, Content:
- ☐ Track #3, Size: 24, Content:
- ☐ Wiegand code

Staff keys

- ☐ Track #1, Size: 16, Content: $ROM
- ☐ Track #2, Size: 16, Content:
- ☐ Track #3, Size: 16, Content:
- ☐ Wiegand code
- ● Profile code
- ○ Constant code

Key types for free assignment lockers

- ● Dynamic keys
- ○ Static keys
- ☑ Control of lockers left closed
- Set locker state as opened
- ☐ Time-limited occupancy: Hours 0, Minutes 0
- ☐ Reset timing when re-capturing locker

Wiegand

Format: A

☐ Do not send data to CUADAP if card rejected

Wiegand code configuration

#	Description	Digit format	Number of digits	Bit order
A		Hexadecimal	6	MSB

Interface format: A

MSB … LSB

Bit composition: PAAAAAAAAAAAAAAAAAAAAAAAAP

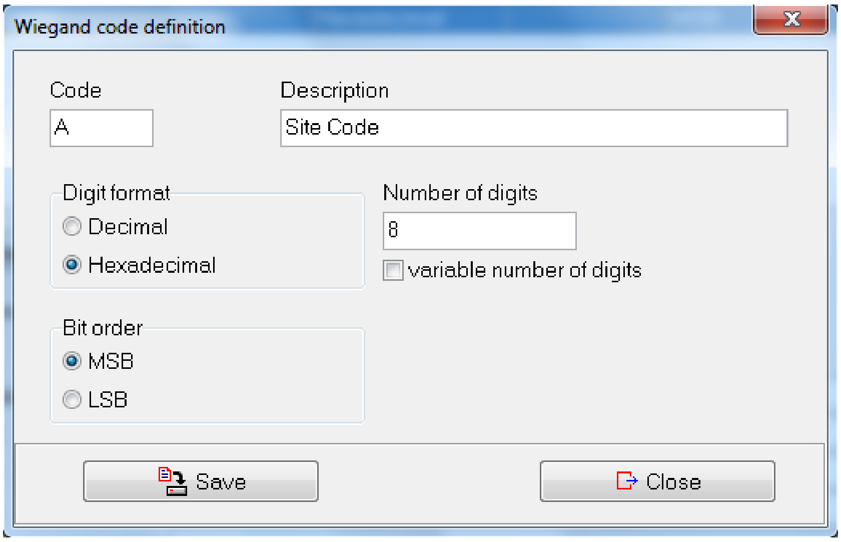
Parity rule1: EXXXXXXXXXXXX-------------

Parity rule2: -------------XXXXXXXXXXXXO

Parity rule3:

Parity rule4:

First of all, the different codes to consist the final Wiegand code must be set up. The New button will allow creating the different parts of the Wiegand code, as well as defining its characteristics.



Wiegand code definition

Code: A

Description: Site Code

Digit format

- ○ Decimal
- ● Hexadecimal

Number of digits: 8

☐ variable number of digits

Bit order

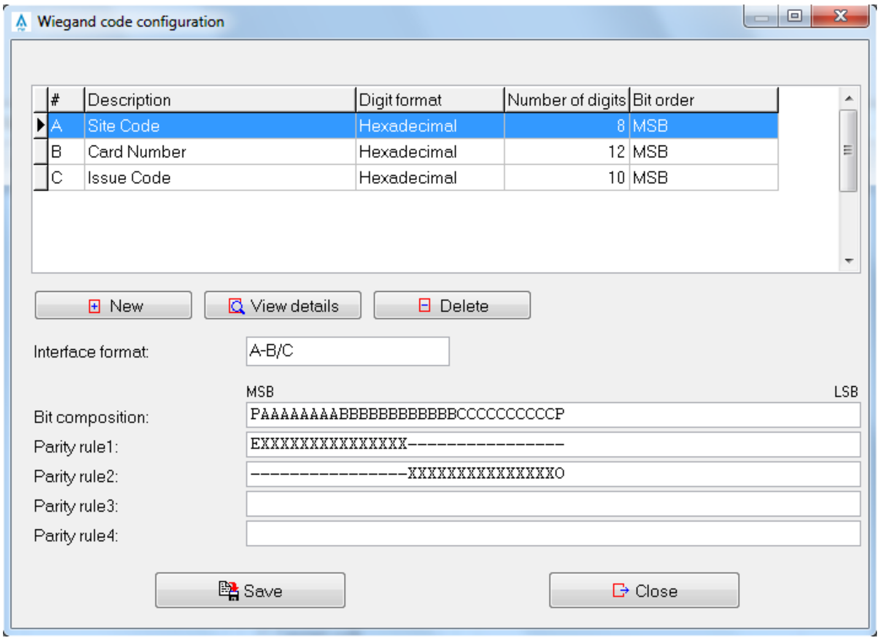
- ● MSB
- ○ LSB

The code will be internally identified with a letter, A in the example above. Any letter can be used to identify the different codes, excepting P, as this is used to identify the Parity of the codes in the beginning and end of the Wiegand code.

In order to help to identify the meaning of the different codes, a short description can be included.

The digit format can be set up to Decimal or Hexadecimal, and the number of digits can be also defined. In case the code has a variable number of digits, the software will allow setting up this characteristic.

Bits can be arranged starting with the Most Significant Bit (MSB) or Less Significant Bit (LSB).



#	Description	Digit format	Number of digits	Bit order
A	Site Code	Hexadecimal	8	MSB
B	Card Number	Hexadecimal	12	MSB
C	Issue Code	Hexadecimal	10	MSB

Interface format: A-B/C

MSB LSB

Bit composition: PAAAAAAAABBBBBBBBBBBBCCCCCCCCCCP

Parity rule1: EXXXXXXXXXXXXXXX----------------

Parity rule2: ----------------XXXXXXXXXXXXXXXO

Parity rule3:

Parity rule4:

Once the codes have been created, the Interface Format will define how the codes are going to be sent and received among the different system components, defining the separators to be used among the codes.
In the example below, code A will be separated from code B using a – (dash), and B will be separated from C using a / (slash).

The table shows how the codes are going to be located, detailing where the MSB and the LSB will be located in the upper side of the table.

The Bit Composition should show how the Wiegand code is going to be arranged, starting and finishing with the Parity (P).

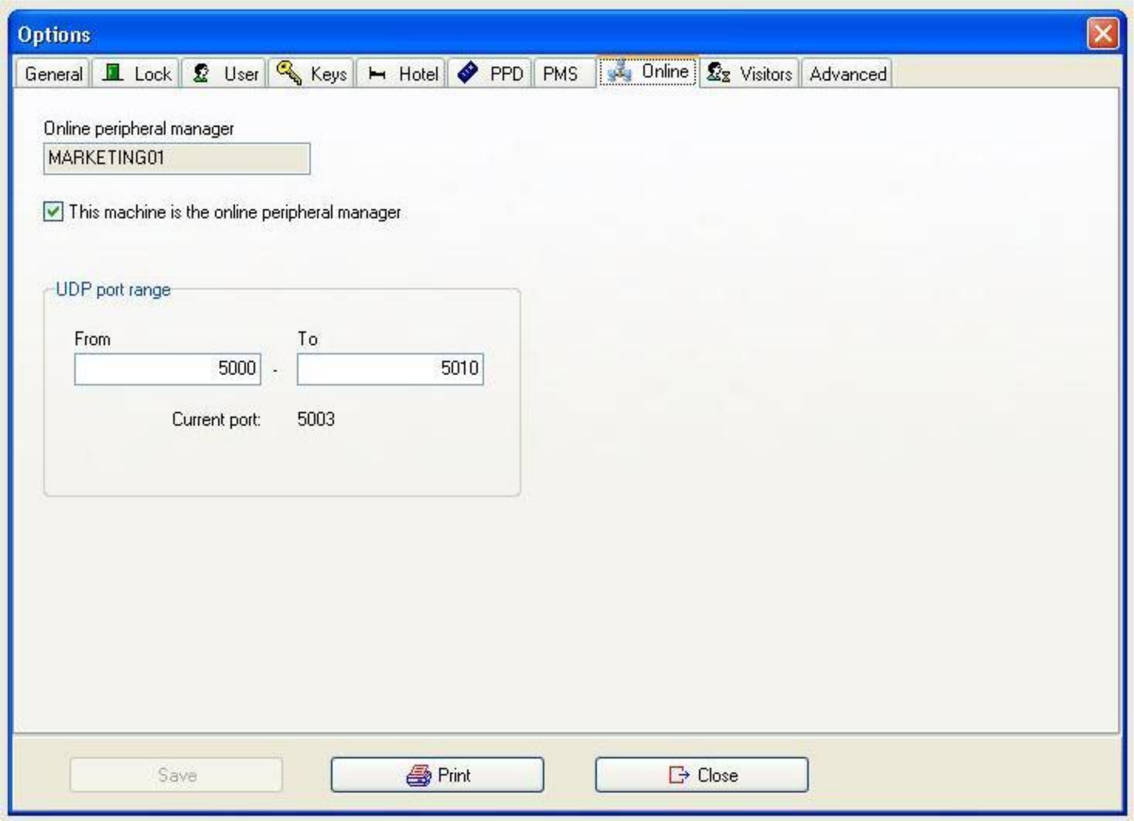
Parity rule 1 and 2 show how the Even (E) and Odd (O) Parities are calculated. The Xs indicate the bits that are going to be taken into account to calculate the Parity, and the dashes (-) the bits that will be ignored for this calculation.

Parity is calculated in the order shown in the lines. This is very important, because a Parity could be calculated taking into account the Parity result bit of another Parity calculation.

Port ranges

By default the PA software works on a range port from 5000 to 10000. For Network security reasons it could be interesting to delimit the range.

That's something very easy to configure on the software. On tools/Configuration/General options/Online:



Online peripheral manager: MARKETING01

☑ This machine is the online peripheral manager

UDP port range

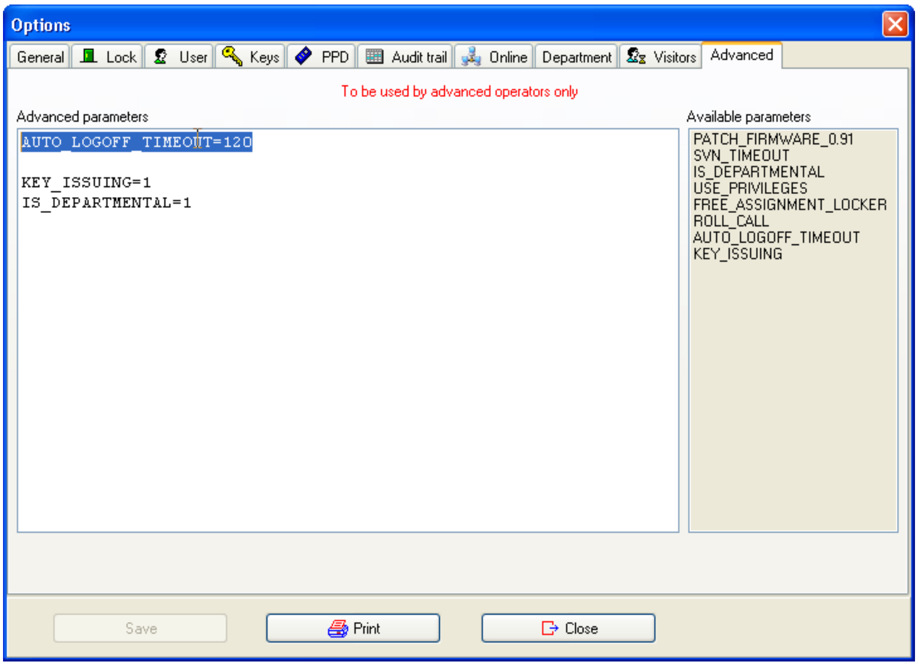
From: 5000 - To: 5010

Current port: 5003

On the UDP port range can be delimited it. Even if it has to be one specific port we could select it just by writing the same number on both boxes.

Auto Logoff

On the advanced parameters we can find this option as well. By means of this parameter we can adjust an automatic logout some time later that any operation is done. The time is the parameter we can adjust.



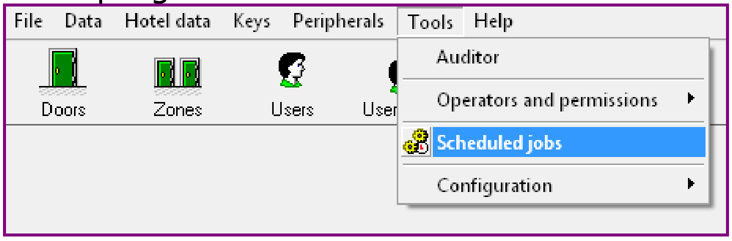
```
AUTO_LOGOFF_TIMEOUT=120

KEY_ISSUING=1
IS_DEPARTMENTAL=1
```

```
PATCH_FIRMWARE_0.91
SVN_TIMEOUT
IS_DEPARTMENTAL
USE_PRIVILEGES
FREE_ASSIGNMENT_LOCKER
ROLL_CALL
AUTO_LOGOFF_TIMEOUT
KEY_ISSUING
```

It is very simple just writing the seconds desired to be counted up before from the last operation done on the software to the Automatic Logout

Automatic Purged

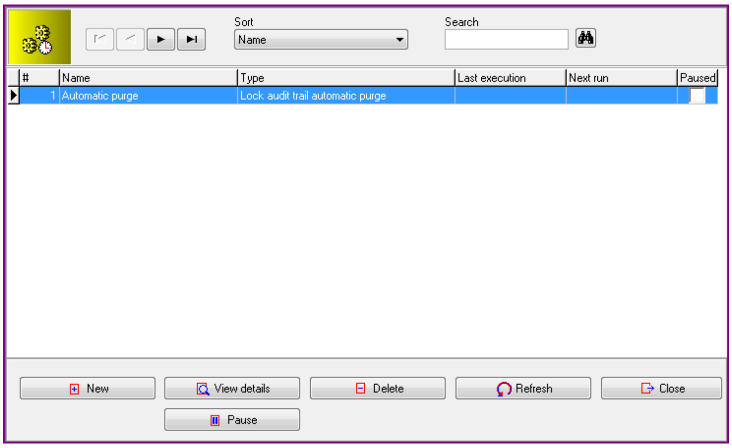
With the option shown below it is possible to have a programmed automatic purge for the audit trail.



The purged events will be placed in a TXT file in order to be able to consult them any time it's needed.

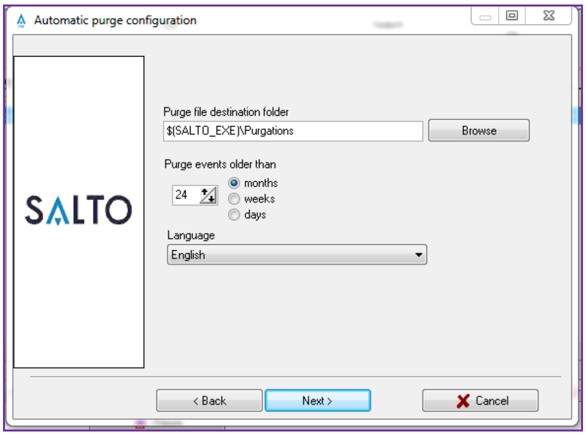
As shown in the next pictures, there are a few options to take into account as, amount of events, % of the auditor to purge, frequency and where to keep the information.

In the next window, the window shows where to start this option set up. A standard set is already done, but it is possible to modify.



#	Name	Type	Last execution	Next run	Paused
1	Automatic purge	Lock audit trail automatic purge			□

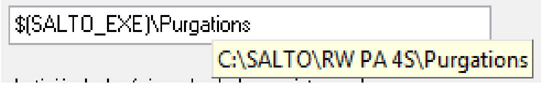
Double click in the “Automatic Purge” row and a window like the one shown in the next picture will appear. This is the wizard to set up the configuration.


Automatic purge configuration

Purge file destination folder: $(SALTO_EXE)\Purgations

Purge events older than: 24 ● months ○ weeks ○ days

Language: English


$(SALTO_EXE)\Purgations

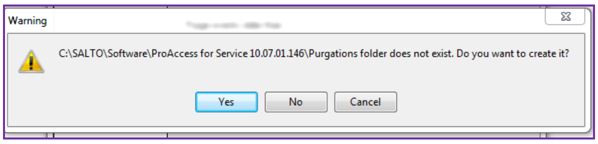
C:\SALTO\RW PA 4S\Purgations

In this first window must be introduced the location where the file will be stored as .txt file. The value $(SALTO_EXE) means, that it uses the installation path of the SALTO file to store the audits.

The value at “Purge events older than” allows specifying what events should be exported. Choose between months, weeks or days. The default by SALTO is, 24 months for export.

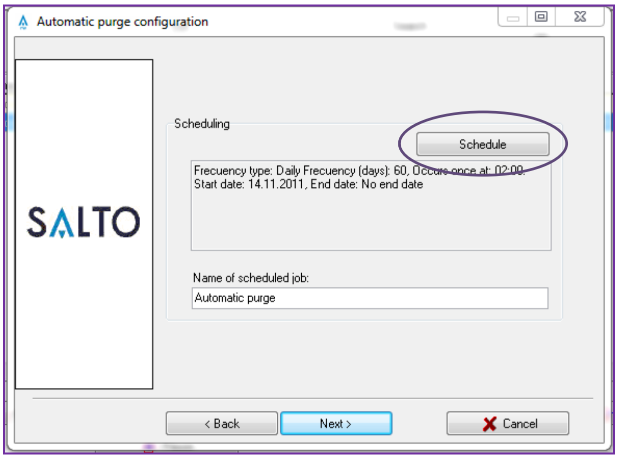
The last point allows to chose the language for this export file, so the file can be read in the preferred language.

When clicking “Next” a message like the one below might appear:


Warning

C:\SALTO\Software\ProAccess for Service 10.07.01.146\Purgations folder does not exist. Do you want to create it?

It means that the specified location does not exist. Please check the path and if it is correct click "Yes". The wizard will create this folder. If the path is not correct, click "Cancel" and change the path in the first line.

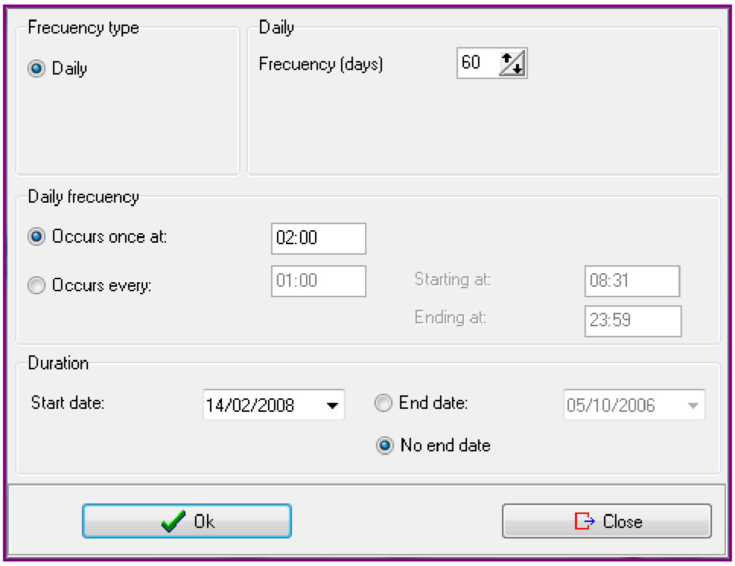


Scheduling

Frecuency type: Daily Frecuency (days): 60, Occurs once at: 02:00.
Start date: 14.11.2011, End date: No end date

Name of scheduled job: Automatic purge

Now must be set up when the job will have to be done automatically. For this you can click on the point "Schedule". In the next window, it is shown how and when must be done.



Frecuency type: ● Daily

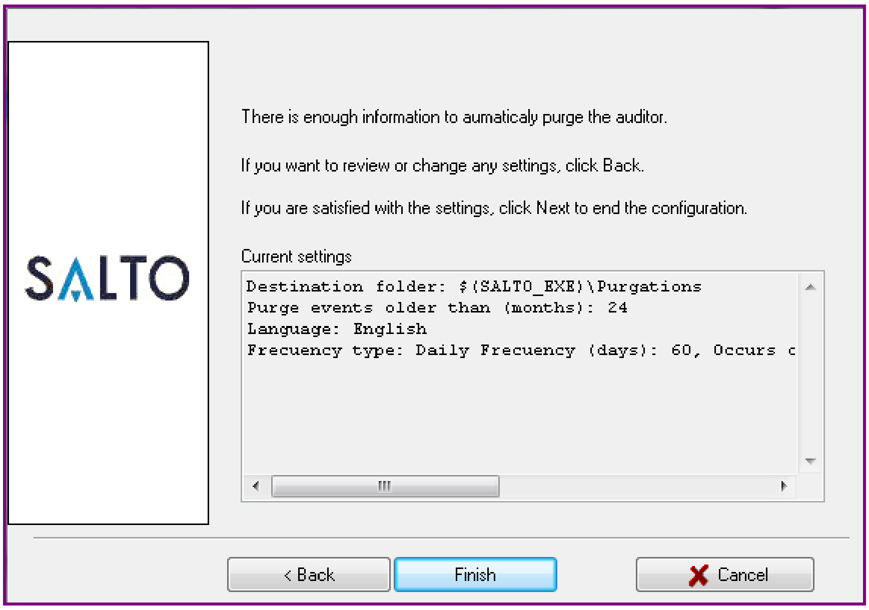
Daily: Frecuency (days) 60

Daily frecuency
● Occurs once at: 02:00
○ Occurs every: 01:00 Starting at: 08:31 Ending at: 23:59

Duration
Start date: 14/02/2008 ○ End date: 05/10/2006
● No end date

By default the wizard programs the automatic purge to run every 60 days starting at 2 o'clock in the morning. First time will start at 14/02/2008 and no end date. This configuration is to be programmed following the need. Then click "Ok".

Select the "Next" button and in the next window it will be indicated that there is enough information for the automatic purge and show have been set up as summary.



There is enough information to aumaticaly purge the auditor.

If you want to review or change any settings, click Back.

If you are satisfied with the settings, click Next to end the configuration.

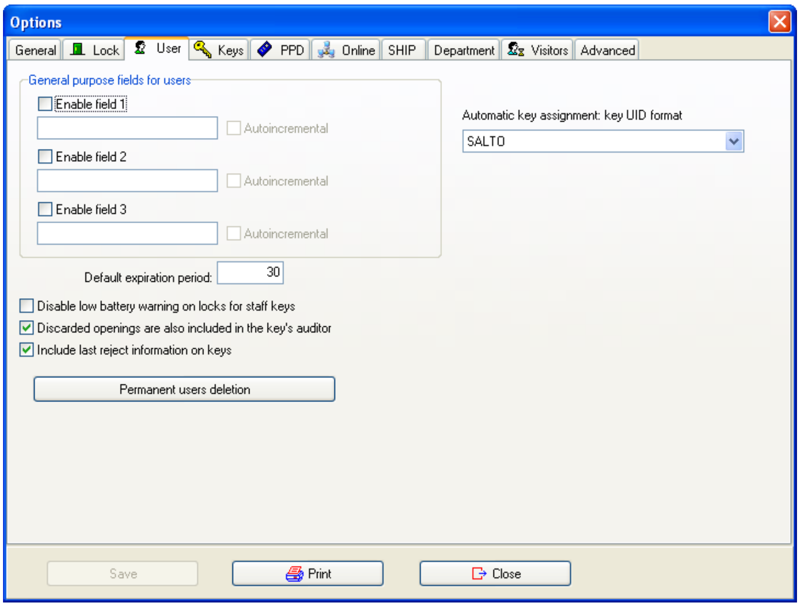
Current settings

```
Destination folder: $(SALTO_EXE)\Purgations
Purge events older than (months): 24
Language: English
Frecuency type: Daily Frecuency (days): 60, Occurs c
```

Permanent User Deletion:

Delete permanently users that have never been used.

In order to enable the Permanent User Deletion Go to: TOOLS/CONFIGURATION/GENERAL OPTIONS and in the User lab click the "PERMANENT USERS DELETION"



General purpose fields for users

□ Enable field 1 □ Autoincremental

□ Enable field 2 □ Autoincremental

□ Enable field 3 □ Autoincremental

Default expiration period: 30

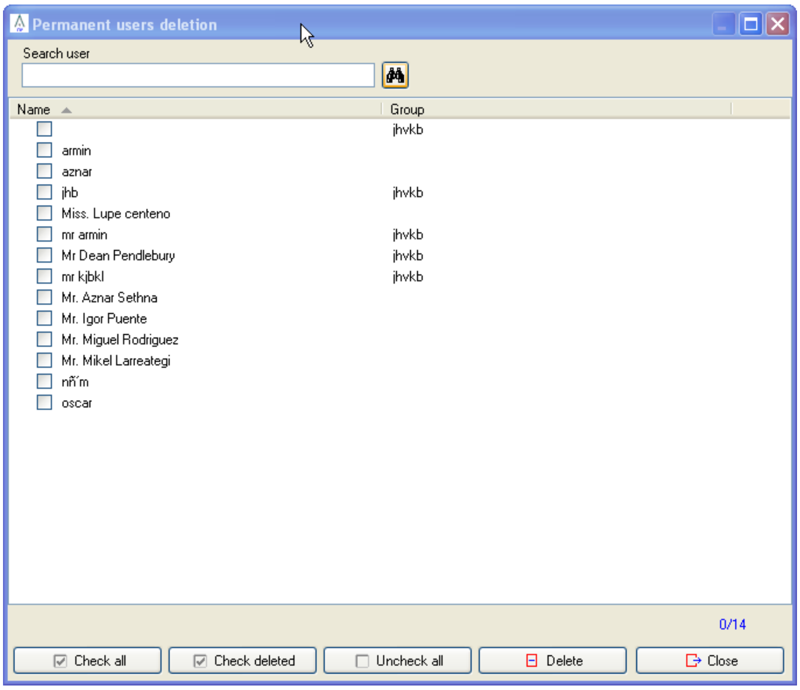
Automatic key assignment: key UID format: SALTO

□ Disable low battery warning on locks for staff keys

☑ Discarded openings are also included in the key's auditor

☑ Include last reject information on keys

Then the following screen will appear:

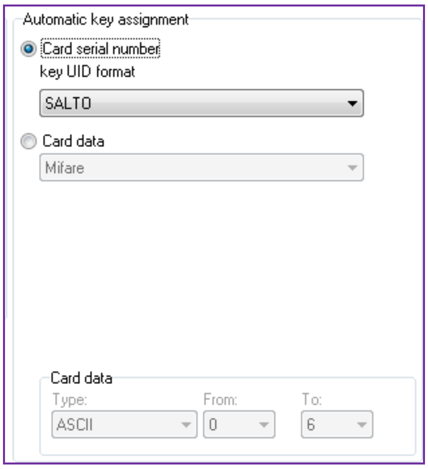


Name	Group
□	jhvkb
□ armin	
□ aznar	
□ jhb	jhvkb
□ Miss. Lupe centeno	
□ mr armin	jhvkb
□ Mr Dean Pendlebury	jhvkb
□ mr kjbkl	jhvkb
□ Mr. Aznar Sethna	
□ Mr. Igor Puente	
□ Mr. Miguel Rodriguez	
□ Mr. Mikel Larreategi	
□ nñ´m	
□ oscar	

This window will show users that were never assigned a key. Either deleted users or not. Select the ones you want to delete and press “delete”.

Automatic Key Assignment

Through this tool the system will be able to assign a card to the user automatically. For that, it is necessary to synchronize the ROM/UID Card code of each user to the Salto DB.


Automatic key assignment

● Card serial number

key UID format: SALTO

○ Card data: Mifare

Card data

Type: ASCII From: 0 To: 6

It is also possible to use a different code instead the Serial/ ROM code. This other code can be allocated on a specific sector in the key, specified by the key manufacturer or the card owner.

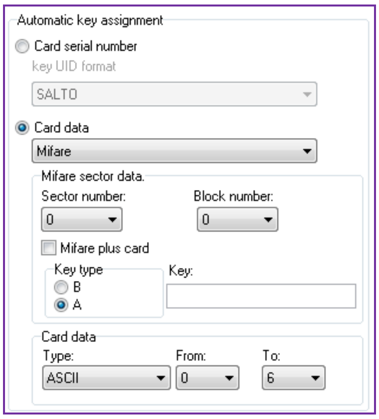
On the advanced options, User tab, you will see the window as follows. Choose the needed options for the auto assignment.

First select the mode for auto assignment. Serial number or card data.

Then select the key UID format depending the card it will be used (Salto, Mifare, DESfire, HIDiclass).

In case another code is about to be used instead the serial number, "Card Data" must be selected.

For Mifare sector data, it is necessary to select the sector and block where the code is located. If the sector is protected, it is necessary to place the key type and the unblocking key. It can be key A or key B. If using Mifare plus, please select the checkbox.



Automatic key assignment

○ Card serial number

key UID format: SALTO

● Card data: Mifare

Mifare sector data.

Sector number: 0

Block number: 0

☐ Mifare plus card

Key type: ○ B ● A

Key:

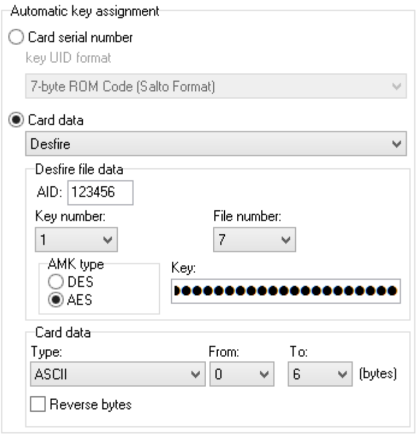
Card data

Type: ASCII

From: 0

To: 6

For DESFire application data, it is important to enter the AID of the application that contains the information. Set the Key number, for what key to use and the file number, when the application uses more than one file. After this enter the Key and specify if it is 3DES or AES.



Automatic key assignment

○ Card serial number

key UID format: 7-byte ROM Code (Salto Format)

● Card data: Desfire

Desfire file data

AID: 123456

Key number: 1

File number: 7

AMK type: ○ DES ● AES

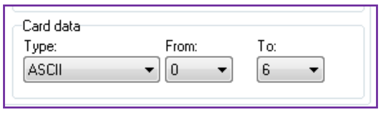
Key: ●●●●●●●●●●●●●●●●●●●●●●

Card data

Type: ASCII From: 0 To: 6 (bytes)

□ Reverse bytes

On the Card data, it is possible to place from what byte to what byte to read the code.



Card data

Type: ASCII From: 0 To: 6

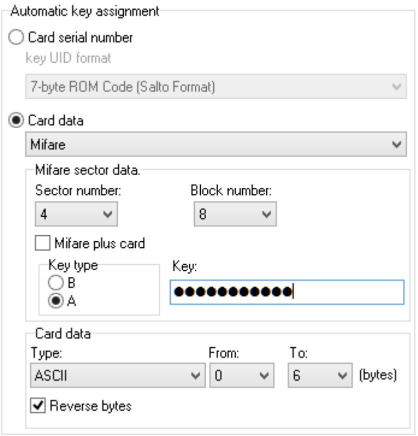
The Card data type specifies the format the information follows:

- ASCII
- WIEGAND (HEX)
- WIEGAND (HEX SWAP) - Nibble swap

This information must supplied by the system to integrate.

Difference between the Wiegand formats:

- Wiegand (HEX): 1A2B3C4D
- Wiegand (HEX SWAP): A1B2C3D4



Automatic key assignment

○ Card serial number

key UID format: 7-byte ROM Code (Salto Format)

● Card data: Mifare

Mifare sector data.

Sector number: 4

Block number: 8

□ Mifare plus card

Key type: ○ B ● A

Key: ●●●●●●●●●●●●

Card data

Type: ASCII From: 0 To: 6 (bytes)

☑ Reverse bytes

Besides the different types, the "Reverse bytes" option can be used to suit the integration needs

Ej.

- Wiegand (HEX): 1A2B3C4D
- Wiegand (HEX) + Reverse bytes: 4D3C2B1A

In order to enable the automatic Key Assignment function Go to: TOOLS/CONFIGURATION/GENERAL OPTIONS and in the advance tab enable the ASSIGN_CARDS_AUTOMATIC

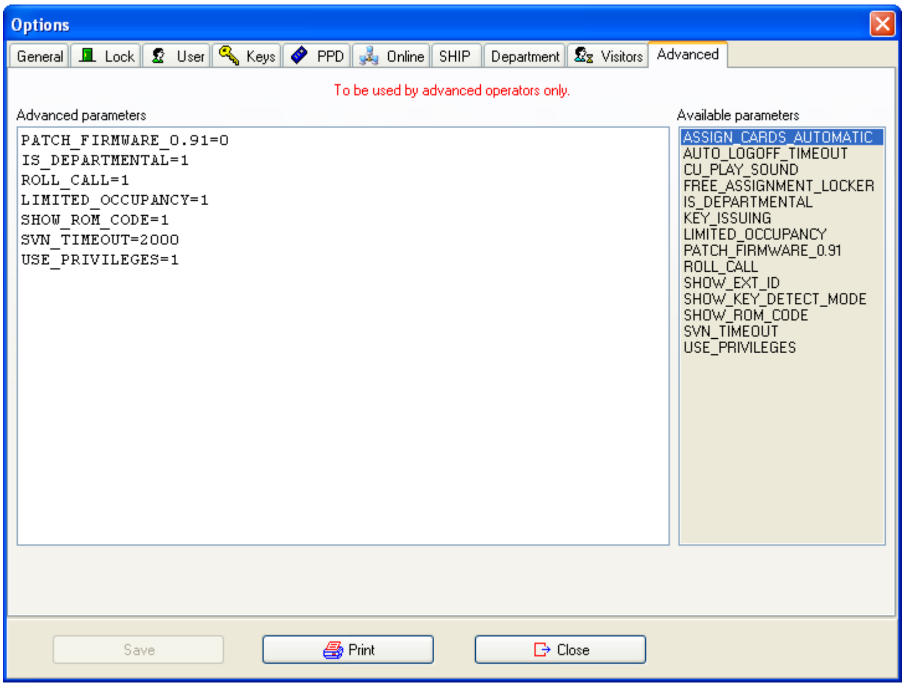
The automatic key assignment is doable by showing an empty key to an encoder or also to a WR. The encoder must be set as updater. There is no need to set a special mode on the WR, the SVN update is enough to auto assign a key.

The FW version must be the following in order to make this feature work;

Ethernet board: version **01.41** or above.

CU5000 board: version **02.02** or above.

WR: version **02.65** or above.



To be used by advanced operators only.

Advanced parameters

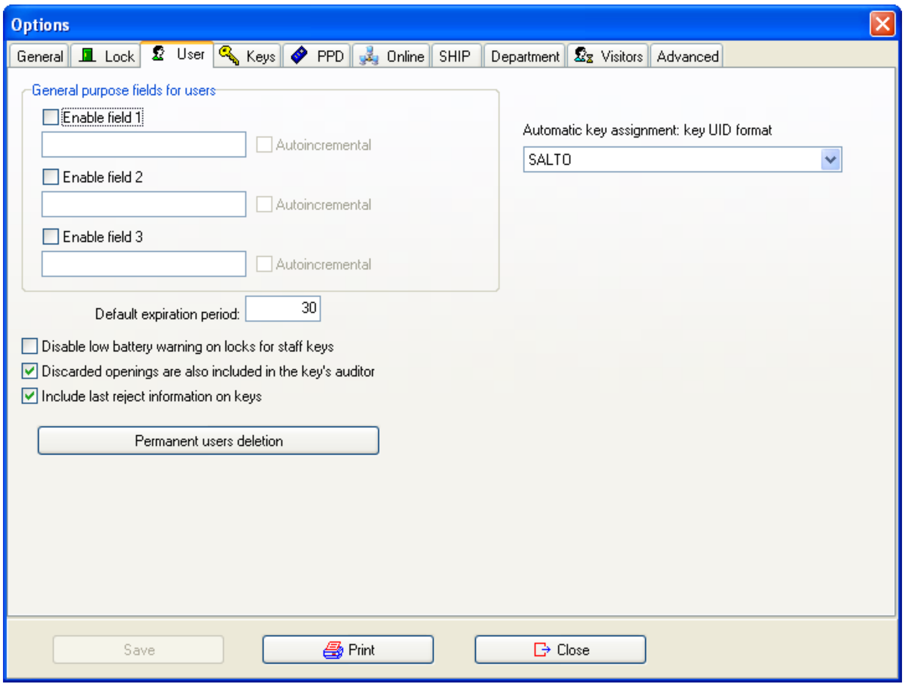
```
PATCH_FIRMWARE_0.91=0
IS_DEPARTMENTAL=1
ROLL_CALL=1
LIMITED_OCCUPANCY=1
SHOW_ROM_CODE=1
SVN_TIMEOUT=2000
USE_PRIVILEGES=1
```

Available parameters

```
ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CU_PLAY_SOUND
FREE_ASSIGNMENT_LOCKER
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
PATCH_FIRMWARE_0.91
ROLL_CALL
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SVN_TIMEOUT
USE_PRIVILEGES
```

Then you have to select the key UID format depending the card it will be used (Salto,Mifare, DESfire, HIDiclass).

To do so, Go to TOOLS/CONFIGURATION/GENERAL OPTIONS/ USERS. On that window it can be selected the UID format:



General purpose fields for users

□ Enable field 1 □ Autoincremental

□ Enable field 2 □ Autoincremental

□ Enable field 3 □ Autoincremental

Default expiration period: 30

□ Disable low battery warning on locks for staff keys

☑ Discarded openings are also included in the key's auditor

☑ Include last reject information on keys

Permanent users deletion

Automatic key assignment: key UID format: SALTO

Then on Keys/Automatic Key update (F9) the automatic key assignment is enabled and the encoder will be waiting to assign the key to the user through the UID.

Key issuing

Key issuing is defined as the process of configuring a brand new carrier for later assigning/encoding in a SALTO encoder. Normally, end users are provided with carriers already issued at SALTO (such as blue, red and yellow smart cards or iButtons). These carriers can be then used in whatever property. However, certain properties require their carriers to be customized at the property according to a specific configuration. As a result, these customized carriers cannot be reused in other properties. The RW software now offers such a key issuing tool. Currently, two types of carrier are supported: PicoPass and certain smart cards. Bear in mind that issuing of certain types of carriers will require a second encoder with a special smart card.

As for the graphic interface, you need first to activate the KEY_ISSUING advanced parameter (see ‘TOOL\GENERAL

OPTIONS\ADVANCED’) before emitting any carrier. A new tab will be shown in the general configuration window as shown in the figure below. Within this tab you may setup all the necessary parameters required for emitting carriers in the property. In addition, a new option will also be shown within the KEYS submenu (see figure 16) to have keys emitted.

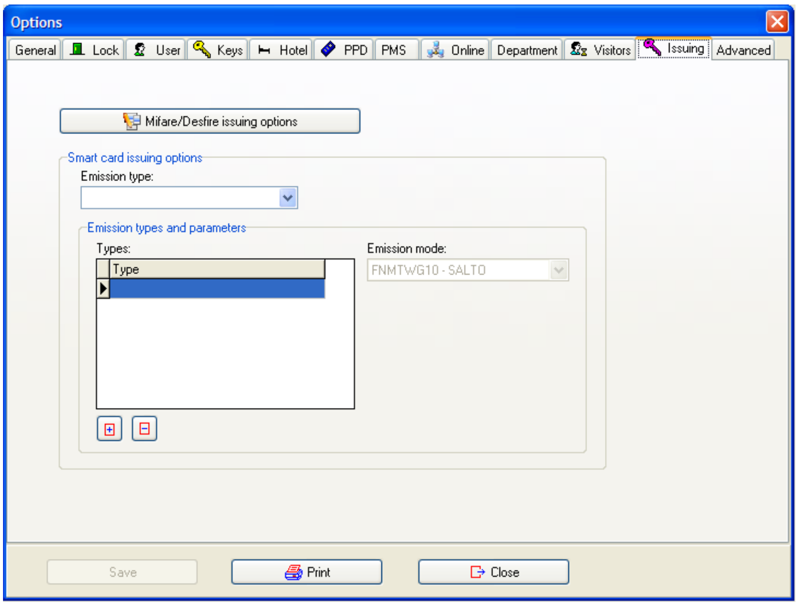


Figure 15: configuration parameters for key issuing.

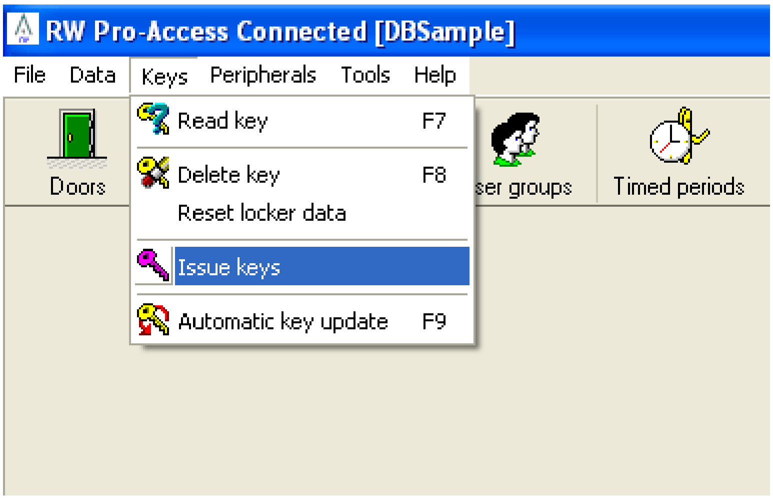


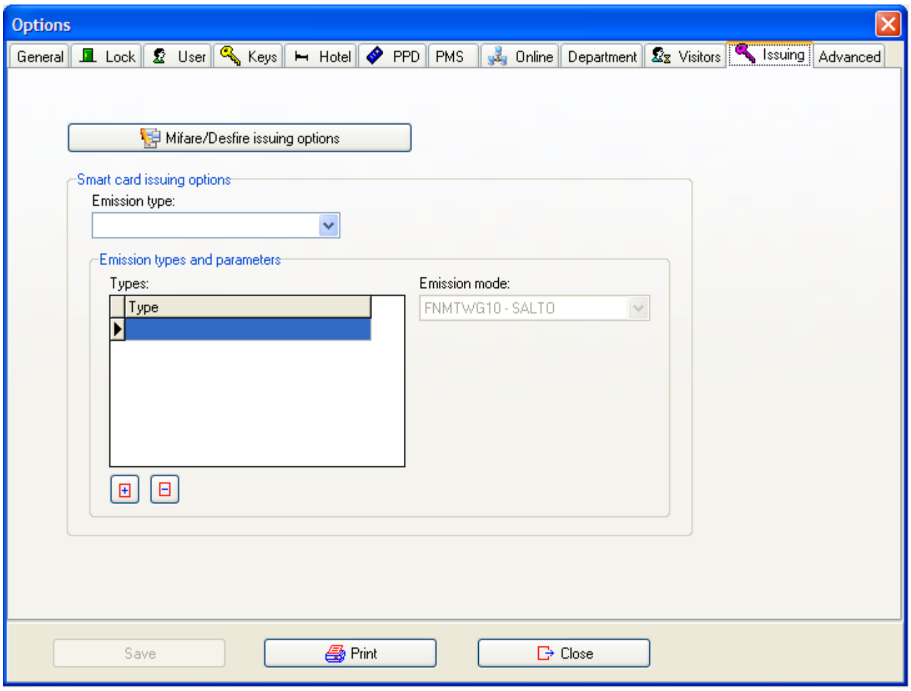
Figure 16: new key issuing option.

Currently, the following types of carriers are available:

- Smart (see references)
- Picopass
- Mifare

- Desfire
- Mifare Plus 2K
- Mifare Plus 4K
- Legic

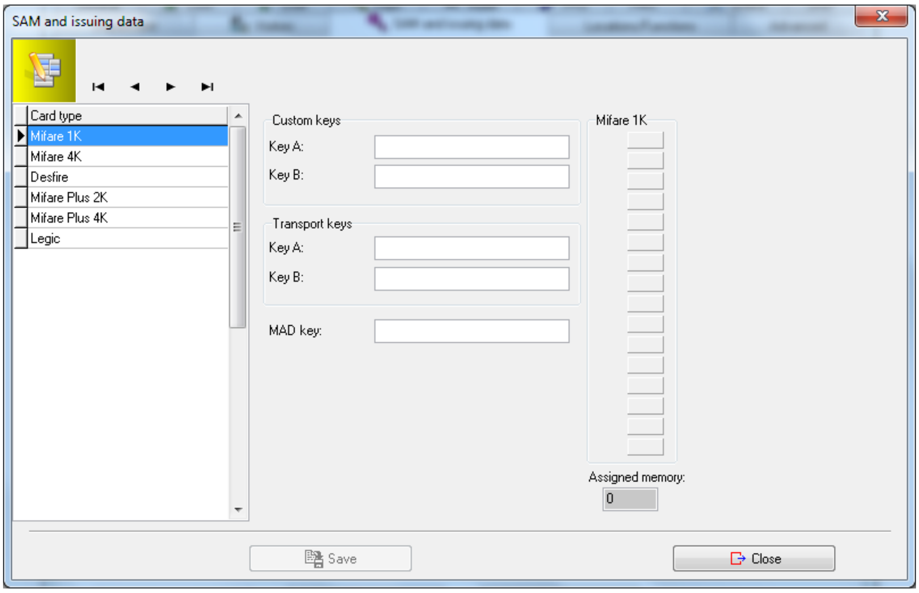
Once the KEY_ISSUING=1 option is activated in General Options, a new tab will be available under the name of "Issuing".



To work with Mifare/Desfire cards, a SAM kit must be ordered with the corresponding card and keys.

CAUTION: the modification of the following parameters must be done only under the strict supervision of a SALTO Systems technical approved technician. SALTO Systems won´t be responsible for any damage caused by a bad use of this tool.

To access to the "Mifare/Desfire issuing options" press on the corresponding button.



Select the card type used in the installation:

- Mifare 1K
- Mifare 4K
- DESFire
- Mifare Plus 2K
- Mifare Plus 4K
- Legic

“Custom keys” fields are used to enter the Salto SAM keys. “Transport keys” fields are optional and may content the carrier supplier keys (customer´s keys).

MAD key is used to unblock MAD sector in case an external application need to use it.

The check box below the MAD key must be activated in case automatic selection of sectors is asked when the card has already some occupied sectors.

The READ SAM CARD button is used to capture the keys from the SAM card (the same way it is done with the SAM software).

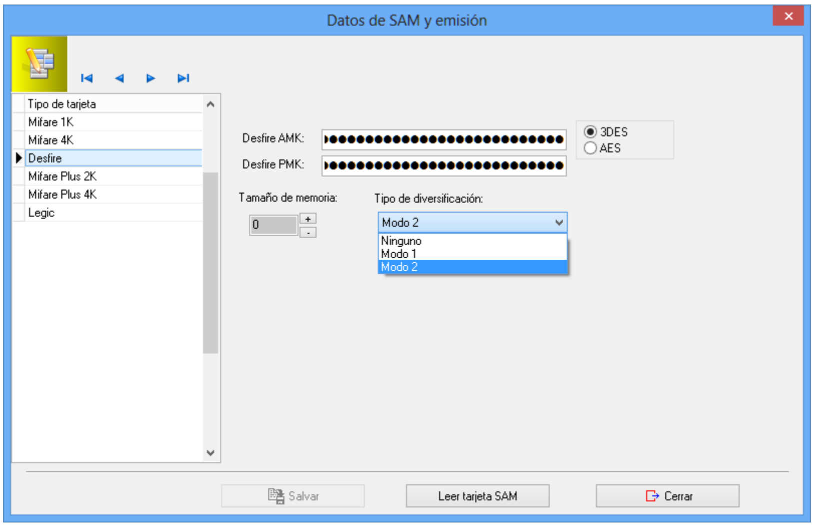
For security reasons, the keys are hidden once the SAVE button is pressed.

INCREASSE THE OCCUPIED SECTORS LATER

It is possible when using the key issuing function to increase the number of reserved sectors on a carrier after the initial issuing of the key. This operation is only possible when using SAM keys distributes by Salto and with third party carriers.

To add more sectors to a carrier, from the ISSUING window select the type of carrier you wish to add and select the sectors. For the changes to take effect on the key, you need to update the key by going to **KEYS / ISSUING AND UPDATE THE KEY**.

DESFire Evolution 1



Datos de SAM y emisión

Tipo de tarjeta
- Mifare 1K
- Mifare 4K
- ▶ Desfire
- Mifare Plus 2K
- Mifare Plus 4K
- Legic

Desfire AMK: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Desfire PMK: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

● 3DES
○ AES

Tamaño de memoria: 0

Tipo de diversificación: Modo 2

This version includes the possibility to work with this type of technology. With 4kbytes and 8kbytes capacities these cards use an AES128bits encryption that is much more complex and secured than the already robust 3DES.

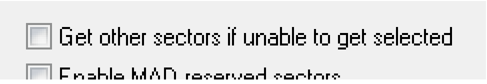
(*) DESFire EV1 cards can be also used under a 3DES encryption.

When Desfire cards are to be used, the Diversification type can be selected in the Desfire cards set up window, as can be seen in the picture below.

Note: This option is only for specific projects developed by SALTO.

MIFARE PLUS

As can be seen in the picture above, Mifare Plus 2K and 4K cards can be selected. The "Get other sectors if unable to get selected" option is not available for the Mifare Plus cards, in comparison to the menus in the standard Mifare 1K and 4K cards.



□ Get other sectors if unable to get selected

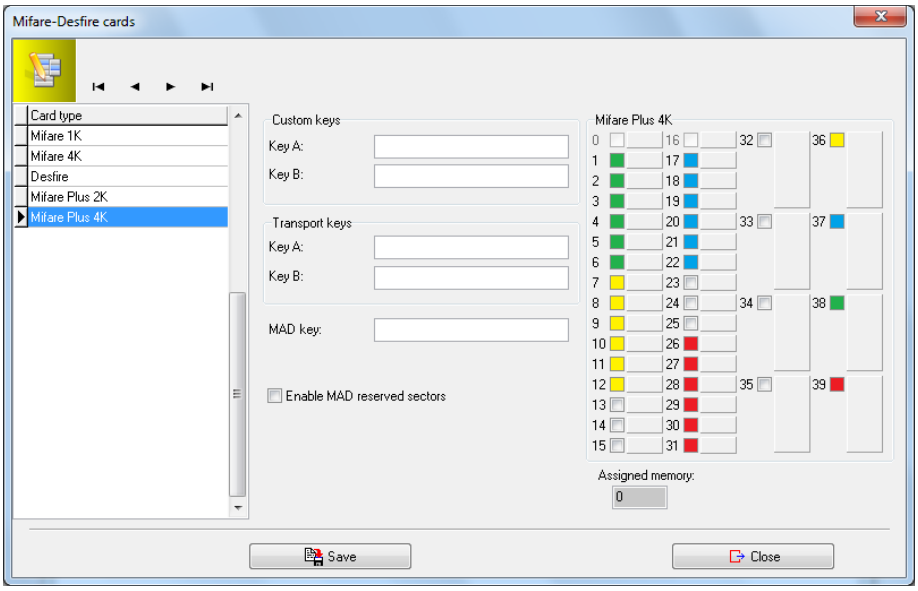
□ Enable MAD reserved sectors

This is a limitation given by the card, and that obliges to know the distribution of the sectors, that is to say, what sectors are free to use, so they can be assigned or set up in the software itself. The lack of the free sectors auto-detect feature must be taken into account then.

In case information from multiple sites must be encoded in the cards, bear in mind the SALTO STANDARD SAM CODES cannot be included in the sectors.

When more than a Salto site is going to use the same card, bear in mind that the at least one of the last 4 sectors of the card must be assigned to each site, being 4 the maximum number of sites to be included in the card.

The example below shows a possible sectors combination in colors. Take into account different sites might require more or less memory than the one selected in the picture, and that the selected sectors do not need to be one next to the other.



Card type
- Mifare 1K
- Mifare 4K
- Desfire
- Mifare Plus 2K
- ▶ Mifare Plus 4K

Custom keys
Key A:
Key B:

Transport keys
Key A:
Key B:

MAD key:

□ Enable MAD reserved sectors

Mifare Plus 4K

0	□	16	□	32	□	36	🟨
1	🟩	17	🟦				
2	🟩	18	🟦				
3	🟩	19	🟦				
4	🟩	20	🟦	33	□	37	🟦
5	🟩	21	🟦				
6	🟩	22	🟦				
7	🟨	23	□				
8	🟨	24	□	34	□	38	🟩
9	🟨	25	□				
10	🟨	26	🟥				
11	🟨	27	🟥				
12	🟨	28	🟥	35	□	39	🟥
13	□	29	🟥				
14	□	30	🟥				
15	□	31	🟥				

Assigned memory:
0

LEGIC PRIME AND ADVANT

STAMPS

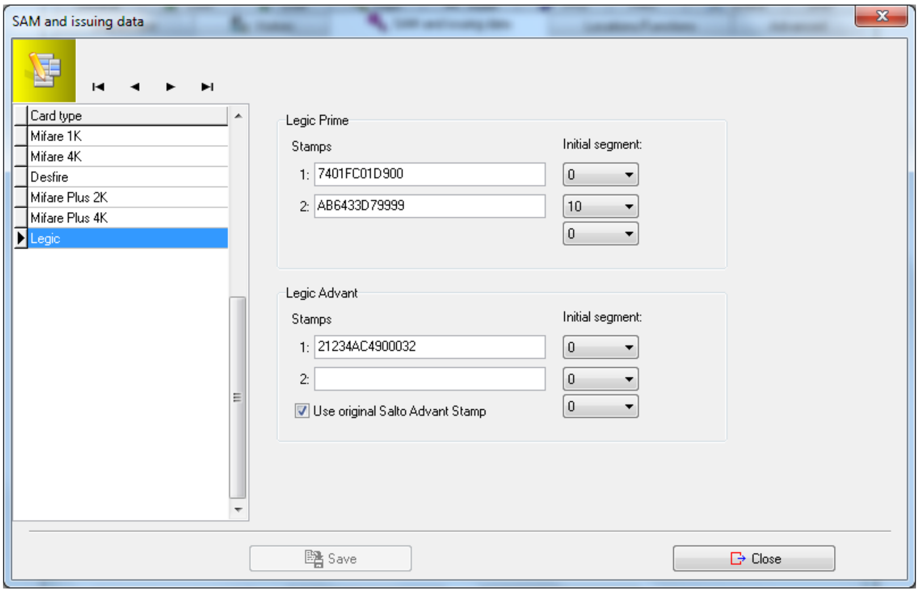
SALTO Legic devices are delivered with SALTO original Prime stamp. The stamps are part of the SAMing customization process.

Go to "TOOLS/CONFIGURATION/GENERAL OPTIONS/SAM AND ISSUING DATA".

Select the needed field depending on the card to be used: Legic Prime (6 hex bytes) or Advant (7 hex bytes) STAMP.

Salto readers can support up to 3 different STAMPS per card type at the same time:

- STAMP 1
- STAMP 2
- Salto original STAMP


SAM and issuing data

Card type
Mifare 1K
Mifare 4K
Desfire
Mifare Plus 2K
Mifare Plus 4K
Legic

Legic Prime

Stamps	Initial segment:
1: 7401FC01D900	0
2: AB6433D79999	10
	0

Legic Advant

Stamps	Initial segment:
1: 21234AC4900032	0
2:	0
☑ Use original Salto Advant Stamp	0

The readers will ONLY be able to read ONE segment in the same card.

When using the Salto original STAMP, any Legic key supplied by Salto can be used.

INITIAL SEGMENTS

In "Initial segment" select what segment the search will start from. If the initial segment is unknown, SALTO recommends leaving it at 0. By doing this the readers will know where to find the Salto application and will speed up the searching process.

If this parameter is wrong, the reader won´t be able to find the application in the card.

These segments can be compared to folders where different applications can be located by the issuing company. There are 128 segments, from 0 to 127.

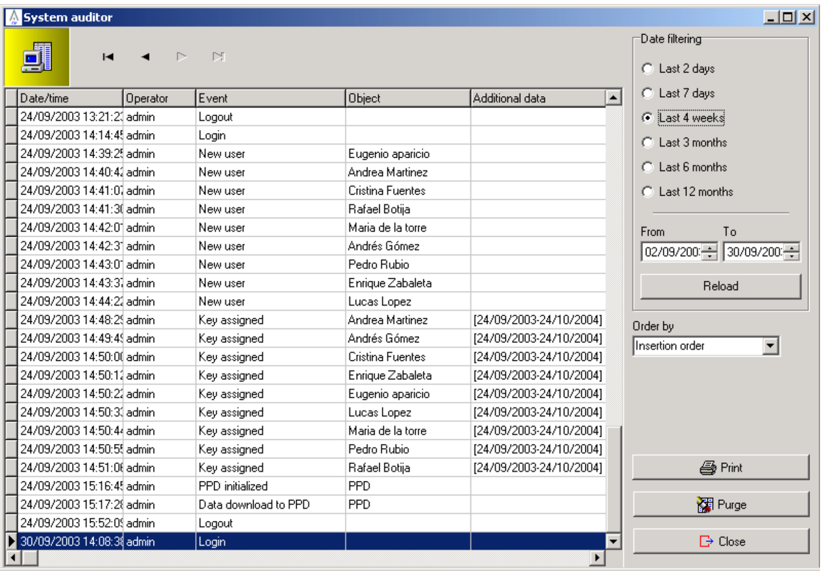
Please refer to the “Legic Prime and Advant SAMING Process” manual for more information.

Auditor

- If you select the AUDITOR option in the TOOLS menu, a window like the following will be shown. Here, all the operations made by every operator will appear in chronological order. You can choose to view the list in order of operators, operations, etc…

- If you want to have a print out of all of this information, just press the button PRINT. Make sure a printer is on line with your computer.

- If you want to clear this window, to get more available memory space, just press the PURGE button.



Date/time	Operator	Event	Object	Additional data
24/09/2003 13:21:2	admin	Logout		
24/09/2003 14:14:4	admin	Login		
24/09/2003 14:39:2	admin	New user	Eugenio aparicio	
24/09/2003 14:40:4	admin	New user	Andrea Martinez	
24/09/2003 14:41:0	admin	New user	Cristina Fuentes	
24/09/2003 14:41:3	admin	New user	Rafael Botija	
24/09/2003 14:42:0	admin	New user	Maria de la torre	
24/09/2003 14:42:3	admin	New user	Andrés Gómez	
24/09/2003 14:43:0	admin	New user	Pedro Rubio	
24/09/2003 14:43:3	admin	New user	Enrique Zabaleta	
24/09/2003 14:44:2	admin	New user	Lucas Lopez	
24/09/2003 14:48:2	admin	Key assigned	Andrea Martinez	[24/09/2003-24/10/2004]
24/09/2003 14:49:4	admin	Key assigned	Andrés Gómez	[24/09/2003-24/10/2004]
24/09/2003 14:50:0	admin	Key assigned	Cristina Fuentes	[24/09/2003-24/10/2004]
24/09/2003 14:50:1	admin	Key assigned	Enrique Zabaleta	[24/09/2003-24/10/2004]
24/09/2003 14:50:2	admin	Key assigned	Eugenio aparicio	[24/09/2003-24/10/2004]
24/09/2003 14:50:3	admin	Key assigned	Lucas Lopez	[24/09/2003-24/10/2004]
24/09/2003 14:50:4	admin	Key assigned	Maria de la torre	[24/09/2003-24/10/2004]
24/09/2003 14:50:5	admin	Key assigned	Pedro Rubio	[24/09/2003-24/10/2004]
24/09/2003 14:51:0	admin	Key assigned	Rafael Botija	[24/09/2003-24/10/2004]
24/09/2003 15:16:4	admin	PPD initialized	PPD	
24/09/2003 15:17:2	admin	Data download to PPD	PPD	
24/09/2003 15:52:0	admin	Logout		
30/09/2003 14:08:3	admin	Login		

Date filtering
○ Last 2 days
○ Last 7 days
● Last 4 weeks
○ Last 3 months
○ Last 6 months
○ Last 12 months

From: 02/09/200 To: 30/09/200

Order by: Insertion order

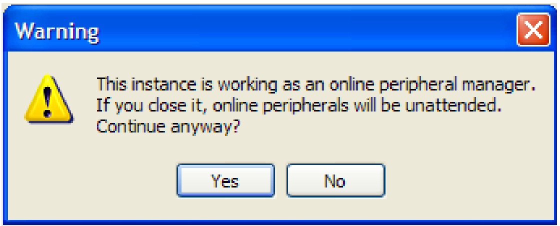
On line

This tag shows the information about which computer is the communication master for online devices (On line wall readers and up daters). If we are working in a Local Area Network, with several work stations against the same data base, only one of these workstations can be the peripheral manager.

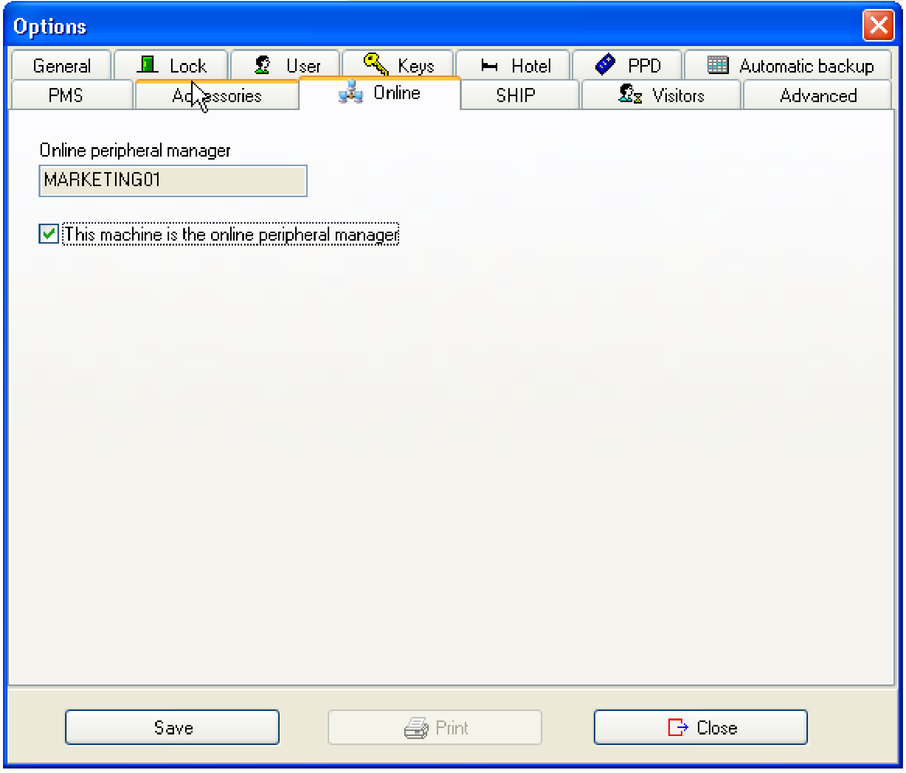
The ONLINE PERIPHERAL MANAGER field shows the name for this computer in the LAN.

The check box THIS MACHINE IS THE ON LINE PERIPHERAL MANAGER only can be ticked off for 1 workstation, should be disabled for the others workstations in the LAN.

The peripheral manager must be always running in order to permit a good synchronization with all the on-line devices.
The following warning will be shown whenever the application is going to be closed.


Warning

This instance is working as an online peripheral manager. If you close it, online peripherals will be unattended. Continue anyway?


Options

Online peripheral manager: MARKETING01

☑ This machine is the online peripheral manager

Peripheral menu

This menu has got 2 important options:

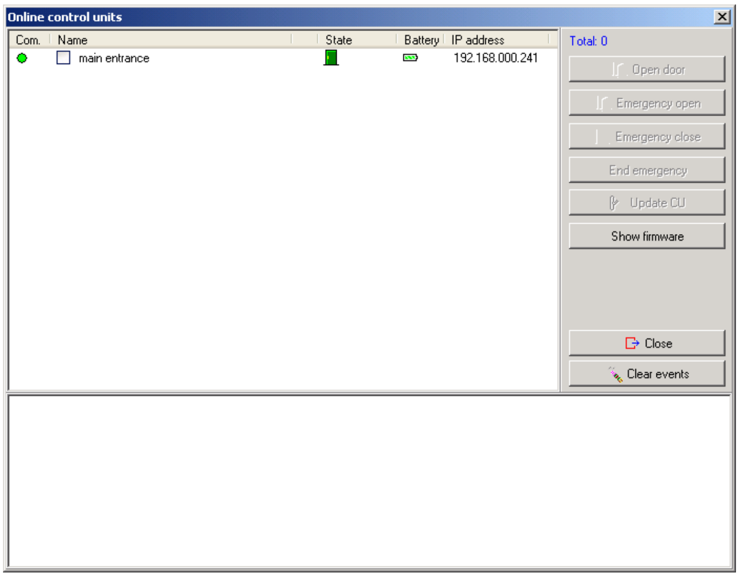
MONITORIZATION OF ON LINE CONTROL UNITS and PERIPHERAL LIST.

Monitoring On Line Control Units

This window will allow us to control in real time, the on line control units status and make some special operations as setting emergency open mode or emergency close mode.

One of the best advantages of the on line control unit is that the black list is transmitted automatically to this door, by pressing the UPDATE CU button (without needing to visit the door with a card just updated- carrying the black list for the cancelled user.)

This black list will be transmitted in real time if we are working with the communication master computer. If we are working with another workstation, the black list can take several minutes to be transmitted to the online control unit.



Online control units

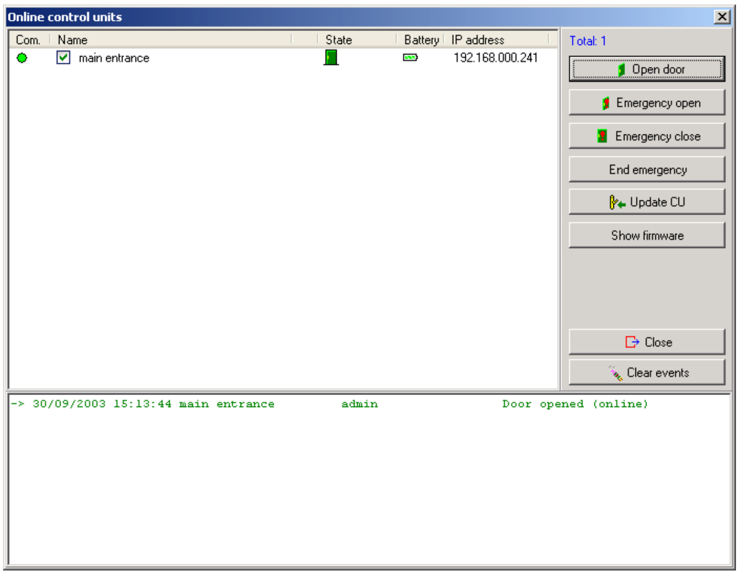
Com.	Name	State	Battery	IP address
●	□ main entrance			192.168.000.241

Total: 0

- Tick off the check box near the CU we are commanding to activate the software buttons.

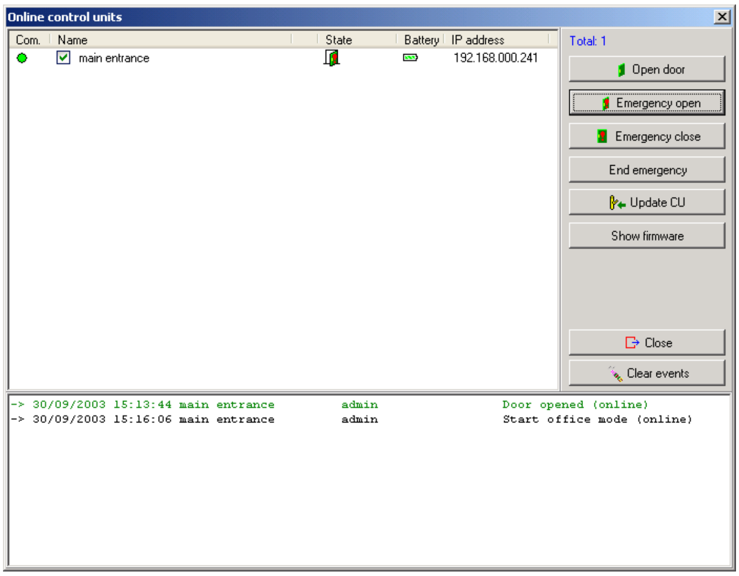
- The OPEN DOOR button can be used to make a remote door opening, if the computer we are working with is the communication manager for peripherals.

- With the OPEN DOOR button we can open remotely several online control units at the same time (the ones selected).



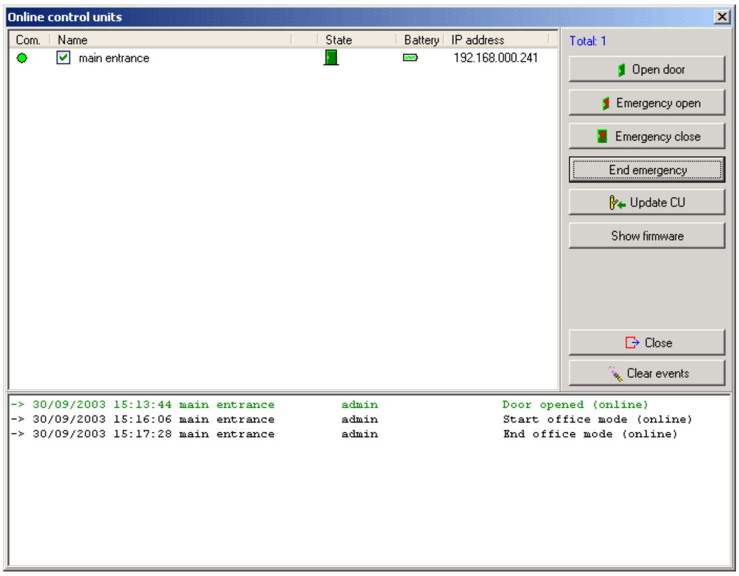
```
-> 30/09/2003 15:13:44 main entrance         admin                  Door opened (online)
```

The EMERGENCY OPEN MODE can be activated if we want the door opened for some time, no matters who is entering at this time. This has nothing to do with the standard office mode, or automatic opening. To finish this special working mode, just click the END EMERGENCY button.



```
-> 30/09/2003 15:13:44 main entrance         admin                  Door opened (online)
-> 30/09/2003 15:16:06 main entrance         admin                  Start office mode (online)
```

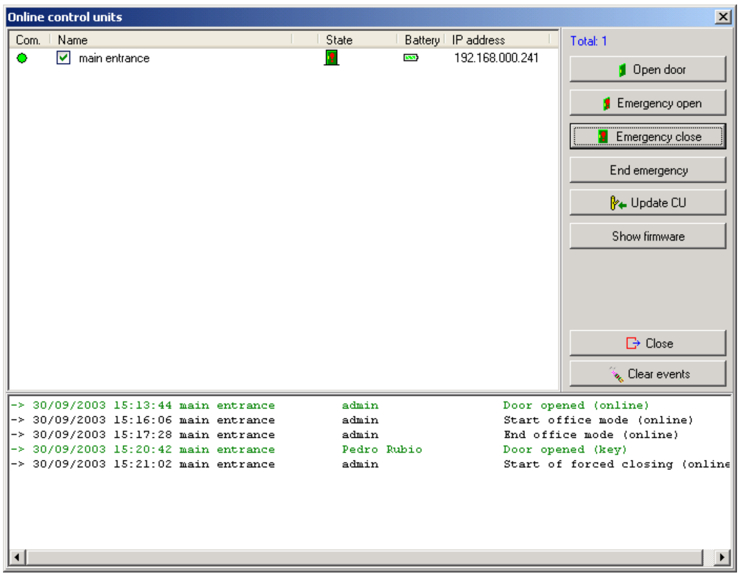
After clicking the END EMERGENCY button, the door will go back to its normal operation.



Com.	Name	State	Battery	IP address
●	☑ main entrance			192.168.000.241

```
-> 30/09/2003 15:13:44 main entrance        admin                Door opened (online)
-> 30/09/2003 15:16:06 main entrance        admin                Start office mode (online)
-> 30/09/2003 15:17:28 main entrance        admin                End office mode (online)
```

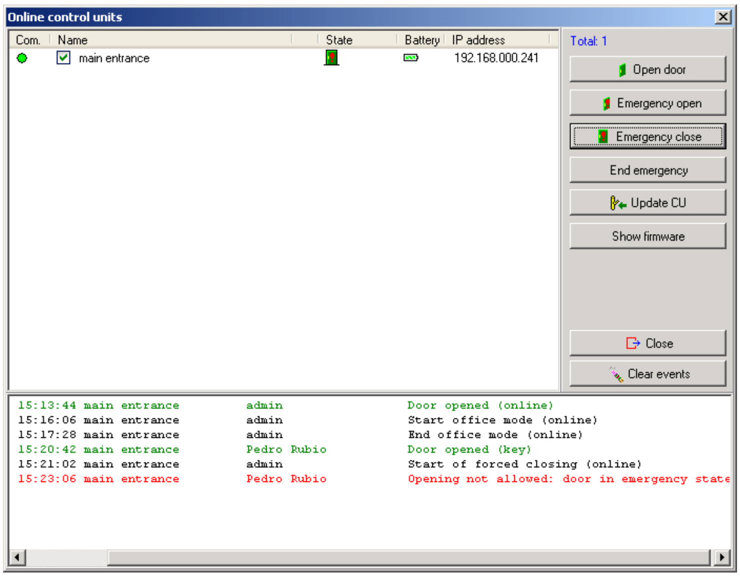
The EMERGENCY CLOSED MODE can be used if we want to maintain the door closed to any user or guest (no matters they are allowed users) for some time. As we have done with the EMERGENCY OPEN before, this EMERGENCY CLOSE MODE finishes by clicking the END EMERGENCY button.



Com.	Name	State	Battery	IP address
●	☑ main entrance			192.168.000.241

```
-> 30/09/2003 15:13:44 main entrance        admin                Door opened (online)
-> 30/09/2003 15:16:06 main entrance        admin                Start office mode (online)
-> 30/09/2003 15:17:28 main entrance        admin                End office mode (online)
-> 30/09/2003 15:20:42 main entrance        Pedro Rubio          Door opened (key)
-> 30/09/2003 15:21:02 main entrance        admin                Start of forced closing (online
```

In the image on top, we can see how 1 allowed user may enter the door. But then, after setting the EMERGENCY CLOSED MODE (3 minutes later) Pedro Rubio is no longer able to enter, because of the emergency closed mode (Image below).

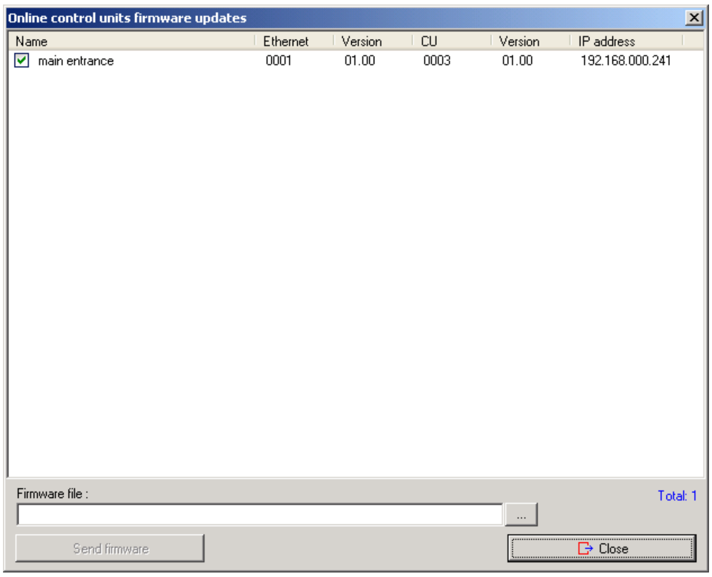


Com.	Name	State	Battery	IP address
●	☑ main entrance			192.168.000.241

```
15:13:44 main entrance        admin              Door opened (online)
15:16:06 main entrance        admin              Start office mode (online)
15:17:28 main entrance        admin              End office mode (online)
15:20:42 main entrance        Pedro Rubio        Door opened (key)
15:21:02 main entrance        admin              Start of forced closing (online)
15:23:06 main entrance        Pedro Rubio        Opening not allowed: door in emergency state
```

- The UPDATE CU button can be used to transmit information to the control unit, when we have made a change in the data base, which implies this control unit to be updated.

- The SHOW FIRMWARE button can be used to see the firmware version for this control unit.

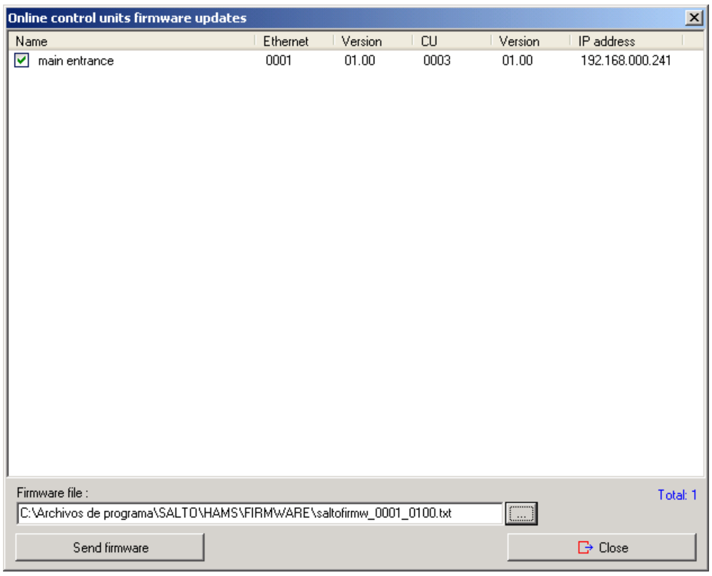


Name	Ethernet	Version	CU	Version	IP address
☑ main entrance	0001	01.00	0003	01.00	192.168.000.241

- A on line control unit is made from 2 elements, the Ethernet board and the CU board. Ethernet online board is shown as device 0001, Ethernet online SVN as 0002 and CU board is shown as device 0003. The firmware version for these elements has not got to be the same for both, mandatory.

- Sometimes, it may be necessary to update the firmware version, to provide the on line control unit with new features. Salto Systems will inform the customers when this operation is required. In order to download a new firmware in a on line control unit , follow these steps:

- Select the file where the new firmware file is kept, in your hard disk. You can do it by clicking the little button with 3 points at the right of the FIRMWARE FILE field.



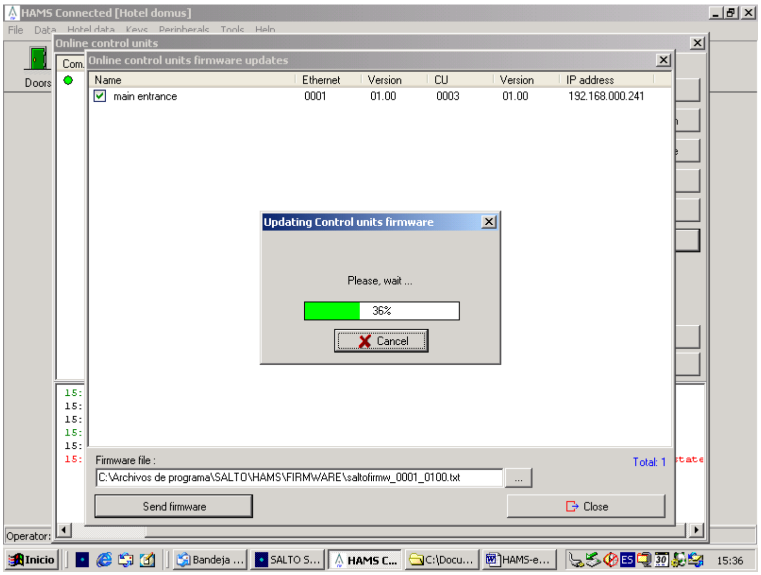
Online control units firmware updates

Name	Ethernet	Version	CU	Version	IP address
☑ main entrance	0001	01.00	0003	01.00	192.168.000.241

Firmware file : C:\Archivos de programa\SALTO\HAMS\FIRMWARE\saltofirmw_0001_0100.txt

Total: 1

In the example, the selected file has 2 numbers: the first means the device it is used for (Ethernet board) and the second is the version for this firmware. Now you can click the SEND FIRMWARE button to transmit the firmware file.



HAMS Connected [Hotel domus]
File Data Hotel data Keys Peripherals Tools Help
Online control units
Doors
Com.
Online control units firmware updates
Updating Control units firmware
Cancel
Send firmware
Close
Operator:
Inicio
15:36

Name	Ethernet	Version	CU	Version	IP address
☑ main entrance	0001	01.00	0003	01.00	192.168.000.241

Please, wait ...

36%

Firmware file :

C:\Archivos de programa\SALTO\HAMS\FIRMWARE\saltofirmw_0001_0100.txt

Total: 1

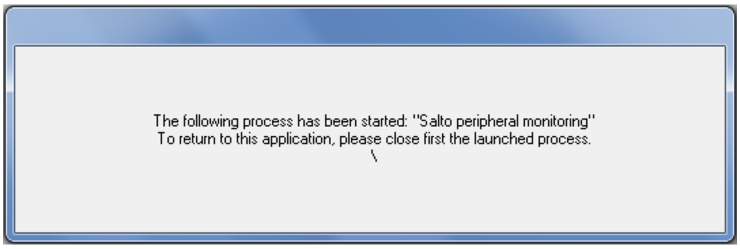
This operation will take several seconds. At the end of the transmission, you will get a confirmation message from the software, to assure the operation has been finished successfully.

It is possible to send the firmware file to several control units at the same time.

Then, you can repeat the procedure with the firmware for device 0003, which is the CU control board. This firmware files will be supplied by Salto when necessary.

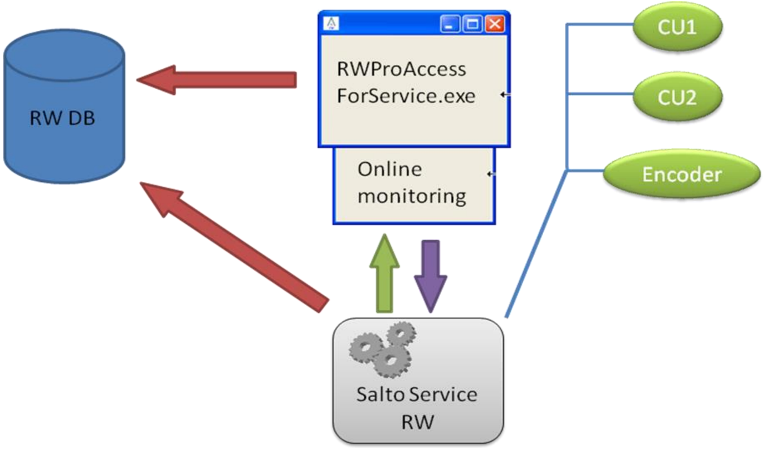
Multiple Online Monitoring (only for Service)

When launching the monitoring window from the peripheral option, the following window will appear letting know that the monitoring module is starting the communication between the service and the software.

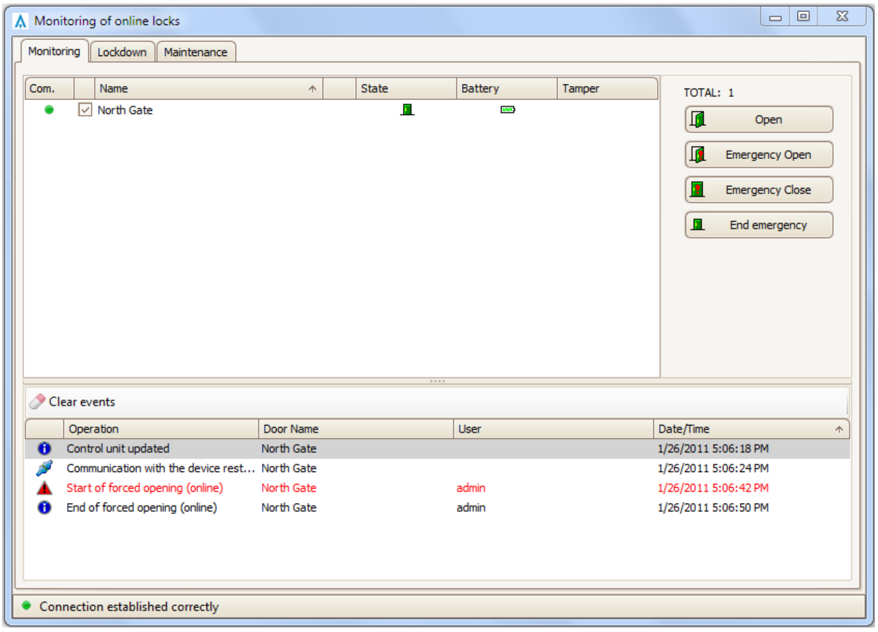


The following process has been started: "Salto peripheral monitoring"
To return to this application, please close first the launched process.

As you can see on the next diagram, all peripherals are on communication with the **Salto Service** and the service is the one that communicates with the data base. This way, all the Salto clients will be able to see the monitoring window even if they are not the peripheral manager.



The monitoring window allows opening, emergency open or close and end of the emergency for the selected online doors.

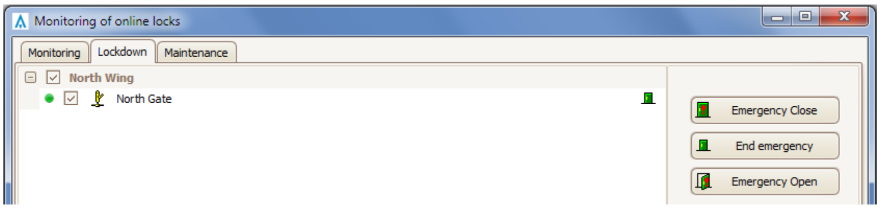


Com.	Name	State	Battery	Tamper
●	☑ North Gate	🟩	🟩	

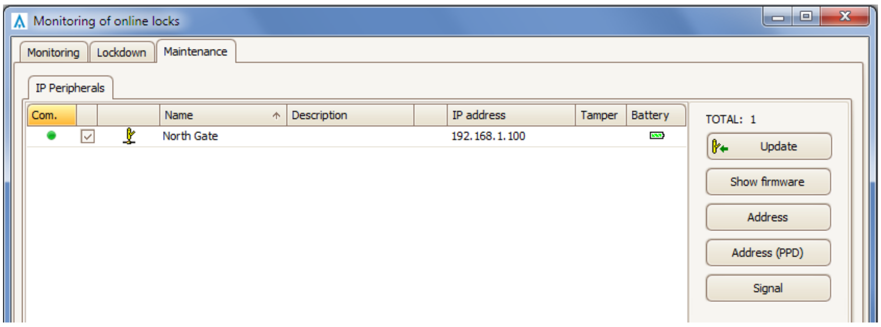
	Operation	Door Name	User	Date/Time
	Control unit updated	North Gate		1/26/2011 5:06:18 PM
	Communication with the device rest…	North Gate		1/26/2011 5:06:24 PM
	Start of forced opening (online)	North Gate	admin	1/26/2011 5:06:42 PM
	End of forced opening (online)	North Gate	admin	1/26/2011 5:06:50 PM

● Connection established correctly

After lockdowns areas are created, as shown below, it is possible to emergency open and close the lockdown selected areas.



In the software for service, the monitoring window, maintenance tab, is the only place where it is possible to initialize online peripherals. It is also the only window where to update, address and do firmware updates.


Monitoring of online locks

Monitoring | Lockdown | Maintenance

IP Peripherals

Com.			Name	Description	IP address	Tamper	Battery
●	☑		North Gate		192.168.1.100		

TOTAL: 1

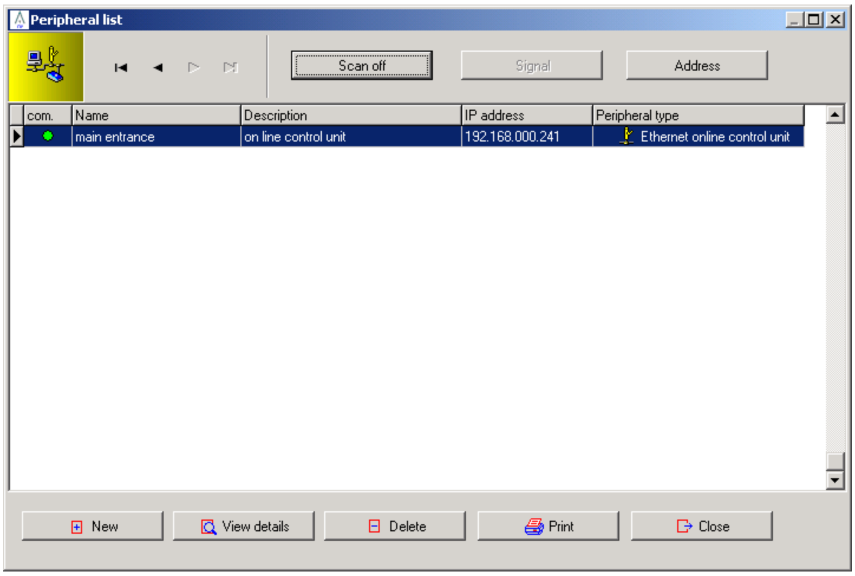
Firmware update on encoders and PPDs

The new PPD unit (*) (see the picture) includes the possibility to load several firmware files at the same time. The updating procedure will be done automatically in the different devices when lower versions are detected.

(*)PPD firmware version 1.16 or higher.

Peripheral List

This list has 2 functions: creating online devices such as online wall readers and updaters, and assigning the IP address to these devices. In our example, the “main entrance” wall reader is already created, because we have created it as a door.



com.	Name	Description	IP address	Peripheral type
●	main entrance	on line control unit	192.168.000.241	Ethernet online control unit

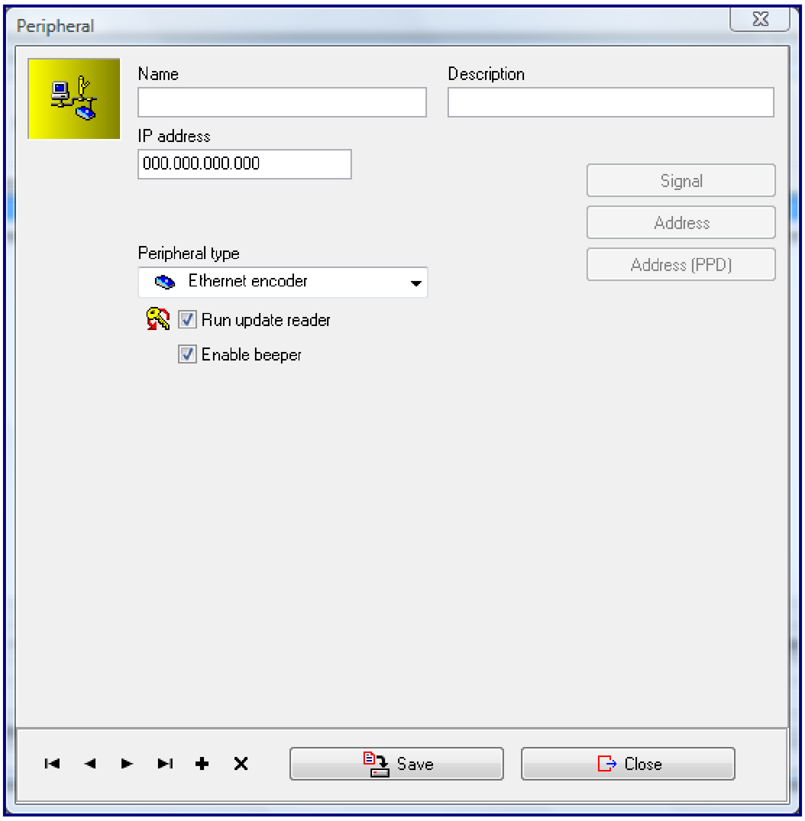
- The top buttons have the following functions:

- SCAN. Can be used for on line wall readers and updaters. It will inform the operator about the communication status for the online device. A green icon means good communication; a red icon means that there is some problem.

- SIGNAL: this button can only be used for updaters, not for on line wall readers. It makes the updater to beep and blink for a while, to locate it, if we are not sure about its physical location.

- ADDRESS: this button can be used for on line wall readers and up daters. After pressing the CLR button for some seconds, (while the green led is blinking) it is necessary to press the ADDRESS button, so the selected IP address will be caught by the on line device. If we do not receive an error message, it is assumed that the IP address has been properly caught by the online device.

- Always make sure that an IP address is free and available, when you are going to assign it to an online device.



Name

Description

IP address 000.000.000.000

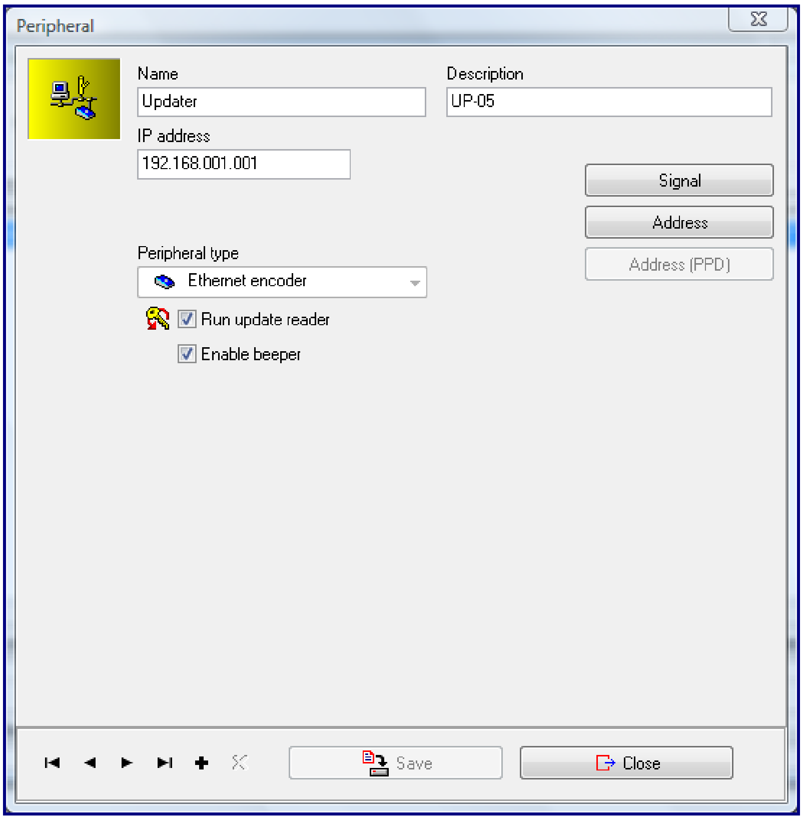
Peripheral type: Ethernet encoder

☑ Run update reader

☑ Enable beeper

We are going to create an updater in our example. This operation can only be made if we are working with the peripheral master computer, (TOOLS/OPTIONS/ON LINE).

Let´s click the new button in the PERIPHERAL LIST and we can give a name to the device. Also it is necessary to write an IP address for it, and select between ETHERNET ENCODER and ON LINE CONTROL UNIT.

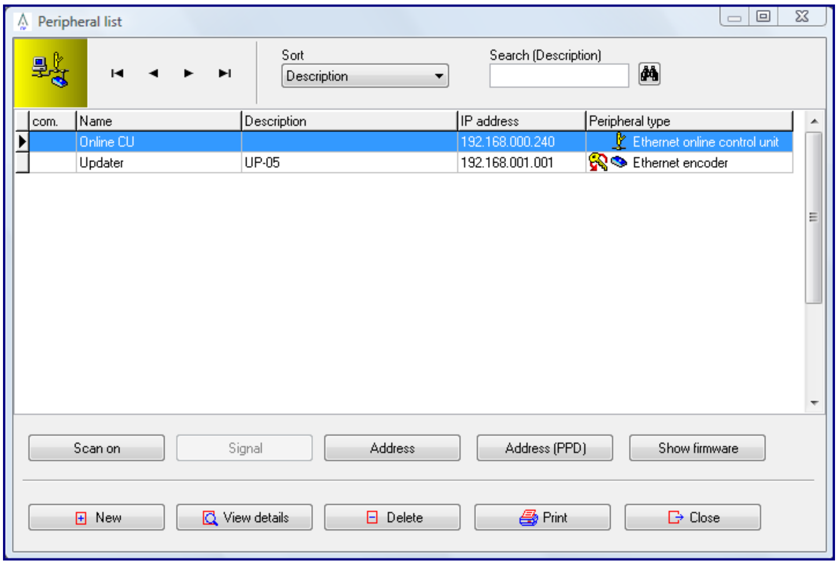


Name: Updater
Description: UP-05
IP address: 192.168.001.001
Peripheral type: Ethernet encoder
☑ Run update reader
☑ Enable beeper

It is necessary to tick off the check box RUN UPDATE READER if we are creating an on line updater.

If we want the updater to beep while in operation, let´s tick off the ENABLE BEEPER check box also. Then, changes must be saved and we can assign the IP address to this device.

The updater will be working continuously, and it will update any staff card which is inserted, giving it a new expiration time which is the one shown in TOOLS/OPTIONS/USER. The updater will also transmit the black list regarding the cancelled user keys. The updater does not update guest cards, it updates staff cards.



com.	Name	Description	IP address	Peripheral type
	Online CU		192.168.000.240	Ethernet online control unit
	Updater	UP-05	192.168.001.001	Ethernet encoder

Peripheral Initialization

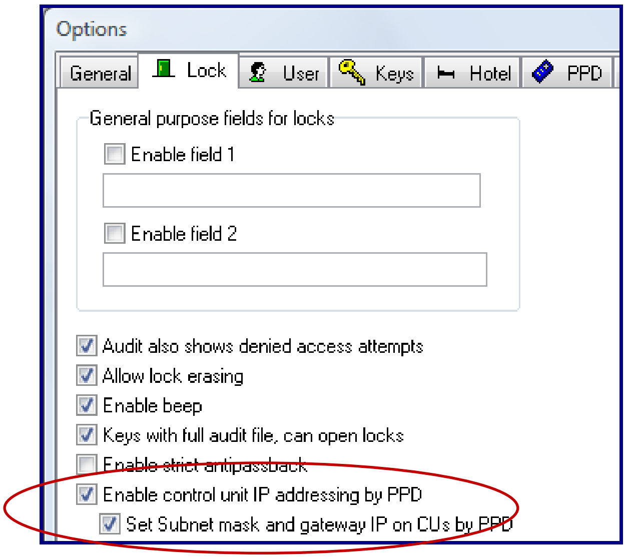
It is necessary to press the CLR button in the updater circuit for 4 seconds until the green LED starts blinking, and then, we must press the ADDRESS button in the software, and wait for some seconds.

It is also possible to address a CU located on a different LAN by using the PPD addressing. It is only needed to download the online doors data to the PPD and initialize the CU manually.

The PPD MUST have the FW version 01.07 or above.

Usually, when the PC sends some data to the CU, the CU answers through the same channel where the request has come. On some installation, the router used, re-route the CU's answer through another channel. In order to work with this type of router, it is possible to set a Subnet mask and a Gateway. To do so, the following is needed;

The "Set Subnet mask and Gateway IP" check box must be activated.



Options

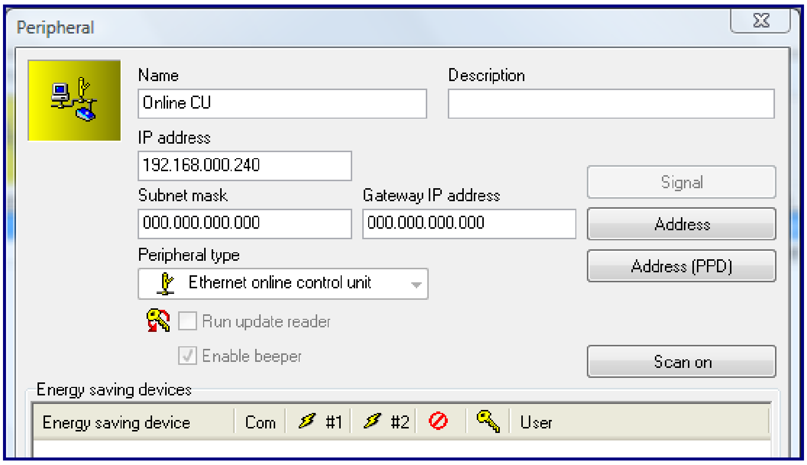
General purpose fields for locks

□ Enable field 1

□ Enable field 2

☑ Audit also shows denied access attempts
☑ Allow lock erasing
☑ Enable beep
☑ Keys with full audit file, can open locks
□ Enable strict antipassback
☑ Enable control unit IP addressing by PPD
☑ Set Subnet mask and gateway IP on CUs by PPD

On the peripheral window, fill the fields with the right Subnet mask address and with the Gateway IP address. Once all this is done, it is needed to use to use the PPD to initialize the CU as told just above.



Peripheral

Name: Online CU
Description:
IP address: 192.168.000.240
Subnet mask: 000.000.000.000
Gateway IP address: 000.000.000.000
Peripheral type: Ethernet online control unit
□ Run update reader
☑ Enable beeper

Energy saving devices

Energy saving device	Com	#1	#2			User

The CU and its Ethernet board must have the following version in order to work with the Subnet mask and Gateway IP;

CU5000 board version: **02.01** or above
Ethernet SVN board version: **01.40** or above

Inhibit Master communication

In certain properties, administrators prefer, for the sake of simplicity, centralising all the software in a unique server machine and running them remotely from workstations through a remote framework, such as Citrix or MS Terminal

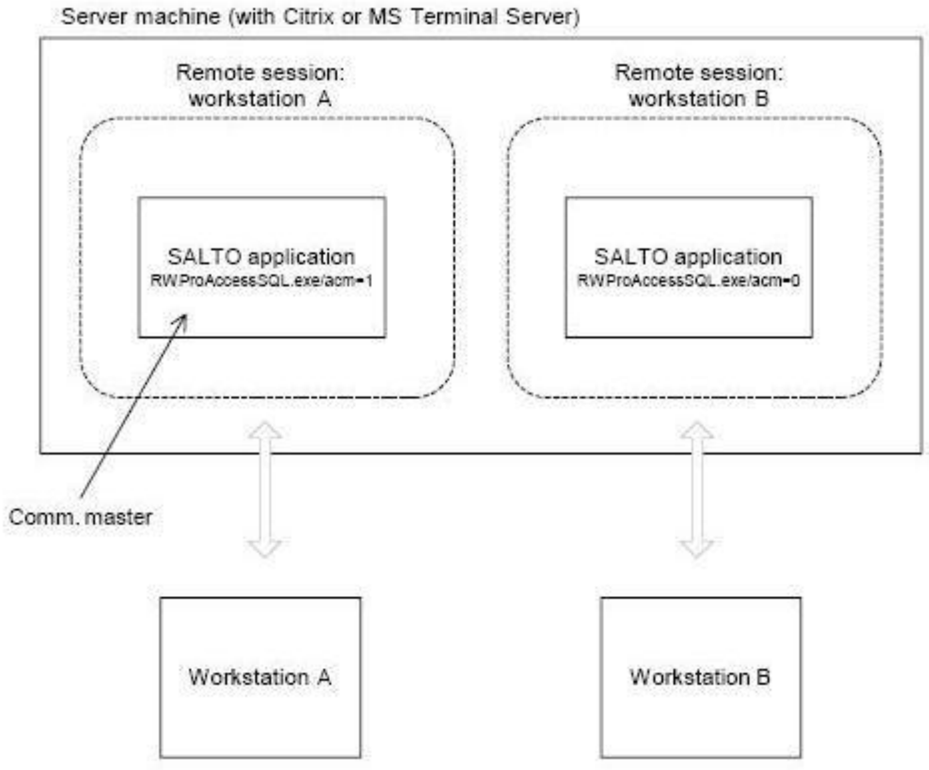
Server. If this is your case, you must take into account the following considerations:

In order to avoid mixing-up local configuration parameters among workstations, there should exist a separated SALTO folder per workstation within the server machine. Each of these SALTO folders should contain the same files as described in the “Installation” section, that is, the SALTO executable file, the message files (*.txt) and, most importantly, the configuration file (cnfg.ini). For example, let’s imagine that there are two workstations A and B from which remote sessions will be opened to run SALTO software within a server machine. In this case, the server machine should have got two SALTO folders (say SALTO_A and SALTO_B) containing the SALTO files as described above. Every Windows session opened from workstation A should be working with the same folder SALTO_A, whereas Windows sessions from workstation B should use folder SALTO_B.

Under Citrix or MS Terminal Server it is possible to run different SALTO instances within the same server machine (though only one SALTO instance per Windows session). This is not problematic by itself except if you have declared the server machine as being the comm. master. In this case, all the SALTO instances within the server machine will try to work in comm. Master mode, though only one of them will eventually be successful (normally, the one that was started first). If you need a particular instance to run as comm. master (no matter if it was started first or last), you must use the command line parameter ‘acm’ (Allow Comm. Master): if this parameter is set to 0, then the comm. master feature will be disabled. On the contrary, if this parameter is set to 1 (default value), the comm. master mode will be just allowed (though not necessarily enabled). Therefore, the SALTO instance that you want to work as comm. master should have got “/acm=1” in the command line and the rest of the instances ‘‘/acm=0’’ (see picture below).

```
C:\?\RWProAccessSQL.exe /acm=0 <- This disables comm. master mode
C:\?\RWProAccessSQL.exe /acm=1 <- This allows comm. master mode
```

In summary, note that two conditions are required for a given SALTO instance to work in comm. master mode: firstly, it must be running in the machine declared as the comm. master; secondly, the ‘acm’ command line parameter, if exists, must be different from 0



Encoder and PPD firmware update

Note: This software option is exclusively limited to the E6000, E7000, EH and E9000 and just to edit cards belonging to system never used by SALTO.

The software permits you to update the key encoder.

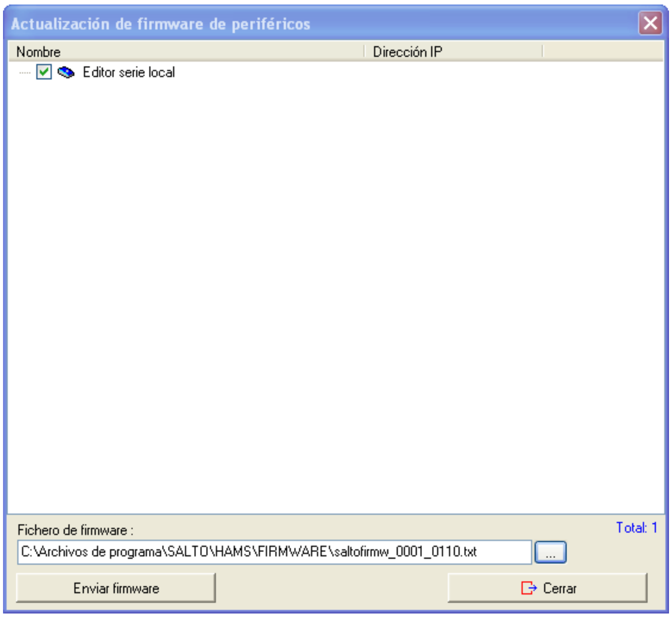
To update the encoder’s firmware you need to go to menu: TOOLS/CONFIGURATION/LOCAL OPTIONS. And click on” Show Firmware”

Next, a screen will appear (Fig.1) This screen will show you all the encoders that are available in our system.

Select the encoder or the encoders that you want to update.

Choose the root where the firmware update is located in our hard disc, clicking on the button with three points (…) located close to the firmware file field.

To transfer the update to the encoder, click on “Send Firmware”



Actualización de firmware de periféricos

Nombre	Dirección IP
☑ Editor serie local	

Fichero de firmware : C:\Archivos de programa\SALTO\HAMS\FIRMWARE\saltofirmw_0001_0110.txt

Total: 1

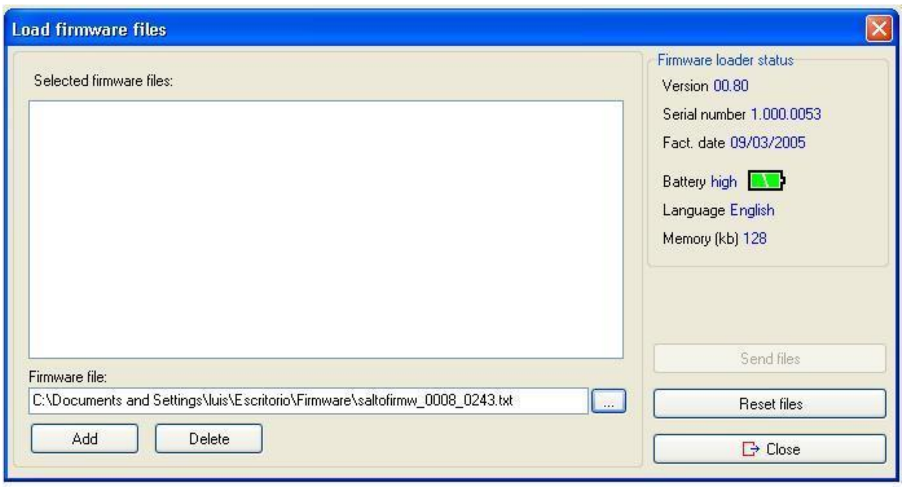
Update the readers:

Important: Please check the reference and lot number of the escutcheon and contact Salto to see if is able to be updated. The E6000, E7000, EH and E9000 could be updated.

The software includes an option to update the readers depending on its technology and manufacturing date. To do this, we will need a special PPD which will be provided for this sort of installations.

When we will click on the PPD icon a special window to configure it the PPD will pop up.

We will need to load those files to the PPD and next, it will necessary to update the readers.



Load firmware files

Selected firmware files:

Firmware file: C:\Documents and Settings\luis\Escritorio\Firmware\saltofirmw_0008_0243.txt

Firmware loader status
Version 00.80
Serial number 1.000.0053
Fact. date 09/03/2005
Battery high
Language English
Memory (kb) 128

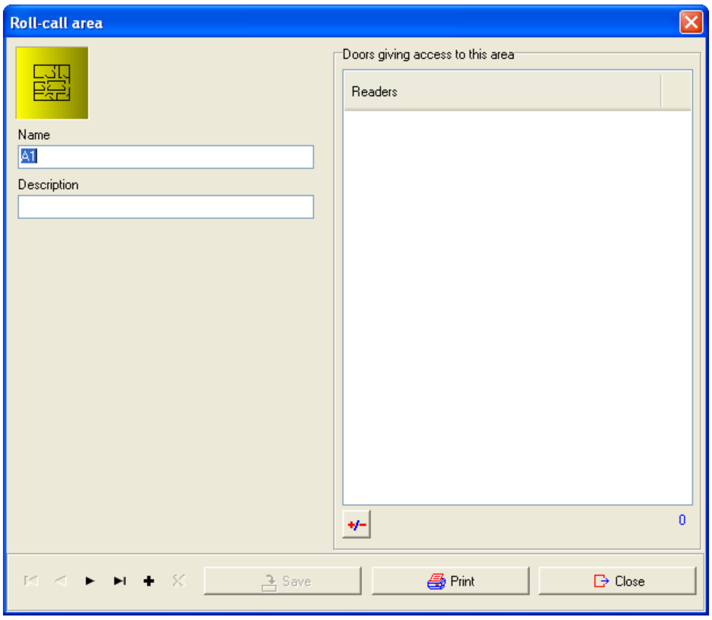
Roll-Call:

This option allows to know how many and which users are in a "Roll-Call" area in every moment. The information on "Roll-Call" areas is automatically updated every minute.

This option is enabled in the menu: TOOLS/ CONFIGURATION/ GENERAL OPTIONS/ ADVANCE/ ROLL-CALL

How to create a Roll-Call area:

In order to create a Roll-Call area we have to go to the menu: DATA/ ROLL-CALL AREA.



Roll-call area

Name: A1

Description:

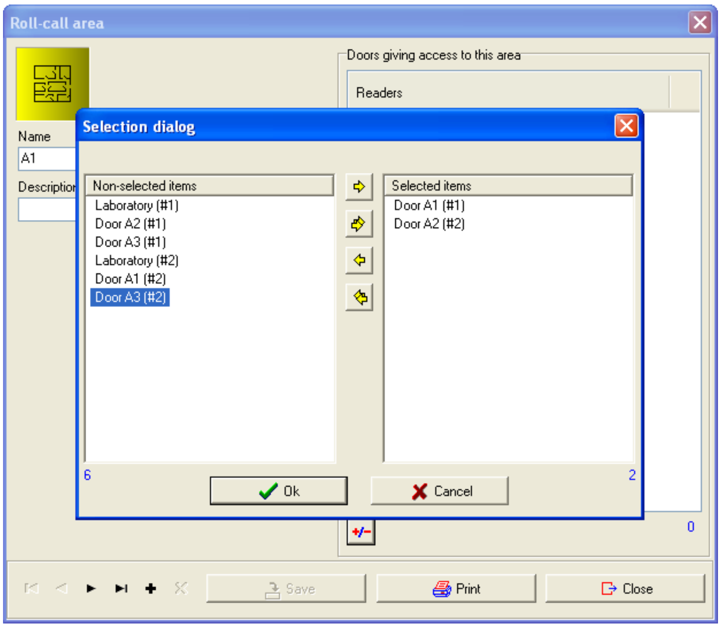
Doors giving access to this area

Readers

0

(Fig 2)

For each Roll-Call area we have to define the online readers that give access to that area. To do this we press the +/- button and a selection screen will appear where for each online door we can find the two readers **(#1 y #2).**



Name: A1

Description

Non-selected items
- Laboratory (#1)
- Door A2 (#1)
- Door A3 (#1)
- Laboratory (#2)
- Door A1 (#2)
- Door A3 (#2)

6

Selected items
- Door A1 (#1)
- Door A2 (#2)

2

0

We have to choose which of the two readers is the entrance to the area reader and pass it to the other side in the selection window.

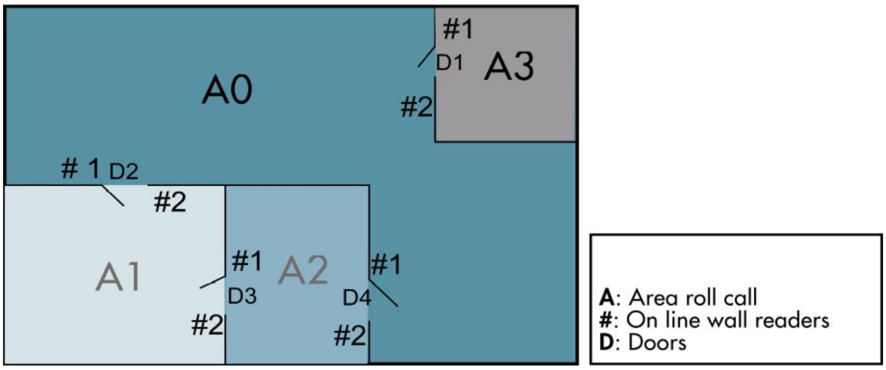
Note: Once we have created all the areas that we want to control we have to create one area more.

Extra Area:

This area will be the reference where we will find thye users when they are not in any of the first created Roll-Call areas. In this software feature there is a very important concept: "Users do not exit an area but enter another one". If we don´t create this area, the software will not be able to interpretate the exit of an area unless this exit is the entry to another area.

In order to create this area we have to select all the online WR that give exit to the previous Roll-Call areas and are not entrance to an already defined area.

Example:



In the example we have defined the different Roll-Call areas that we want to control (A1, A2, A3)

A1: entrance readers: D2 (#1), D3 (#1)
A2: entrance readers: D3 (#2), D4 (#1)
A3: entrance readers: D1 (#2)

Once we have defined this Roll-Call area is necessary to create a new area A0. This area will show us How many and What Users are not in this areas (A1, A2, and A3)

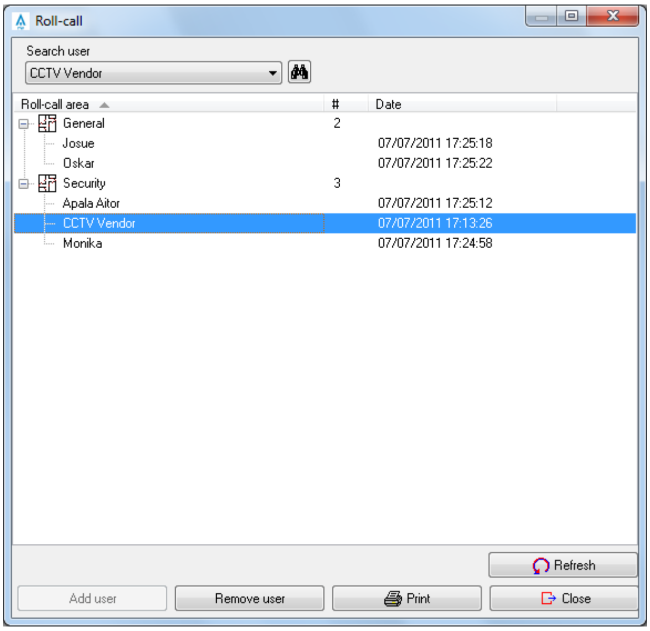
A0 will have the following configuration:

A0: entrance readers: D1(#1), D2 (#2), D4 (#2)

Monitoring of Roll-Call areas

To access to the information that the Roll-Call areas provide to us we have to go to the menu PERIPHERALS/ ROLL-CALL.

The Roll Call window will show the number of users and visitors in each of the defined Roll Call Areas, including their names and the time and date they went into that area.



Search user: CCTV Vendor

Roll-call area	#	Date
General	2	
Josue		07/07/2011 17:25:18
Oskar		07/07/2011 17:25:22
Security	3	
Apala Aitor		07/07/2011 17:25:12
CCTV Vendor		07/07/2011 17:13:26
Monika		07/07/2011 17:24:58

(Fig. 2)

As can be seen in the picture above, if a user or visitor has to be located, it can be searched by selecting their name in the list, and clicking in the search button. The name will be highlighted, and located.

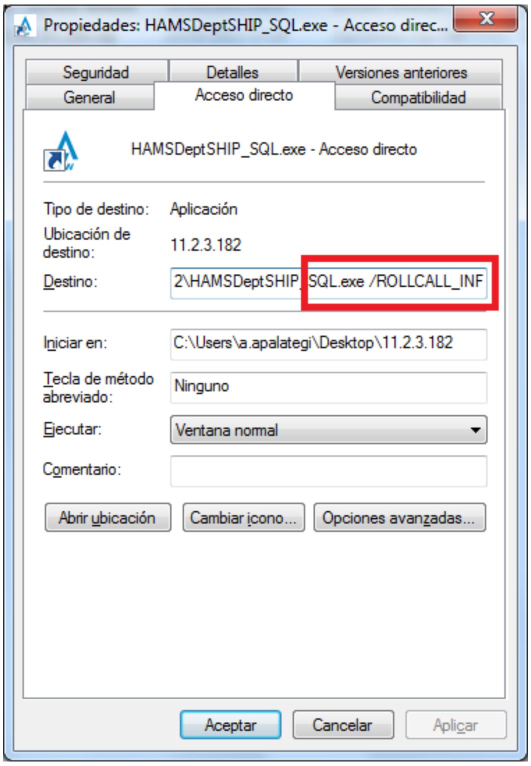
There is an option to add or remove users manually. To do this, we have to press the buttons of the bottom of the screen.

There is also a pop-up window with these options if we press the right button of the mouse.

Note: Be aware that the SALTO Roll-Call feature depends on the physical door control installation of your building. Without such hardware (i.e. turnstiles) it will be difficult to obtain a correct Roll-Call information report, as people can exit and enter in access levels without presenting their id-carriers.

The Pro Access / HAMS software allows the system user to run the software on a limited mode that would show the Roll Call window to monitor where the users are located.

The advanced parameter /ROLLCALL_INF should be added to the Target of the shortcut:



Propiedades: HAMSDeptSHIP_SQL.exe - Acceso direc...

HAMSDeptSHIP_SQL.exe - Acceso directo

Tipo de destino: Aplicación

Ubicación de destino: 11.2.3.182

Destino: 2\HAMSDeptSHIP_SQL.exe /ROLLCALL_INF

Iniciar en: C:\Users\a.apalategi\Desktop\11.2.3.182

Tecla de método abreviado: Ninguno

Ejecutar: Ventana normal

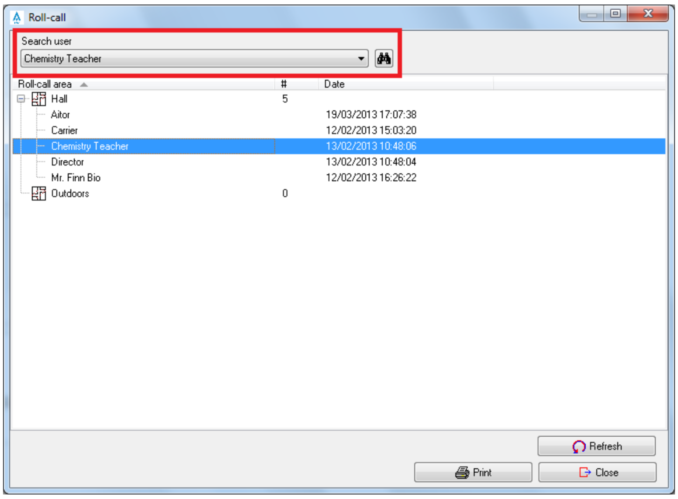
Comentario:

(Fig. 3)

This advance parameter will make the software run as a single full screen Roll Call monitoring window when double clicking over the shortcut.

This mode allows a reduced use of the normal Roll Call function included in the Pro Access / HAMS software.

The location of a specific user can be found by selecting the user on the drop down list, and clicking over the binocular button:



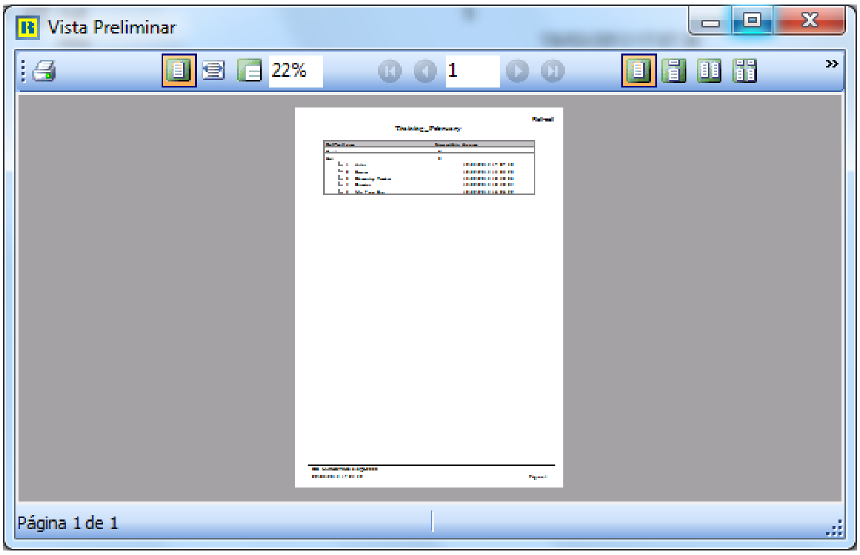
Roll-call

Search user: Chemistry Teacher

Roll-call area	#	Date
Hall	5	
Aitor		19/03/2013 17:07:38
Carrier		12/02/2013 15:03:20
Chemistry Teacher		13/02/2013 10:48:06
Director		13/02/2013 10:48:04
Mr. Finn Bio		12/02/2013 16:26:22
Outdoors	0	

(Fig. 4)

The Print button allows printing the report that includes the location of the users of the system, as can be seen below:



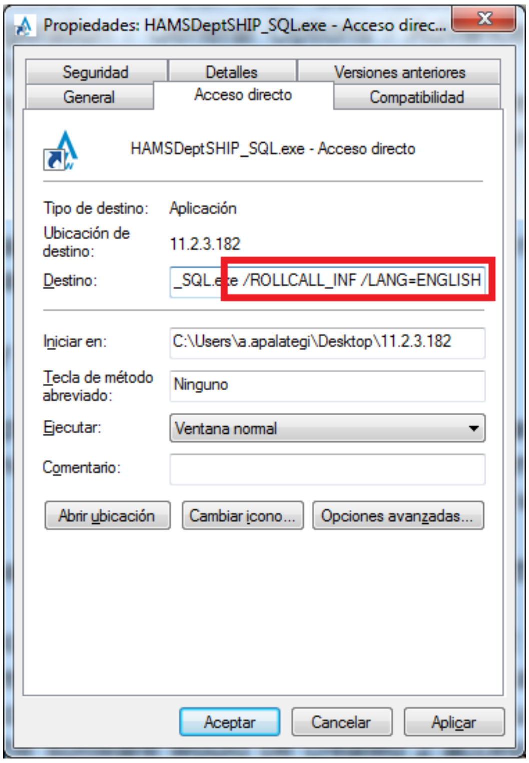
(Fig. 5)

Finally, the Close button will shut down the Roll Call monitoring window, quitting the software itself.

IMPORTANT NOTES: Roll Call function must be active in the Tools / Configuration / General Options / Advanced tab in order to run this specific Roll Call mode.

Running this Roll Call mode does not require any password. It will be shown just by running the shortcut of the software.

This Roll Call monitoring mode can also be run with a specific language always, just by adding the /LANG=selectedlanguage, as can be seen below:



Propiedades: HAMSDeptSHIP_SQL.exe - Acceso direc...

HAMSDeptSHIP_SQL.exe - Acceso directo

Tipo de destino: Aplicación

Ubicación de destino: 11.2.3.182

Destino: _SQL.exe /ROLLCALL_INF /LANG=ENGLISH

Iniciar en: C:\Users\a.apalategi\Desktop\11.2.3.182

Tecla de método abreviado: Ninguno

Ejecutar: Ventana normal

Comentario:

(Fig.6)

Limited occupancy

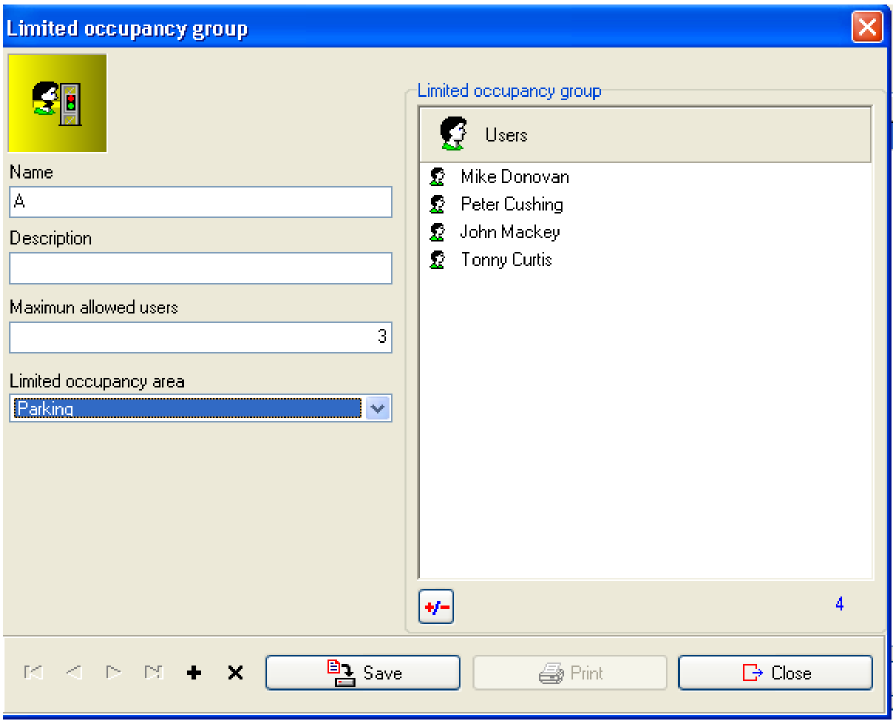
This option allows creating different zones and access levels. On the access levels we can delimit the maximum number of users. So we will be able to create different access levels with different access capability.

The managing of this tool has to be done through a CU50EN or higher.

The most usual case and example for that would be a common parking where different companies would have access. For example company A could have a maximum capacity of 6 users and company B 8 users. On the software would be created 2 groups A and B with a maximum of 6 and 8 users respectively. Then when the 7 user of A wants to entrance he will have to wait until one of those A users leaves the parking.

To configure that option we have to go Tools/General options/Advance and enable the Limited occupancy option.

Then on data we will see the limited occupancy available. The first thing that has to be done will be to create a new group:



Name

A

Description

Maximun allowed users

3

Limited occupancy area

Parking

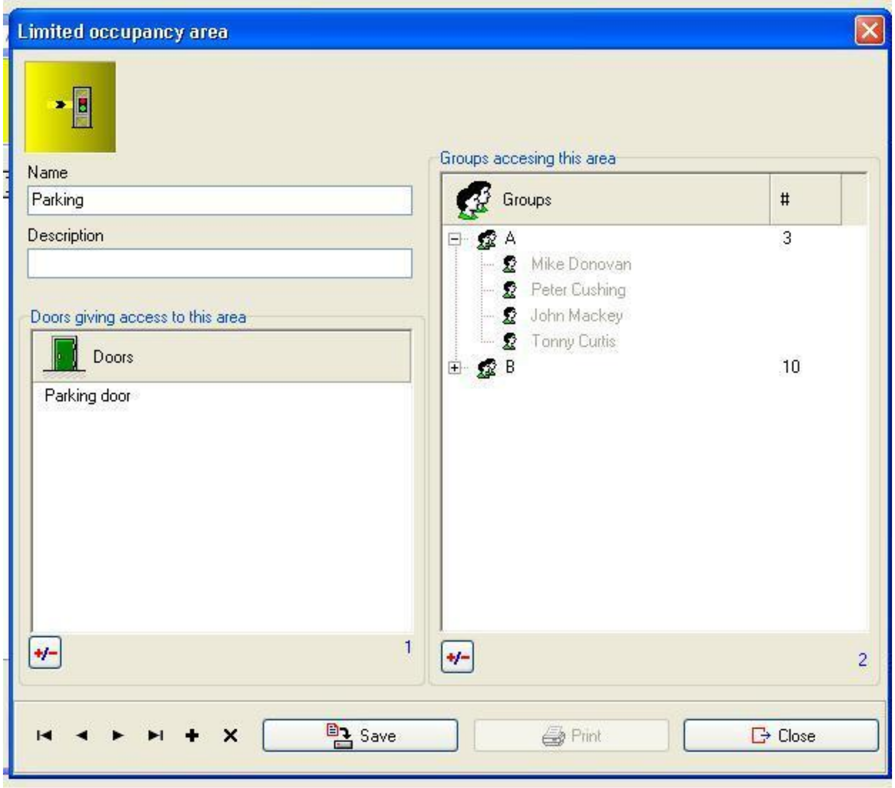
Limited occupancy group

Users
Mike Donovan
Peter Cushing
John Mackey
Tonny Curtis

4

On that window has to be created the Group name, the maximum users allowed, the users who belong to the group and the area which the group has access.

After that we can create the zone:



Name: Parking

Description:

Doors giving access to this area

Doors
Parking door

1

Groups accesing this area

Groups	#
A	3
Mike Donovan	
Peter Cushing	
John Mackey	
Tonny Curtis	
B	10

2

In the same way it has to be specified the on line door which delimits the zone and the access levels which can access to the area.

Something important to keep in mind is that all the users who belong to each of those access levels and have access to the parking need to have access to the online door which delimit the area. In this example each of the user would need access to the Parking door (online)

Going back to the example if Mike Donovan, Peter Cushing and John Mackey have already inside the parking Tony Curtis would have to wait until one of those 3 leave the area.

Language. Language change.

As default language, Salto RW software for access control has English, although you may modify it clicking on the LANGUAGES key from the front desk main menu, and choosing another amongst those in the list.

Log-out. Change operator.

When the administrator wants to make use of the access control application, he has only to click on the LOG OUT key from the front desk menu to get the login window again.

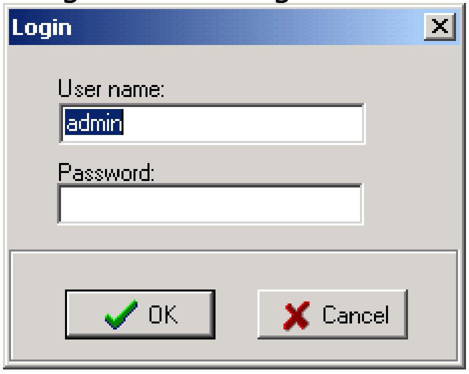


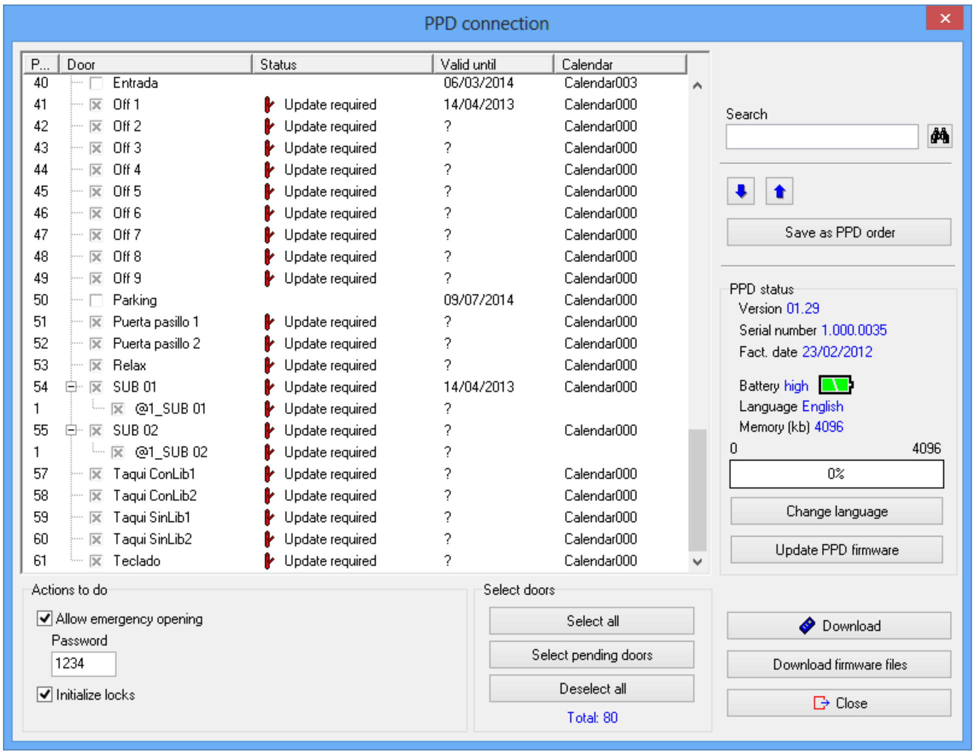
Figure 81

The administrator can then type in their password (if it was set on the TOOLS/OPERATORS AND PERMISSIONS option), and click on the OK button to enter the program with administrator privileges.

PPD connection. Portable programmer.

You may need to connect PPD to your computer in order to carry out an emergency opening, for example. This may be necessary if a door electronic lock runs out of battery.

To perform an emergency opening, follow the steps explained below. Then, click on the PPD menu option from the front desk main menu.



PPD connection

P...	Door	Status	Valid until	Calendar
40	□ Entrada		06/03/2014	Calendar003
41	☒ Off 1	Update required	14/04/2013	Calendar000
42	☒ Off 2	Update required	?	Calendar000
43	☒ Off 3	Update required	?	Calendar000
44	☒ Off 4	Update required	?	Calendar000
45	☒ Off 5	Update required	?	Calendar000
46	☒ Off 6	Update required	?	Calendar000
47	☒ Off 7	Update required	?	Calendar000
48	☒ Off 8	Update required	?	Calendar000
49	☒ Off 9	Update required	?	Calendar000
50	□ Parking		09/07/2014	Calendar000
51	☒ Puerta pasillo 1	Update required	?	Calendar000
52	☒ Puerta pasillo 2	Update required	?	Calendar000
53	☒ Relax	Update required	?	Calendar000
54	☒ SUB 01	Update required	14/04/2013	Calendar000
1	☒ @1_SUB 01	Update required	?	
55	☒ SUB 02	Update required	?	Calendar000
1	☒ @1_SUB 02	Update required	?	
57	☒ Taqui ConLib1	Update required	?	Calendar000
58	☒ Taqui ConLib2	Update required	?	Calendar000
59	☒ Taqui SinLib1	Update required	?	Calendar000
60	☒ Taqui SinLib2	Update required	?	Calendar000
61	☒ Teclado	Update required	?	Calendar000

Search

PPD status
Version 01.29
Serial number 1.000.0035
Fact. date 23/02/2012
Battery high
Language English
Memory (kb) 4096
0 4096
0%

Actions to do
☑ Allow emergency opening
Password
1234
☑ Initialize locks

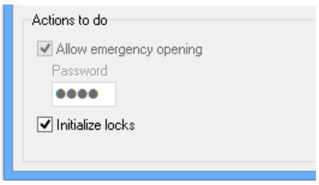
Select doors

Total: 80

Figure 78

On the lower left-hand side corner we find a box called *ACTIONS TO DO.* In this box, select the ALLOW EMERGENCY OPENING option. Select the door from the door list you want the PPD to be able to open in emergency. Once this option will be selected, the “Password” field will be enabled for you to use a password in the PPD.

If a password has been pre-selected from the GENERAL OPTION on the PPD tab, this option will be greyed and the password will be always required.



Actions to do
☑ Allow emergency opening
Password
●●●●
☑ Initialize locks

In any of these two previous cases, the PPD will require this password before opening the door.

If the field is left blank, no password will be required for emergency opening from PPD.

And then, click on the DOWNLOAD button to transfer data on to the PPD.

NOTE that this option will only work on PPD since FW version 01.29.

- Data transfer will last a few seconds. When the progress bar reaches al 100%, disconnect the PPD from the serial cable and go to the door that requires an emergency opening.

- Turn the PPD on, clicking once on the red key, and choose EMERGENCY OPENING menu option. Use the scroll arrows provided to browse through the menu options.

- Click on the green key to validate you choice. PPD display will prompt you this message window: CONNECT TO LOCK.

- Connect PPD to the lock using a communication cable equipped with a special card on its end. Insert this card on the slot so that the conductors point towards chip side.

- You will hear the lock engine sound, and in a few seconds, the door will be ready to be opened and the PPD display will prompt you this message window: DOOR OPEN,

We recommend you to replace lock batteries of the newly opened door immediately. Salto locks are equipped with 3 alkaline batteries, LR03 AAA, 1, 5 V model.

After battery replacement, you must update the electronic lock with PPD, since when running out of batteries, the internal clock stops and time zones and calendars settings are lost. In order to learn how to perform a PPD update, refer to the PPD Smart User´s Manual that you will find included in the RW software CD-ROM.

Audit Trail. Collecting door opening data.

It is possible to know who has opened a hotel door and at what time, by performing an audit trail on our facilities doors. To audit a door, follow the following procedure (only if it is an off line door):

- Take PPD and go to the door to be audited. Turn PPD on clicking once on the red key and browse the COLLECT OPENINGS menu option.

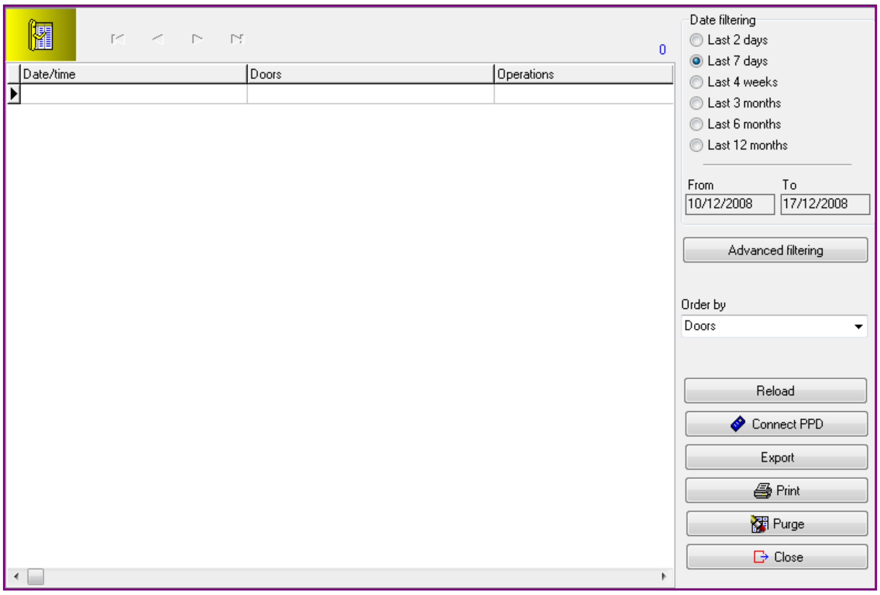
- Press the green key to validate the choice, and PPD will prompt you a CONNECT TO LOCK message.

- Connect PPD to lock using a communication cable which ends on a special card and you will see data transfer in progress.

- Go back to the computer and connect the PPD to the serial port.

- If you get the CONNECT TO LOCK message on PPD display, press the red key to upgrade one menu level. If you fail to do so, you will not be able to communicate with your computer.

- Click on the AUDIT TRAIL option from the front desk menu. A window like the one below will be displayed:



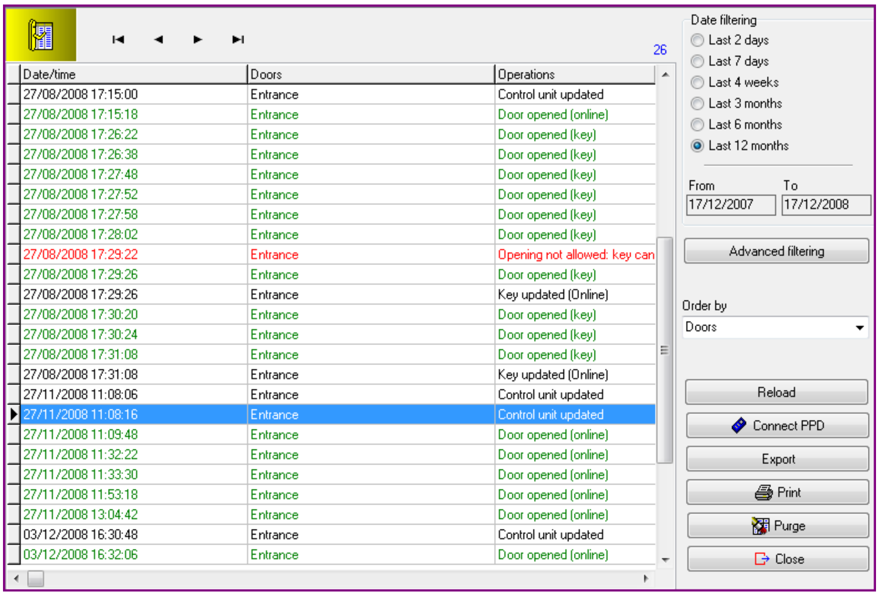
Date filtering
○ Last 2 days
● Last 7 days
○ Last 4 weeks
○ Last 3 months
○ Last 6 months
○ Last 12 months

From 10/12/2008 To 17/12/2008

Order by: Doors

Date/time	Doors	Operations

Now, click on the CONNECT PPD button in the application active window. The data collected with PPD will be shown in the window. SORT BY button may help you to view data according to the most convenient criterion, by date, by user, by door, etc.



Date filtering
○ Last 2 days
○ Last 7 days
○ Last 4 weeks
○ Last 3 months
○ Last 6 months
● Last 12 months

From 17/12/2007 To 17/12/2008

Order by: Doors

Date/time	Doors	Operations
27/08/2008 17:15:00	Entrance	Control unit updated
27/08/2008 17:15:18	Entrance	Door opened (online)
27/08/2008 17:26:22	Entrance	Door opened (key)
27/08/2008 17:26:38	Entrance	Door opened (key)
27/08/2008 17:27:48	Entrance	Door opened (key)
27/08/2008 17:27:52	Entrance	Door opened (key)
27/08/2008 17:27:58	Entrance	Door opened (key)
27/08/2008 17:28:02	Entrance	Door opened (key)
27/08/2008 17:29:22	Entrance	Opening not allowed: key can
27/08/2008 17:29:26	Entrance	Door opened (key)
27/08/2008 17:29:26	Entrance	Key updated (Online)
27/08/2008 17:30:20	Entrance	Door opened (key)
27/08/2008 17:30:24	Entrance	Door opened (key)
27/08/2008 17:31:08	Entrance	Door opened (key)
27/08/2008 17:31:08	Entrance	Key updated (Online)
27/11/2008 11:08:06	Entrance	Control unit updated
27/11/2008 11:08:16	Entrance	Control unit updated
27/11/2008 11:09:48	Entrance	Door opened (online)
27/11/2008 11:32:22	Entrance	Door opened (online)
27/11/2008 11:33:30	Entrance	Door opened (online)
27/11/2008 11:53:18	Entrance	Door opened (online)
27/11/2008 13:04:42	Entrance	Door opened (online)
03/12/2008 16:30:48	Entrance	Control unit updated
03/12/2008 16:32:06	Entrance	Door opened (online)

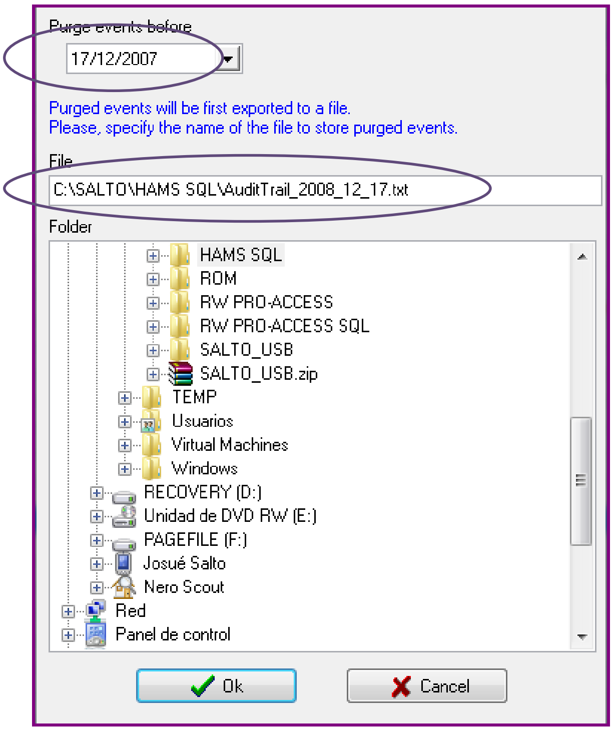
Picture 79

The FILTER box allows you to view the audit trail regarding only to a particular user, door, operator … You will have to select the user, door, operator… particular item in the field SAME AS.

In RED, are shown the denied openings, by users that don't have access to the door or guest that don't have Access to a room.

PURGE: It is highly recommended to make audit trail purges at least once a month. When the audit trail is not too full, all the communications with online units are faster and lighter, i.e. communication with Control Units, upload and download of PPD contain, and moreover, the search for audits is also faster.

For the purge, press the Purge button shown in Picture 79, and a window like the one shown below will appear.



Purge events before: 17/12/2007

Purged events will be first exported to a file.
Please, specify the name of the file to store purged events.

File: C:\SALTO\HAMS SQL\AuditTrail_2008_12_17.txt

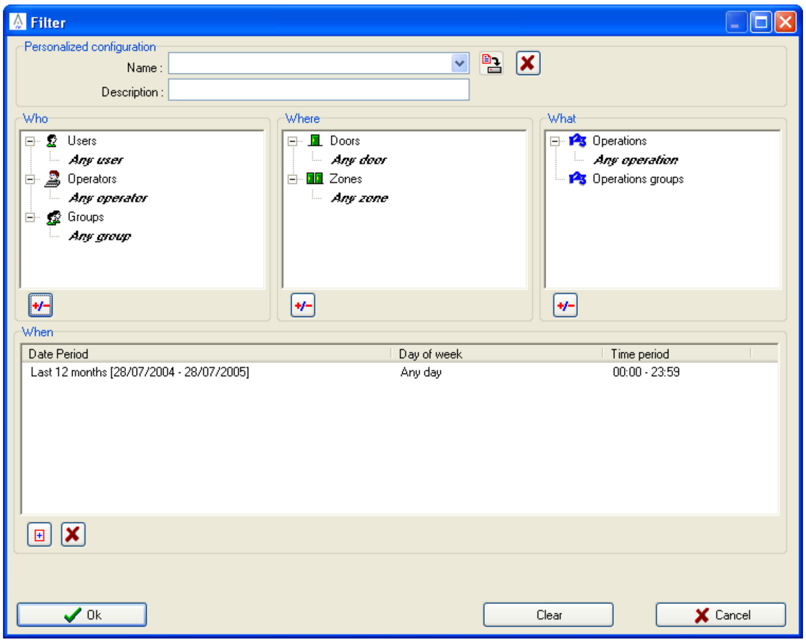
- All events previous to the date indicated in the "Purge events before" field will purged.
- On "File" and "Folder" fields, it is possible to select where the TXT created file will have to be kept
- If you want to turn the text in this window into a text file, just press the EXPORT button and you will be able to choose the folder to where you want to save this file.

- If you want to have all this information printed on paper, just press the PRINT button and you will have the AUDIT TRAIL printed out. Make sure a printer is connected to your computer.

- It is recommended, from time to time, to purge the AUDIT TRAIL window because the audit trail data will increasingly occupy more computer memory. In order to do this, just press the PURGE button.

New filter

To make and save special filters we have to press the "Advanced Filtering" button in the Audit Trail window. Once we press this button we will find the following window (Fig. 1)



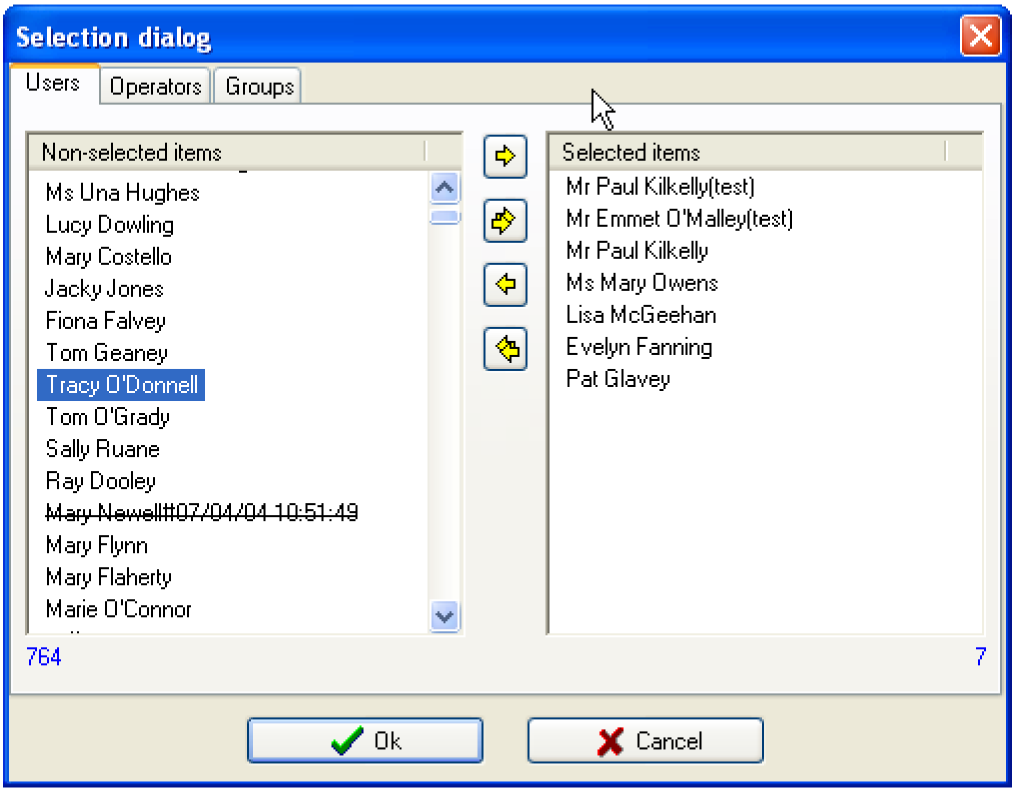
Date Period	Day of week	Time period
Last 12 months [28/07/2004 - 28/07/2005]	Any day	00:00 - 23:59

(Fig 1)

This filter allows to filter the events by Who (user, operator and or access level) has done the event, Where (Door, Zone) it has been done. What operation or kind of operation has done and When has the operation been done.

Create a new filter

We have to select who we want to filter. To do this, we have to press the +/- button in the botton of the "Who" window. We will see the following window (Fig. 2):



Non-selected items
Ms Una Hughes
Lucy Dowling
Mary Costello
Jacky Jones
Fiona Falvey
Tom Geaney
Tracy O'Donnell
Tom O'Grady
Sally Ruane
Ray Dooley
~~Mary Newell#07/04/04 10:51:49~~
Mary Flynn
Mary Flaherty
Marie O'Connor

764

Selected items
Mr Paul Kilkelly(test)
Mr Emmet O'Malley(test)
Mr Paul Kilkelly
Ms Mary Owens
Lisa McGeehan
Evelyn Fanning
Pat Glavey

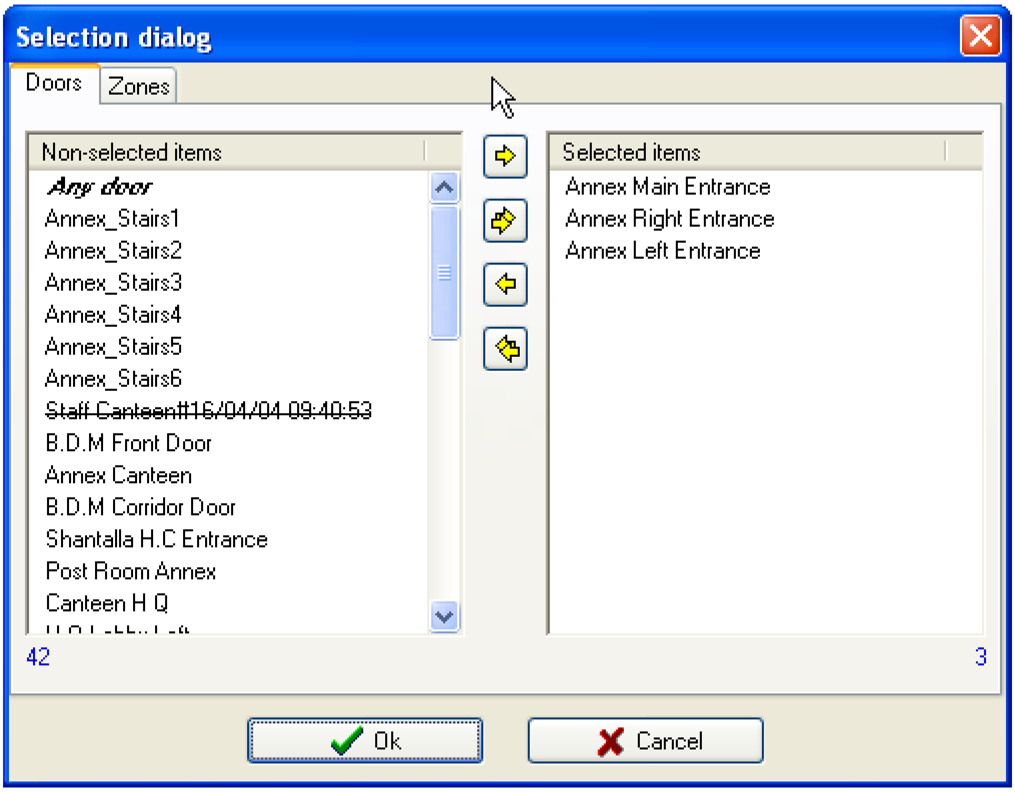
7

(Fig. 2)

We have to select the users that we want to filter, in the same way we will select the operators and access levels of users that we want to filter.

Note: If we want all the Users, Operators, Access levels to be shown we will leave in the right side f the window any user, any operator and any access level.

The next selection window is Where. This window allows us to select the Doors and Zones that we want to Filter. We will press again the +/- button to select the Doors and Zones that we want to filter.(Fig. 3)



Selection dialog

Doors | Zones

Non-selected items:

- ***Any door***
- Annex_Stairs1
- Annex_Stairs2
- Annex_Stairs3
- Annex_Stairs4
- Annex_Stairs5
- Annex_Stairs6
- ~~Staff Canteen#16/04/04 09:40:53~~
- B.D.M Front Door
- Annex Canteen
- B.D.M Corridor Door
- Shantalla H.C Entrance
- Post Room Annex
- Canteen H Q

42

Selected items:

- Annex Main Entrance
- Annex Right Entrance
- Annex Left Entrance

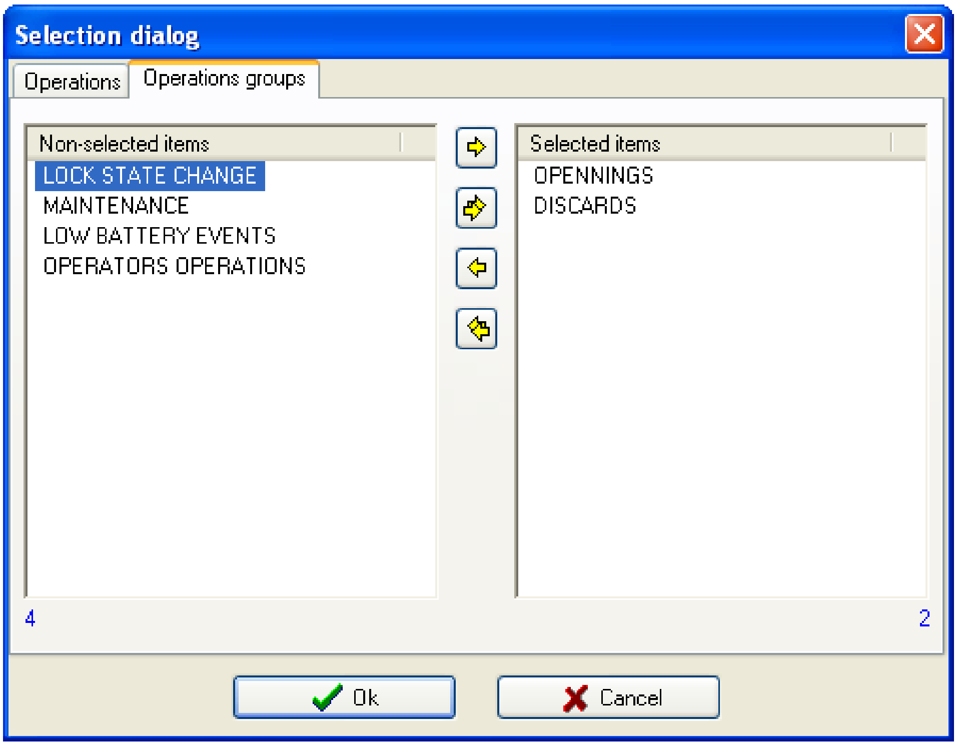
3

(Fig 3)

In the same way we will include the Zones that we would like to filter.

Note: If we want to show the events in all Doors or Zones we will select the option “Any door” or “any zone”

The filter also permits to select the operation or access level of operations that we want to Filter. To do this we will press +/- button and we will select the operation or Access level of operations that we will want to filter. (Fig 4)



Selection dialog

Operations | Operations groups

Non-selected items
- LOCK STATE CHANGE
- MAINTENANCE
- LOW BATTERY EVENTS
- OPERATORS OPERATIONS

4

Selected items
- OPENNINGS
- DISCARDS

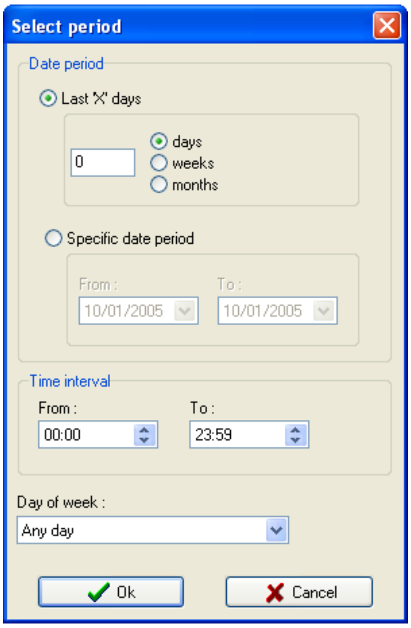
2

✓ Ok | ✗ Cancel

(Fig. 4)

Note: If we want to see all the operations that these users have made we will select "any operation"

Finally we can select the dates of our filter. To do this we will press the ⊞ button and we will see the following window (Fig 5):



Select period

Date period

● Last 'X' days

0 — ● days ○ weeks ○ months

○ Specific date period

From : 10/01/2005 To : 10/01/2005

Time interval

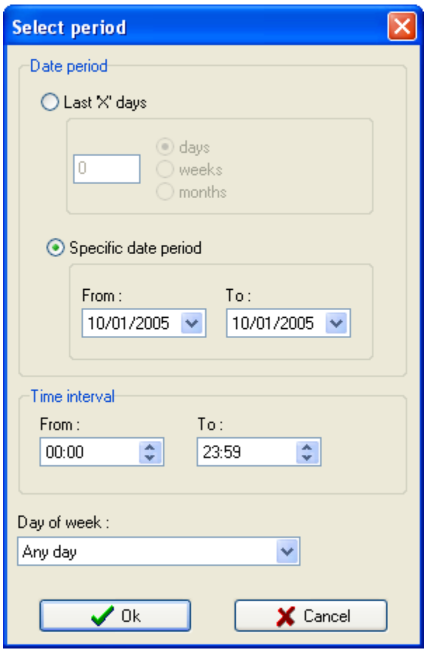
From : 00:00 To : 23:59

Day of week : Any day

✓ Ok | ✗ Cancel

(Fig. 5)

This window allows us select the filter period: selecting the last days, weeks or months or from other side select the period between 2 dates (by activating the option "Use specific period time" as well as the day or days of the week that we want to filter. (Fig. 6).



Select period

Date period

○ Last 'X' days

0 ● days ○ weeks ○ months

● Specific date period

From : 10/01/2005 To : 10/01/2005

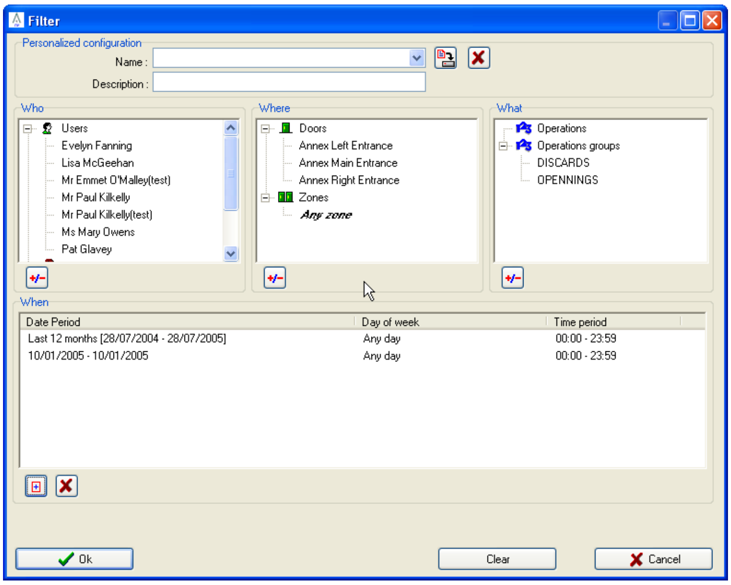
Time interval

From : 00:00 To : 23:59

Day of week : Any day

(Fig. 6)

Once we have made all the selections we will see them in the following window (Fig 7).



Filter

Personalized configuration

Name :

Description :

Who

- Users
  - Evelyn Fanning
  - Lisa McGeehan
  - Mr Emmet O'Malley(test)
  - Mr Paul Kilkelly
  - Mr Paul Kilkelly(test)
  - Ms Mary Owens
  - Pat Glavey

Where

- Doors
  - Annex Left Entrance
  - Annex Main Entrance
  - Annex Right Entrance
- Zones
  - *Any zone*

What

- Operations
- Operations groups
  - DISCARDS
  - OPENNINGS

When

Date Period	Day of week	Time period
Last 12 months [28/07/2004 - 28/07/2005]	Any day	00:00 - 23:59
10/01/2005 - 10/01/2005	Any day	00:00 - 23:59

(Fig. 7)

To see the results of the filters we press the ✓ OK button.

The selected filter can be exported to a txt. and xls. File by pressing the export option.

Save the filter:

The software allows to save these filters for future times. To do this we have to press 💾 button. We have to fill the name and description of the filter.

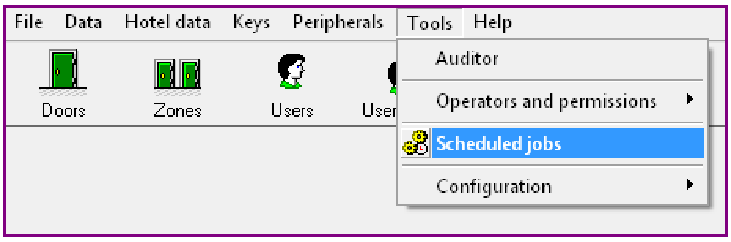
Automatic Audit Trail export

(only software for Service)

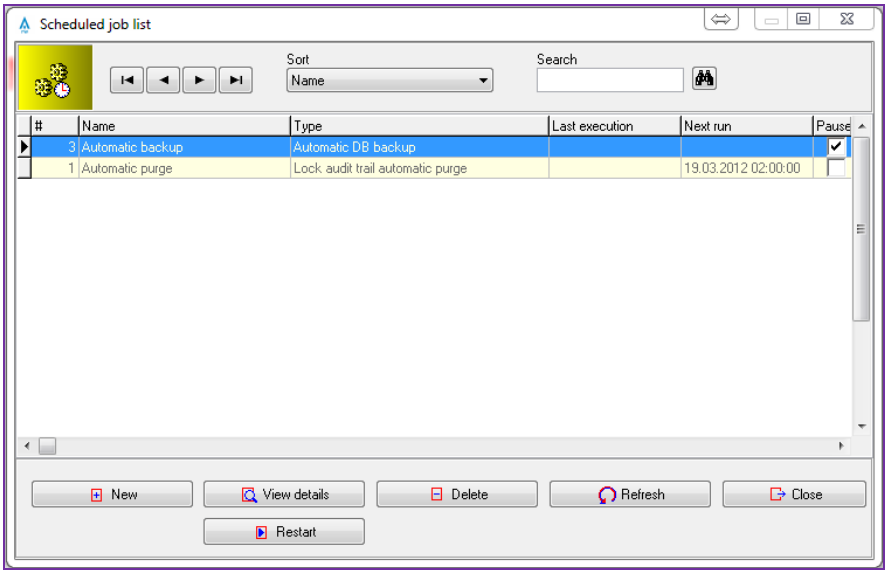
It is possible, to setup the Software to do an automatic export of the audit trail in a CSV File. This will export the audit without deleting the entries in the software So it is still possible to read it by opening the Audit Trail. This option is done to give the opportunity to deliver the audit trail to other software solutions, for example a time recording system.

Keep in mind, when the events are purged from Audit trail, it is not possible to read it anymore, because they will be deleted from the database.

To enable this parameter go to Scheduled jobs in the Tools Menu.



This list shows all automatic tasks that are created in the system. For the automatic export create a new one and choose “Lock audit trail automatic export”. When pressing Ok, the Wizard will open.



Scheduled job list

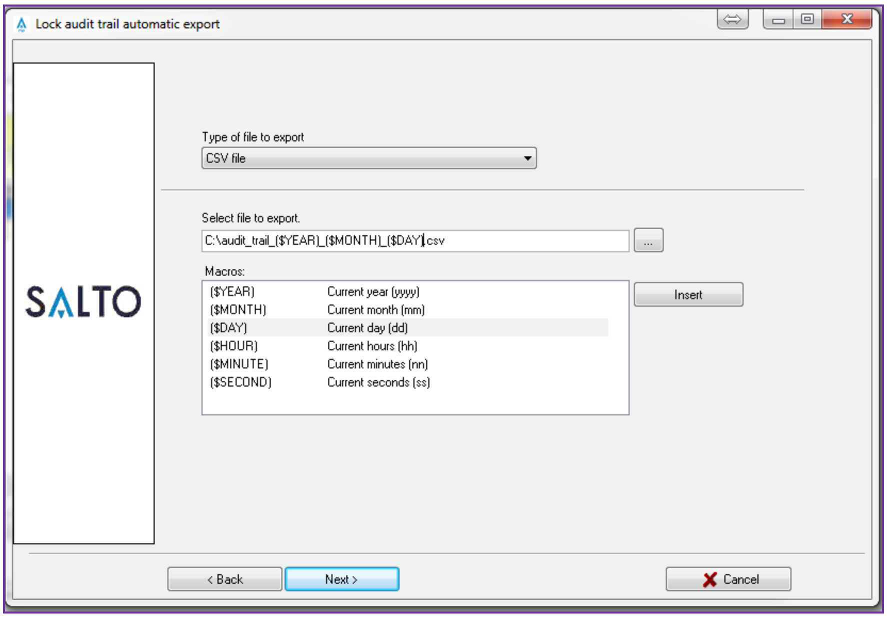
Sort: Name

Search:

#	Name	Type	Last execution	Next run	Pause
3	Automatic backup	Automatic DB backup			☑
1	Automatic purge	Lock audit trail automatic purge		19.03.2012 02:00:00	□

The wizard appears and shows that the set up will start.

Into the "Select file to export" we must place a name for the file that will be exported.



Lock audit trail automatic export

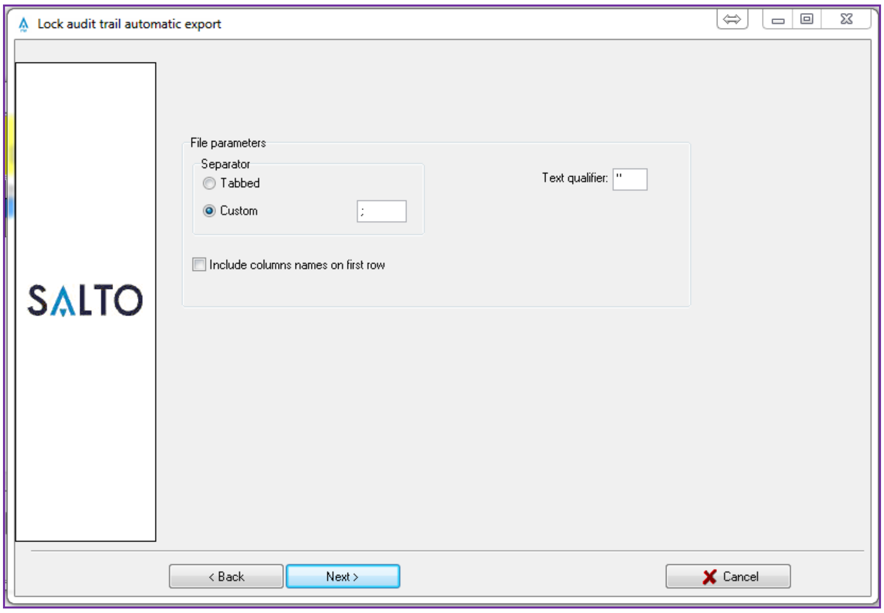
Type of file to export: CSV file

Select file to export: C:\audit_trail_($YEAR)_($MONTH)_($DAY).csv

Macros:

($YEAR)	Current year (yyyy)
($MONTH)	Current month (mm)
($DAY)	Current day (dd)
($HOUR)	Current hours (hh)
($MINUTE)	Current minutes (nn)
($SECOND)	Current seconds (ss)

In this example it will be stored in C:\ and its name is "audit_trail_ _($YEAR)_($MONTH)_($DAY).csv". This means that when the job gets started on 24.01.2012 the file will be named "audit_trail_2012_01_24.csv". A shown, it is possible to use macros to save the file with a unique name so it is not overwritten by the next file. To add a macro to the filename, place the cursor on the position where the macro is needed, select it from the list and press insert. Then, press next to go on.



Lock audit trail automatic export

File parameters

Separator

○ Tabbed

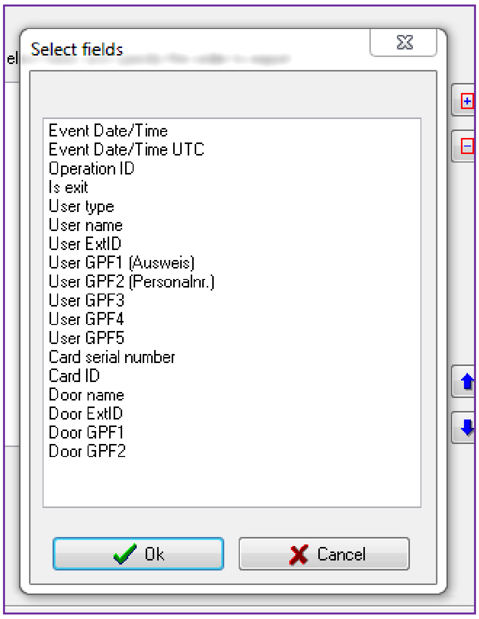
● Custom ;

Text qualifier: "

□ Include columns names on first row

With these parameters, we can specify the way we store the audit trail in the file. Choose the separator, the Text qualifier and also the option to include the column names to the first line of the file. By default "," is uses as field separator and when a value contains spaces the Text qualifier " to surround the complete text position. Next and we go on.

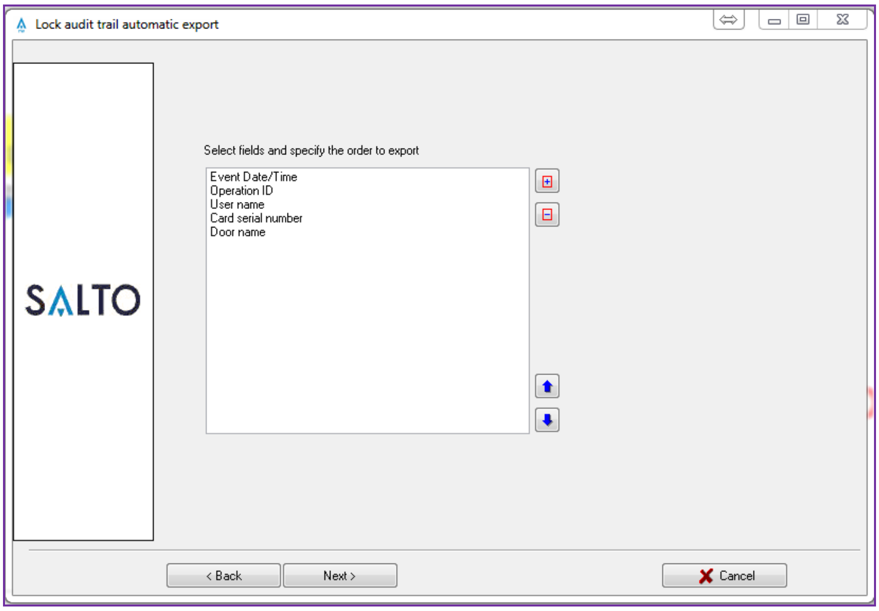
Now, choose what to export and in which arrangement. By pressing the "+" button, add values from a list. To understand the exact meaning of each value, please see the document "SALTOAutomaticExportOfAuditTrail_1_0.pdf". Contact the SALTO partner to request this document.



Select fields

Event Date/Time
Event Date/Time UTC
Operation ID
Is exit
User type
User name
User ExtID
User GPF1 (Ausweis)
User GPF2 (Personalnr.)
User GPF3
User GPF4
User GPF5
Card serial number
Card ID
Door name
Door ExtID
Door GPF1
Door GPF2

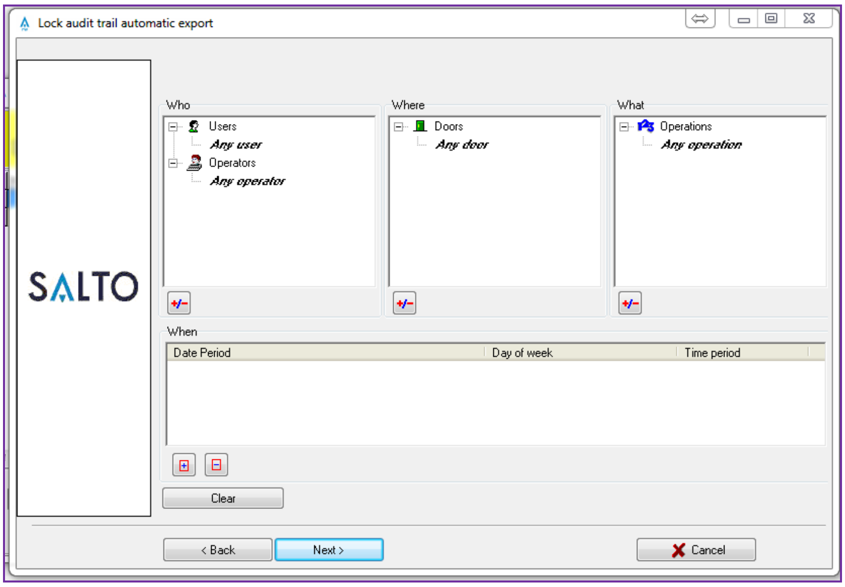
As soon as the configuration is the needed, please click next. The example below, shows a summary of what would be a good export.


Lock audit trail automatic export

Select fields and specify the order to export

Event Date/Time
Operation ID
User name
Card serial number
Door name

On the next window, we can filter the parts that are needed. If left by default, all audits from the audit trail will be exported as who, where, what and when.

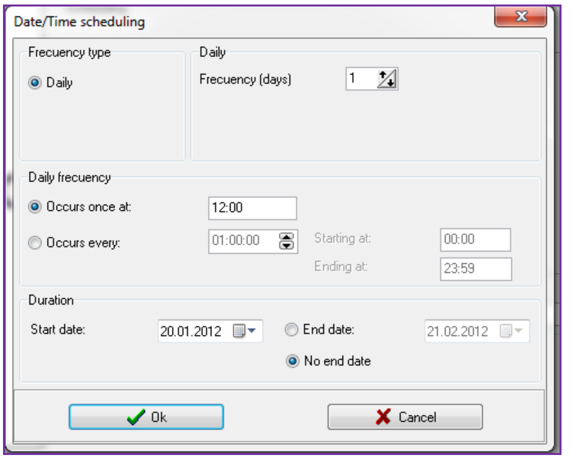

Lock audit trail automatic export

Who: Users – Any user; Operators – Any operator
Where: Doors – Any door
What: Operations – Any operation

When

Date Period	Day of week	Time period

On the last step of the setup, enter the schedule timing and period; when the task will be launched. For this click on the "Schedule" button and setup the prefer values.



Date/Time scheduling

Frecuency type

● Daily

Daily

Frecuency (days) 1

Daily frecuency

● Occurs once at: 12:00

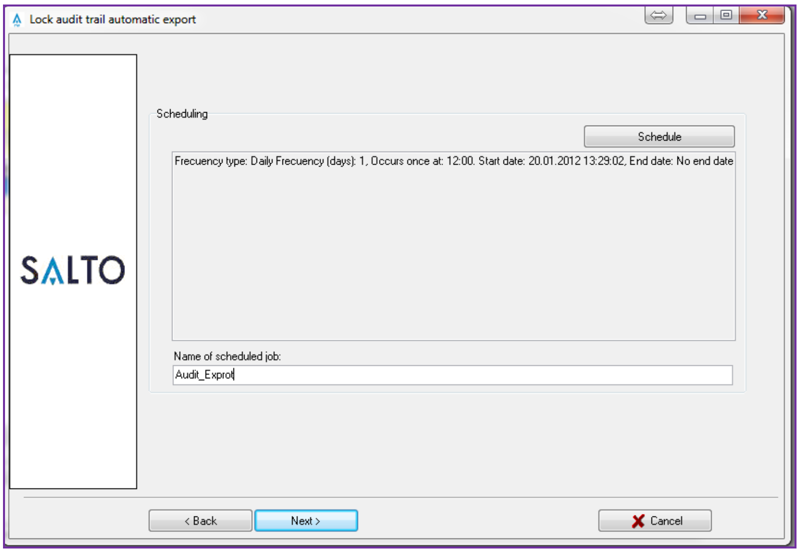
○ Occurs every: 01:00:00 Starting at: 00:00 Ending at: 23:59

Duration

Start date: 20.01.2012 ○ End date: 21.02.2012

● No end date

In the example it starts every day at 12:00 o'clock and start on 20/01/2012. It has no end date. As soon as the Salto Service is running the task will keep running. The task can be paused or deleted from the scheduled task list.



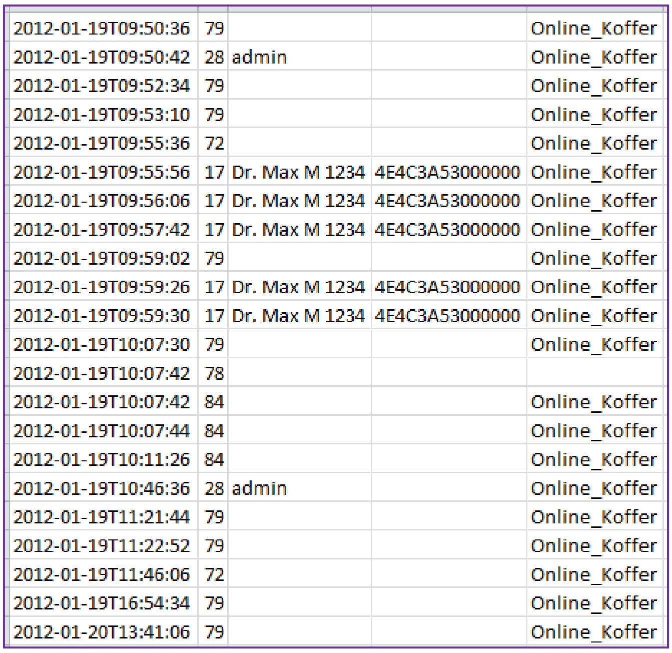
Lock audit trail automatic export

Scheduling

Frecuency type: Daily Frecuency (days): 1, Occurs once at: 12:00. Start date: 20.01.2012 13:29:02, End date: No end date

Name of scheduled job: Audit_Exprot

At the end, a summary will be shown with the set up and the contain of the job. Click Finish and the job will be saved and will start with the next period. If it is the first time, the service could last about 10 min before the task is launched. Next is an example of an exported file:



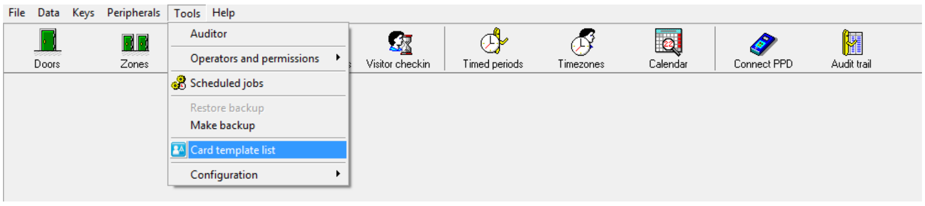
2012-01-19T09:50:36	79			Online_Koffer
2012-01-19T09:50:42	28	admin		Online_Koffer
2012-01-19T09:52:34	79			Online_Koffer
2012-01-19T09:53:10	79			Online_Koffer
2012-01-19T09:55:36	72			Online_Koffer
2012-01-19T09:55:56	17	Dr. Max M 1234	4E4C3A53000000	Online_Koffer
2012-01-19T09:56:06	17	Dr. Max M 1234	4E4C3A53000000	Online_Koffer
2012-01-19T09:57:42	17	Dr. Max M 1234	4E4C3A53000000	Online_Koffer
2012-01-19T09:59:02	79			Online_Koffer
2012-01-19T09:59:26	17	Dr. Max M 1234	4E4C3A53000000	Online_Koffer
2012-01-19T09:59:30	17	Dr. Max M 1234	4E4C3A53000000	Online_Koffer
2012-01-19T10:07:30	79			Online_Koffer
2012-01-19T10:07:42	78			
2012-01-19T10:07:42	84			Online_Koffer
2012-01-19T10:07:44	84			Online_Koffer
2012-01-19T10:11:26	84			Online_Koffer
2012-01-19T10:46:36	28	admin		Online_Koffer
2012-01-19T11:21:44	79			Online_Koffer
2012-01-19T11:22:52	79			Online_Koffer
2012-01-19T11:46:06	72			Online_Koffer
2012-01-19T16:54:34	79			Online_Koffer
2012-01-20T13:41:06	79			Online_Koffer

For more details, please see "SALTOAutomaticExportOfAuditTrail_1_0.pdf" for a more technical documentation.

Badging

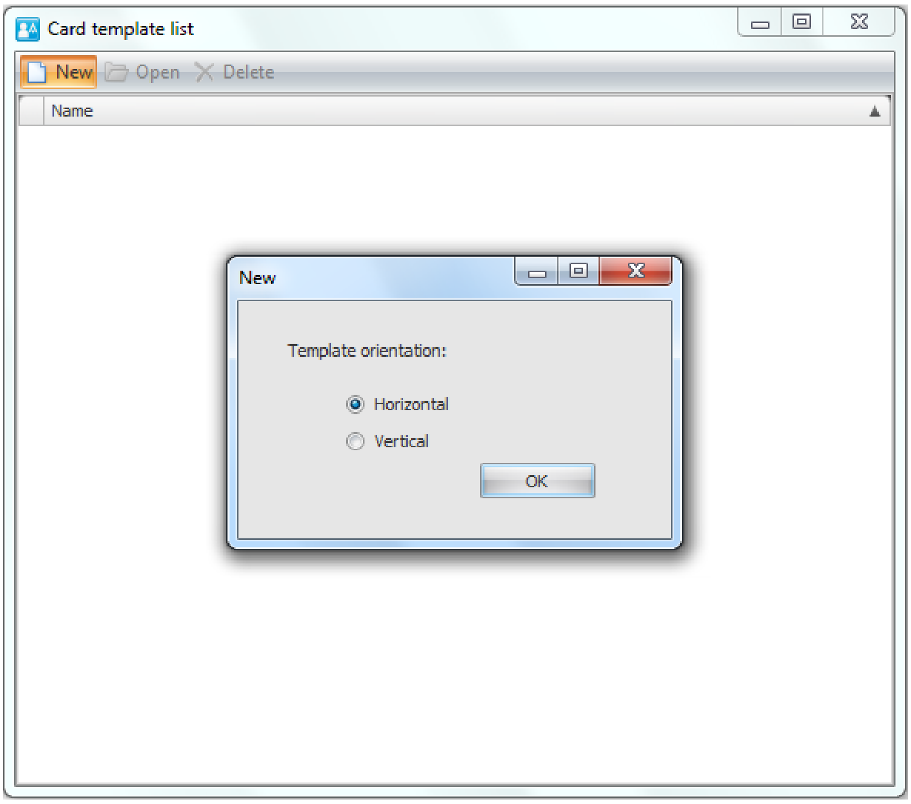
(only for Service).

The SALTO Software allows creating different templates to print the users' cards with them. These templates can include pictures and text, and can be created by using the Card Template List option in the Tools menu, as can be seen in the picture below.



The option will run a separate application that will run over the SALTO Service, and will take the users' information from the active database.

In order to create a cards template, click on the New button and select if the design is going to be Horizontal or Vertical.

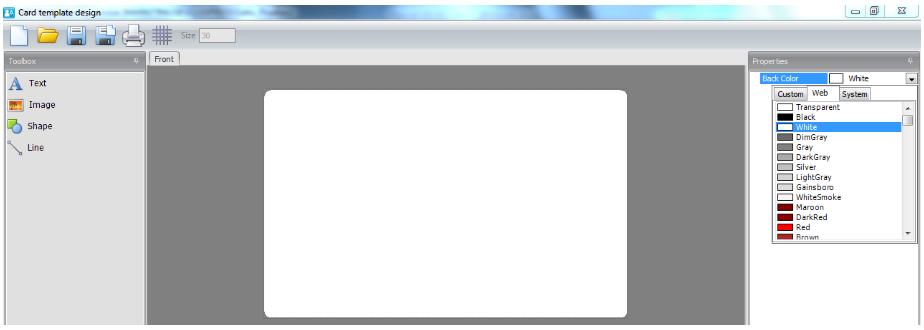


Template orientation:

● Horizontal

○ Vertical

Once the orientation is selected, the rest of the options to design the card will appear, as well as the standard options related to this tool.



Size 30

Back Color: White

In the left hand column, some tools to add elements to the card template can be selected:

TEXT:

This option allows defining the typical text characteristics, like Color, Font, Location and Size.

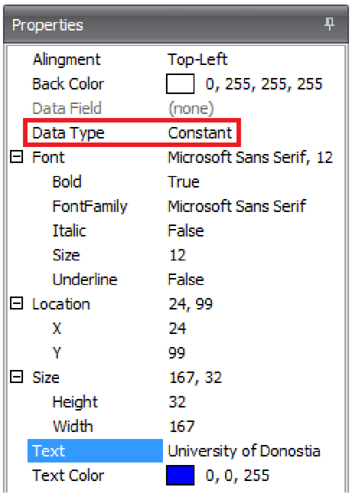
Apart from this option, the Text can be defined to be a Constant Text, or can be a Dynamic Text.

A Constant text is a fixed text that does not change.

A Dynamic text is a text field that changes depending on the set up, and that lays on the information contained in the SALTO database.

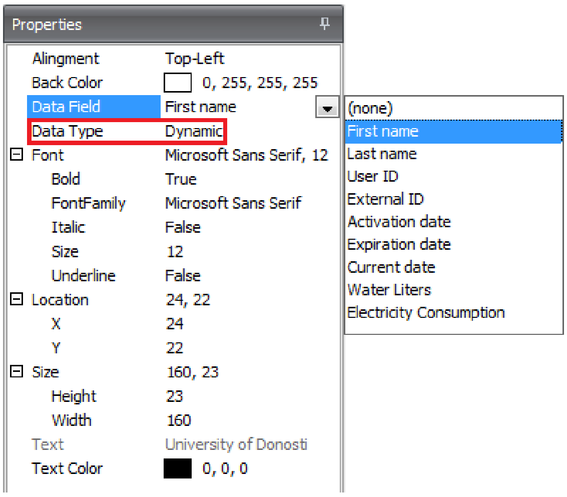
As can be seen in the left picture below, when the Data Type is set up to Constant, the Text can be defined in the TEXT option below (highlighted in blue).

In the other hand, when the Data type is set up to Dynamic, the Data Field option is activated, and different data information belonging to the users in the installation can be included, like First Name, Last Name, User ID, External ID, Activation / Expiration Date, and General Purpose Fields. See picture on the right below.



Properties

Alingment	Top-Left
Back Color	□ 0, 255, 255, 255
Data Field	(none)
Data Type	Constant
⊟ Font	Microsoft Sans Serif, 12
Bold	True
FontFamily	Microsoft Sans Serif
Italic	False
Size	12
Underline	False
⊟ Location	24, 99
X	24
Y	99
⊟ Size	167, 32
Height	32
Width	167
Text	University of Donostia
Text Color	🟦 0, 0, 255



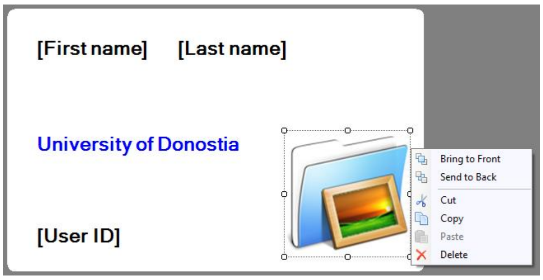
Properties

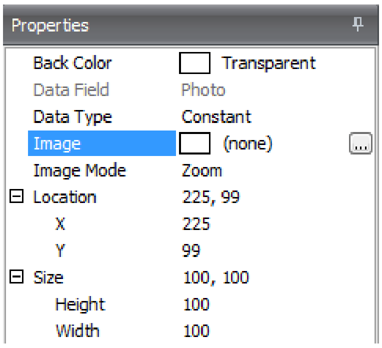
Alingment	Top-Left
Back Color	□ 0, 255, 255, 255
Data Field	First name
Data Type	Dynamic
⊟ Font	Microsoft Sans Serif, 12
Bold	True
FontFamily	Microsoft Sans Serif
Italic	False
Size	12
Underline	False
⊟ Location	24, 22
X	24
Y	22
⊟ Size	160, 23
Height	23
Width	160
Text	University of Donosti
Text Color	■ 0, 0, 0

IMAGE:

Images can be imported into the card design by using this option. As well as in the Text, images could be Constant or Dynamic.

In case Constant is selected, an image to be included in all the cards could be loaded into the template, just by clicking in the three dots button on the right of the Image option.



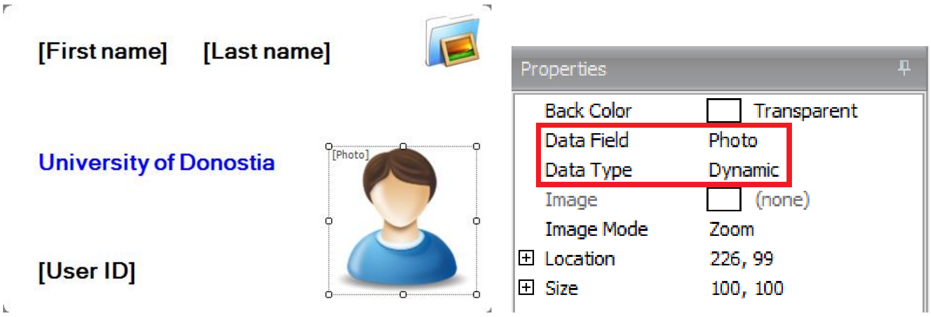


Properties

Back Color	□ Transparent
Data Field	Photo
Data Type	Constant
Image	□ (none)
Image Mode	Zoom
⊟ Location	225, 99
X	225
Y	99
⊟ Size	100, 100
Height	100
Width	100

Pictures can be located in the Front or Back plane of the card, just by clicking with the right button over the picture, and selecting the appropriate option. Other available options are Cut, Copy, Paste or Delete.

Dynamic option allows including the picture already loaded in the User set up window, in the SALTO Software.

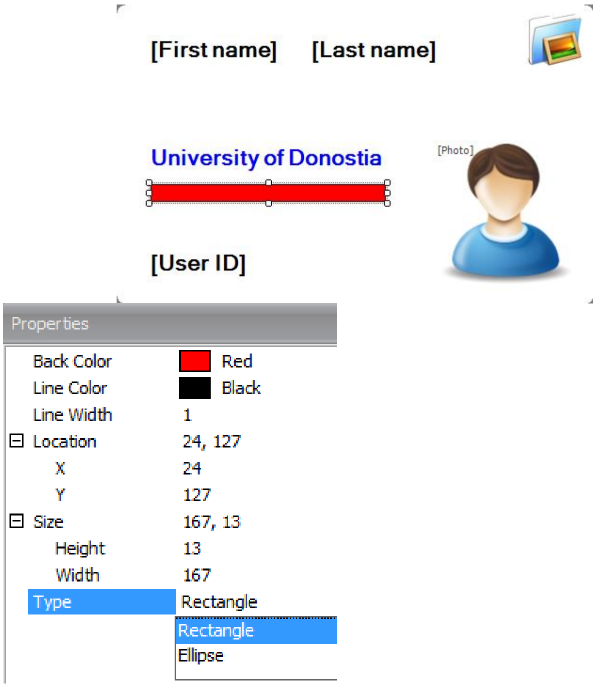


Properties

Back Color	□ Transparent
Data Field	Photo
Data Type	Dynamic
Image	□ (none)
Image Mode	Zoom
⊞ Location	226, 99
⊞ Size	100, 100

SHAPE:

Shapes can be also included in the card design. Rectangles and Ellipse could be added, specifying the back and line colors, as well as the width of the line.

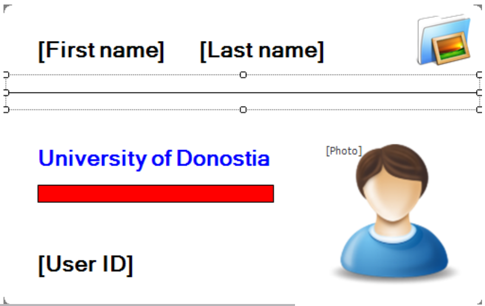


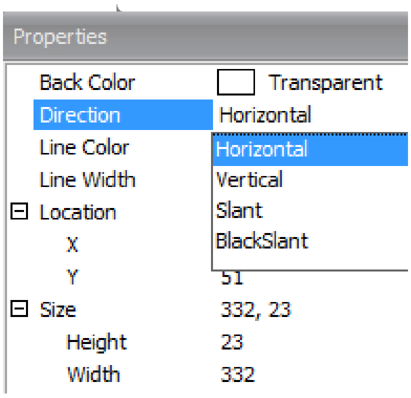
Properties

Back Color	🟥 Red
Line Color	■ Black
Line Width	1
⊟ Location	24, 127
X	24
Y	127
⊟ Size	167, 13
Height	13
Width	167
Type	Rectangle
	Rectangle Ellipse

LINE:

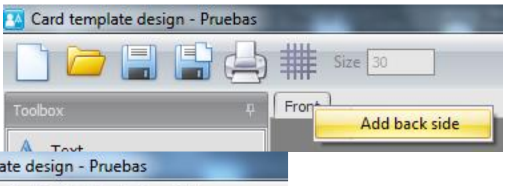
Lines can be added to the design, in different positions: Horizontal, Vertical, Slant and Backslant. Colors and width can also be defined, as can be seen in the pictures below.

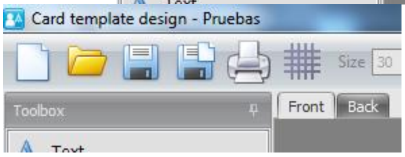



Properties

Back Color	□ Transparent
Direction	Horizontal
Line Color	Horizontal Vertical Slant BlackSlant
Line Width	
⊟ Location	
X	
Y	51
⊟ Size	332, 23
Height	23
Width	332

In case the card is meant to have information in both sides, just by clicking in the Front tab with the right button of the mouse, a new tab for the Back design will appear:

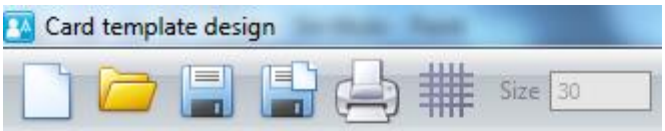




Tools to be used and options for this design would be the same as for the Front side. Please check the explanations above to complete it.

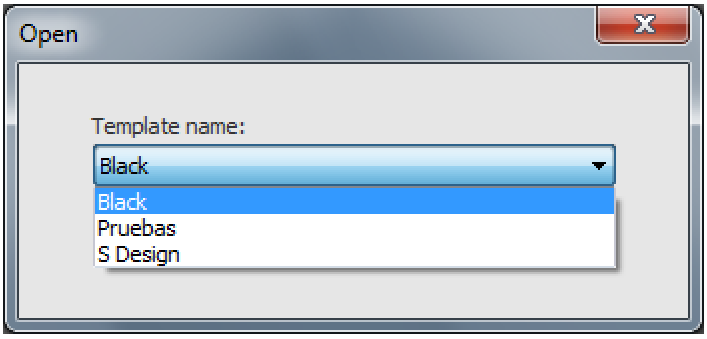
Once the complete design has been done, it has to be saved.

The upper left side of the window contains the general options to manage the different card designs: New, Open, Save, Save As, Print, Grid, and Size (of the Grid).



The New option allows creating new card templates.

The Open option allows selecting any of the already created templates, so they can be modified:

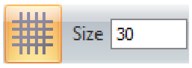


Template name: Black

The Save option allows saving the designs that are finished.

Save As options allows saving the designs with different names, in case it is necessary to sue a design base for different card designs.

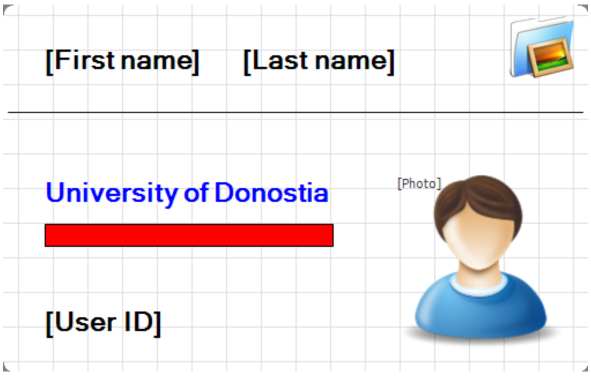
Card designs can be printed into any card printer with the correct drivers related to the Pc's Operating System.



Size 30

A Grid can be added to the card design at the time of designing, so there are reference lines to properly locate the different elements.

The size of this Grid could be changed, so the squares are bigger or smaller.



Department data base configuration

(This option is available on PA Department software or highest)

This document contains basic explanations about the 'department operator' feature. The main goal of this feature is to provide tools for managing independent departments within the same installation and for sharing common access control elements (doors, users, ...) among departments.

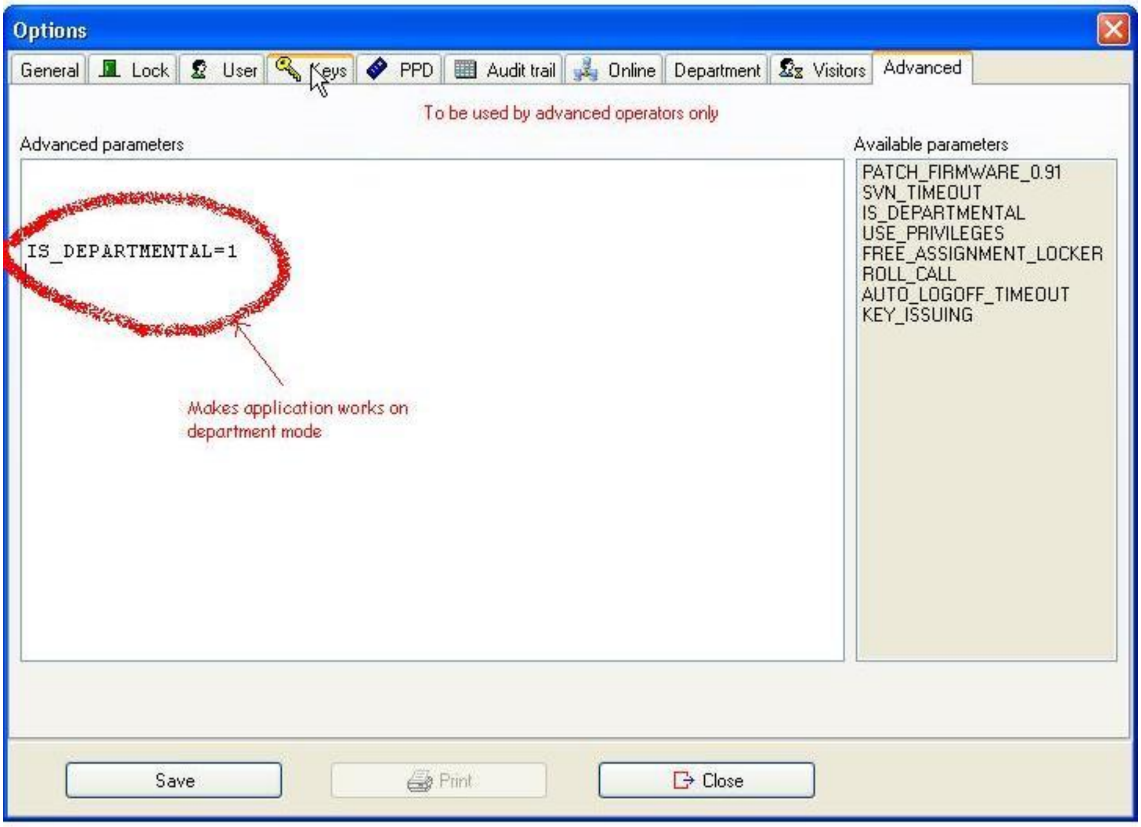
Some concepts must be taken in care:

Internal element: An element of the same department as the operator’s.
External element: An element of another department, shared with the operator’s department.

Activate departments feature

The first thing that the software administrator should do after creating the DB, is to create the departments planning, that is, decide how many departments there will be in the installation, which doors, users... will belong to each department…Once the department configuration is set up, the departments administrators are free to start working on their own department configuration as if it was an independent installation, creating their elements(users, doors, zones…) and sharing them as their own.

To make the application work on department mode, this option must be activated. So go to “Tools→ Configuration→ General options”, an activate the advanced option “IS_DEPARTMENTAL” (see figure 1).



```
IS_DEPARTMENTAL=1
```

Available parameters:

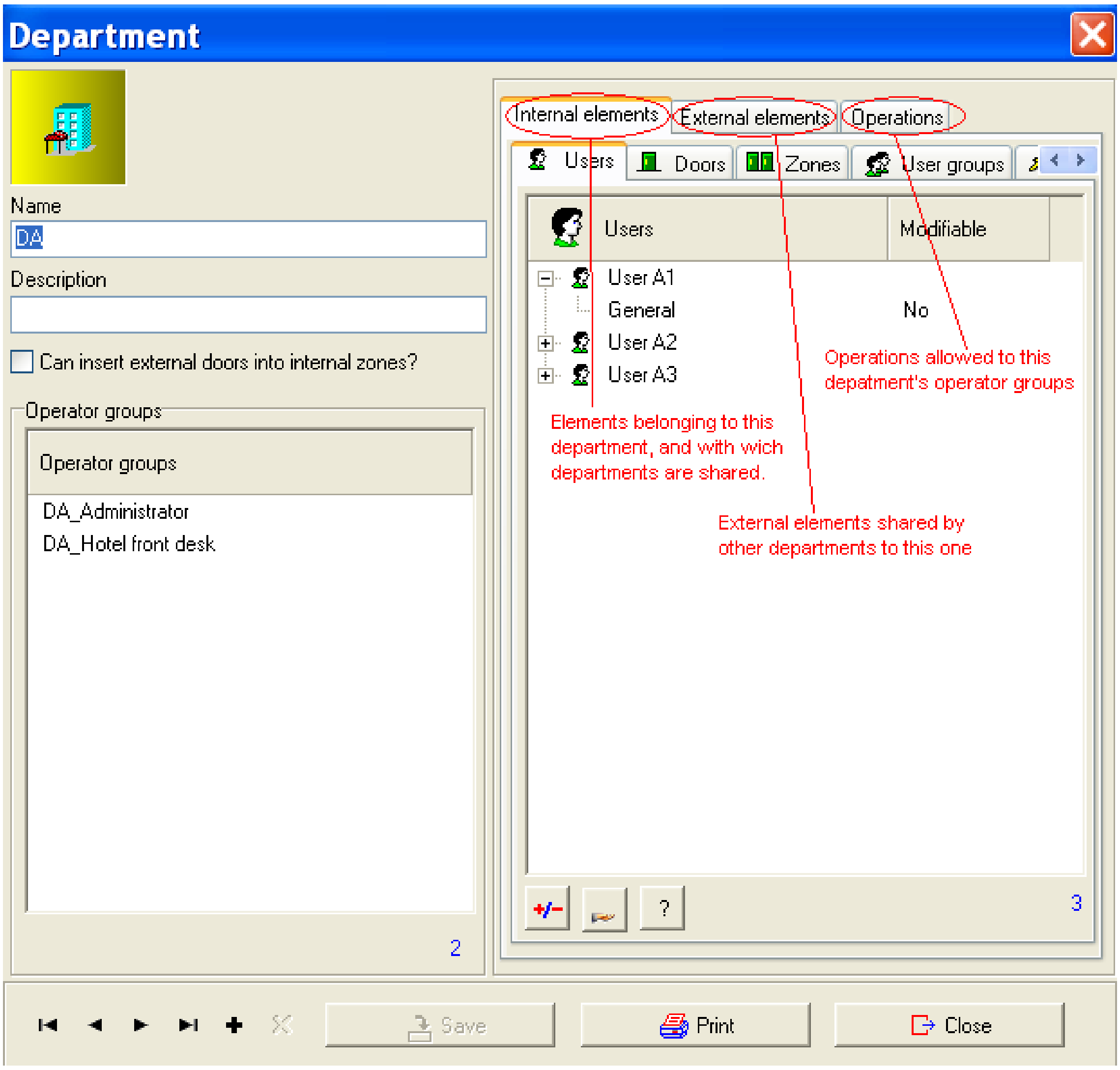
PATCH_FIRMWARE_0.91
SVN_TIMEOUT
IS_DEPARTMENTAL
USE_PRIVILEGES
FREE_ASSIGNMENT_LOCKER
ROLL_CALL
AUTO_LOGOFF_TIMEOUT
KEY_ISSUING

Figure 1: Advanced option to activate department feature.

How to create departments

After activating departments feature, it is possible to create new departments on "Tools→Operators and permissions→Departments", where it is possible to see a list of existing departments, create new departments, remove departments, change departments profiles... Departments can only be created and removed by the super-admin. An administrator of a department, can make changes in his department profile, and can change elements from his department to other departments. After creating a new department, an operator group (2 if the software is PA) is created, called "DepartmentName_Administrator", and an operator called "DepartmentName_admin" without password. (See figure 2). These operator groups and operators, can not be deleted, unless the department is deleted, by the super-admin. The administrator of each department, can also create new, modify or delete operator groups and operators for their department.

The super-admin, is also the only one allowed to allow other departments insert external doors into their internal zones.



Department

Name: DA

Description:

□ Can insert external doors into internal zones?

Operator groups

Operator groups
DA_Administrator
DA_Hotel front desk

Users	Modifiable
User A1	
General	No
User A2	
User A3	

Elements belonging to this department, and with wich departments are shared.

External elements shared by other departments to this one

Operations allowed to this depatment's operator groups

Figure 2: Screenshot of a department profile.

There are 3 main concepts in department profile (see figure 2):

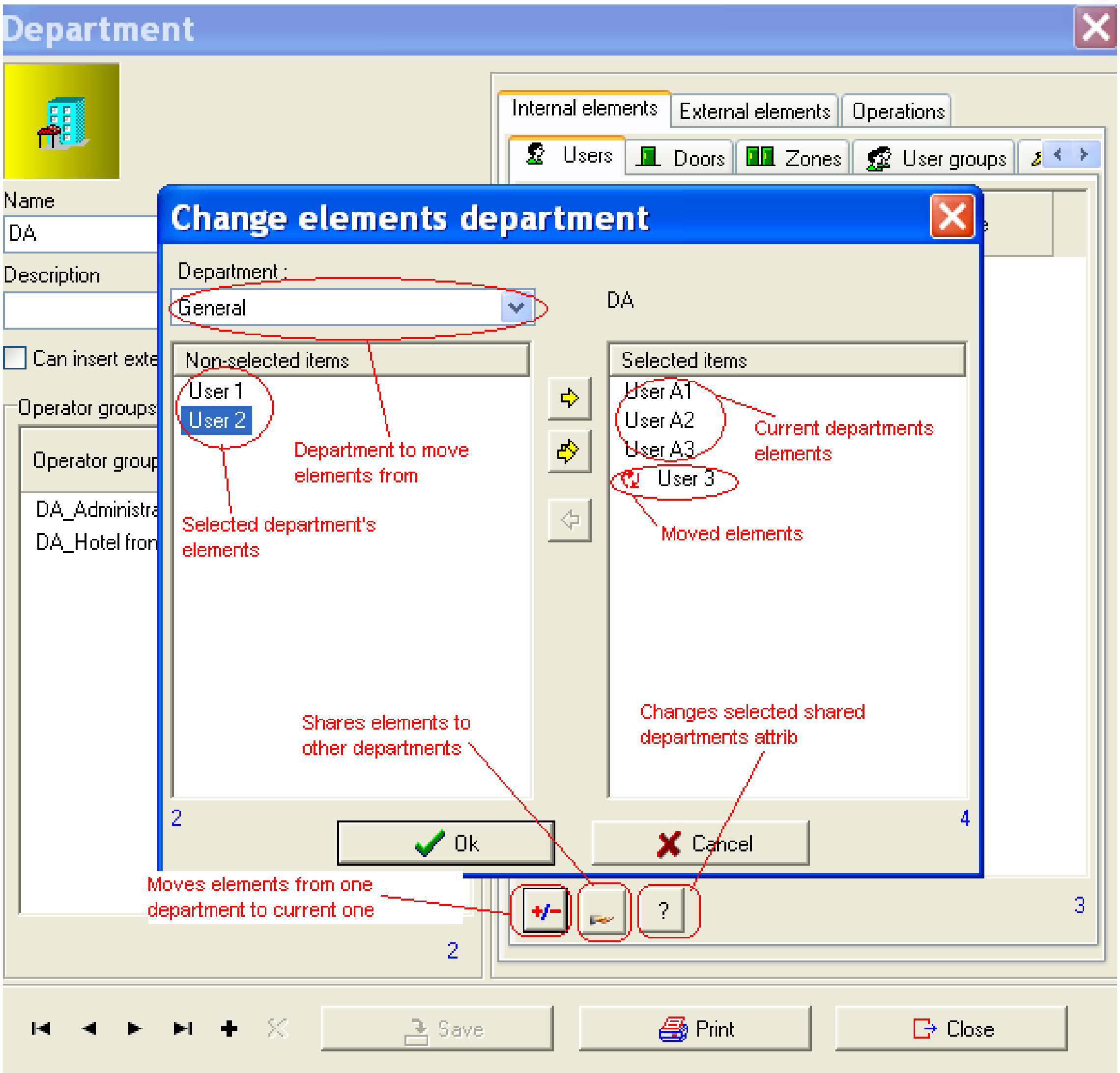
Internal elements: Here it is possible to see department internal elements, and with which department they are being shared and in which way (Modifiable or assignable).

External elements: Here it is possible to see department’s external elements, that is, elements of other departments that operators of this department can modify or assign depending on the way they are shared (Modifiable or assignable).

Operations: Here it is possible to specify which operations is allowed to do the administrator of this department.

Internal elements

Here it is possible to see internal elements of the department, and which elements are being shared with which departments and in which way (Modifiable or assignable). It is possible to modify an element's owner. An element is added to a department, every time an operator of that department creates a new one. To move an element from one department to another, go to the profile of the destination department, select the 'internal elements' tab and then click on +/- button. A new window will appear as shown in figure 3. In the right side of the screen, there are the elements belonging to current department, and in the left side of the screen, the elements of the department from which elements can be moved. So if we want to make an element belong to a department, first select the department from which the element is to be moved, and then move it with the arrows. For example, to make that User A from Dpt A belong to Dpt B, go to Dpt B profile, select internal elements and then click on +/- button. Then, in the right combo box, select Dpt A, and from the list below move User A. That will cause User A to belong to Dpt B. The super-admin, can select elements from any department, but a department administrator, can only select elements from his department.



Department

Name: DA

Description:

Change elements department

Department : General

DA

Non-selected items: User 1, User 2

Selected items: User A1, User A2, User A3, User 3

Department to move elements from

Selected department's elements

Current departments elements

Moved elements

Shares elements to other departments

Changes selected shared departments attrib

Moves elements from one department to current one

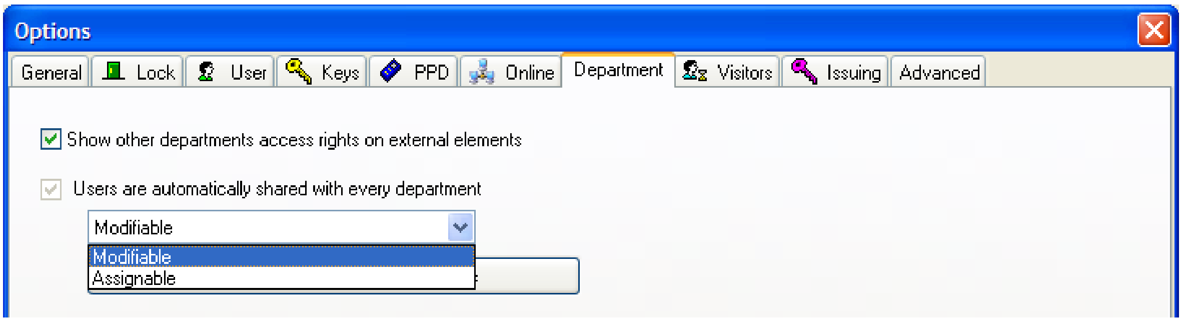
Figure 3: Screenshot of an element department change window.

When moving elements from one department to another it is necessary to consider certain aspects: either the access rights list of the moved elements must be updated accordingly or new sharing relations must be set up for keeping department integrity. For example, consider a door A in dpt A being accessed by a user B from dpt B. If door A is moved to Dpt C, then if user A is not shared with Dpt C, or if not Door A is shared with Dpt B, User B will not be allowed to access it, so there are 2 options; remove that access or set up a relation with assignable attrib, between Door A and Dpt B. So when there is the need of moving elements from one department to another, try moving all the elements that must be moved at the same time before saving, in order not to create unnecessary relations, or not to remove needed accesses relations. The software will ask every time elements are moved between departments what to do in this case (create new relations, or remove accesses relations).

Share elements

It is possible to share users automatically between all the departments by clicking the corresponding option from "general options".

This sharing can be defined in two different ways, Modifiable and Assignable:



☑ Show other departments access rights on external elements

☑ Users are automatically shared with every department

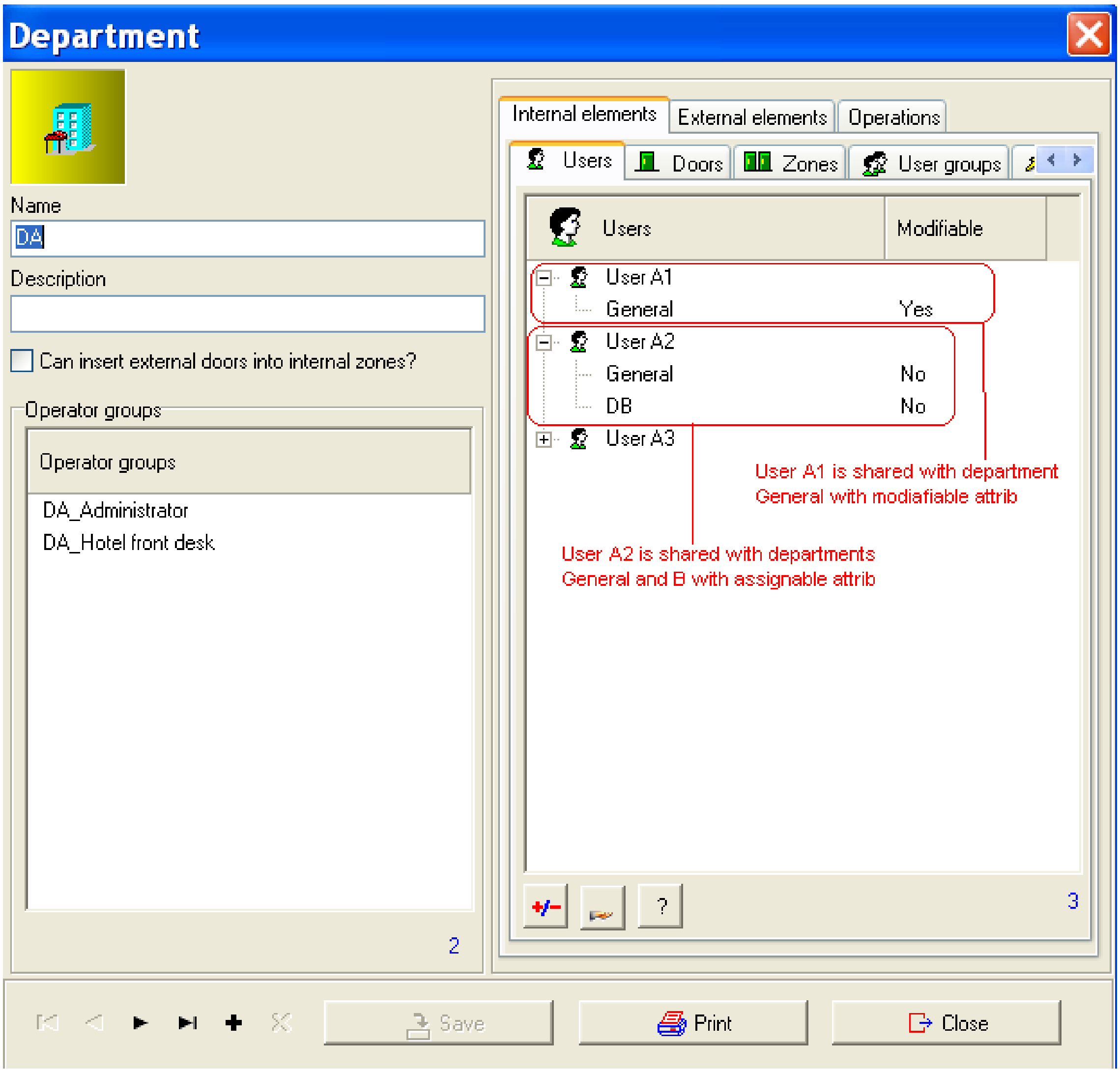
Modifiable

- Modifiable

Both types of information, user options and user access can be modified.

- Assignable

Only the user access will be modifiable



User A1 is shared with department General with modiafiable attrib

User A2 is shared with departments General and B with assignable attrib

Figure 4: Screenshot of a department shared elements window.

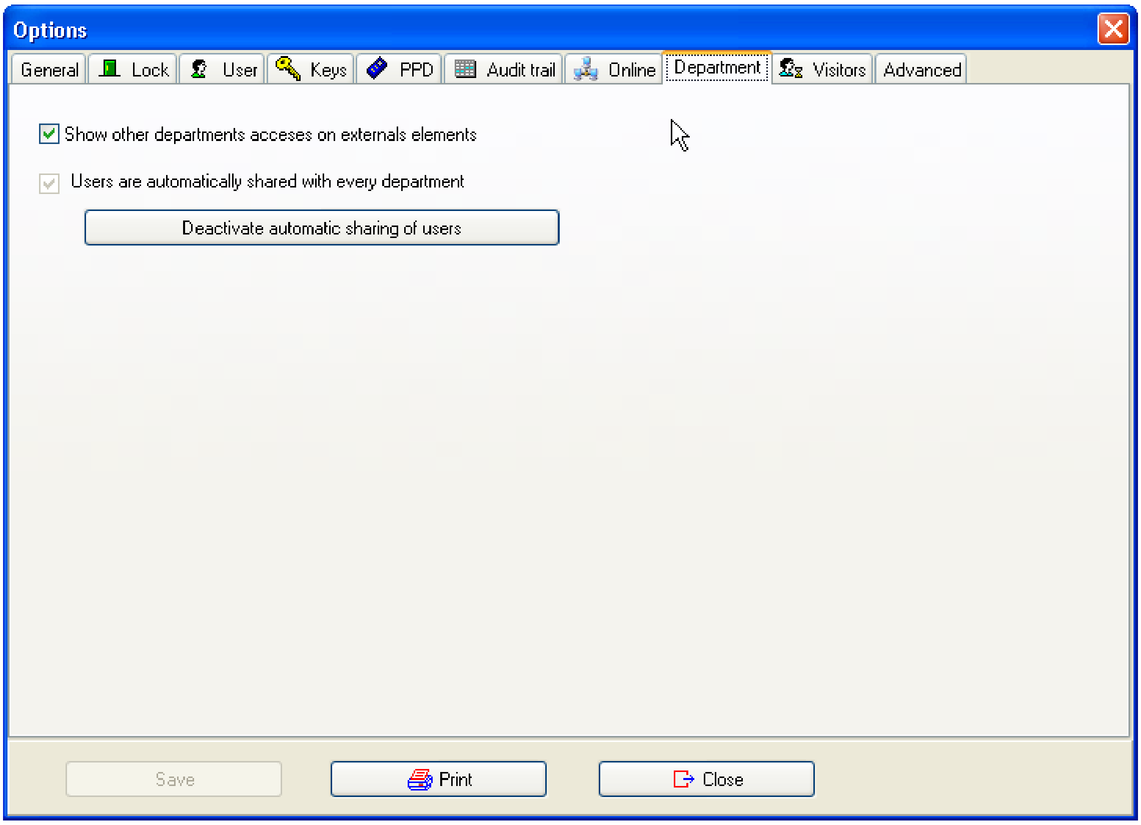
This option is the one that a department administrator must use to share or to remove sharing internal elements to other departments.

Caution must be taken when removing the sharing of an element with other departments since it will also imply the removal of all the external access rights. For example, consider a door A in dpt A being accessed by a user B from dpt B. If door A is not shared any longer, then user A will not be allowed to access it unless User B is shared with Dpt A.

Users automatically shared

Through this option we can share automatically all users with every department. We can find this command on general options/Department.

You will see the next window and just pushing the command automatically all users will be shared with every department.

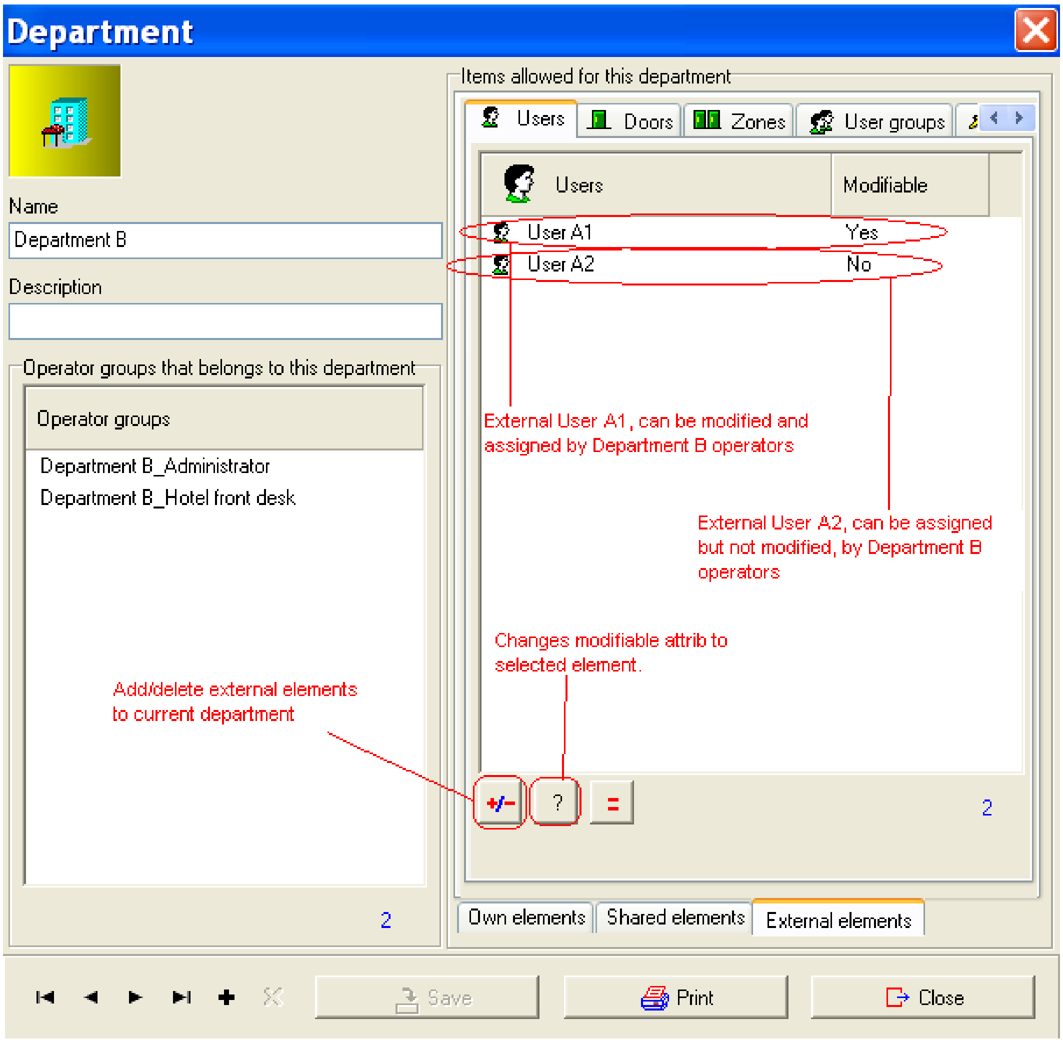


☑ Show other departments acceses on externals elements

☑ Users are automatically shared with every department

External elements

Here it is possible to see current department's external elements, that is, elements of other departments that operators of this department can modify or assign depending on the way they are shared (Modifiable or assignable)(see figure 5). To add external elements to current department, click on +/- button, and select the external elements that want to be added or removed. To change the modifiable attrib, select the element, and click on '?' button, and select the corresponding attrib value. These operations can only be done by Super-admin, other departments administrators, can only remove external elements, but never can add external elements, neither change modifiable attrib.



Name: Department B

Description:

Operator groups that belongs to this department

Operator groups
Department B_Administrator
Department B_Hotel front desk

2

Users	Modifiable
User A1	Yes
User A2	No

2

External User A1, can be modified and assigned by Department B operators

External User A2, can be assigned but not modified, by Department B operators

Changes modifiable attrib to selected element.

Add/delete external elements to current department

Figure 5: Screenshot of a department external elements window.

Operations

Here it is possible to specify which operations is allowed to do the administrator of the department, and this department’s operator groups. The way to do that, is the same as in operator groups.

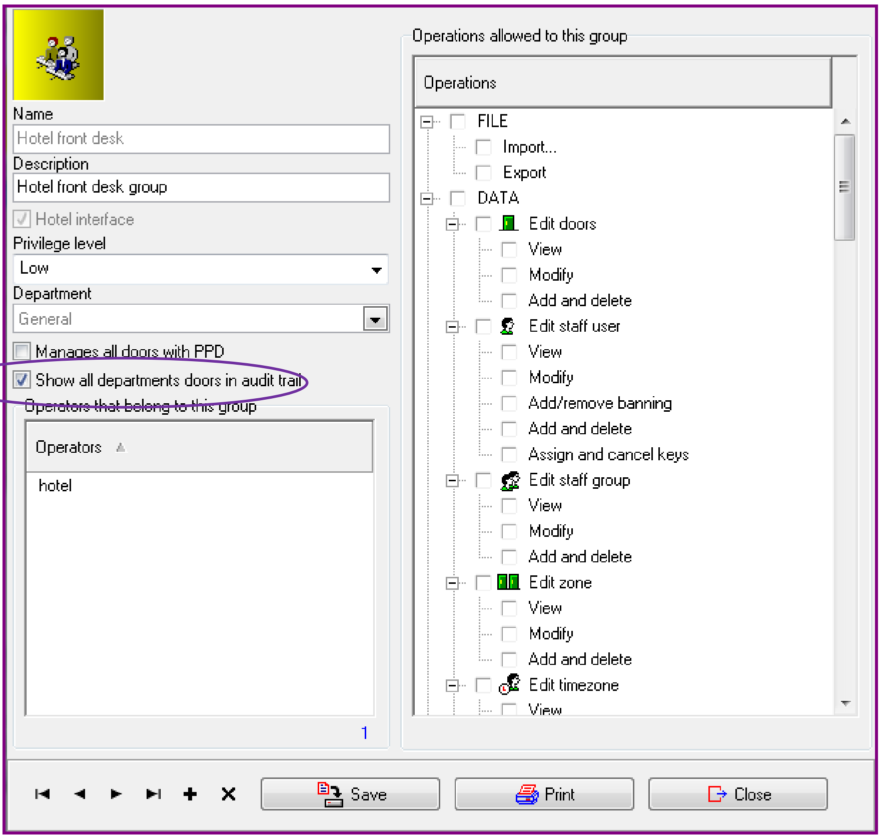
Operator Groups

The way to create operator groups has not change, but there are some new issues on them (see figure 6). Permissions are now decomposed into more detailed ones, for example, now it is possible to specify if an operator can make changes in doors, users… if he can add or delete doors, users… if he can assign and cancel users keys… An operator group, can never have more permissions than his departments administrator. That is, if a department administrator has no permission for modifying doors, the operator groups of that department, will neither had permission for modifying them. Also it is possible to specify the privilege level of each operator. So if an operator group have low privilege level, its operators would not be able to make changes in medium or high level elements, even if they have got the modify element attrib activate, neither assign them. In order to use privilege levels, it is necessary to activate it in the configuration window, in the advanced options tab.

So far, for a non departmental application, there was no restriction for downloading any door onto the PPD for initialization, updating or emergency opening.

Now with the departmental feature, such restriction exists: an operator is allowed to download only doors belonging to his department. Even the emergency opening option in the PPD is valid only for the department's doors. (Provided that the PPD firmware version is '1.01' or higher).

However, sometimes it is desirable not to have such restriction (e.g., maintenance operator group). By removing the tick in the "Manages all doors with PPD" checkbox, it is possible for an operator to download any door (even other department's doors) onto the PPD



Name: Hotel front desk
Description: Hotel front desk group
☑ Hotel interface
Privilege level: Low
Department: General
□ Manages all doors with PPD
☑ Show all departments doors in audit trail

Operators that belong to this group

Operators
hotel

1

Operations allowed to this group

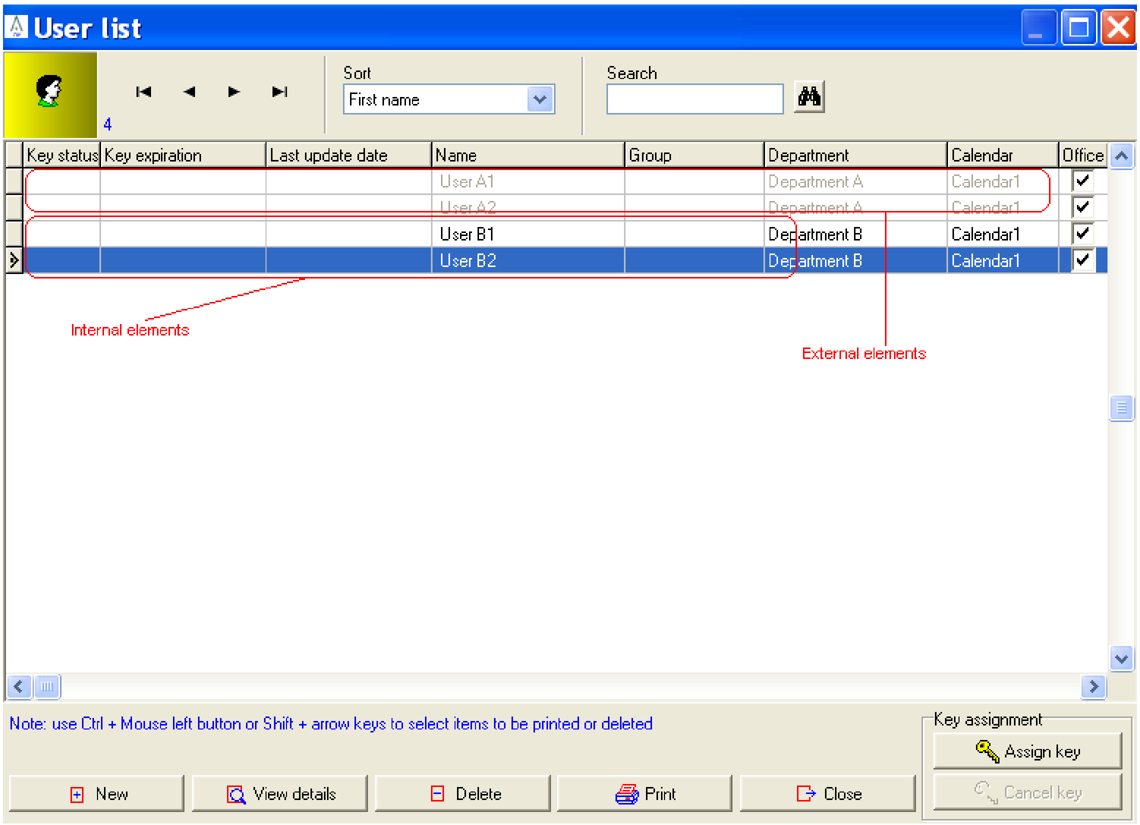
Operations
- □ FILE
  - □ Import...
  - □ Export
- □ DATA
  - □ Edit doors
    - □ View
    - □ Modify
    - □ Add and delete
  - □ Edit staff user
    - □ View
    - □ Modify
    - □ Add/remove banning
    - □ Add and delete
    - □ Assign and cancel keys
  - □ Edit staff group
    - □ View
    - □ Modify
    - □ Add and delete
  - □ Edit zone
    - □ View
    - □ Modify
    - □ Add and delete
  - □ Edit timezone
    - □ View

Figure 6: Example of an operator group profile. It can be appreciated, how permissions are decomposed into more detailed ones, and how it can be specified the privilege level and the way to work with PPD.

How to work with external elements

In order to explain how to work with external elements, the explanation is going to be based on Users and zones, but this could be applied to the rest of elements of the application, that is, Access levels, doors, outputs, rooms…

When an operator accesses an element window, he can see 2 kinds of elements; internal elements and external elements that are shown in a different color (see figure 7). The operator can not delete the external elements (unless the operator is super-admin), he can modify the profile and its accesses, if it is shared with the modifiable attrib, or only change its accesses if is shared with the assignable attrib.



Key status	Key expiration	Last update date	Name	Group	Department	Calendar	Office
			User A1		Department A	Calendar1	☑
			User A2		Department A	Calendar1	☑
			User B1		Department B	Calendar1	☑
			User B2		Department B	Calendar1	☑

Note: use Ctrl + Mouse left button or Shift + arrow keys to select items to be printed or deleted

Figure 7: Example of a user list window. It can be appreciated external elements in a different color.

When the time comes for an operator to edit and modify a profile of a given element, he might find some restrictions due to different reasons such as: the element is external, the required privilege level is too high, the external element is not shared with the modifiable attrib, operator has no permission for performing modifications…

In order for an operator to know whether the profile can be edited or modified and to which extent, a helpful icon is shown with the following meaning:

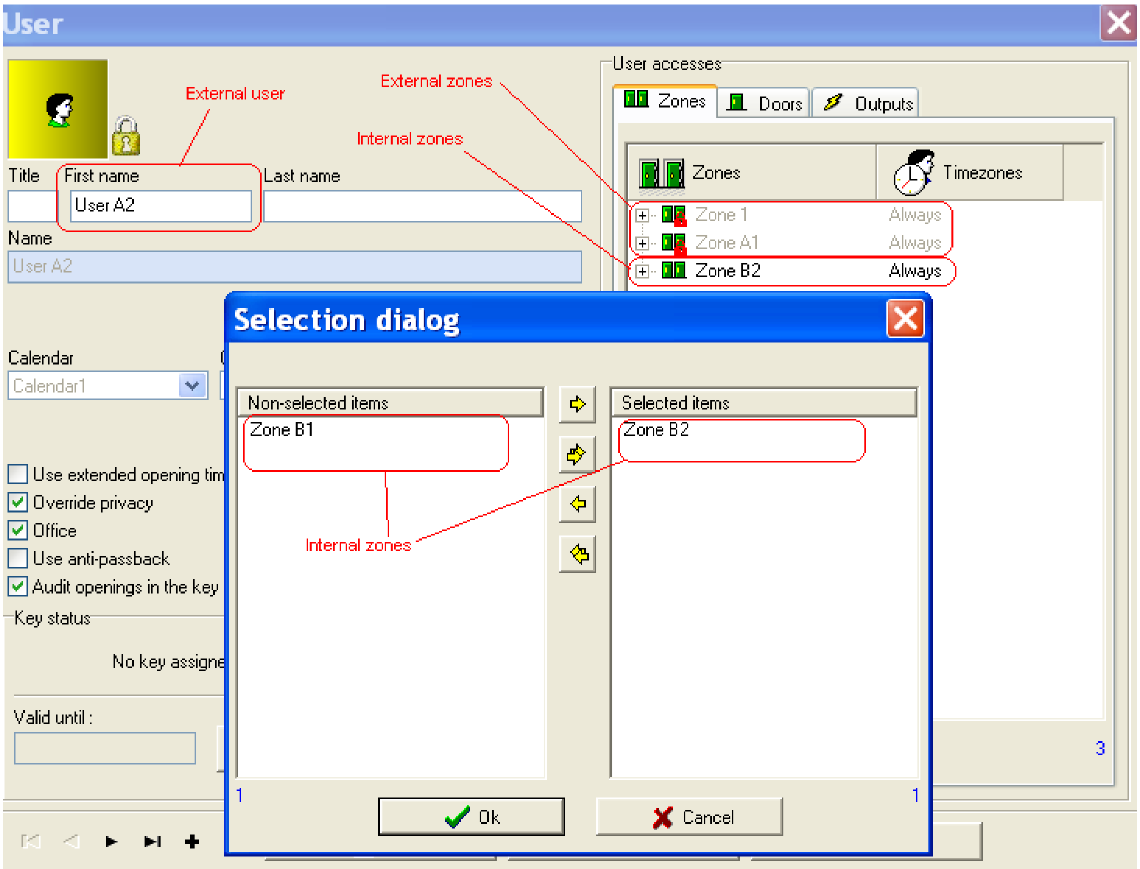
- No padlock: The operator has most control on that user if is an internal user (he can not modify external accesses timezones if user is not shared for example), and the most control if is external (he can no change users access level, and he can not remove or add external accesses for example).

- 🔒 yellow: The operator can only change the accesses for that user, that is, add or delete operators internal doors, zones…but he can not do any change on the user profile. This occurs because the user is shared without modifiable attrib.

- 🔒 red: The operator can not do any change on the user. That occurs because the operator has not enough privilege level, or is not able to make changes to users.

To modify a user accesses, there are some consideration to take in care, depending on whether the user is internal or external.

When the user is an external one, the operator is only allowed to add/remove internal accesses only, never external ones (see figure 8). Also, the operator must have enough privilege level on that internal elements. That is, even if another department’s zone has being shared to current operator’s department, this zone could not be assigned to an operator’s external user. And even if that zone is internal, if the operator has not enough privilege level to modify that zone, the operator is not going to be able to add/remove that zone. The elements accesses that can not be added/removed or changed, will appear with a red padlock icon.



User

Title:
First name: User A2
Last name:
Name: User A2
Calendar: Calendar1

☐ Use extended opening tim
☑ Override privacy
☑ Office
☐ Use anti-passback
☑ Audit openings in the key

Key status: No key assigne
Valid until :

User accesses

Zones	Timezones
Zone 1	Always
Zone A1	Always
Zone B2	Always

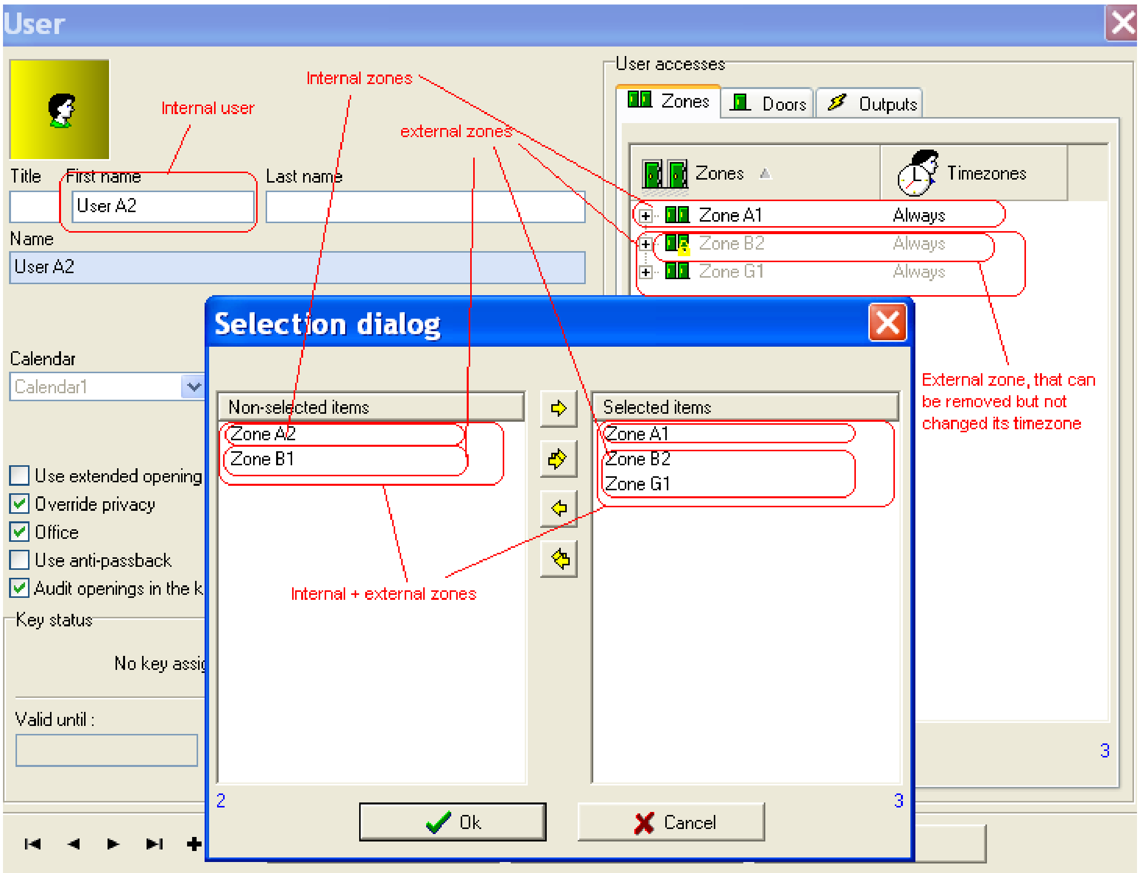
Selection dialog

Non-selected items: Zone B1

Selected items: Zone B2

Figure 8: Example of an external user profile. It can be appreciated external elements in a different color and the impossibility to add/remove external zones to an external user.

When the user is an internal one, the operator is allowed to add/remove any access with lower or same privilege level as the operator's, no matter if it is internal or external one (see figure 9). Has total control on internal users, with the only exception, that it is not possible to change the assigned timezone to an external access, if the external element is not shared. This case will be represented with a yellow padlock. That is, DptA.User A accesses a Dpt B.Zone B, with a Timezone, if DptA.user A is shared with DptB, then, the Timezone can not be modified, because we assume that the owner of the zone has given access to the user with the timezone he wants for that user to access his zone, but if DptB.Zone B is shared with DptA, then the timezone can be modified, because is the user owners who gives access to the zone.



Title:
First name: User A2
Last name:
Name: User A2
Calendar: Calendar1

☐ Use extended opening
☑ Override privacy
☑ Office
☐ Use anti-passback
☑ Audit openings in the k

Key status: No key assig
Valid until :

Zones	Timezones
Zone A1	Always
Zone B2	Always
Zone G1	Always

Non-selected items: Zone A2, Zone B1

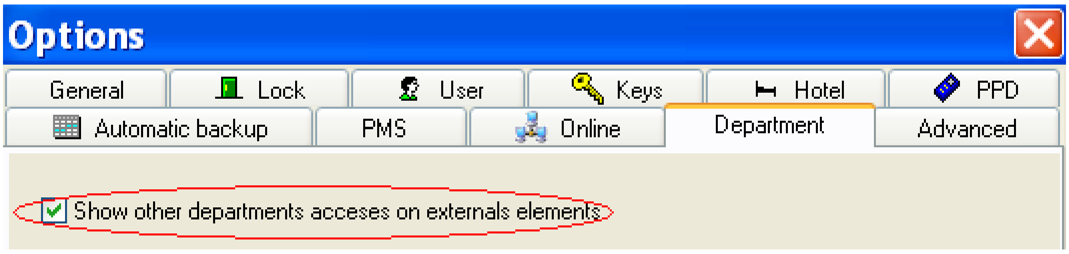
Selected items: Zone A1, Zone B2, Zone G1

Figure 9: Example of an internal user profile. It can be appreciated external elements in a different color and how can add/remove external + internal zones to an internal user.

So, to add for example an internal zone, to an external user there are 2 ways to do; Going to the profile of the external user, and adding the access to the department's internal zone, or going to the profile of the internal zone, and adding the access to the external user.

For example: To add the access DptB.UserB1 – DptA.ZoneA1, with ZoneA1 being shared to DptB, that is, ZoneA1 is DptB's external zone, there are 2 ways to do that; going to internal UserB1's profile and adding external ZoneA1, or going to external Zone A1 profile, and adding internal UserB1. And even, DptB.Operator, must have same or higher privilege level as UserB1 and ZoneA1.

In figure 8, the external accesses of an external user are shown, but these external accesses could be hidden, by going to "Tools→Configuration→General options" and in the Department window, unchecking the "Show other departments on externals elements" option. This will cause to be hidden external accesses on external elements (see figure 10).

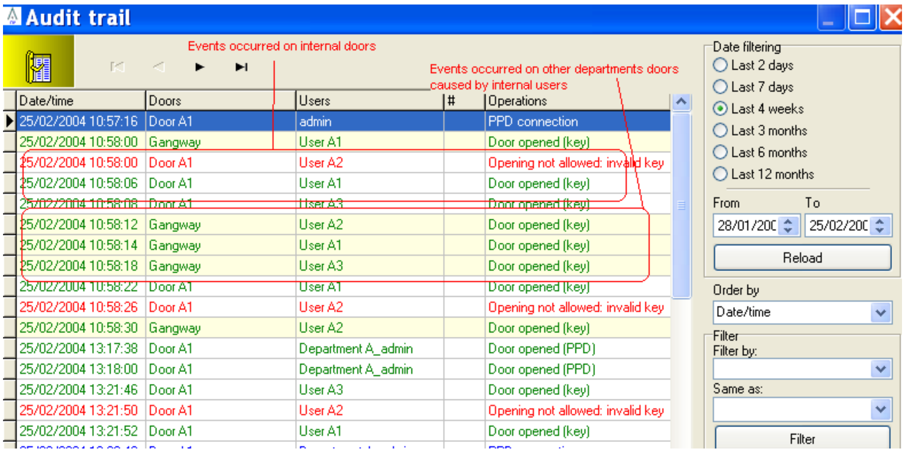


☑ Show other departments acceses on externals elements

Figure 10: Example of how to hide external accesses on external elements.

Audit trail

On audit trail window, an operator will see all the events occurred in his department's doors, and the events occurred in other department's doors caused by his department's users. This last type of events will be shown on a different color (see figure below).



Date/time	Doors	Users	#	Operations
25/02/2004 10:57:16	Door A1	admin		PPD connection
25/02/2004 10:58:00	Gangway	User A1		Door opened (key)
25/02/2004 10:58:00	Door A1	User A2		Opening not allowed: invalid key
25/02/2004 10:58:06	Door A1	User A1		Door opened (key)
25/02/2004 10:58:08	Door A1	User A3		Door opened (key)
25/02/2004 10:58:12	Gangway	User A2		Door opened (key)
25/02/2004 10:58:14	Gangway	User A1		Door opened (key)
25/02/2004 10:58:18	Gangway	User A3		Door opened (key)
25/02/2004 10:58:22	Door A1	User A1		Door opened (key)
25/02/2004 10:58:26	Door A1	User A2		Opening not allowed: invalid key
25/02/2004 10:58:30	Gangway	User A2		Door opened (key)
25/02/2004 13:17:38	Door A1	Department A_admin		Door opened (PPD)
25/02/2004 13:18:00	Door A1	Department A_admin		Door opened (PPD)
25/02/2004 13:21:46	Door A1	User A3		Door opened (key)
25/02/2004 13:21:50	Door A1	User A2		Opening not allowed: invalid key
25/02/2004 13:21:52	Door A1	User A1		Door opened (key)

○ Last 2 days
○ Last 7 days
● Last 4 weeks
○ Last 3 months
○ Last 6 months
○ Last 12 months

From: 28/01/200 To: 25/02/200

Order by: Date/time

Figure 11: Screenshot of audit trail window where it is possible to see events on internal doors, and events on externals.

Note that when an operator purge the DB, only events occurred on internal doors will be removed. So, if another department's operator purge the DB, all the events occurred on those doors caused by internal users, will be also removed.

On the system auditor, an operator will only see events caused by operators of his same department.

Programming and spare keys

Each department will only be allowed to make programming and spare keys, only for their department's rooms. The super admin can make keys for any department's room, by first selecting the department for which the key wants to be done (see figure 12).

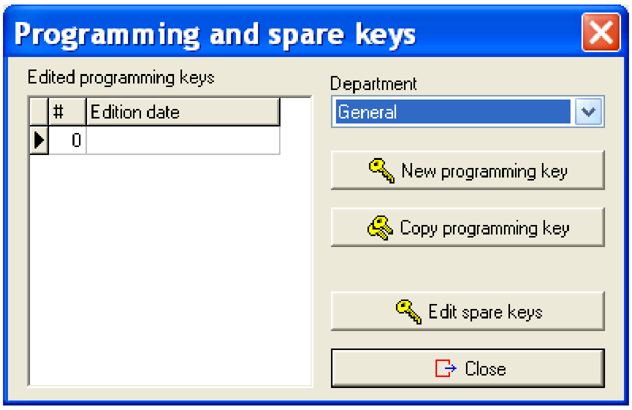


Figure 12: Screenshot of programming and spare keys window. It can be appreciated the combo box for selecting the department the key wants to be done.

8. Automatic user data synchronisation tool

Note: This feature is only available for PA Connected or higher software.

This feature is intended for synchronizing user data between two systems, SALTO's and an external one (called master), by means of text files. The master system is responsible for producing sync. data files and SALTO is responsible of processing them and alter its DB accordingly.

Basically, this feature works as follows (see the corresponding specs document for further details): the master system produces a text file containing a list of users. For each user in the list, the master must specify, among other parameters, the operation to be performed on the SALTO DB. So far, the supported operations are: 1) add a new user to the SALTO DB; 2) modify the data attributes of an existing user; 4) delete a user; 5) cancel a user's key. Therefore, unlike the IMPORT tool, which just adds new elements to the SALTO DB, the synchronization tool is more flexible since allows users to be created, modified or deleted.

Bear in mind that the current synchronization tool ONLY works for USERS; you cannot synchronizes any other kind of entity (such as doors, time zones, etc.) In the future, the synchronization tool MIGHT BE extended to the rest of the entities. Similarly, other types of format MIGTH BE also supported (such as Excel) in the future.

Note also that the synchronization process is only performed by that SALTO instance declared as comm. master.

The software provides a wizard to guide the operator through the setup of a synchronization job. Basically, within this wizard, the operator is requested to specify the type and location of sync. data files, the significance of each column within the sync. files and the time scheduling plan (see figures 9 to 13).

Effectively, sync. jobs may be scheduled according to a flexible time planning: for example, as shown in figure 13, it is possible to execute a sync. job on a regular basis (every ten minutes in every day). Thanks to this flexible time scheduling, master systems may synchronize their user data in an automatic way without any manual intervention in the SALTO software.

Please refer to the corresponding specs document to learn the user data model on which the synchronization tool is based. Not every user data is synchronizable: for example, in this current version, it is not allowed to synchronize data concerning access permissions (doors/zones and time zones).

As for the graphic interface, you may create a user synchronization job in two different ways, as seen in the pictures below: either by selecting the 'FILE\ IMPORT/EXPORT\SYNCHRONISATION' menu option or the 'TOOLS\SCHEDULED JOBS' one. Whichever option you choose, you end up with a new sync job added to the list of scheduled jobs, as seen in figure 8. You may modify the settings of an already scheduled sync job at any time by clicking on the 'View details' button in the job list window. By doing so, the same wizard will be launched again for you to perform the desired changes.

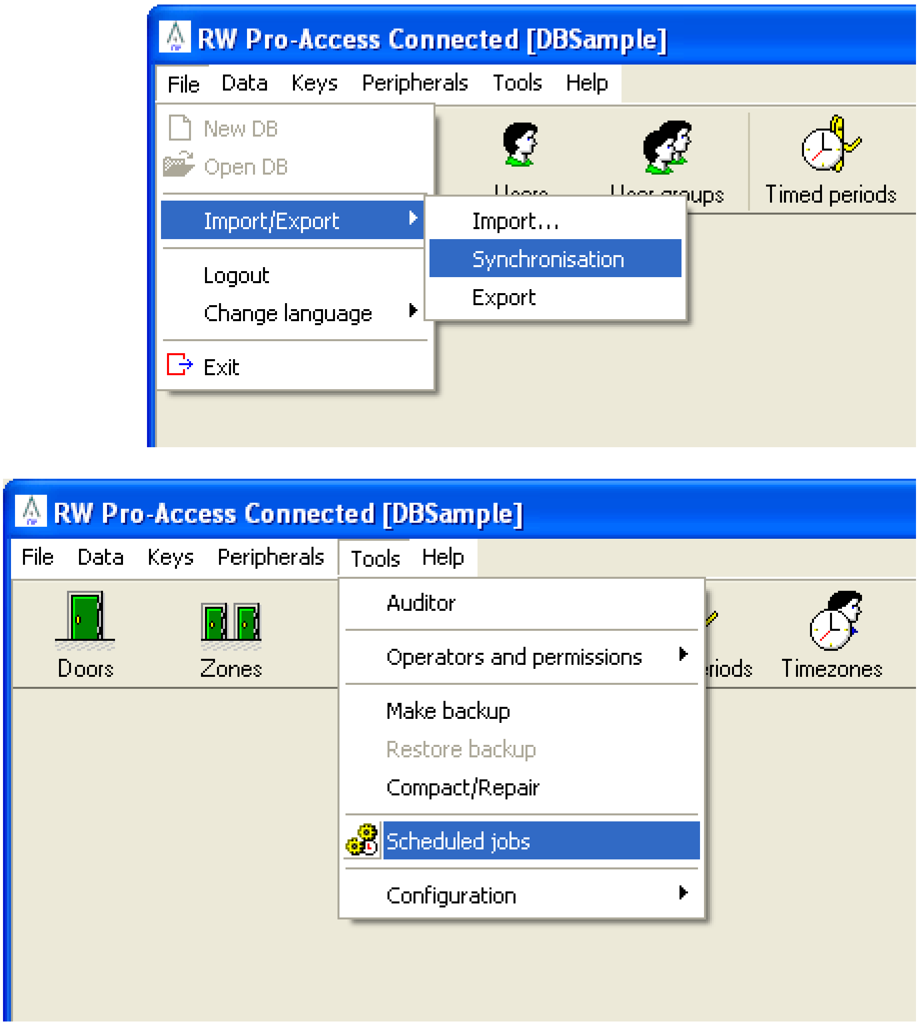
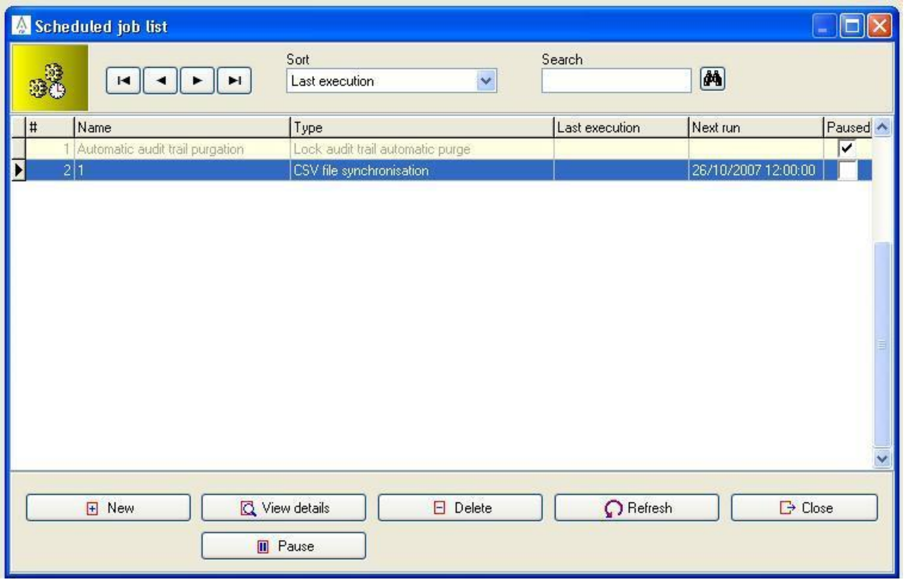


Figure 7: two different options for executing a synchronization job.



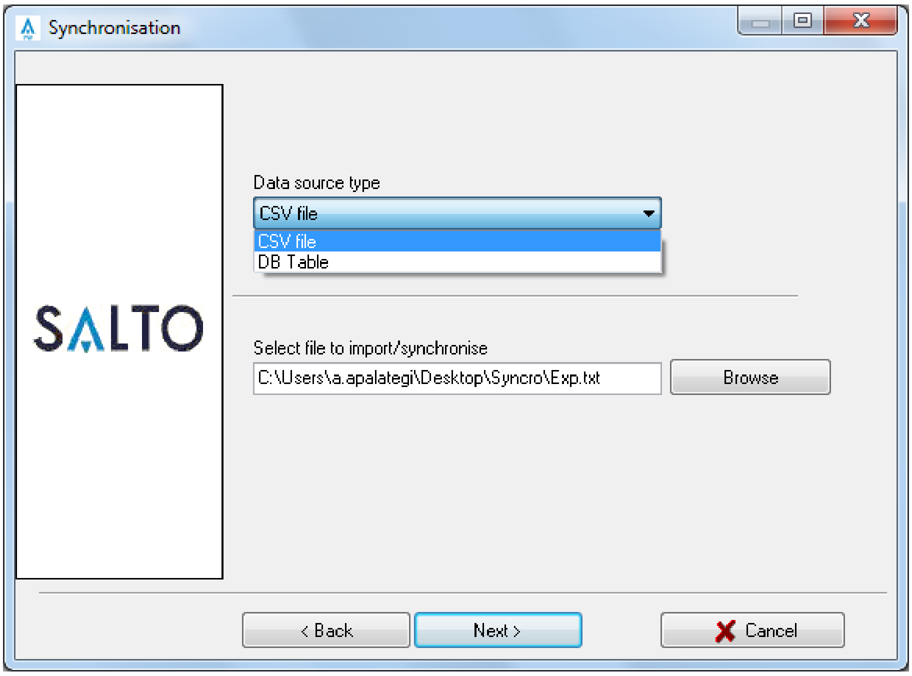
Scheduled job list

Sort: Last execution

Search:

#	Name	Type	Last execution	Next run	Paused
1	Automatic audit trail purgation	Lock audit trail automatic purge			✓
2	1	CSV file synchronisation		26/10/2007 12:00:00	□

Figure 8: list of scheduled jobs.



Synchronisation

Data source type: CSV file

CSV file
DB Table

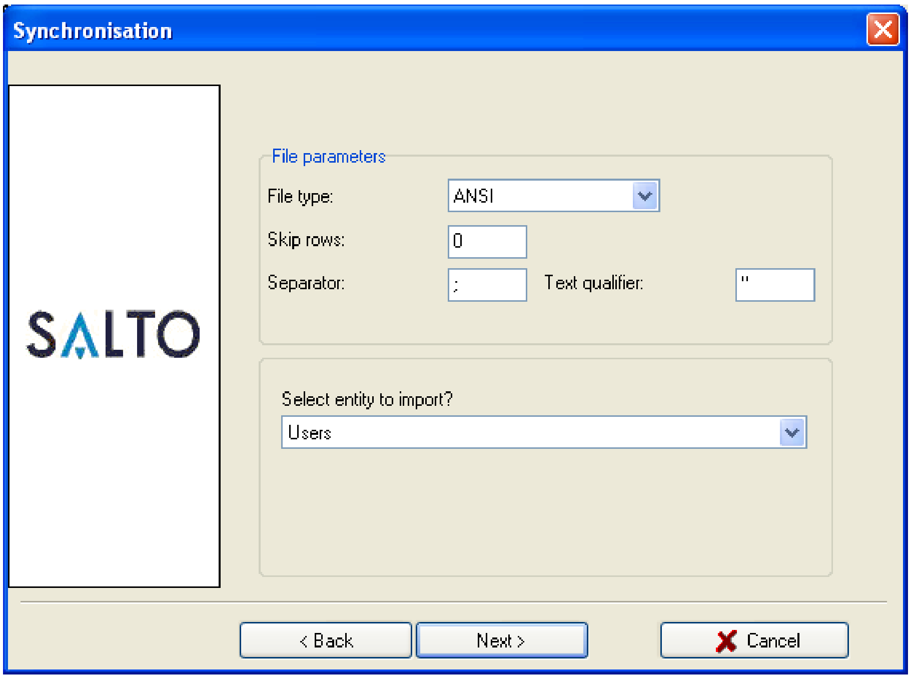
Select file to import/synchronise: C:\Users\a.apalategi\Desktop\Syncro\Exp.txt

Figure 9: data sync wizard. Specifying the type and location of data.

The Data source type can be selected, depending of the type of file to be used in the Synchronization task. The file could be a CSV file (*.csv, *.txt files) or a Database Table (DB Table, like SQL Server, Oracle or ODBC Data sources tables). This last option is only for Pro Access For Service.

Please refer to the following documents to have more details about the data synchronization for:

CSV files: SALTO_Data_Sync_x_x document.
DB Tables: SALTO_User_Sync_Staging_Table_x_x document.



File parameters

File type: ANSI

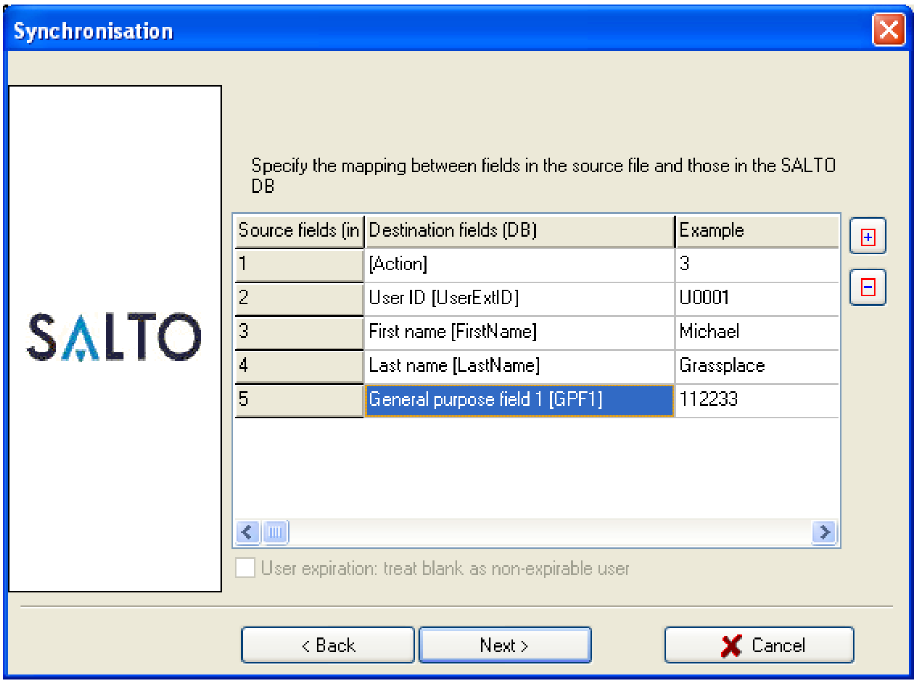
Skip rows: 0

Separator: ;

Text qualifier: "

Select entity to import? Users

Figure 10: data sync wizard. Specifying the CSV parameters and type of entity.

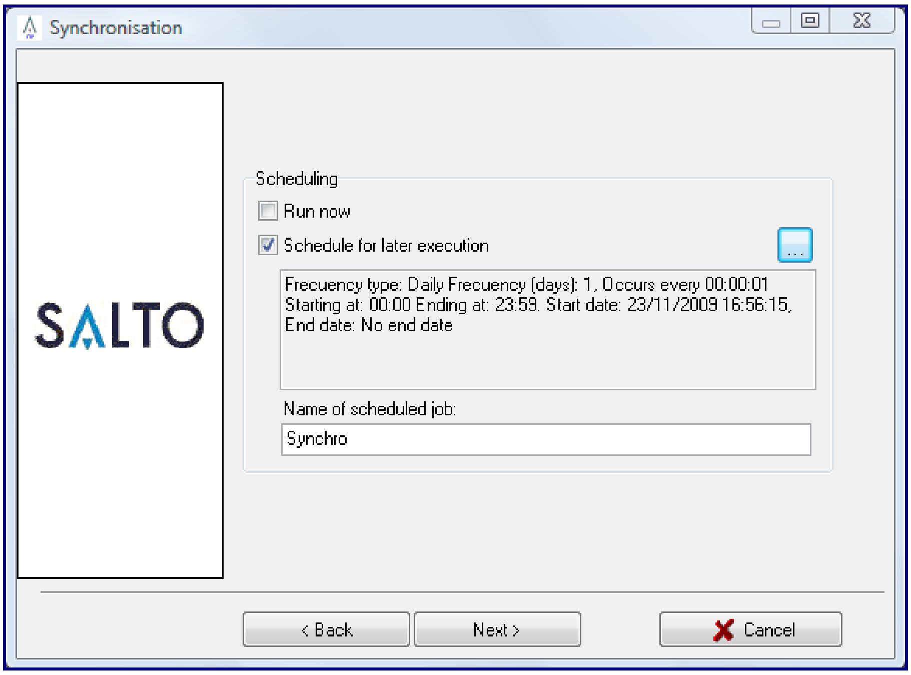


Specify the mapping between fields in the source file and those in the SALTO DB

Source fields (in	Destination fields (DB)	Example
1	[Action]	3
2	User ID [UserExtID]	U0001
3	First name [FirstName]	Michael
4	Last name [LastName]	Grassplace
5	General purpose field 1 [GPF1]	112233

□ User expiration: treat blank as non-expirable user

Figure 11: data sync wizard. Specifying the significance of columns within the CSV file.



Scheduling

□ Run now

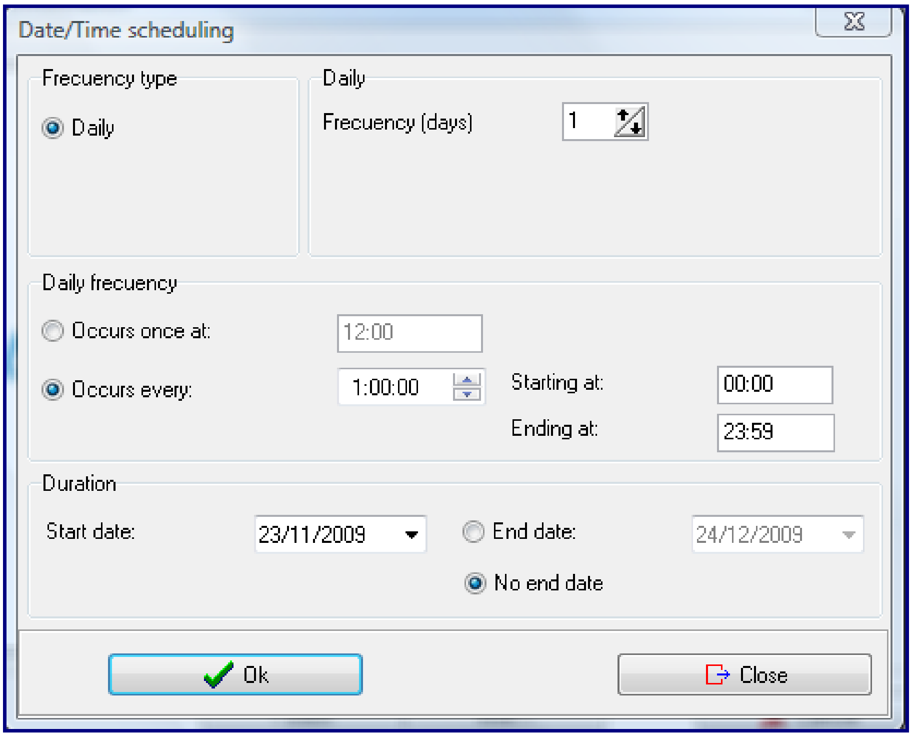
☑ Schedule for later execution

Frecuency type: Daily Frecuency (days): 1, Occurs every 00:00:01 Starting at: 00:00 Ending at: 23:59. Start date: 23/11/2009 16:56:15, End date: No end date

Name of scheduled job:

Synchro

Figure 12: data sync wizard. Specifying the time scheduling plan and name of the job. It is possible to program synchronization every 1 second.



Frecuency type

● Daily

Daily

Frecuency (days) 1

Daily frecuency

○ Occurs once at: 12:00

● Occurs every: 1:00:00

Starting at: 00:00

Ending at: 23:59

Duration

Start date: 23/11/2009

○ End date: 24/12/2009

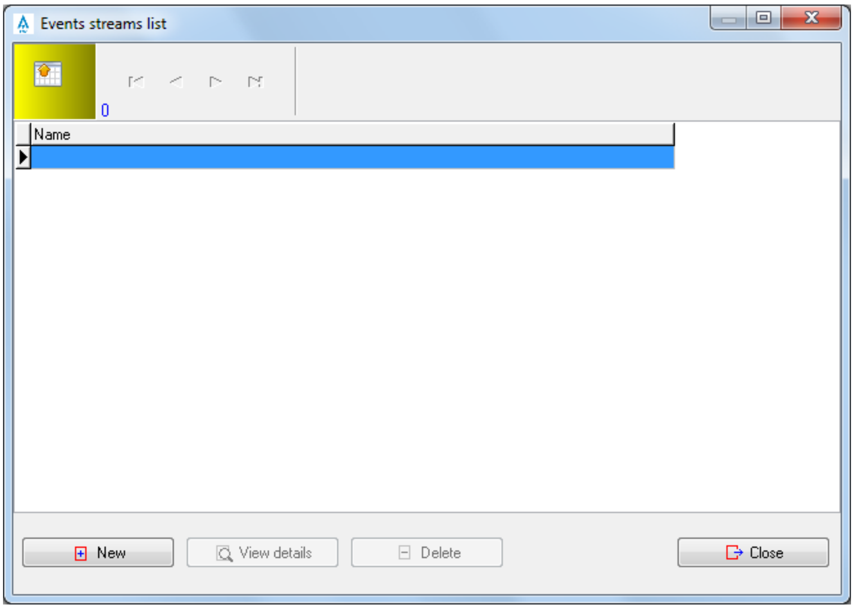
● No end date

Figure 13: data sync wizard. Specifying the time scheduling planning.

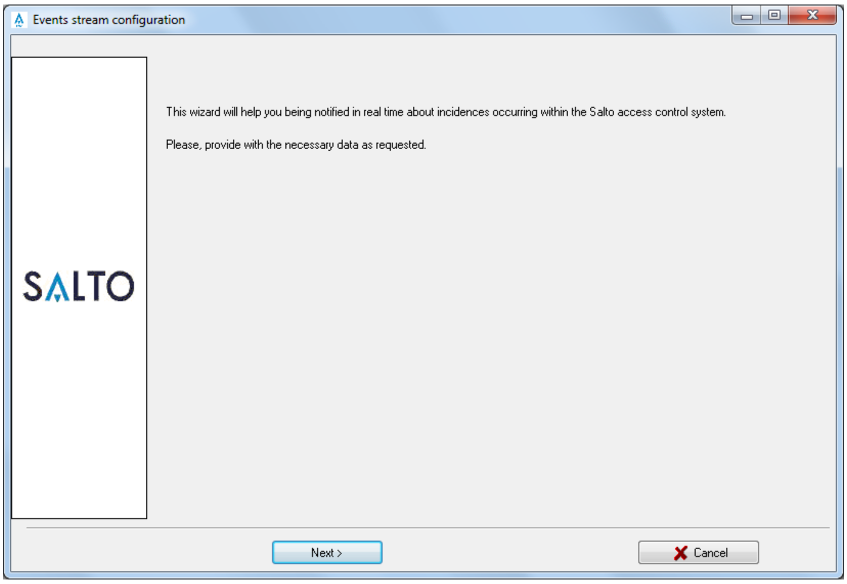
Events Streams (SALTO Service only!)

The Events Streams option generates real time notifications to third party systems.
The idea is to filter the auditrail and send the selected events in order that the order system can process the received information and perform a real time action.

The following steps have to be followed to establish an event streams communication.
Open the Events streams wizard by clicking on: “TOOLS/EVENTS STREAMS”



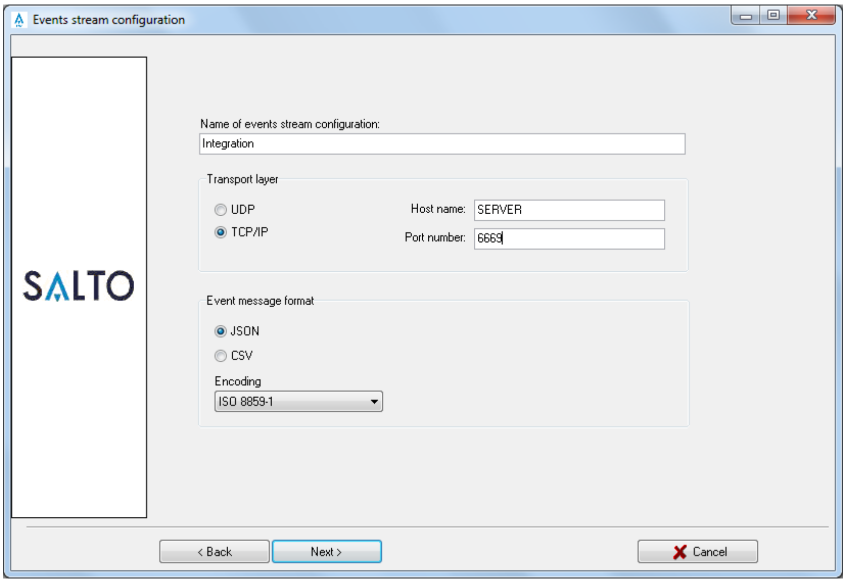
The “NEW” button will start the configuration wizard.



This wizard will help you being notified in real time about incidences occurring within the Salto access control system.

Please, provide with the necessary data as requested.

Select a name for the events stream configuration.
A UDP or TPC port has to be opened to communicate with the client software.
Specify the HOST name and the port number



Name of events stream configuration: Integration

Transport layer

○ UDP
● TCP/IP

Host name: SERVER
Port number: 6669

Event message format

● JSON
○ CSV

Encoding: ISO 8859-1

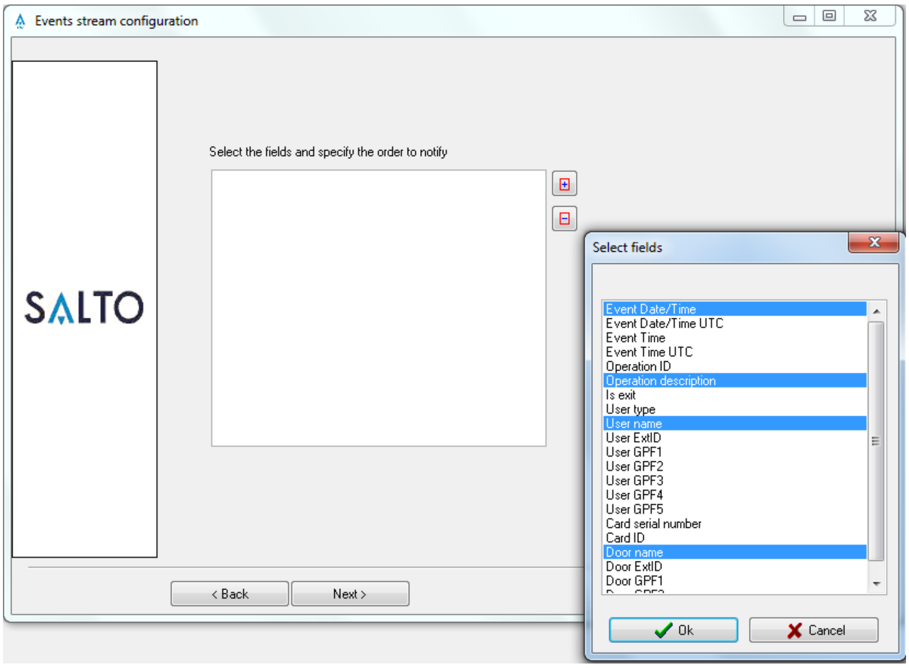
Notification events may be represented in two formats: JSON or CSV-like message.
JSON is a text-based open standard. The following example should give the reader a raw idea of what a SALTO event might look like in JSON format:

```
[
{
"EventID" : "11223344556677889900",
"EventDateTime" : "2012-04-14T13:03:20",
"EventTime" : "13:03:20",
"EventDateTimeUTC" : "2012-04-14T11:03:20Z",
"OperationID" : 17,
"OperationDescription": "Door opened: key",
"IsExit" : false,
"UserType" : 0,
"UserName" : "John Smith",
"UserGPF3" : "Marketing department",
"DoorName" : "Gym",
"DoorGPF1" : "Leisure area",
}
]
```

CSV is the Comma-Separated Values standard. Example:

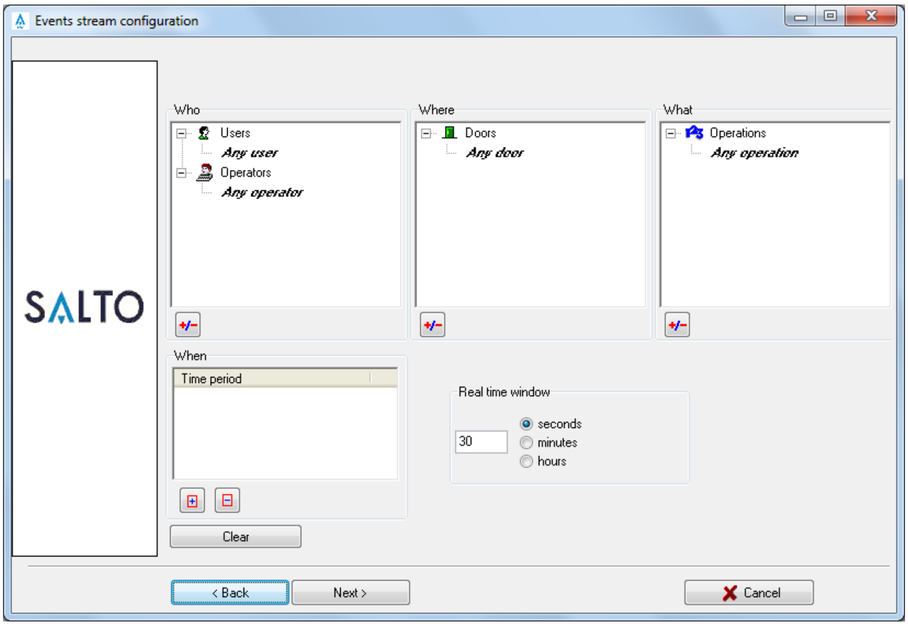
EVENT_START "11223344556677889900"; 2012-04-14T13:03:20; 13:03:20; 2012-04-14T13:03:20z; 17; "Door opened: key"; false; 0; "John Smith"; "Marketing department"; "Gym"; "Leisure area" EVENT_END

Press “NEXT”



Select the information that is going to be sent from the “Select fields” list.

Press “NEXT”

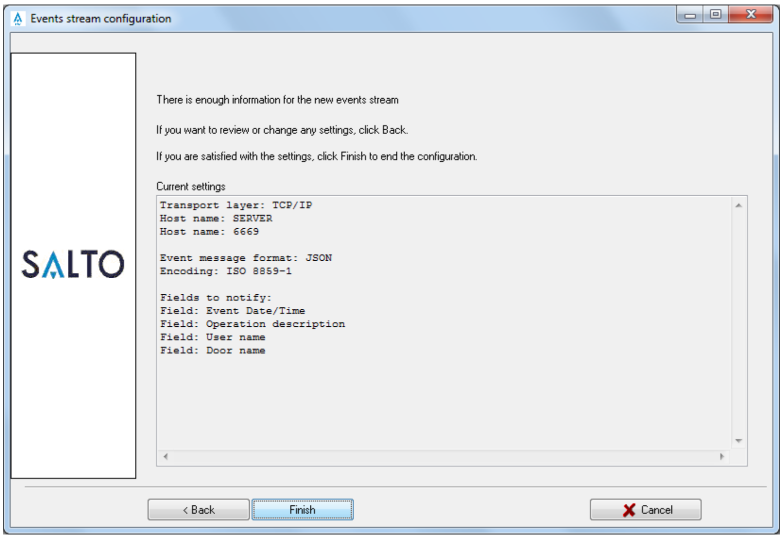


This filter window allows filtering among the following parameters:

- Who
- Where
- What
- When

The “Real time window” limits the number of events within the time. For example, a value of 1 minute will be streaming the events that have occurred during this time (audits collected from cards for example).

Press “NEXT”



There is enough information for the new events stream

If you want to review or change any settings, click Back.

If you are satisfied with the settings, click Finish to end the configuration.

Current settings

```
Transport layer: TCP/IP
Host name: SERVER
Host name: 6669

Event message format: JSON
Encoding: ISO 8859-1

Fields to notify:
Field: Event Date/Time
Field: Operation description
Field: User name
Field: Door name
```

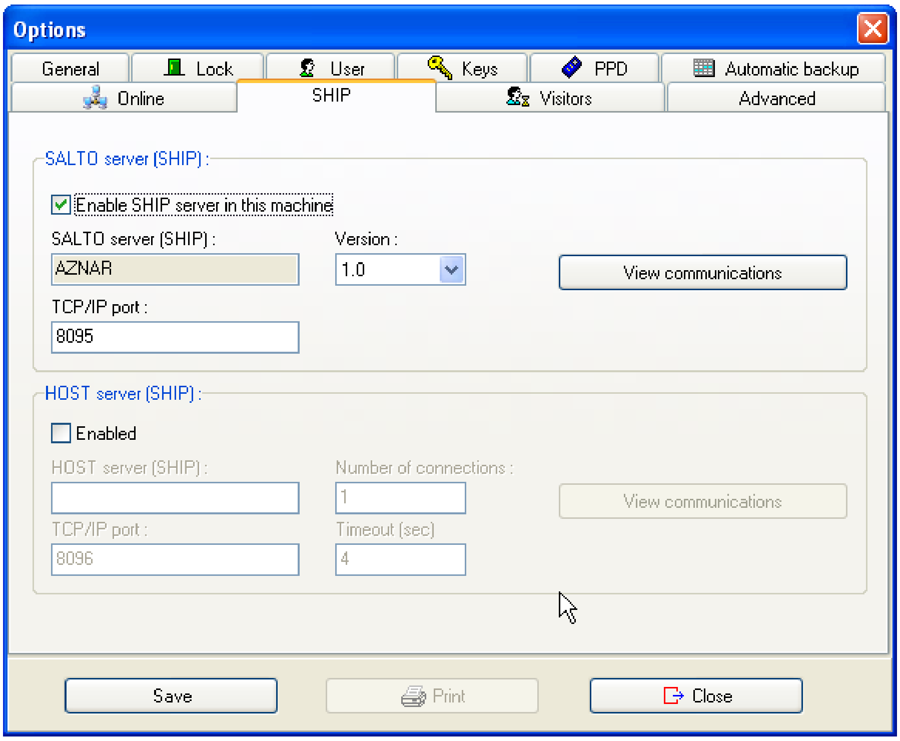
Press “FINISH”

Note: please refer to the “SaltoEventStream_x_x technical manual” for the full complete data model and list of events operations description.

9.SALTO Host Interface Protocol SHIP

Important: This option only is available on PA Department SHIP and PA Department SHIP

In order to activate the SHIP feature we have to go to the menu TOOLS/CONFIGURATION/GENERAL OPTIONS and press the SHIP tab. We will find the following window (Fig. 1).



SALTO server (SHIP) :

☑ Enable SHIP server in this machine

SALTO server (SHIP) : AZNAR

Version : 1.0

TCP/IP port : 8095

HOST server (SHIP) :

□ Enabled

HOST server (SHIP) :

Number of connections : 1

TCP/IP port : 8096

Timeout (sec) 4

(Fig. 1)

Activate communication SALTO (server) – Host (client)

When SALTO acts like server first of all we have to activate the following checkbox :

☑ Enable SHIP server in this machine

Once we have activated it we will see the name of the PC that is going to work as Server "SALTO server (Ship)

Finally we have to select the TCP/IP port from where the communication is going to be made.

The option will allow us to view all the information shared between the SALTO server and all the clients connected.

Activate communication SALTO (client) – Host (Server)

When the HOST is the server we have to enable the following checkbox:

Once enabled we have to fill up the "HOST server (ship)" with the name or IP address of the PC that is going to make this function.

After that we have to fill up the number of connections that we are going to establish and the TCP/IP port where the communications are going to be made.

The "Timeout" is the time that a client SALTO waits for the server HOST to answer a request and return a result.

The option will allow us to view all the information shared between the SALTO server and all the connected clients.

MATRIX

Advanced option LOCATION_FUNCTION_MATRIX

Introduction

This section reviews the software option Matrix for the use in Salto software. It is recommended to obtain and seek advice from your Salto certified installer before activate the function.

Function *(Background)*

The Matrix location and function is applied for large Salto Systems installations where the default limits are not enough for the access plan or there is the need to use this function to assign access rights based upon locations and door functions.

To get a picture or an idea on what location and functions are, we can use a small example.
There are three shopping malls that we can define as locations;

- *Mall 1*
- *Mall 2*
- *Mall 3*

There are different shops into these malls. These shops can be named as functions.

- Shop 1 (places in Mall 1 + 2)
- Shop 2 (places in Mall 1 + 3)
- Shop 3 (place in Mall 1)
- Shop 4 (place in Mall 2 + 3)

The doors of Shop 1 in Mall 1 will get the location “Mall 1” and as function “Shop 1” The doors of Shop 1 in Mall 2 as location “Mall 2” and function “Shop 1”.

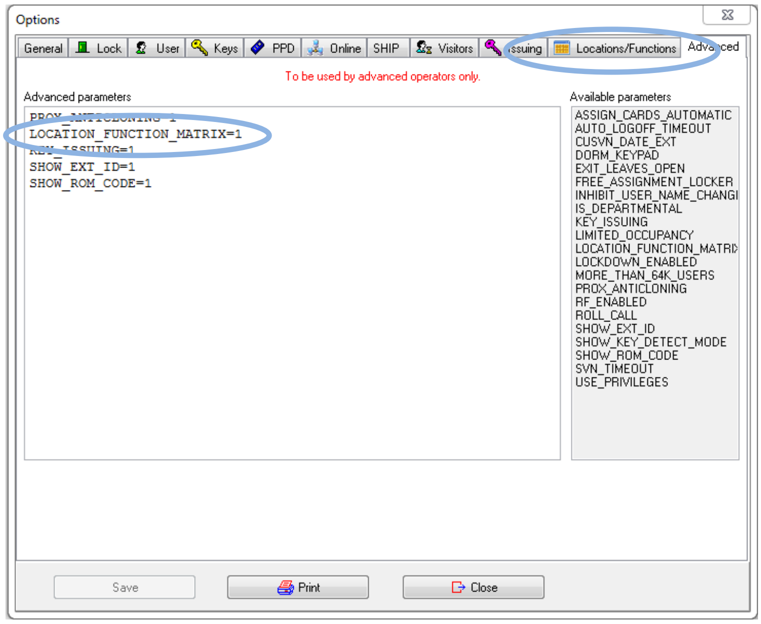
Then it is possible to assign rights to a person, to open all doors with function “Shop 1” only in the location “Mall 1” but not in “Mall 2”.

It is important to have different locations, this option allows to have a very strong tool for access plan, but it is also important to make a very good planning on how to work with this. Please be contact a SALTO partner to discuss this function before trying to use it.

Getting started

Step 1 Activate “Location_Function_Matrix”
Step 2 Set up Groups for locations and functions
Step 3 Set up Location and Function
Step 4 Assign doors for Location and Function
Step 5 Assign Access and time right to user

Step 1. Activate “Location_Function_Matrix”



To be used by advanced operators only.

Advanced parameters

```
PROX_ANTICLONING=1
LOCATION_FUNCTION_MATRIX=1
KEY_ISSUING=1
SHOW_EXT_ID=1
SHOW_ROM_CODE=1
```

Available parameters

```
ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CUSVN_DATE_EXT
DORM_KEYPAD
EXIT_LEAVES_OPEN
FREE_ASSIGNMENT_LOCKER
INHIBIT_USER_NAME_CHANGI
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
LOCATION_FUNCTION_MATRI
LOCKDOWN_ENABLED
MORE_THAN_64K_USERS
PROX_ANTICLONING
RF_ENABLED
ROLL_CALL
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SVN_TIMEOUT
USE_PRIVILEGES
```

To activate the function, set “LOCATION_FUNCTION_MATRIX=1” in Tools -> Configuration -> General Options -> Advanced tab.
Once saved, a new Tab called “Locations/Functions” to set up the groups will appear.

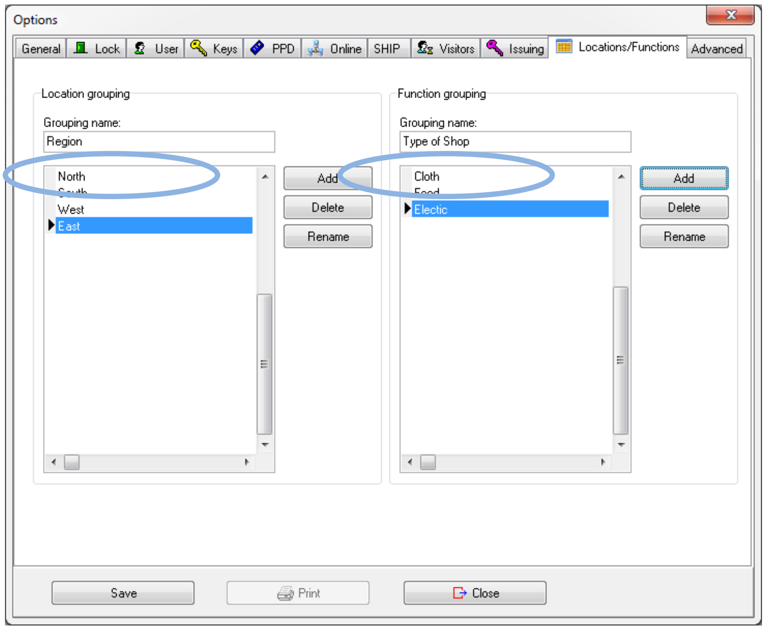
Step 2. Set up Groups for Locations and Functions

(*optional)

In this Menu we can name the Location groups or Function groups.

Important there must have a name in the free field.

The groups name is then shown. In our example "Region" and "Type of Shop"



Options

Location grouping

Grouping name: Region

North
South
West
East

Function grouping

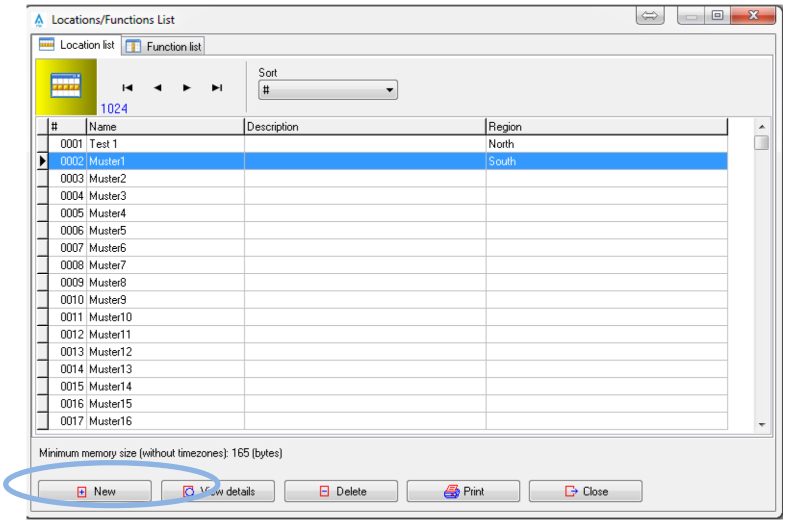
Grouping name: Type of Shop

Cloth
Food
Electic

Step 3. Set up Location and Function

In order to create different locations and functions go to Data -> Locations/Functions. The menu locations and function will appear. Then create the actual locations and functions by selecting the Tab and pressing "New".

There are some limitations on how many, within the software:
For Location max 1024
For Functions max 256.

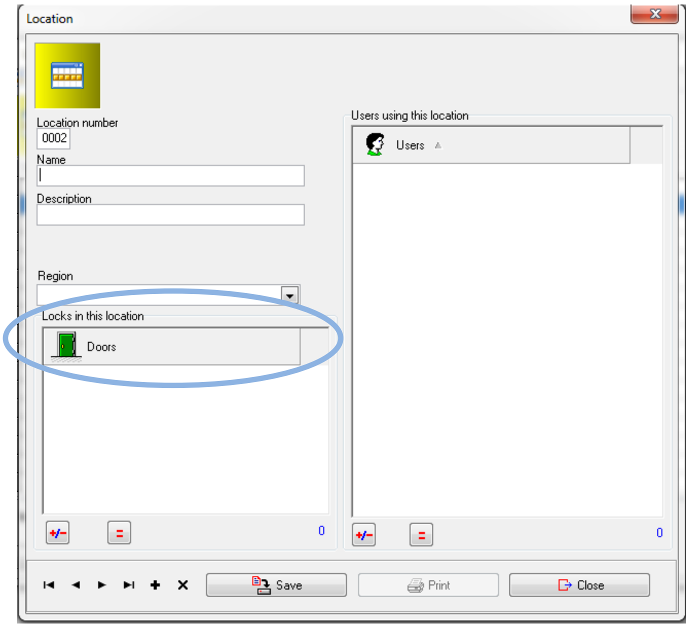


#	Name	Description	Region
0001	Test 1		North
0002	Muster1		South
0003	Muster2		
0004	Muster3		
0005	Muster4		
0006	Muster5		
0007	Muster6		
0008	Muster7		
0009	Muster8		
0010	Muster9		
0011	Muster10		
0012	Muster11		
0013	Muster12		
0014	Muster13		
0015	Muster14		
0016	Muster15		
0017	Muster16		

Minimum memory size (without timezones): 165 (bytes)

By creating a new location, it is mandatory to name it.
It is recommended that the chosen names are relevant to the installation and it is advisable also to add a Description. It is possible to assign it to a "group"
In this example it was name Region
Look at step 2.
When this information is saved create the rest of the needed locations and functions.

When everything is set up, start adding the selected doors into to the matrix respectively for Locations and Functions.



Location number
0002
Name
Description
Region

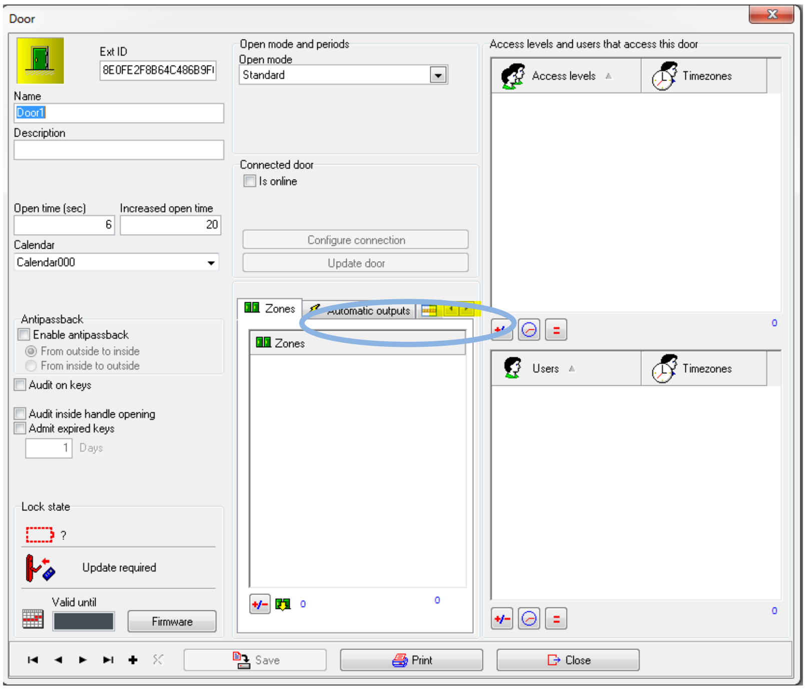
Important:
The "add" doors can be selected in Location and Function. A user has to be assign to both, a location and a function.
There is no Time involved yet.

Step 4. Assign doors for Location and Function

It is also possible to assign Functions and locations on the Doors window. In Door -> View details

Scroll right in the middle of the screen to see the locations and functions tab.

To assign a door to the location and function, just select it in the menu.


Door

Ext ID: 8E0FE2F8B64C486B9FI
Name: Door1
Description:
Open time (sec): 6
Increased open time: 20
Calendar: Calendar000
Antipassback
☐ Enable antipassback
○ From outside to inside
○ From inside to outside
☐ Audit on keys
☐ Audit inside handle opening
☐ Admit expired keys
1 Days
Lock state: ?
Update required
Valid until

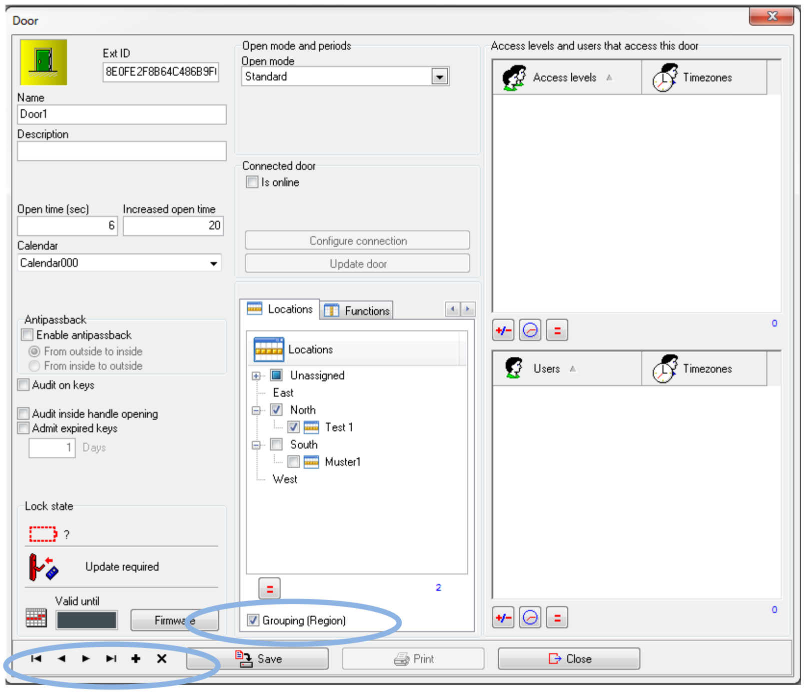
Open mode and periods
Open mode: Standard
Connected door
☐ Is online

Access levels and users that access this door

For a better view we can check the box “Grouping” to find a door faster or assign a complete group in one shot.

This can be done with all doors.

Important:
All the doors have to be updated.
The doors must know that they are part of the matrix.


Door

Ext ID: 8E0FE2F8B64C486B9FI
Name: Door1
Description:
Open time (sec): 6
Increased open time: 20
Calendar: Calendar000
Antipassback
☐ Enable antipassback
○ From outside to inside
○ From inside to outside
☐ Audit on keys
☐ Audit inside handle opening
☐ Admit expired keys
1 Days
Lock state: ?
Update required
Valid until

Open mode and periods
Open mode: Standard
Connected door
☐ Is online

Locations
- ☐ Unassigned
- East
- ☑ North
  - ☑ Test 1
- ☐ South
  - ☐ Muster1
- West

☑ Grouping (Region)

Access levels and users that access this door

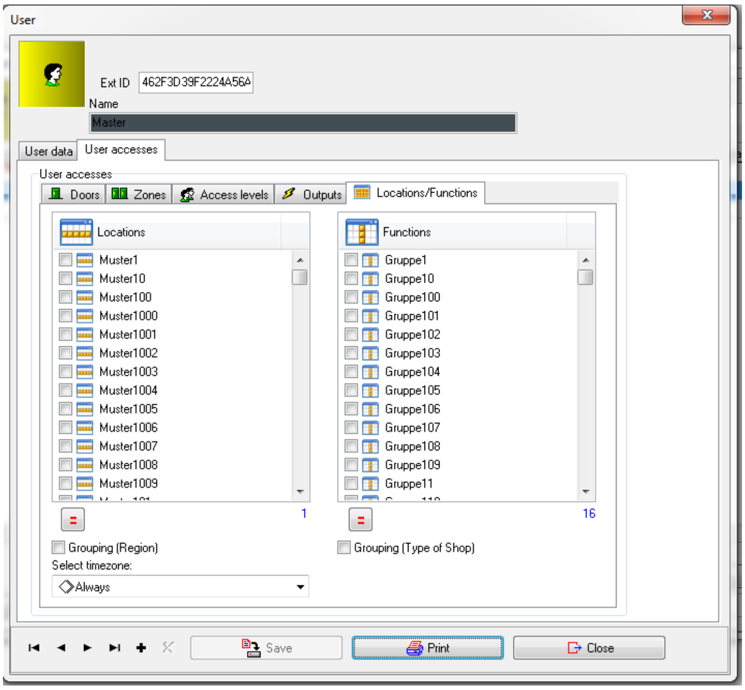
Step 5. Assign Access and time right to user

The last step for a correct set up is assigning locations and functions to the users so each user has granted access through the doors at the right time.

In User -> View details -> User accesses.

Select every needed location and function.

Be advised, the person that have been assigned to a location and a function, will be able to open all doors that have the same combination of location and function assigned.



User

Ext ID 462F3D39F2224A56A

Name Master

User accesses

Locations

- □ Muster1
- □ Muster10
- □ Muster100
- □ Muster1000
- □ Muster1001
- □ Muster1002
- □ Muster1003
- □ Muster1004
- □ Muster1005
- □ Muster1006
- □ Muster1007
- □ Muster1008
- □ Muster1009

Functions

- □ Gruppe1
- □ Gruppe10
- □ Gruppe100
- □ Gruppe101
- □ Gruppe102
- □ Gruppe103
- □ Gruppe104
- □ Gruppe105
- □ Gruppe106
- □ Gruppe107
- □ Gruppe108
- □ Gruppe109
- □ Gruppe11

□ Grouping (Region)

□ Grouping (Type of Shop)

Select timezone: Always

For a better and easier view activate the “Grouping” on both lists.

The last point here is to set the correct time zone.

Important
It is only possible to assign **one** time zone for all accesses.

For more information please be in contact with your Salto certified installer.

SALTO Wireless

System Setup

Together with the offline locks the system can be improved with the use of the Salto Wireless escutcheons. This section describes the steps to setup a complete Wireless installation.

Two working ways will be shown in this section;

- Working with RF1 MODE 1
- Working with RF2 MODE 2 (only for services versions)

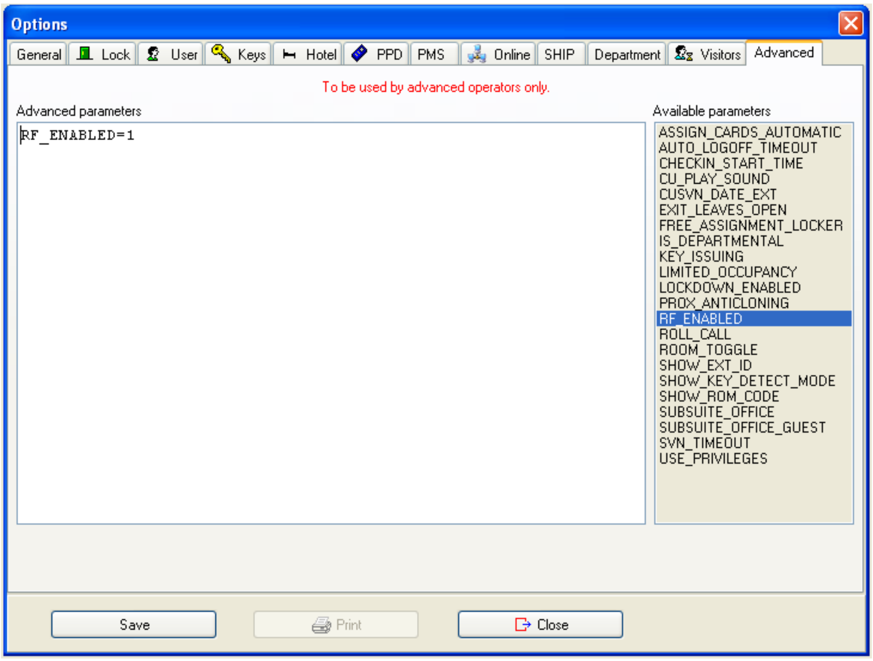
The main difference between the two systems is the gateways and the configuration. The first part of this section is common for both working modes.

9.1 RF_ENABLED=1

To start setting up the Wireless system, the radio frequency (RF) module must be activated.

Follow the next steps:

Tools
Configuration
General options
Advanced



To be used by advanced operators only.

Advanced parameters

```
RF_ENABLED=1
```

Available parameters

ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CHECKIN_START_TIME
CU_PLAY_SOUND
CUSVN_DATE_EXT
EXIT_LEAVES_OPEN
FREE_ASSIGNMENT_LOCKER
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
LOCKDOWN_ENABLED
PROX_ANTICLONING
RF_ENABLED
ROLL_CALL
ROOM_TOGGLE
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SUBSUITE_OFFICE
SUBSUITE_OFFICE_GUEST
SVN_TIMEOUT
USE_PRIVILEGES

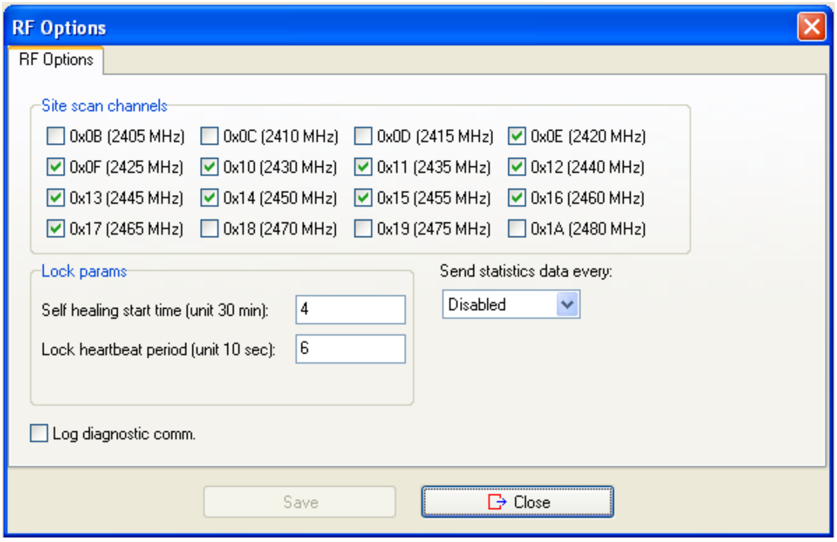
RF Options

Under RF OPTIONS the general parameters of the system are defined.

Follow the next steps:

Tools
Configuration
RF options

Site scan channels



RF Options

RF Options

Site scan channels

□ 0x0B (2405 MHz)	□ 0x0C (2410 MHz)	□ 0x0D (2415 MHz)	☑ 0x0E (2420 MHz)
☑ 0x0F (2425 MHz)	☑ 0x10 (2430 MHz)	☑ 0x11 (2435 MHz)	☑ 0x12 (2440 MHz)
☑ 0x13 (2445 MHz)	☑ 0x14 (2450 MHz)	☑ 0x15 (2455 MHz)	☑ 0x16 (2460 MHz)
☑ 0x17 (2465 MHz)	□ 0x18 (2470 MHz)	□ 0x19 (2475 MHz)	□ 0x1A (2480 MHz)

Lock params

Self healing start time (unit 30 min): 4

Lock heartbeat period (unit 10 sec): 6

Send statistics data every: Disabled

□ Log diagnostic comm.

The SALTO Wireless system uses the IEEE 802.15.4 protocol transmitting the signal at a high frequency range of 2,4GHz. This window shows the 16 different channels showing the name (in hexadecimal) and the corresponding frequency.

In order to improve the quality of the transmissions, a channels filter is suitable. Contact with your SALTO dealer for more details.

Lock parameters

. Self healing start time

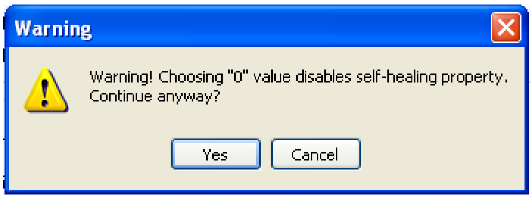
This parameter (in units of 30min) defines the time the system will wait to start with the Self healing process.

The Self healing process is started by the Wireless lock to look for a new parent device (Gateway or Repeater) when the communication has been lost.

. Lock heartbeat period

This parameter (in units of 10s) defines the frequency of the lock´s heartbeat. It consists in a brief signal the lock emits to be seen by its parent device (Gateway or Repeater)

Note: If there is no parent device redundancy, it is recommended to use “0” to disable the self healing process.



Warning

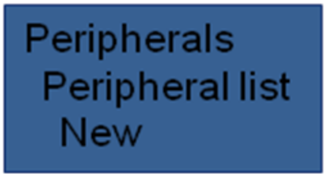
Warning! Choosing "0" value disables self-healing property. Continue anyway?

WORKING WITH MODE 1

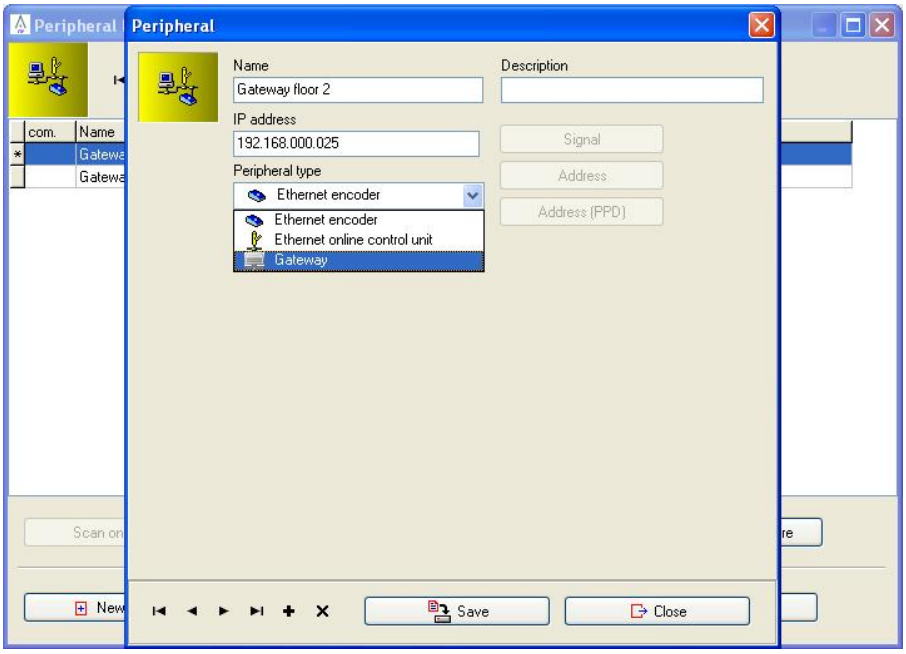
Gateways RF1

The different Gateways must be declared with their static IP address.

Follow the next steps:



Peripherals
Peripheral list
New



Peripheral

Name: Gateway floor 2

Description:

IP address: 192.168.000.025

Peripheral type: Ethernet encoder

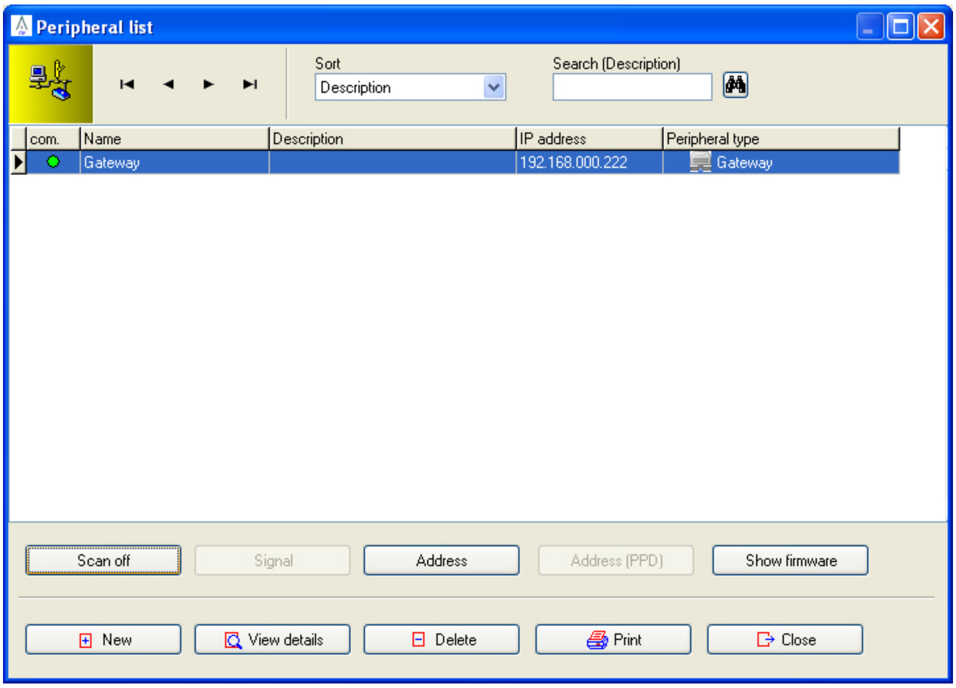
Once the Gateway is declared it must be addressed to establish the communication.

Follow the next steps:

Peripherals
Peripheral list
Address

The CLR button must be pressed to put the Gateway in address mode. Then the Address button must be used.

By clicking on the “Scan on” button the “com.” led will show the status of the Gateway.



Sort: Description

com.	Name	Description	IP address	Peripheral type
●	Gateway		192.168.000.222	Gateway

Repeaters RF1

The Repeaters are managed through a separate window.

Follow the next steps:

Peripherals
Repeaters
New

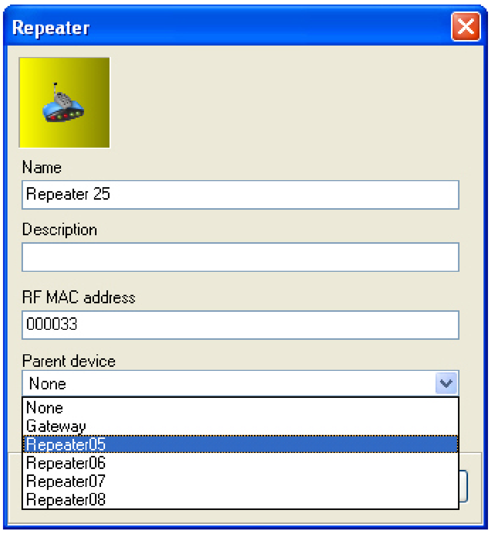
2 parameters define this device:

- RF MAC address

This parameter consists of 3 pairs of hexadecimal numbers and is printed on the Repeater RF antennae.

- Parent device

The Repeater has to be associated to another Gateway or Repeater (its parent device).



Repeater

Name: Repeater 25

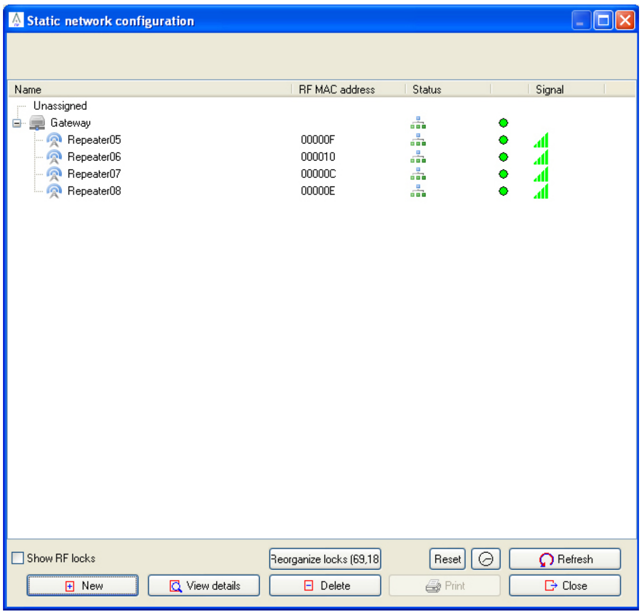
Description:

RF MAC address: 000033

Parent device: None

Note: the Gateway does not have any MAC address.

Once everything is setup, the Repeaters will associate themselves to their parent device establishing the communication.



Static network configuration

Name	RF MAC address	Status		Signal
Unassigned				
Gateway			●	
Repeater05	00000F		●	
Repeater06	000010		●	
Repeater07	00000C		●	
Repeater08	00000E		●	

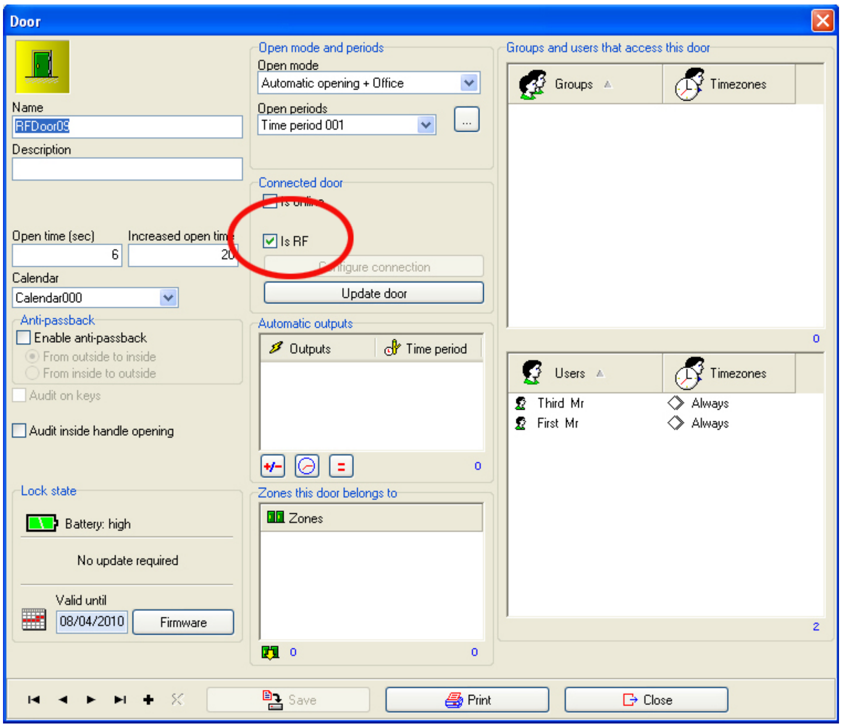
□ Show RF locks

Wireless Locks RF1

The wireless locks are created through the DOORS menu.

Follow the next steps:

Doors
New



Door

Name: RFDoor09

Description:

Open time (sec): 6

Increased open time: 20

Calendar: Calendar000

Anti-passback

☐ Enable anti-passback

○ From outside to inside

○ From inside to outside

☐ Audit on keys

☐ Audit inside handle opening

Lock state

Battery: high

No update required

Valid until: 08/04/2010

Open mode and periods

Open mode: Automatic opening + Office

Open periods: Time period 001

Connected door

☐ Is online

☑ Is RF

Automatic outputs

Outputs	Time period

0

Zones this door belongs to

Zones

0 0

Groups and users that access this door

Groups	Timezones

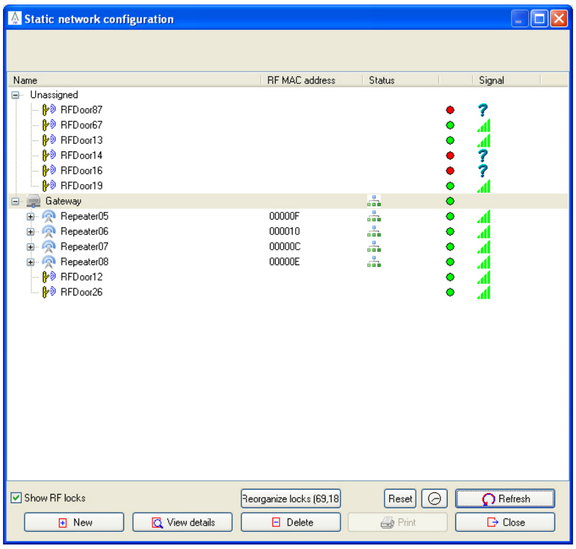
0

Users	Timezones
Third Mr	Always
First Mr	Always

2

Mark the RF option in order to make it Wireless.

Once the different doors are created they have to be initialized with the PPD. The escutcheons start the process to look for the available static devices (Gateways / Repeaters) and associate to them.



Name	RF MAC address	Status		Signal
⊟ Unassigned				
RFDoor87			🔴	?
RFDoor67			🟢	▂▄▆█
RFDoor13			🟢	▂▄▆█
RFDoor14			🔴	?
RFDoor16			🔴	?
RFDoor19			🟢	▂▄▆█
⊟ Gateway		🖧	🟢	
⊞ Repeater05	00000F	🖧	🟢	▂▄▆█
⊞ Repeater06	000010	🖧	🟢	▂▄▆█
⊞ Repeater07	00000C	🖧	🟢	▂▄▆█
⊞ Repeater08	00000E	🖧	🟢	▂▄▆█
RFDoor12			🟢	▂▄▆█
RFDoor26			🟢	▂▄▆█

☑ Show RF locks

Monitoring of online locks

The online wireless system can be monitor through this window.

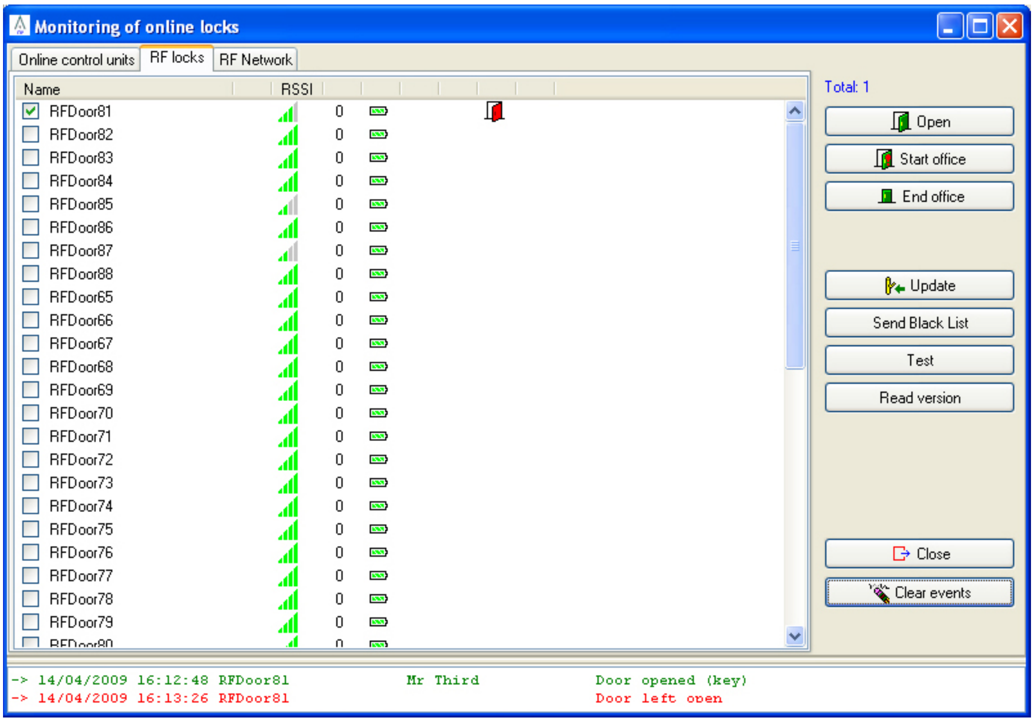
Follow the next steps:

Peripherals
Monitoring of online locks

Two new tabs give information about the status of the wireless escutcheons.

RF locks

This window allows monitoring the status of the wireless locks. Together with the door name, parameters like the coverage (level of signal), the battery status, door left open and intrusion signals are displayed.



Name	RSSI		
☑ RFDoor81		0	
☐ RFDoor82		0	
☐ RFDoor83		0	
☐ RFDoor84		0	
☐ RFDoor85		0	
☐ RFDoor86		0	
☐ RFDoor87		0	
☐ RFDoor88		0	
☐ RFDoor65		0	
☐ RFDoor66		0	
☐ RFDoor67		0	
☐ RFDoor68		0	
☐ RFDoor69		0	
☐ RFDoor70		0	
☐ RFDoor71		0	
☐ RFDoor72		0	
☐ RFDoor73		0	
☐ RFDoor74		0	
☐ RFDoor75		0	
☐ RFDoor76		0	
☐ RFDoor77		0	
☐ RFDoor78		0	
☐ RFDoor79		0	
☐ RFDoor80		0	

```
-> 14/04/2009 16:12:48 RFDoor81          Mr Third             Door opened (key)
-> 14/04/2009 16:13:26 RFDoor81                               Door left open
```

While the bottom part shows the events in real time, on the right hand side the following options are available:

Open

It allows a remote timed opening of the selected wireless locks (the opening delay is based on the “Increased open time”).

Start office

End office

The selected locks can be opened remotely (and stay opened). Prior to use this option, the lock must have the office mode enabled.

Update

An online update can be performed in order to send the last hardware modifications.

Send Black List

Whenever a user is cancelled the black list is periodically sent to the online devices (CU + wireless locks). This option permits to force a manual sending of this information.

Test

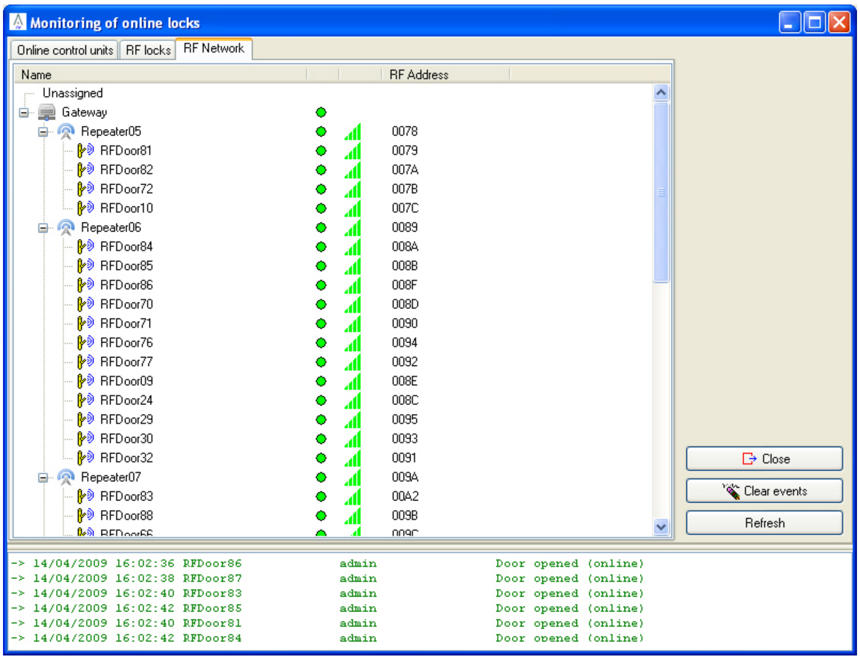
This option sends a test signal that returns a “beep” from the escutcheon confirming the communication.

The wireless lock firmware version will be displayed:

- RF antennae
- Control
- Reader

RF Network

The different wireless locks will associate automatically to the best possibility of parent device (Gateway / Repeater) in terms of availability and signal level.



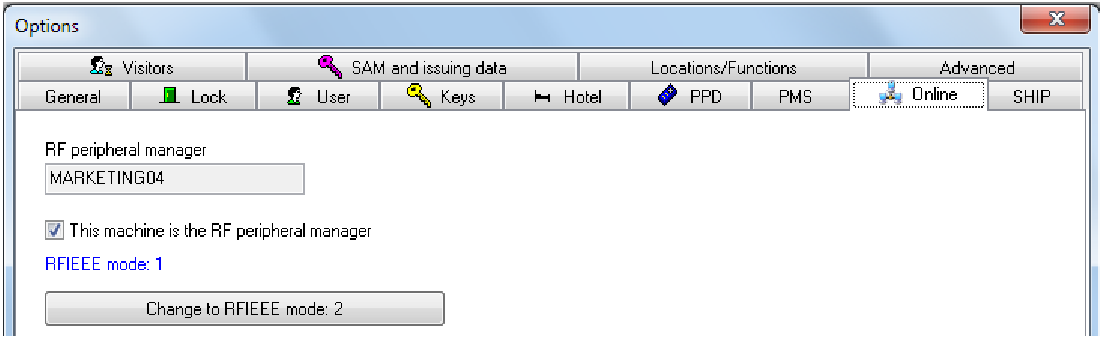
Name			RF Address
Unassigned			
Gateway	●		
Repeater05	●	📶	0078
RFDoor81	●	📶	0079
RFDoor82	●	📶	007A
RFDoor72	●	📶	007B
RFDoor10	●	📶	007C
Repeater06	●	📶	0089
RFDoor84	●	📶	008A
RFDoor85	●	📶	008B
RFDoor86	●	📶	008F
RFDoor70	●	📶	008D
RFDoor71	●	📶	0090
RFDoor76	●	📶	0094
RFDoor77	●	📶	0092
RFDoor09	●	📶	008E
RFDoor24	●	📶	008C
RFDoor29	●	📶	0095
RFDoor30	●	📶	0093
RFDoor32	●	📶	0091
Repeater07	●	📶	009A
RFDoor83	●	📶	00A2
RFDoor88	●	📶	009B
RFDoor66	●	📶	009C

```
-> 14/04/2009 16:02:36 RFDoor86           admin               Door opened (online)
-> 14/04/2009 16:02:38 RFDoor87           admin               Door opened (online)
-> 14/04/2009 16:02:40 RFDoor83           admin               Door opened (online)
-> 14/04/2009 16:02:42 RFDoor85           admin               Door opened (online)
-> 14/04/2009 16:02:40 RFDoor81           admin               Door opened (online)
-> 14/04/2009 16:02:42 RFDoor84           admin               Door opened (online)
```

WORKING WITH MODE 2

To start working in MODE 2, go to General Options/ Online tab, and make sure the blue inscription is "**RFIEEE mode: 2**". If not, click the "**Change to RFIEEE mode: 2**" button.

MODE 1;



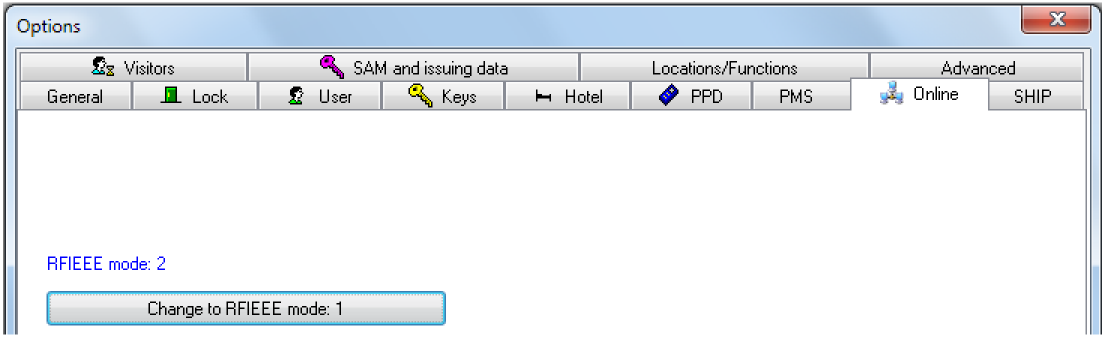
RF peripheral manager

MARKETING04

☑ This machine is the RF peripheral manager

RFIEEE mode: 1

MODE 2;



RFIEEE mode: 2

In MODE 2 ALL the communications are managed by the Service, including the RF communications. In MODE 1, the RF communications are managed by the SW itself, PA/HAMS.

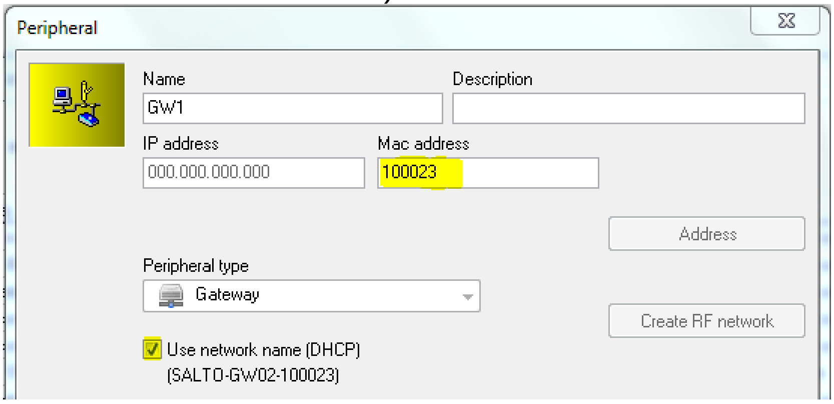
Once in MODE2, start creating GATEWAYS and Nodes;
IMPORTANT: Bear in mind that to work in MODE 2, it is mandatory to use Gateways 2, the PPD FW version must be 01.24 or above, AElement control board FW version must be 01.19 or above and XS4 01.24 or above.

Gateways RF 2

The Gateways will do the NETWORK link. Go to Peripheral/ Peripheral List and start creating each of the needed gateways.
There are two ways to set the configuration;

1/ Using DHCP
2/ Static IP address

1/ **Using DHCP**, bear in mind that a DHCP server is needed. This one will automatically assign an IP address to the gateway. Enable the "**Use network name (DHCP)**" option. There is no need to fill the IP address fields, only the MAC address must be written on the "**MAC address**" field. This MAC address is located on the Ethernet board of the gateway RF2 (not to confuse with the one on the antenna/node)



Name: GW1
Description:
IP address: 000.000.000.000
Mac address: 100023
Peripheral type: Gateway
☑ Use network name (DHCP)
(SALTO-GW02-100023)

To address the Gateway 2 connect it to the LAN (DO NOT USE A CROSSED CABLE). Press the CLR button for about 5 seconds until the led becomes **orange.**
Once this is done, go to the internet browser and type address **192.168.0.234**, select **DHCP** and then click "Send".

2/ **<u>Using a STATIC IP</u>**, the "**Use network name (DHCP)**" option must be disabled and then fill both fields, **IP** address and **MAC** address and then "Save".
Connect the Gateway 2 to the LAN (DO NOT USE A CROSSED CABLE). Press the CLR button for about 5 seconds until the led becomes **orange.**
Once this is done, go to the internet browser, type address **192.168.0.234**, write the same IP than in the SW for this device and select **STATIC**, then click "Send".

Automatically, in both cases, DHCP and STATIC, the Gateway will start communicating with the SALTO Service by itself without the need do any other operation.

<u>NOTE</u>: The Gateways are compatible with PoE routers. For more info, consult the Gateways technical documentation.

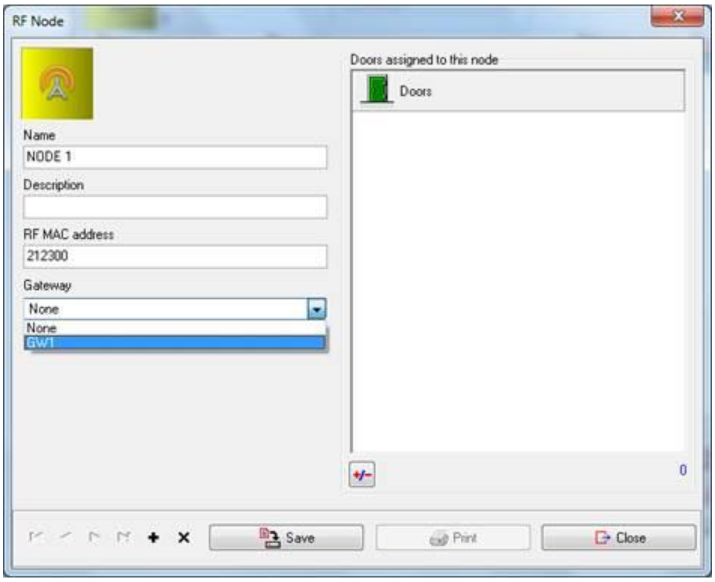
Nodes RF2

After the Gateway is created, the **Nodes** to be used must be created. The Node can be 2 different ways;

1/ Just an RF antenna to plug into the Gateway, called mini node.

2/ Independent; looking as a SALTO modular wall reader and to be connected with a RS485 connection.

Go to Peripheral and click on RF Node; the following window will appear;



RF Node

Name: NODE 1

Description:

RF MAC address: 212300

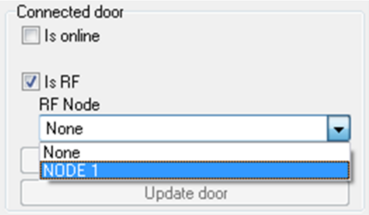
Gateway: None

Write a name for the Node and a description if needed. On the "**RF MAC address**" field, type the **MAC** of the ANTENNA (NOT to confuse with the Ethernet board MAC). In "**Gateway**" select the Gateway where it will be connected to. This connection is STATIC; the Node will always be connected to this Gateway and will never switch to another Gateway by itself. Then click on "Save".

Once the Gateway is connected to the Service, the Node will start communicating by itself.

Creating the LINK with DOORS

Create the door as shown previously on this manual and select the "Is RF" option. Then select the Node where the door will be connected to, and then click "Save".



Connected door

□ Is online

☑ Is RF

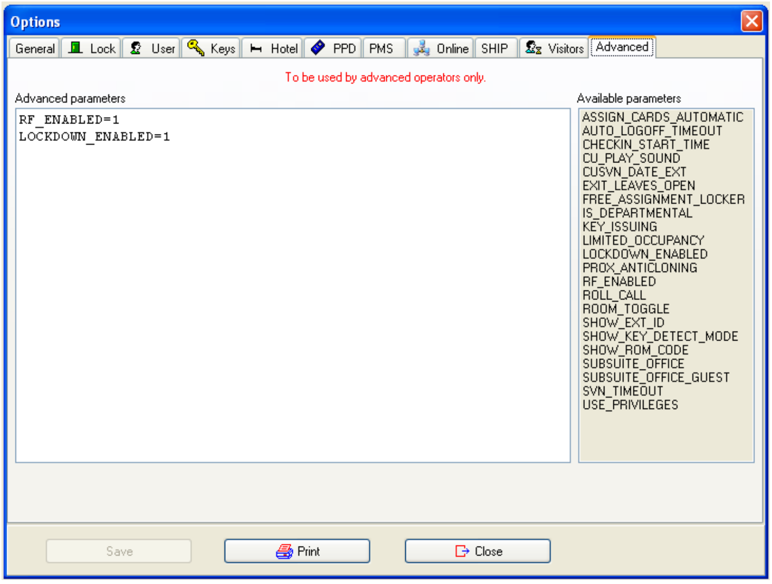
RF Node: None

Only after this is done, download the PPD information and initialize the locks. **DO NOT DO IT BEFORE**, if so the locks won't start communicating. The PPD will inform each door about the network so every door knows what NODE to connect to.

Lockdown

This option allows securing a defined area with CU and Wireless locks in order to easily close all the accesses in an emergency situation.

An activation of this feature is needed in the “Advanced” tab of the “General Options”: LOCKDOWN_ENABLED=1



To be used by advanced operators only.

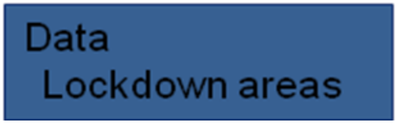
Advanced parameters

```
RF_ENABLED=1
LOCKDOWN_ENABLED=1
```

Available parameters

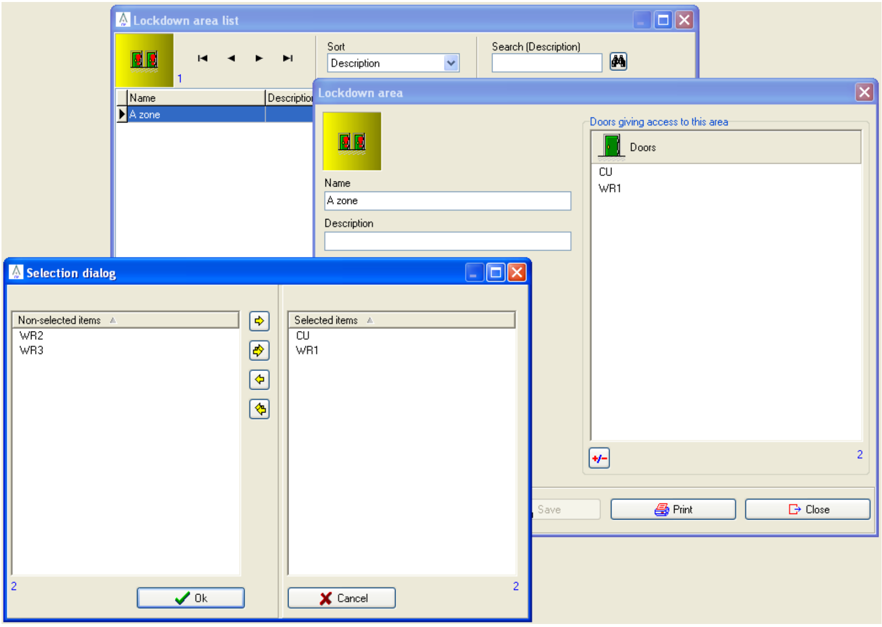
ASSIGN_CARDS_AUTOMATIC
AUTO_LOGOFF_TIMEOUT
CHECKIN_START_TIME
CU_PLAY_SOUND
CUSVN_DATE_EXT
EXIT_LEAVES_OPEN
FREE_ASSIGNMENT_LOCKER
IS_DEPARTMENTAL
KEY_ISSUING
LIMITED_OCCUPANCY
LOCKDOWN_ENABLED
PROX_ANTICLONING
RF_ENABLED
ROLL_CALL
ROOM_TOGGLE
SHOW_EXT_ID
SHOW_KEY_DETECT_MODE
SHOW_ROM_CODE
SUBSUITE_OFFICE
SUBSUITE_OFFICE_GUEST
SVN_TIMEOUT
USE_PRIVILEGES

Follow the next steps:



Data
  Lockdown areas

The lockdown area will group a list of online wall readers together with wireless locks.



Lockdown area list: A zone (1)

Lockdown area — Name: A zone; Description: (empty)

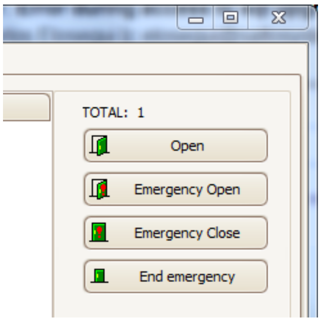
Doors giving access to this area: CU, WR1 (2)

Selection dialog — Non-selected items: WR2, WR3 (2); Selected items: CU, WR1 (2)

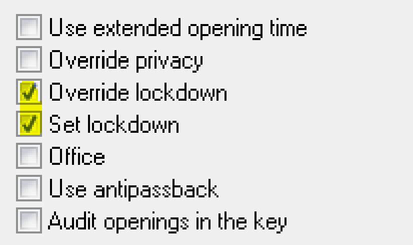
Follow the next steps:

Peripheral Lockdown

Once the areas are defined the “Emergency close” button can be used to remotely close all (or the selected) the doors within an area or “Emergency Open” if necessary.



The access to these units will be denied (even if the user has the rights on the card) until “End emergency” button is pressed.
Only the authorized users with the “Override lockdown” options will be able to open them.



☐ Use extended opening time
☐ Override privacy
☑ Override lockdown
☑ Set lockdown
☐ Office
☐ Use antipassback
☐ Audit openings in the key

AMOK

This function is only available on the AMOK escutcheon. This escutcheon can be placed in AMOK (crisis) mode.

The AMOK mode is a sort of standalone lockdown. This can be activated by presenting a card on the inside reader. In case of an emergency situation, where it is safer to be locked in the inside of the classroom or office, the AMOK mode enables to lockdown instantly the escutcheon just by presenting a valid user with **SET LOCKDOWN** privilege. Once this mode enabled no one can enter. Only a user with **OVERRIDE LOCKDOWN** can remove the escutcheons from the Lockdown mode.

OVERRIDE LOCKDOWN, will allow opening if the door is closed by lockdown.
SET LOCKDOWN, will allow to enable or disable the lockdown mode.

The **LOCKDOWN_ENABLED=1** option must be enabled in the Pro-Access software. Go to **TOOLS / CONFIGURATION / GENERAL OPTIONS / ADVANCED TAB.**