SALTO

inspiredaccess

www.saltosystems.com

Pro-Access READ/ WRITE ACCESS CONTROL

Manual de usuario V 11.04.x.x

SALTO SOFTWARE PARA CONTROL DE ACCESOS

INTRODUCCIÓN: 8

INSTALACIÓN DEL PROGRAMA 9

SERVIDOR SQL 10

Configurar servicios para admitir conexiones remotas 17

Apertura de la BD 19

Configuración del servidor SQL 20

SALTO SERVICE RW 24

Requerimientos de Hardware y Sistema 24

Instalación 25

OPERADORES DEL SOFTWARE. COMPETENCIAS 32

Crear Base de datos NUEVA 32

Migración de una BBDD Access 35

Competencias de los operadores 36

IMPORTAR DESDE UNA BD SALTO (Merging) 43
Origen de la DB 43
Versión de la BD inválida 44
NOTAS importantes 45

EXPORTAR 46

OPERADOR ADMINISTRADOR. 50

PUERTAS 51

LIMITAR EL ACCESO DE USUARIOS 61

ZONAS 63

SALIDAS 69

Salidas automáticas **71**

PERIODOS. **72**

HORARIOS. **75**

CALENDARIOS. **77**

CAMBIO HORARIO. **80**

Cambios temporales automáticos **83**

NIVELES DE ACCESO **88**

LISTA DE USUARIOS **94**

Actualización de clave de teclado a través de SVN **99**

EXPIRACION POR DEFECTO EN HORAS Y DIAS. **103**

Asignación de llaves a los usuarios **107**

Taquillas: **111**
Crear taquillas: 111
Zona de Libre Asignación: 112
Crear una Zona de Libre Asignación: 112
Múltiples Zonas de libre asignación: 113
Cierre libre: 114
Tipos de Llaves: 115
Ocupación de taquilla limitada: 116
Reiniciar la temporización al volver a capturar: 116
Taquillas & Visitas: 116
Inicialización de Taquillas: 116
Información del número de la Taquilla capturada: 116

VISITAS: **118**

Check in de visitas: **120**

LISTA NEGRA **122**

CONFIGURACIÓN DE LISTA NEGRA **122**

ACTUALIZACIÓN AUTOMÁTICA DE LLAVES **124**

UTILIZAR EL PPD .INICIALIZAR **126**
Menú principal 126

Inicializar las puertas: **127**

OPCIONES AVANZADAS **131**

Identificar su instalación **131**

Estado del PPD. **133**

Opciones Locales **134**

Estado del Editor. **135**

Estado de las puertas **136**

SALIDAS TEMPORIZADAS **138**

ON LINE **139**

ROLL-CALL: **140**
Crear Áreas Roll-Call: 141
Área Externa: 142

MONITORIZACIÓN DE LAS ÁREAS ROLL-CALL **143**

Limitación de accesos (Parking): **147**

MOSTRAR EL CÓDIGO ROM: **149**

Mostrar el código Wiegand: **150**

GENERADOR DE FORMATO WIEGAND FLEXIBLE **151**

AUTO LOGOFF **154**

PURGADO AUTOMÁTICO **154**

USUARIO **157**

Escribir información adicional en las pistas **158**

Escribir información extra en las llaves de usuarios/clientes. **159**

RANGO DE PUERTOS **161**

Eliminación de usuarios permanentes **161**

ASIGNACIÓN AUTOMÁTICA DE USUARIOS **163**

EMISIÓN DE LLAVES **166**

Llaves MIFARE **168**

AUMENTO DE SECTORES EMITIDOS **169**

DESFire Evolution 1 **169**

PMK diversificada **170**

MIFARE PLUS **170**

LEGIC PRIME y ADVANT **171**

AUDITOR **173**

Filtro avanzado **173**

Crear un filtro nuevo: **174**

EXPORTACIÓN AUTOMÁTICA DEL AUDITOR DE CERRADURAS **180**

BADGING **185**

MENÚ DE PERIFÉRICOS **192**
Monitorización de unidades de control online 192

Monitorización Múltiple online **198**

ACTUALIZACIÓN DEL FIRMWARE DE EDITORES & PPD **200**

Actualización de lectores: **201**

LISTA DE PERIFÉRICOS **203**

Inicialización de Periféricos **206**

Configuración de editores Ethernet: **207**

Inhibir maestro de comunicaciones **209**

IDIOMAS. CAMBIO DE IDIOMA. **211**

LOG-OUT. CAMBIAR DE OPERADOR. 211

CONFIGURACIÓN DE UNA BASE DE DATOS DEPARTAMENTAL 212

Introducción 212

Activar la opción departamental 212

Como crear departamentos 213

Elementos Internos: 214

Compartir Elementos 217

Elementos externos: 218

Operaciones 219

Grupos de Operadores 220

Cómo trabajar con elementos Externos 222

CONECTAR EL PPD 226

Programador Portátil 226

AUDITOR DE CERRADURAS. 228

Recoger las aperturas en una puerta. 228

LLAVES DE REPUESTO Y PROGRAMADORAS 230

SINCRONIZACIÓN AUTOMÁTICA Y STADGING TABLE 231

STREAMS DE EVENTOS (SOLO DISPONIBLE EN SERVICIO SALTO!) 237

SALTO HOST INTERFACE PROTOCO - SHIP 241

Activar comunicación SALTO (Servidor) – Host (Cliente) 241

Activar la comunicación SALTO (Cliente) – Host (Servidor) 242

ACCESOS POR MATRIZ 242
Paso 1. Activando “Location_Function_Matrix” 243
Paso 2. Creando agrupaciones para Ubicaciones y Funciones 244
Paso 3. Creando Ubicaciones y Funciones. 245
Paso 4. Asignando puertas a Ubicaciones y Funciones: 246

Paso 5. Asignando Accesos y horarios a usuarios. 247

SALTO WIRELESS **249**
Configuración del sistema 249
Configuración RF 250
Parámetros de cerradura 250

TRABAJANDO EN MODO 1 **251**
Gateways RF1 251
Repetidores RF1 252
Cerraduras Wireless 254
Monitorización de cerraduras online 255
Cerraduras RF 255
Red RF 257

TRABAJANDO EN MODO 2 **257**
Gateways RF2 258
Nodos RF2 259
Crear enlace con PUERTAS 260

LOCKDOWN **261**

LOCKDOWN en AMOK **263**

Introducción:

El programa de SALTO PARA CONTROL DE ACCESOS ha sido diseñado para gestionar el control de acceso a una instalación hostelera o residencial en la que se utilizan elementos de identificación de *lectura-escritura*.

Con este sistema es posible realizar 2 tareas fundamentales:

- diseñar el plan de cierre y realizar la inicialización primera de las cerraduras electrónicas.
- Mantener una aplicación que puede ser usada por los usuarios de la instalación

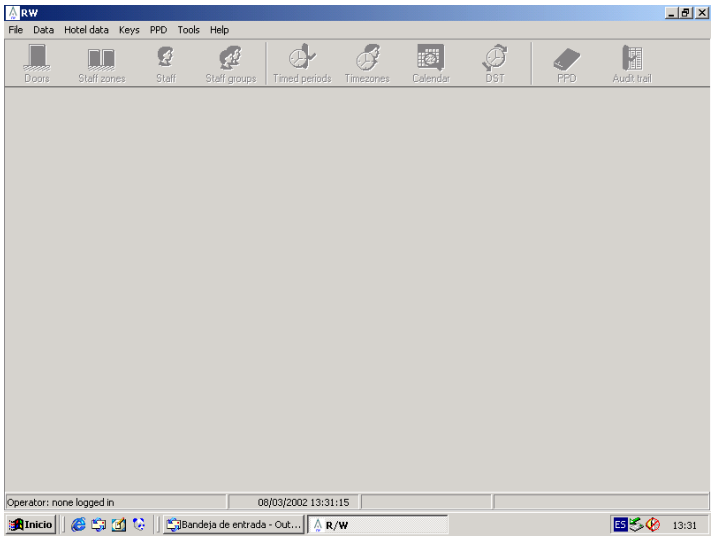


Figura 1.

Una vez elaborado el plan de cierre, trasladaremos toda esa información a cada una de las puertas de nuestra instalación, mediante el PPD, pequeño dispositivo de programación portátil, que va a ser indispensable para la puesta en marcha de la instalación, y para auditar las puertas siempre que se desee.

En resumen, usted necesitará los siguientes elementos para la gestión del control de accesos en el hotel:

1. Software RW de Salto instalado en 1 ordenador PC. (o en el servidor de su red de área local)
2. Tarjetas Smart, tanto para la plantilla del hotel como para los huéspedes.
3. Escudos electrónicos Smart para las puertas que necesiten control de acceso.
4. 1 editor de tarjetas.
5. 1 programador portátil (PPDX00).

Instalación del programa

Para instalar el software suministrado por SALTO, su ordenador necesita unos requerimientos mínimos, que son los siguientes:

SQL DB

RAM: 1GB.
Procesador: 1 GHz or mayor. 32Bits o 64Bits.
Espacio disponible en **disco duro**: 10 GB. (Aprox. Depende de la BD)
Sistema operativo: Windows XP, Windows Vista, Windows 7 (32bits y 64bits), Windows Server 2003, Windows Server 2008, Windows 8 (32bits y 64bits)
MS-SQL: MS-SQL 2000, MS-SQL 2005, 2008, 2008R2 and 2012 – todas las ediciones, incluido el MS-SQLExpress -
Resolución mínima: 1024x768

Puntos específicos para la plataforma SQL+SERVICIO:

MS-SQL: MS-SQL 2005, 2008, 2008R2 y 2012 – incluido el MS-SQLExpress - (MS-SQL 2000 no es compatible!)
.NET Framework 3.5 (obligatorio)
MS-Windows Installer 3.1
Sistema de Nombres de Dominio (DNS - Domain Name System)
Entorno con **Dominio**: Muy recomendado

ATENCIÓN**: asegúrese que el reloj de su PC está en hora, y no adelanta ni atrasa, ya que la hora del sistema dependerá de la hora de su PC.**

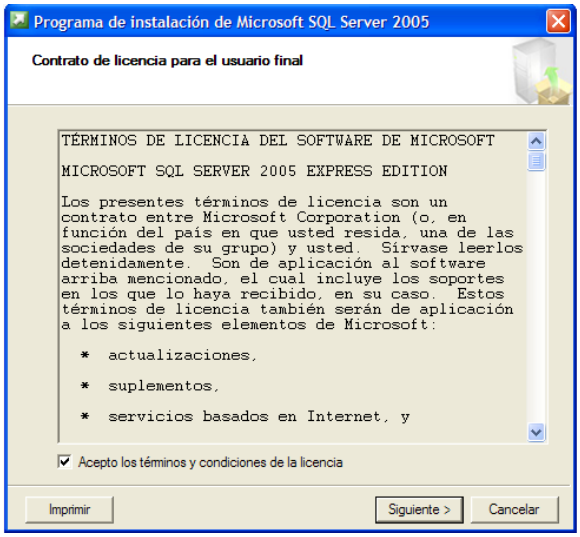
El software de Salto permite trabajar en modo multipuesto, es decir, se puede trabajar con el programa en diferentes PCs al mismo tiempo contra la misma base de datos. La condición indispensable es que cada usuario tenga acceso a la carpeta que contiene la base de datos con privilegios de lectura/escritura. Es preferible que la base de datos esté ubicada en el servidor, en caso de que éste exista.

Servidor SQL

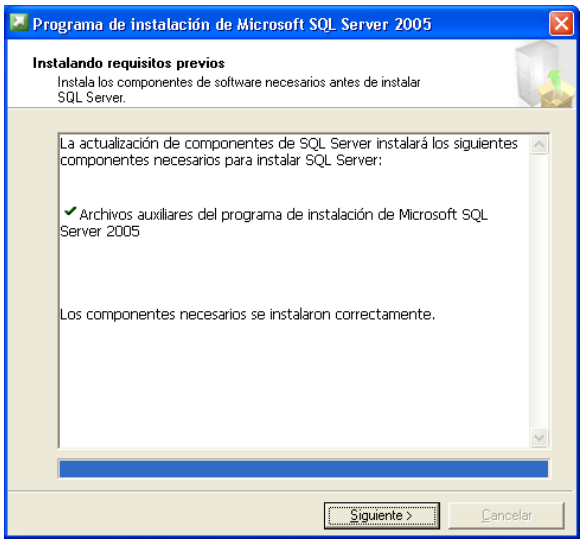
El software SALTO SQL necesita de la instalación previa de un servidor SQL el cual se encargará de gestionar las consultas de los distintos clientes hacia y desde la base de datos.

Si no se dispone de dicha herramienta, SALTO recomienda la utilización de la solución gratuita de Microsoft: SQL Server 2005 Express (o superior). Este programa está disponible en el siguiente enlace:

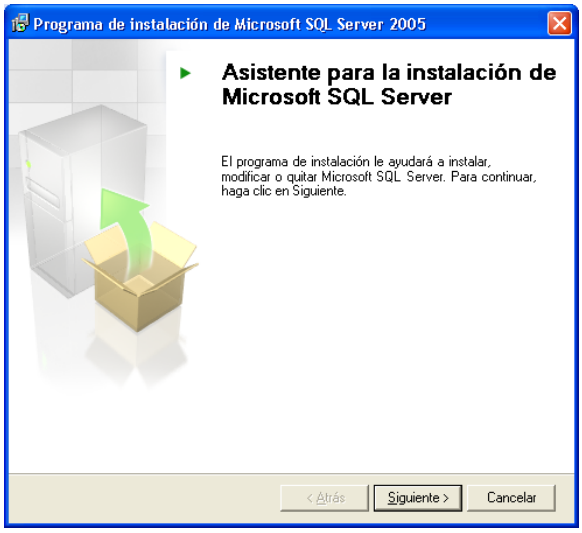
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=220549b5-0b07-4448-8848-dcc397514b41



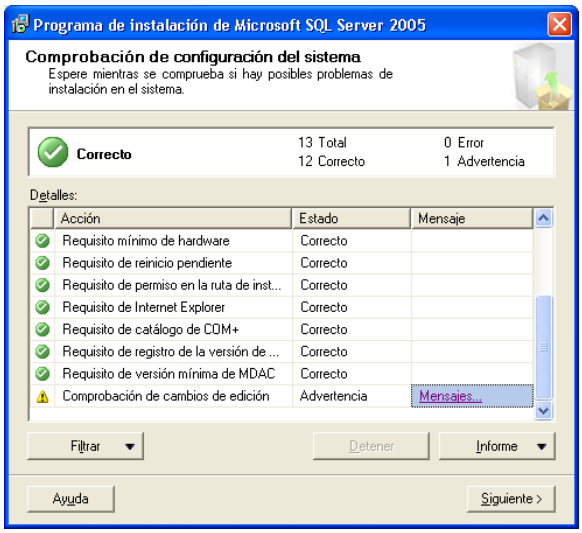
Aceptar los términos de licencia.



Tras revisarse los requisitos previos, pulsar Siguiente.

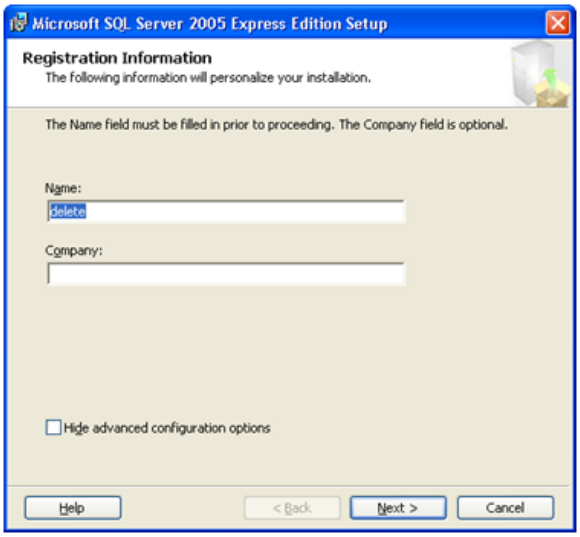


Pulsar Siguiente,

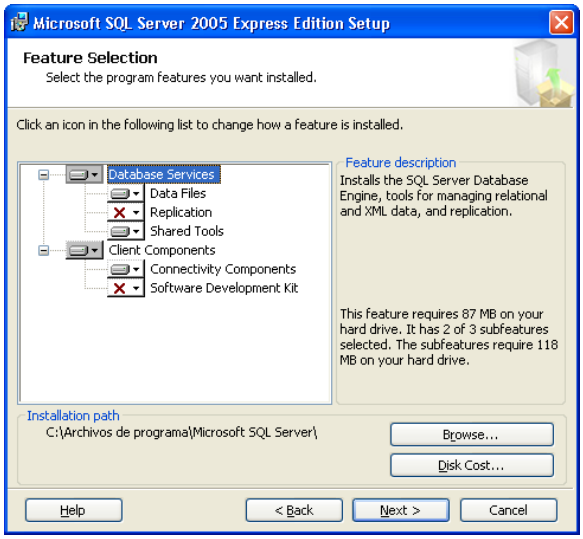


Una vez terminada la comprobación, pulsar Siguiente.

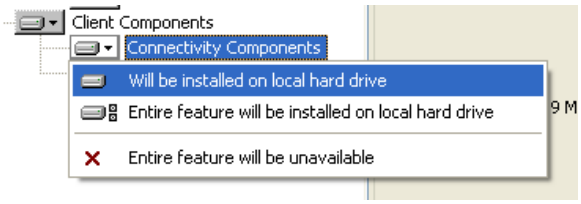
En caso de errores, solucionar los mismos antes de continuar con la instalación. Un posible error puede ser la falta del 'Microsoft .NET Framework 2.0 o superior'. Si no se dispone del mismo, es necesaria la instalación del mismo antes de continuar.

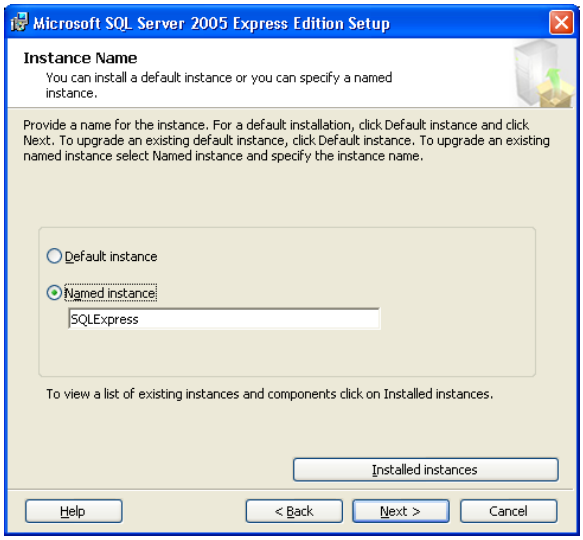


Escribir un nombre y la compañía. El nombre hay que escribirlo, la compañía es opcional. Desmarcar la opción de 'Ocultar opciones avanzadas'.

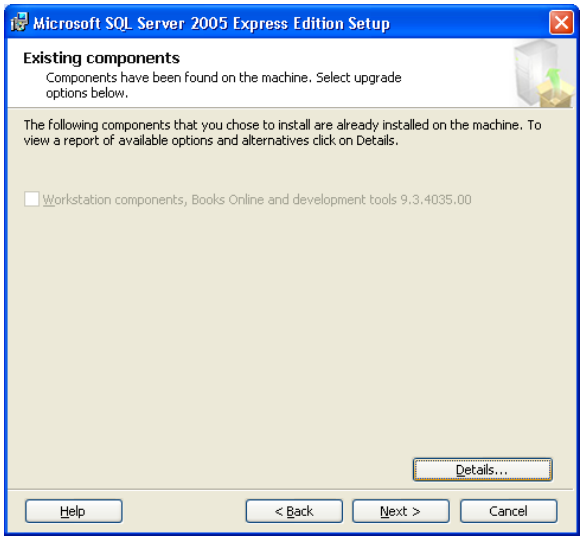


Elegir el destino donde instalar el SQL Server Express y los componentes a instalar. Son necesarios Data Files, Shared Tools, y Connectivity Components. Para seleccionarlos, click sobre la opción deseada, y elegir 'will be installed on local hard drive'

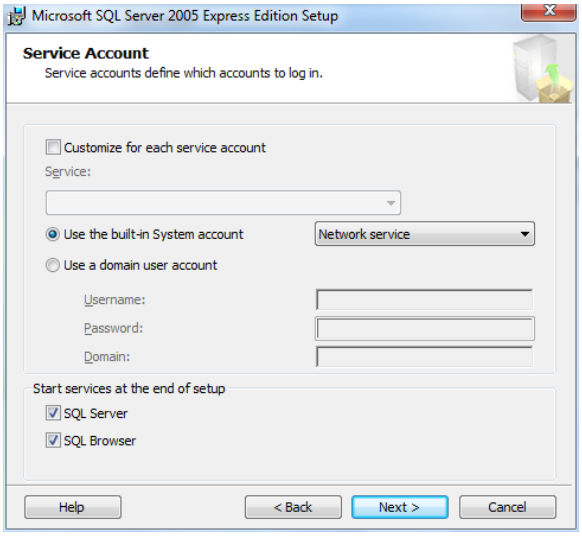




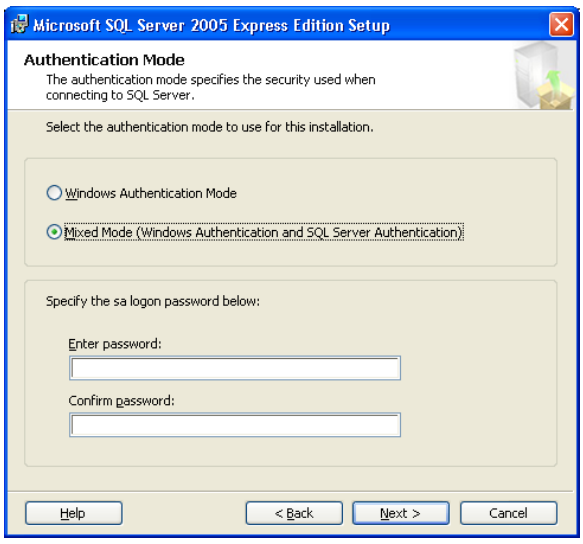
Elegir el nombre de la instancia a instalar. Si sólo va a haber esta, puede elegirse la opción de instancia por defecto, para la cual a la hora de identificar la conexión en el software de Salto, bastaría con poner el nombre de la máquina. Si se especifica un nombre a la instancia, para conectarse a la misma, habría que poner **'Nombre_máquina\Nombre_Instancia'**



Después de actualizarse los componentes existentes de la máquina, pulsar Siguiente.



Asegurarse que estén marcadas las opciones de "Start services at the end of setup", SQL Server y SQL Browser. Si no se hace aquí, se pueden activar más adelante como se verá después.



En esta ventana hay que elegir el tipo de autenticación que se va a utilizar para conectarse a la BDD. Si se dispone de un dominio de red en la empresa, y cada usuario se va a conectar a la BDD autenticándose con su login Windows, elegir autenticación Windows. Si por el contrario, no existe un dominio de red, o se quiere conectar a la BDD mediante un usuario SQL, elegir el modo mixto, y especificar una contraseña para el usuario administrador (sa), la cual debe de ser una contraseña segura, es decir;

1. Las contraseñas seguras no pueden usar condiciones ni términos prohibidos, entre los que se incluyen:

a. Una condición NULL ni en blanco

b. "Password"

c. "Admin"

d. "Administrator"

e. "sa"

f. "sysadmin"

2. Las contraseñas seguras no pueden usar los siguientes términos asociados al equipo de instalación:

a. El nombre del usuario que ha iniciado la sesión actual en el equipo.

b. El nombre del equipo.

3. Una contraseña segura debe tener una longitud mínima de seis caracteres y satisfacer al menos tres de estos cuatro criterios.

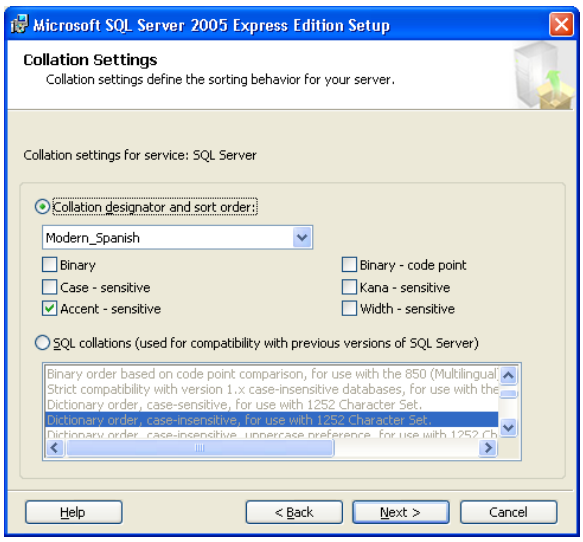
a. Debe contener letras en mayúscula.

b. Debe contener letras en minúscula.

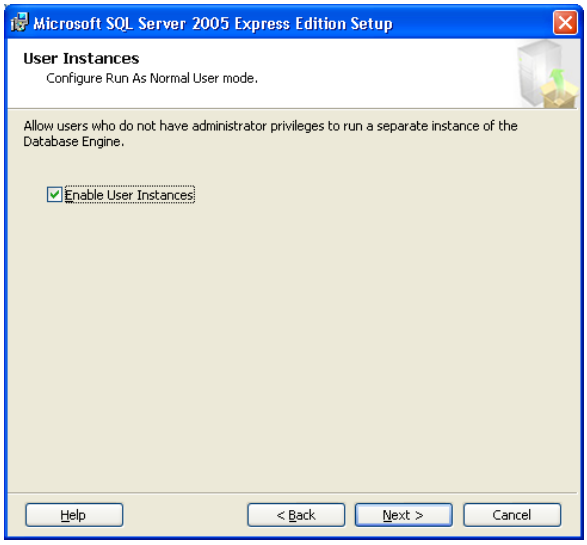
c. Debe contener números.

d. Debe contener caracteres no alfanuméricos, por ej., #, % o ^.

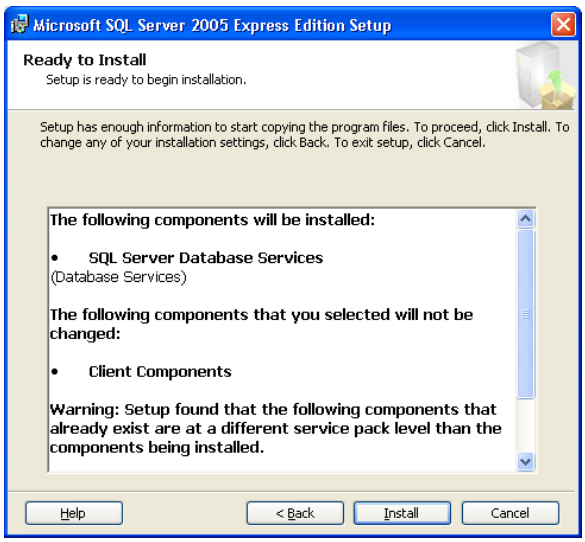
Si no se está seguro del tipo de conexión a utilizar, se recomienda activar la opción mixta, puesto que admite los 2 tipos de conexión, y puesto que de lo contrario, para poder modificar el tipo de conexión una vez finalizada la instalación, será necesario instalar una aplicación adicional (Microsoft SQL Server Management Studio) para poder modificar el modo de autenticación.



Marcar sólo la opción Accent-sensitive. Las otras desmarcadas.

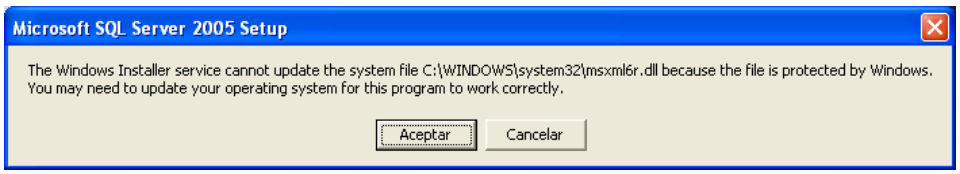


Dejar como viene por defecto y pulsar siguiente.



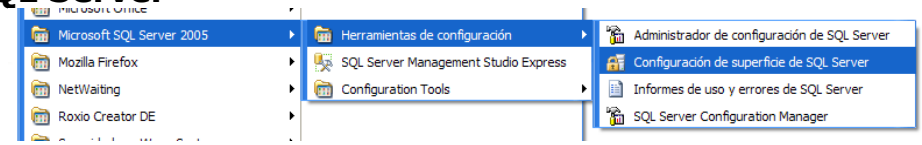
Finalmente, pulsar 'Instalar' para comenzar la instalación.

Durante la instalación, se puede producir el siguiente error cuando se intenta instalar una versión de SQL Server 2005 o 2008 en inglés, en un ordenador con un sistema operativo Windows XP con SP3 no inglés. Si se produce este error, descargarse de la web de Microsoft el instalador de SQL Server Express en el mismo idioma que el del sistema operativo, o en un idioma diferente al inglés.



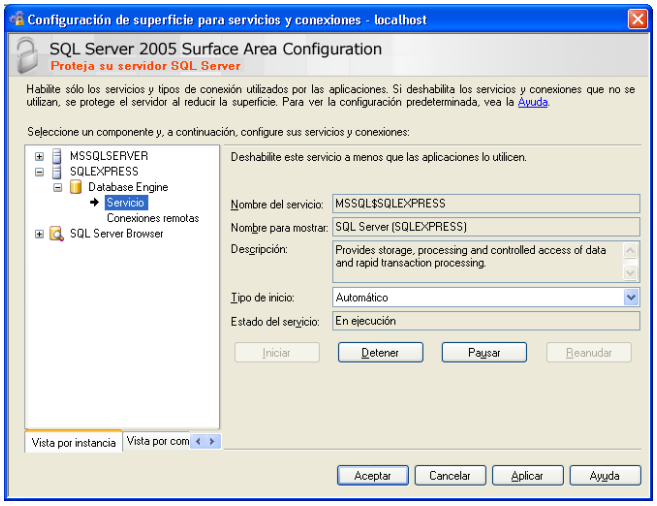
Configurar servicios para admitir conexiones remotas

A continuación se utilizará la **"Configuración de superficie de SQL Server"**



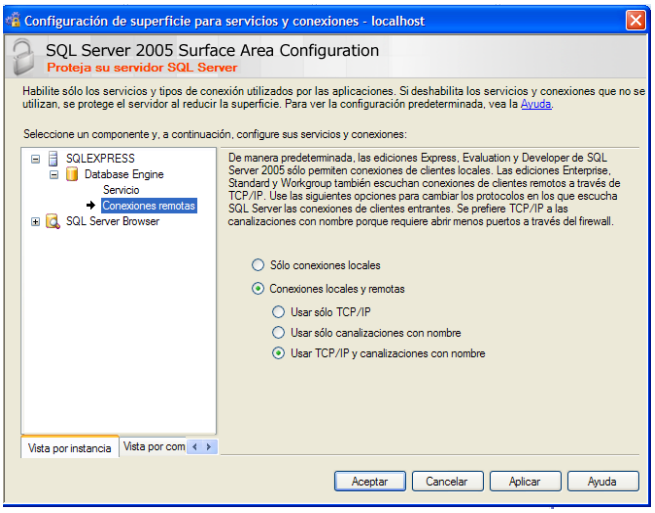
Aquí, se selecciona la opción de **"Configuración de superficie para servicios y conexiones"**

Se selecciona el **"Servicio"** de SQL Server, (**"SQLEXPRESS"** en el ejemplo**)** y se verifica que el tipo de inicio esté en la opción **"Automático".** Si no lo estuviera, ponerlo en automático e iniciar el servicio.

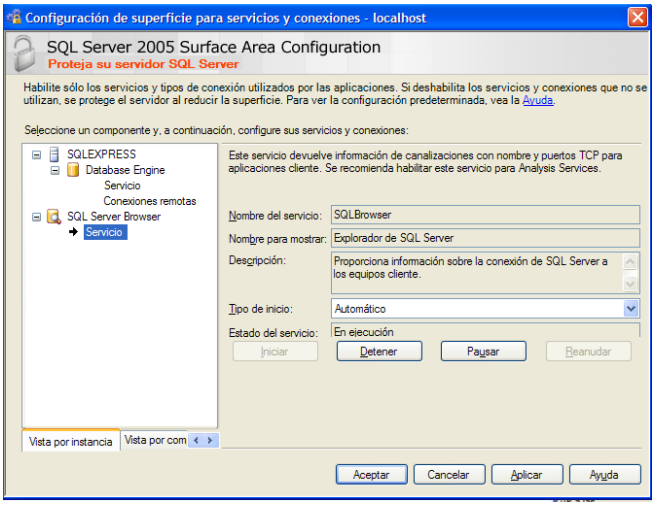


En la opción de "Conexiones remotas", se chequean las siguientes opciones:

- **Conexiones locales y remotas**
- **Usar TCP/IP y canalizaciones con nombre**



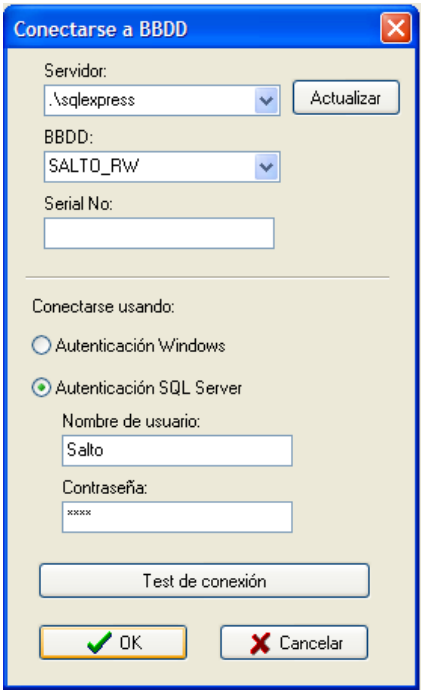
A continuación se selecciona el **"Servicio"** de **"SQL Server Browser"** y se verifica que el tipo de inicio este en la opción **"Automático".** Si no lo estuviera, ponerlo en automático e iniciar el servicio.



Apertura de la BD

Con todo esto, solo resta lanzar el software SALTO en el PC terminal.

Se pulsa la opción **"Fichero/Abrir BBDD"** y se selecciona el nombre del servidor y el nombre de la base de datos ("SALTO_RW" en este ejemplo) utilizando el modo de autenticación deseado.

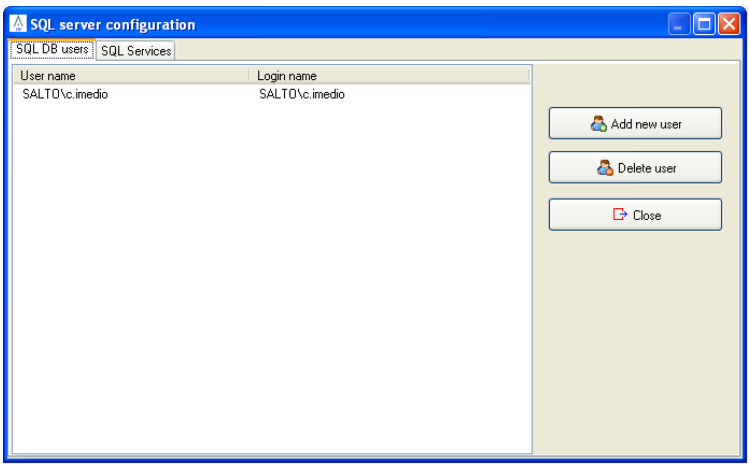


Configuración del servidor SQL

Esta opción es una alternativa a los programas de gestión de bases de datos SQL para la creación de inicios de sesión.

La creación de estos inicios de sesión permitirá el acceso a la base de datos desde distintos PCs de manera a poder tener una instalación compartida entre distintos equipos.

El menú Herramientas/Configuración/Configuración del servidor SQL da acceso a la siguiente pantalla:

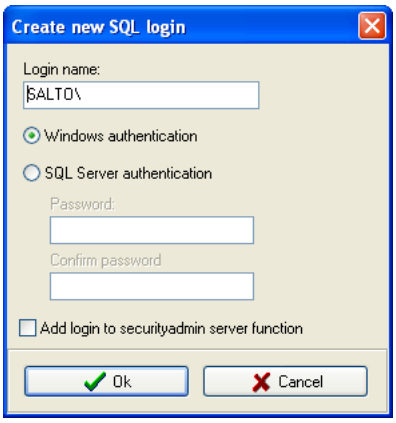


Desde aquí se tiene acceso a los distintos logins que tienen acceso a la base de datos SQL.

Al pulsar sobre "Añadir nuevo usuario", la ventana da acceso a la creación de un nuevo inicio de sesión con las siguientes opciones:

- Nombre de conexión (Login name)

La estructura de este nombre va a depender del tipo de autenticación elegida (Windows o SQL)



La autenticación Windows utiliza usuarios de red existentes. Por defecto, el campo muestra el dominio de red actual de manera a añadir la parte correspondiente a las credenciales del usuario.

Ej. SALTO\c.imedio

La autenticación SQL permite crear nuevos nombres independientes de la actual configuración de red.

Ej. John

En este caso, la elección del nombre no depende de la configuración de la red.

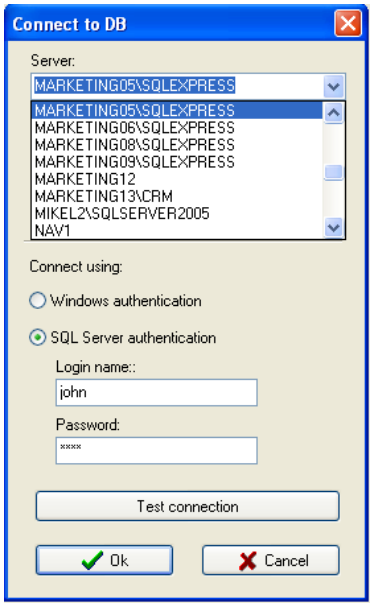
La opción de contraseña es opcional aunque reforzará el nivel de seguridad en el momento de la conexión a la base de datos.

Estos datos se utilizarán para conectar con la base de datos.

Atención!

Es importante elegir correctamente el servidor SQL. La lista desplegable mostrará los distintos servidores de la red.

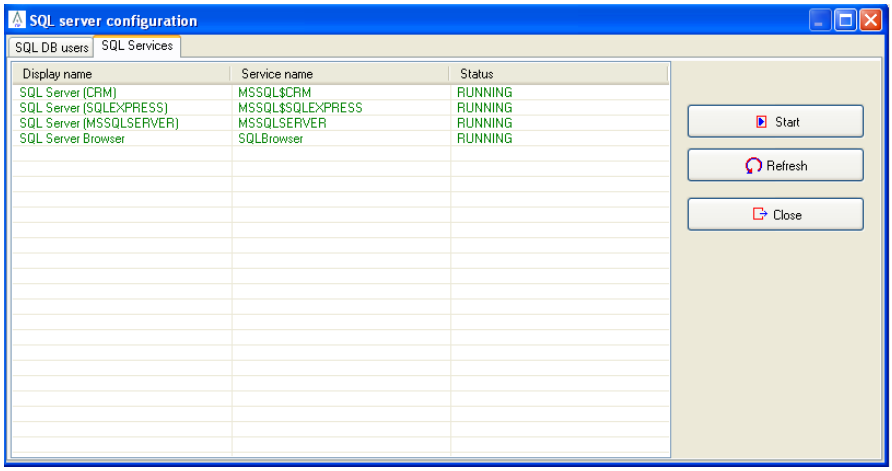
En el caso de utilizarse el SQL Express se elegirá la opción xxx\SQLEXPRESS donde xxx representa el nombre de la máquina (Marketing05 en el ejemplo).



Añadir conexión a la función de servidor securityadmin

Al chequear esta función, los usuarios creados podrán a su vez crear nuevos inicios de sesión.

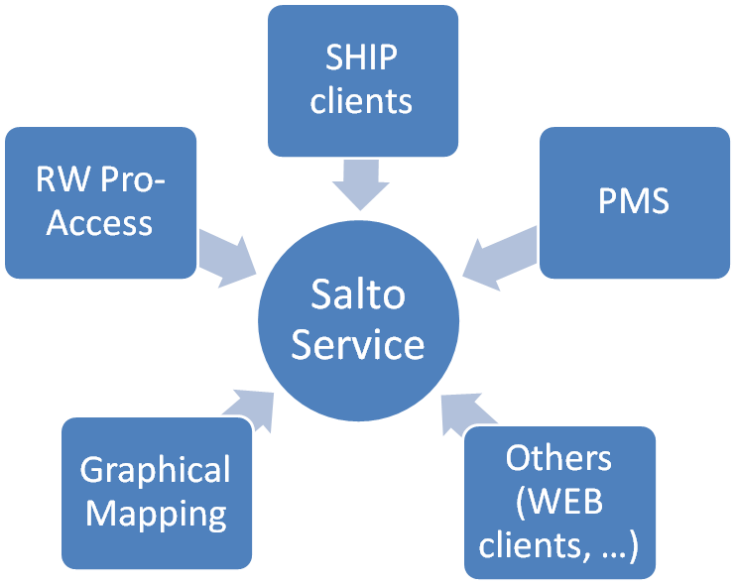
En la pestaña de Servicios SQL se muestran los nombres de los distintos servidores SQL instalados. Desde aquí se monitorizan dichos servicios pudiéndose iniciar.


SQL server configuration
SQL DB users
SQL Services
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
Start
Refresh
Close

SALTO Service RW

La versión SALTO RW Pro-Access for Service está basada en un servicio de Windows denominado SALTO Service RW que se encarga de gestionar las comunicaciones con los elementos on-line: CUs, editores (las cerraduras wireless no están incluidas en esta versión).

Este servicio está llamado a ser el núcleo central del Software SALTO atendiendo a los distintos programas: Pro Access, PMS,…



Requerimientos de Hardware y Sistema

Los requerimientos de hardware y sistema del Servicio Salto son los siguientes:

- Sistemas Operativos compatibles: Microsoft Windows XP (SP3), Vista, Server 2003, Server 2008 y Windows 7. 32-bit or 64-bit. Edicion Server recomendada, es decir, 2003 ó 2008.
- Hardware mínimo: 400 MHz CPU, 512 MB RAM, tarjeta gráfica de color de 800x600 de resolución y 256 colores.
- Hardware recomendado: CPU de 1.0 GHz o superior, 1 GB o más de memoria RAM, tarjeta gráfica de 32-bits con resolución de 1024x768.
- .NET framework 3.5 o superior.
- Hasta 3 GB de disco duro pueden ser necesarios, dependiendo del tamaño del plan de cierre.

- Microsoft SQL Server 2005 or 2008 (edición Express incluida). Importante: si la base de datos de Salto fue creada originalmente en SQL Server 2000 y posteriormente migrada a una versión superior, comprobar que el nivel de compatibilidad está fijado a 90 o superior.

- Sistema de nombres de dominio: el software Salto puede usar nombres de PC (en lugar de IPs fijas)par alas comunicaciones entre PCs. En este sentido, se requiere de un sistema de nombres de dominio (Domain Name System, o DNS) para resolver correctamente la relación entre nombres de PC y sus correspondientes IPs. En caso de que no haya ningún sistema de nombres de dominio, ciertas aplicaciones cliente de Salto pueden dejar de comunicar correctamente con el Servicio Salto.

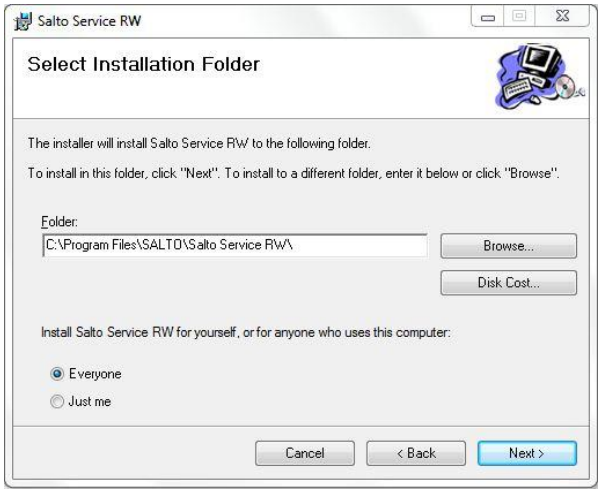
- Entorno de dominio: a pesar de que no es estrictamente necesario, se recomienda encarecidamente el uso de entornos de dominio en lugar de configuraciones de grupos de trabajo, para, de esta manera, simplificar significativamente las configuraciones de seguridad y permisos, consiguiendo así que la configuración del software Salto sea menos engorrosa y más segura.

- El programa de instalación del Servicio Salto (setup.exe) requiere el MS-Windows Installer 3.1.

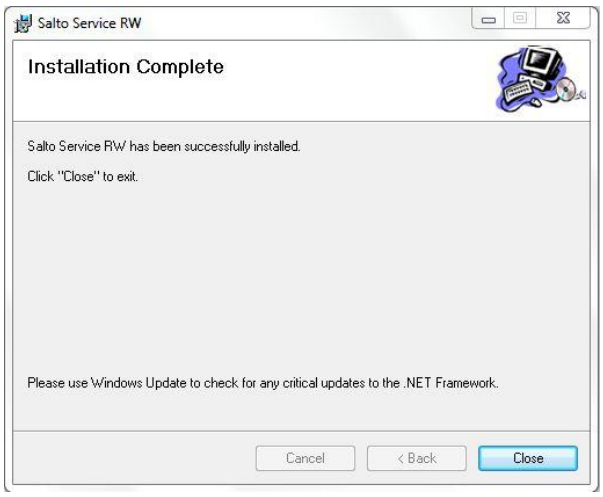
Instalación

La instalación se realiza desde el archivo *SetupSALTOService.msi* y además del propio servicio, instalará una pequeña aplicación dedicada a su configuración para su óptimo funcionamiento con RW Pro-Access.

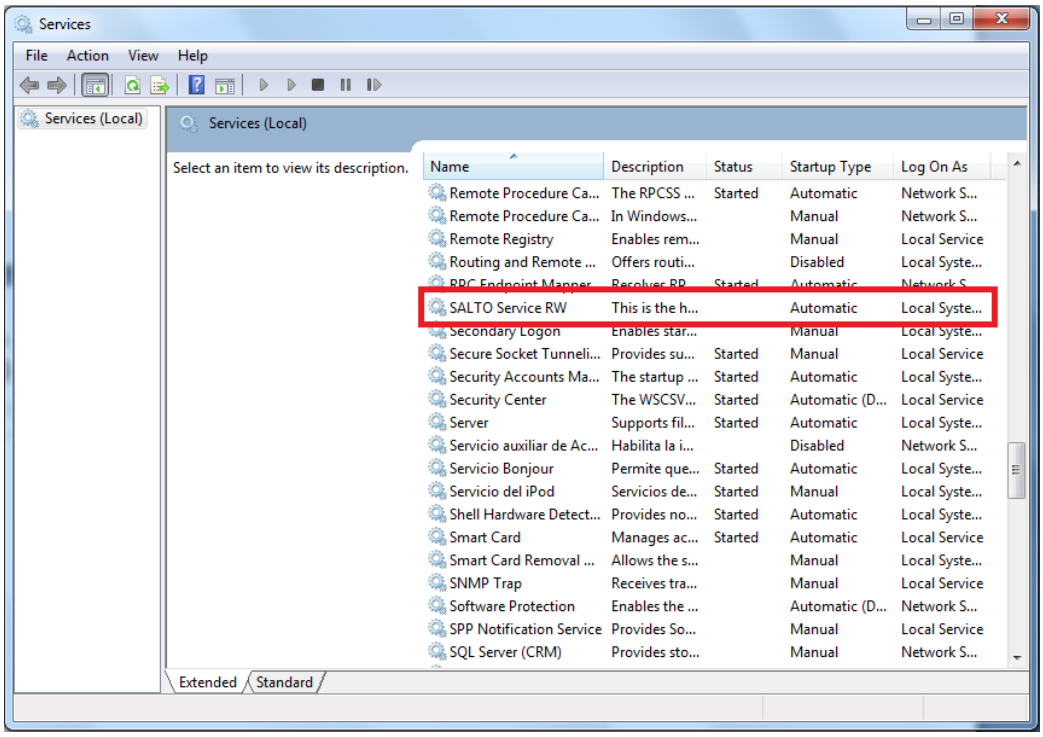
Tras aceptar los términos y condiciones de la licencia, se tiene que elegir la carpeta de instalación y pulsar sobre "Next" para comenzar con esta.



Una vez terminada, el botón "Close" terminará el proceso dejando el servicio instalado.



Este quedará reflejado en la lista de servicios de Windows con el nombre **SALTO Service RW.**



Configurador del Servicio

Si bien la configuración del servicio puede realizarse utilizando las herramientas propias del sistema operativo, el Configurador aporta una serie de opciones más específicas para su administración.

El Configurador del Servicio se compone de tres pestañas principales:

- Base de Datos
- Puertos del Servicio
- Propiedades del Servicio

Base de datos

Esta pestaña contiene la información propia a la conexión con la base de datos SQL.

- Nombre de servidor

Se trata del nombre o dirección IP de la máquina que contiene la base de datos (ATENCIÓN: en el caso de utilizar las versiones "Express" del servidor SQL hay que añadir "\SQLEXPRESS" a continuación del nombre del PC).

- Base de datos

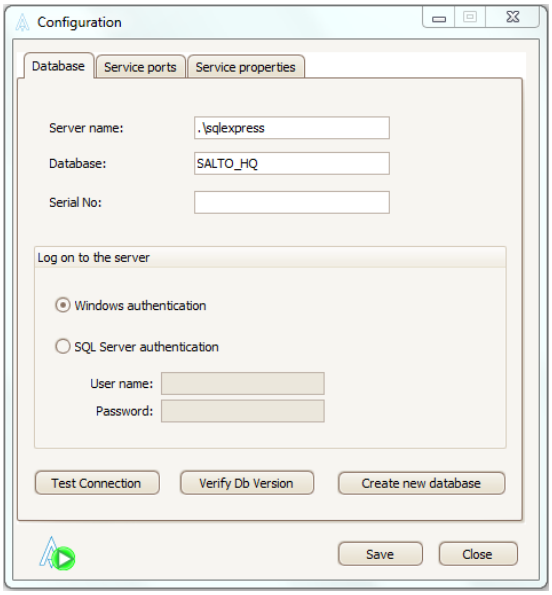
Aquí se apunta a la base de datos que se va a utilizar.

- Serial No.

Número de licencia del software (campo no obligatorio).

- Autenticación de servidor

Aquí se define el tipo de autenticación pudiéndose optar por una autenticación Windows o SQL (NOTA: La autenticación SQL conlleva la creación de un usuario).



- Test de Conexión

Desde aquí es posible chequear la conexión con la base de datos.

- Verificar Versión Bd

La base de datos SQL tiene que ser compatible con la versión del servicio. Bases de datos anteriores requieren ser actualizadas desde el Pro-Access para poder ser compatibles con el servicio.

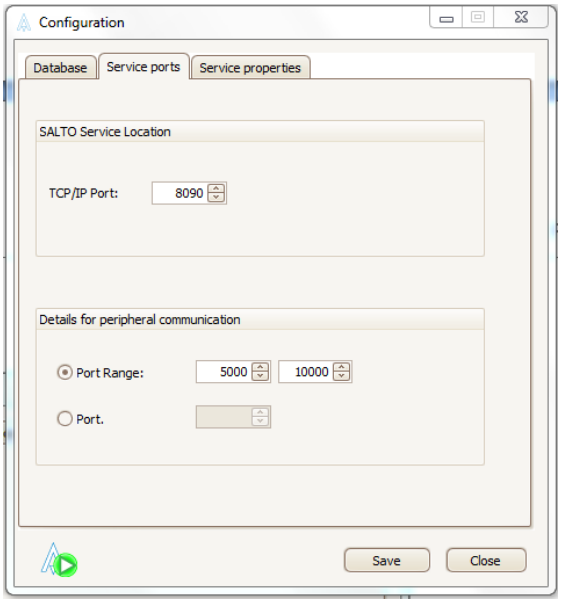
- Crear nueva base de datos

Esta opción permite crear una base de datos nueva para poder ser abierta por el Pro-Access.

Puertos del Servicio

Desde aquí se abren los puertos a utilizar.

Por un lado se define el puerto de entrada de las distintas aplicaciones SALTO – Localización del Servicio SALTO – mientras que la parte inferior se permite configurar un puerto o rango de puertos a través del cual el Servicio SALTO se comunicará con los distintos periféricos – Detalles para la comunicación con periféricos -



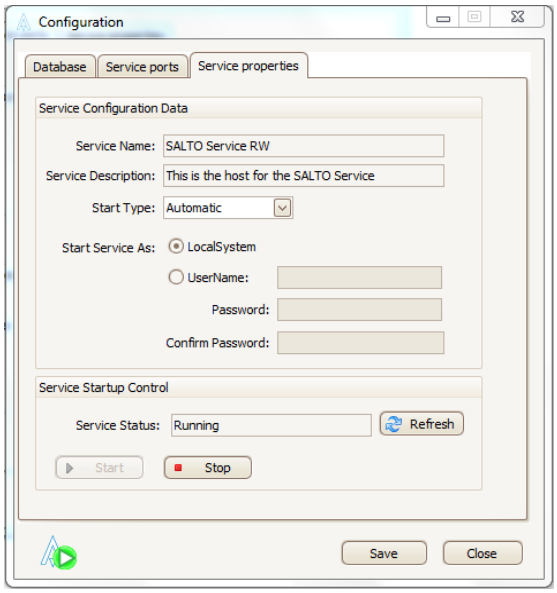
Propiedades del Servicio

Esta pantalla es similar a la ofrecida por las Propiedades del servicio en Windows.

Desde aquí se puede indicar el tipo de inicio (Automático, Manual, Deshabilitado).

Se visualiza también el estado del servicio, pudiéndose Iniciar y Detener.

(*) Se recomienda utilizar la opción de LocalSystem para iniciar el Servicio.



Una vez iniciado, el siguiente icono indica que el

servicio está en ejecución (Este icono se muestra también en el Pro-Access).

Operadores del software. Competencias

Crear Base de datos NUEVA

La primera vez que se abre el programa, se debe comenzar la sesión como administrador.

Para abrir el programa haga doble clic en el icono de acceso directo que encontrará en su escritorio.

Verá una ventana como la de la figura 1, en la que existen 2 campos:

Nombre de usuario: escriba con letras minúsculas **admin.**
Contraseña: la primera vez, no es preciso escribir ninguna.

Valide los 2 campos haciendo clic en la tecla OK.

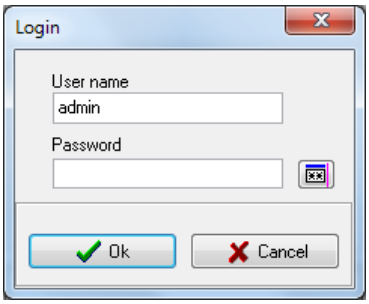


Figura2.

Como es la primera vez que abrimos el programa, los iconos de la barra de herramientas aparecen deshabilitados (en color gris claro).

Para que la barra de herramientas se vuelva activa, es necesario dar un nombre a la base de datos sobre la que vamos a trabajar,

Y asignarle una ruta y directorio dentro de nuestro ordenador.

- Pinchamos el menú desplegable *FICHERO.*
- Seleccionamos la opción *Nueva BD.* Figura 3
- Se abrirá una ventana como la de la Figura 3.

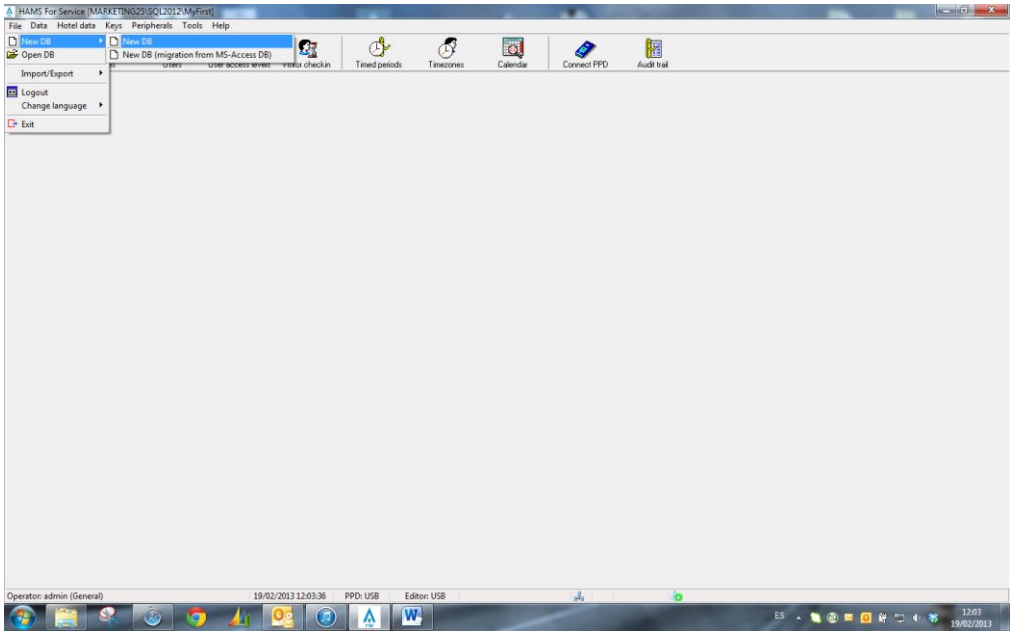


Figura 2

- Para abrir o crear una nueva BBDD ir a fichero/ Nueva BBDD. Entonces en la ventana hay que escribir por un lado el nombre del programa MS SQL contra el que vamos a trabajar. En la casilla inferior hay que escribir el nombre de la BBDD que se quiere crear.

- Se puede escribir el número de serie del software adquirido.

- Validamos el nombre y la ubicación de la base de datos.(pinchamos la tecla OK)

- Seleccionar el modo de autentificación con el que se necesita trabajar, Windows o SQL.

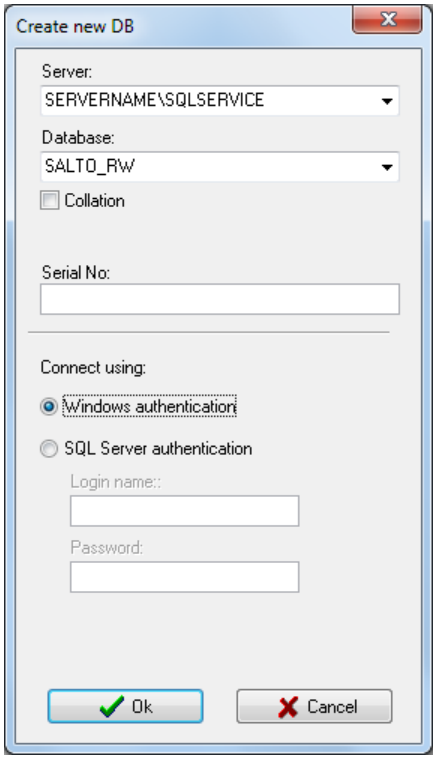
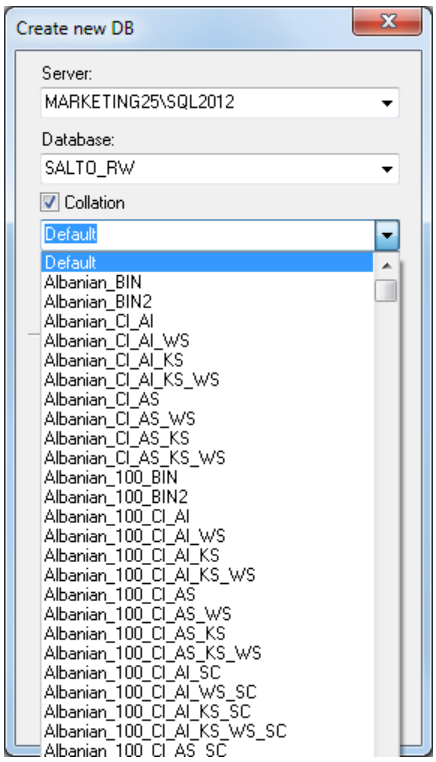


Figura 4

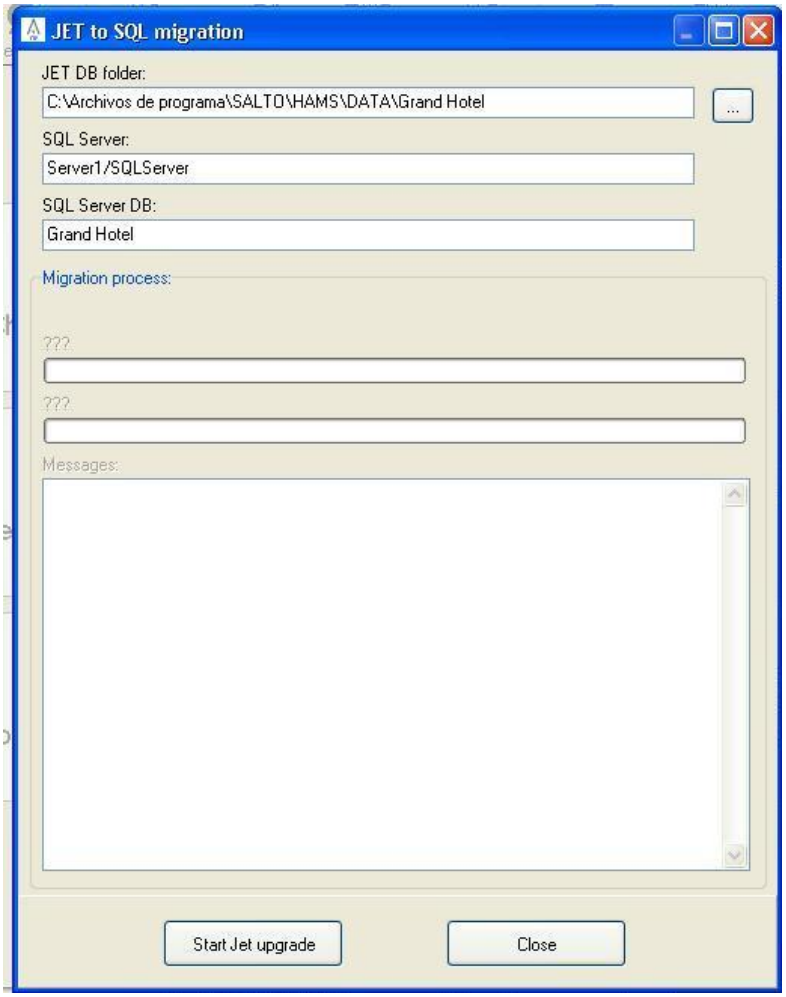
Por defecto, las BD de SALTO se crean en modo CI (Case Insensitive). En el caso en que el servidor SQL esté programado en CS (Case Sensitive), al crear una BD nueva se puede seleccionar el lenguaje y el tipo de sensibilidad.



Migración de una BBDD Access

En ciertas ocasiones puede ocurrir que el cliente no necesite crear una BBDD nueva ya que igual quieren migrar los datos de una BBDD Access previamente creada. El proceso de migración de datos es muy sencillo ya que está automatizado.

Para ejecutar la migración hay que ir a Fichero/Nueva BBDD/Migración desde Access. Se mostrará la siguiente pantalla:



Entonces haciendo clic en el botón de la derecha podemos encontrar la BBDD Access sobre la que queremos hacer la migración. Entonces hay que darle el nombre a la BBDD SQL y hay que especificar el programa MS SQL sobre el que se va a trabajar. Una vez que todo esto se ha especificado se puede pulsar en el botón “Comenzar migración” Si todo se ha especificado de forma correcta la migración se llevará a cabo sin problemas.

Competencias de los operadores

El administrador debe establecer quiénes van a ser los operadores del programa, y cuáles van a ser sus competencias, es decir qué opciones del menú principal podrán utilizar y cuáles no. También podrá establecer contraseñas de acceso al programa, para sí mismo y para los operadores del programa.

Vaya al menú desplegable HERRAMIENTAS/ OPERADORES Y PERMISOS/ OPERADORES, como se ve en la figura.

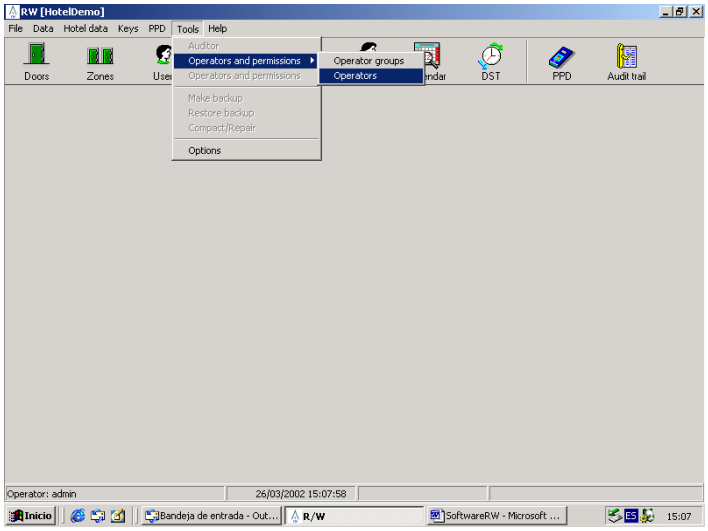


figura 5.

El sistema trae dos operadores por defecto, ADMINISTRADOR. En la figura siguiente puede verse la lista de operadores, cada uno de ellos pertenece a un grupo con distintas competencias.

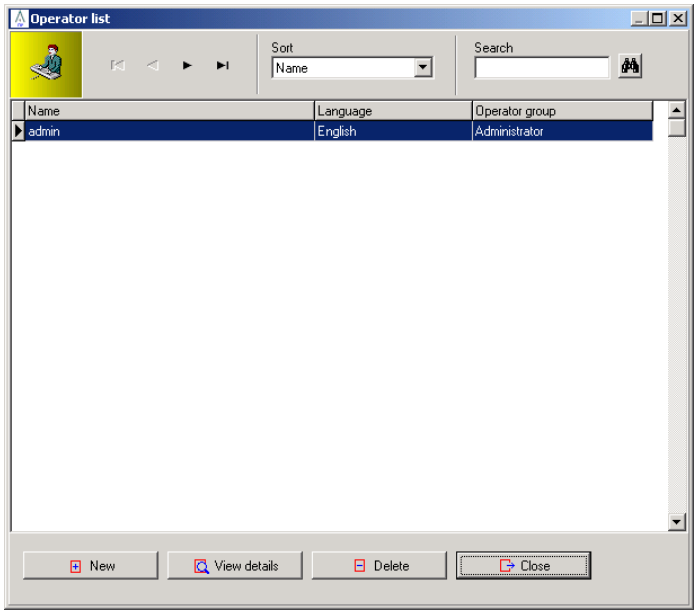


Figura 6

Probablemente usted necesitará crear más operadores de recepción, según el número de empleados que el hotel disponga para esta función.

Para crear un operador nuevo, pulse el botón NUEVO de la parte inferior de la ventana. Se abrirá una ventana en blanco, como la de la figura siguiente:

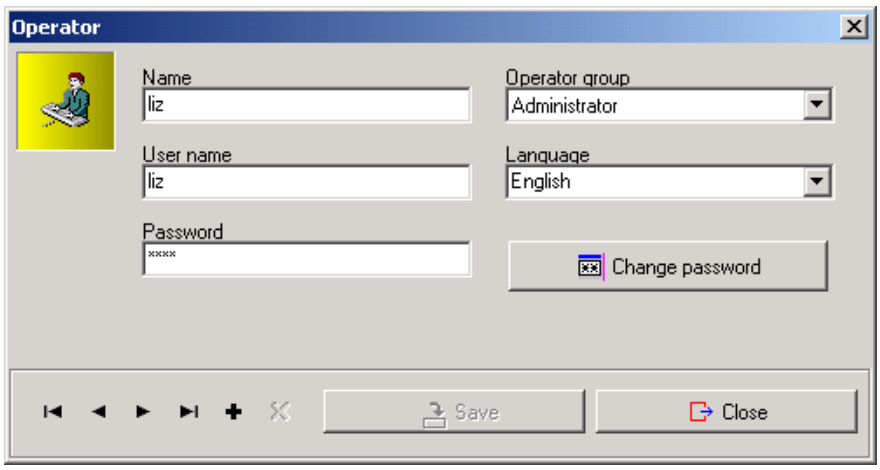


Figura 7

- Tendrá que rellenar el nombre del operador, su nombre de usuario (que es el que se carga al iniciar la sesión), y una contraseña.

- También especifique el idioma que este operador utilizará para ejecutar el programa.

- A continuación, guarde los cambios y cierre la ventana.

- Se debe comunicar inmediatamente la contraseña al operador que acaba de registrar, ya que va a necesitarla para trabajar con la aplicación.

Repita esta operación con cuantos operadores nuevos necesite crear, y verá como se va incrementando la lista de operadores.

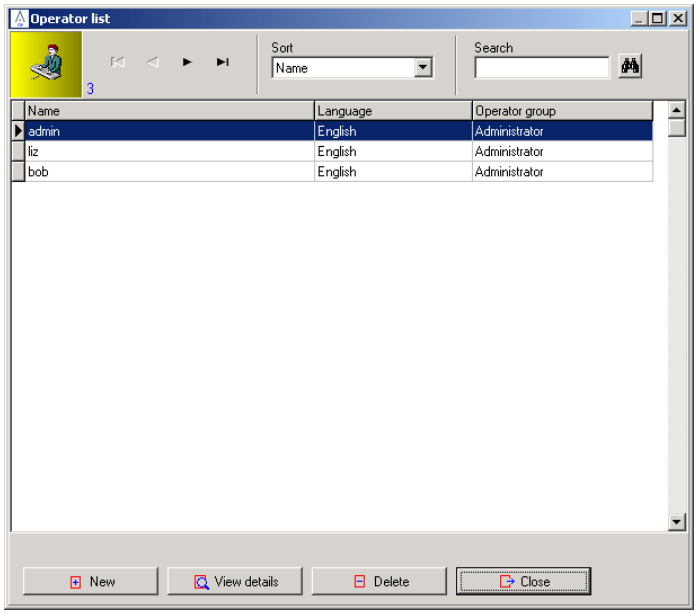


Figura 8

Una vez que ha creado los operadores necesarios en su sistema, puede cerrar esta ventana y volver al menú desplegable HERRAMIENTAS/ OPERADORES Y PERMISOS/ GRUPOS DE OPERADORES. Aquí se pueden establecer las competencias de cada operador.

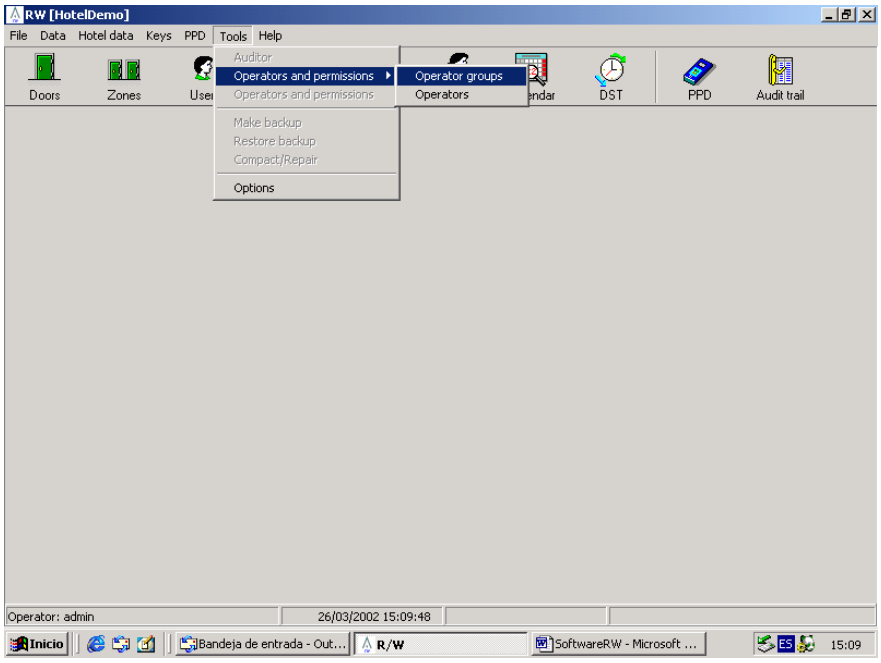


Figura 9

Los operadores que pertenecen al grupo ADMINISTRADOR tienen a su disposición todas las opciones de menú del programa.

Si se desea que ciertos operadores no tengan acceso a ciertas opciones de menú, bastará con incluir a esos operadores en otro grupo que no sea ADMINISTRADOR, y quitarles las opciones de menú que no se desea que utilicen.

Las competencias de los operadores de recepción son iguales para todos los miembros del grupo, todos tienen los mismos privilegios.

El administrador puede crear más grupos de operadores, si lo estima conveniente.

Para crear un grupo nuevo, debe hacer clic en el botón NUEVO de la parte inferior de esta ventana.

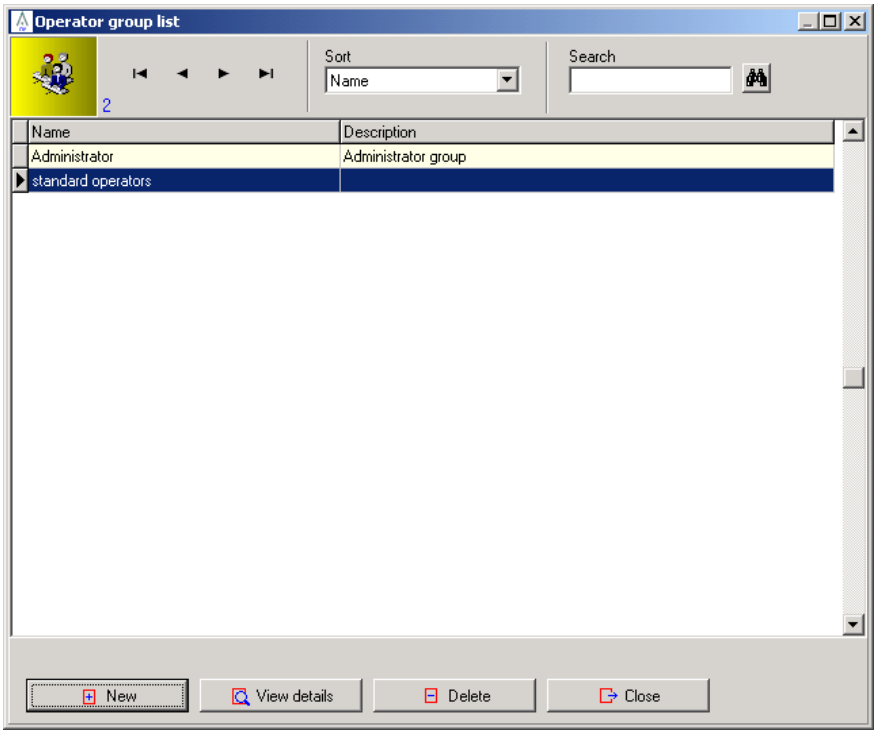


Figura 10

Para modificar las competencias de un grupo que ya existe, debe seleccionar este grupo de la lista (la línea se pone de color azul) y pulsar el botón VER DETALLES.

Se abrirá una ventana como la de la figura 11.

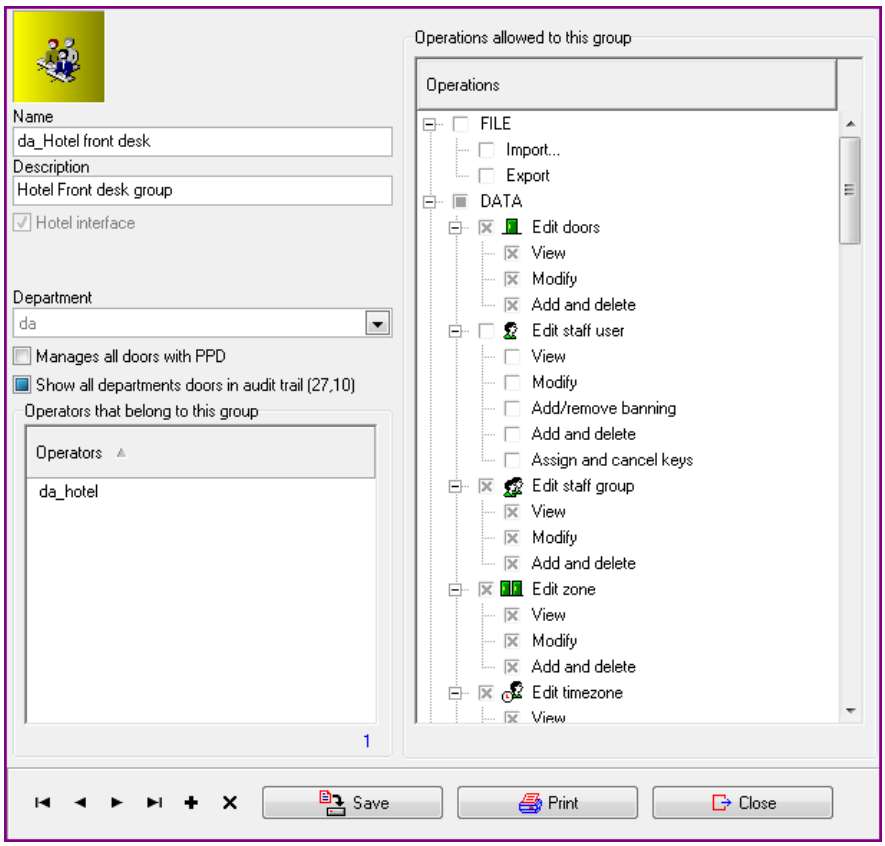


Figura 11

Para modificar las competencias de un grupo que ya existe, debe seleccionar este grupo de la lista (la línea se pone de color azul) y pulsar el botón VER DETALLES.

Se abrirá una ventana como la de la figura 11.

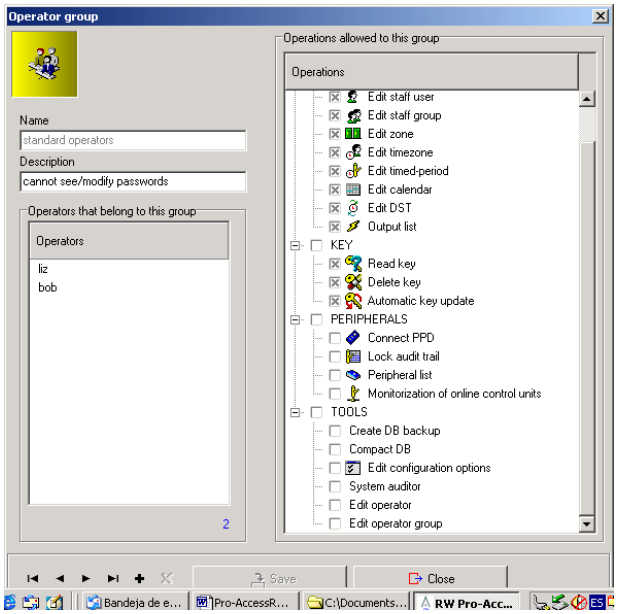
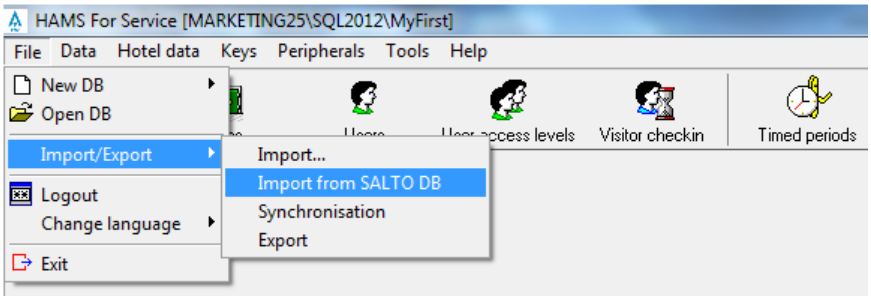


Figura 11

- En esta ventana el administrador puede añadir o quitar opciones de programa, haciendo clic con el ratón en las "check boxes" que aparecen a la izquierda de cada opción. Cuando la opción está marcada, quiere decir que aparecerá como opción de menú activa para el operador que maneje el programa. Si la opción no está marcada, quiere decir que no aparecerá como opción de menú activa para un operador de este grupo.

- El administrador debe guardar los cambios cuando termine de añadir o quitar opciones de menú para los operadores de recepción.

IMPORTAR DESDE UNA BD SALTO (Merging)

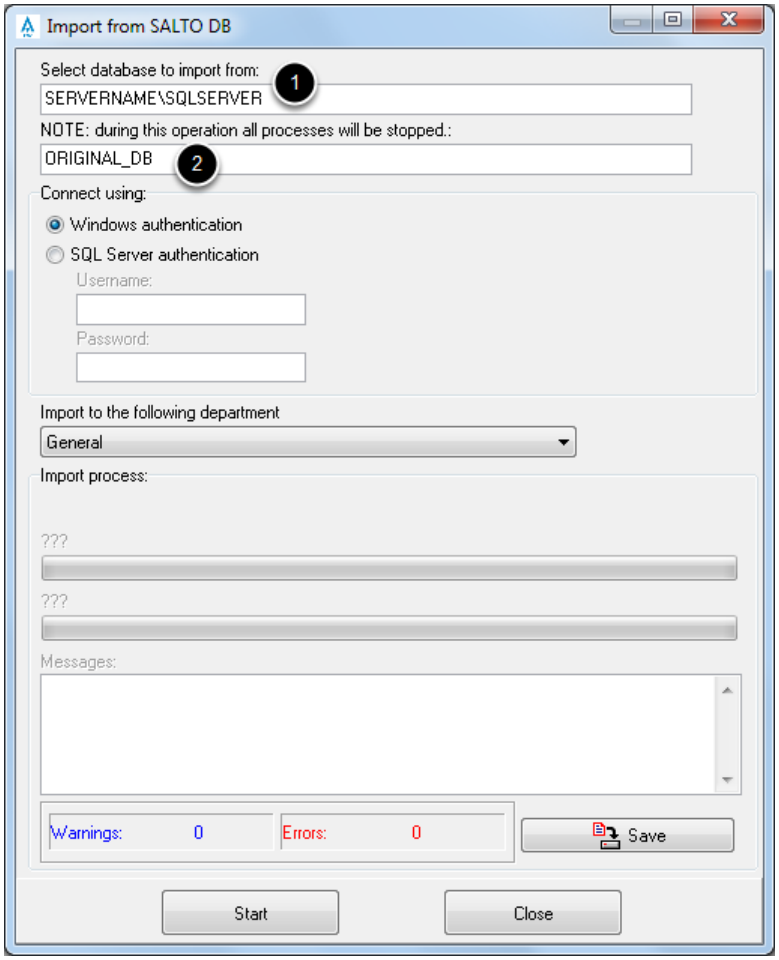


Con la herramienta de importación de base de datos, se pueden juntar varias bases de datos en una sola.

La opción de departamental deberá estar deshabilitada en la base de datos original y todos los componentes deberán transferirse al departamento general.

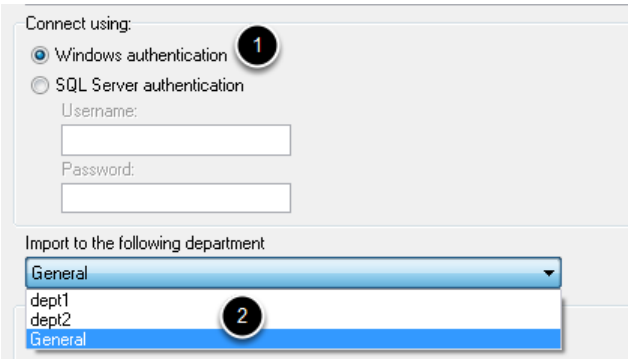
La BD de destino puede tener uno o varios departamentos. Al momento de la importación, es posible seleccionar el departamento general o cualquier otro departamento previamente creado.

Origen de la DB



Al presionar en "Importar de una BD SALTO" la ventana mostrada arriba aparecerá.

Rellene el campo con el ORIGEN de la BD (1) y su NOMBRE (2).

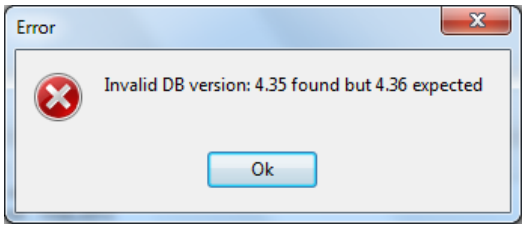


Seleccione el tipo de autentificación, Windows o SQL (1), mostrado arriba.

Finalmente seleccione el departamento donde los datos importados serán ubicados. Si en la BD de destino solo existe un departamento, seleccione el General.

Entonces, haga clic en "Comenzar".

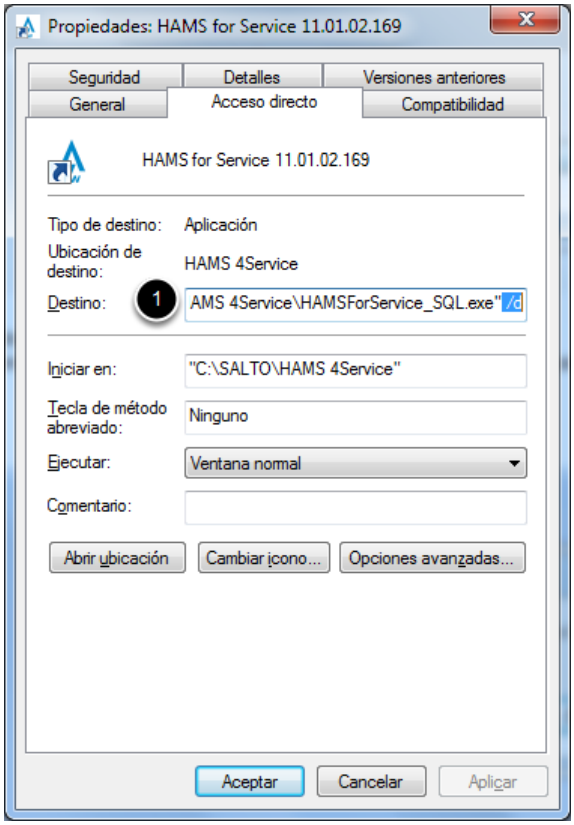
Versión de la BD inválida



En el caso en el que la DB de origen no tenga la misma versión que la de destino, el mensaje de arriba aparecerá.

Para solucionarlo, deberá abrir la BD original con un programa SALTO utilizado con la BD de destino. Entonces, repita el proceso y presione en Comenzar.

NOTAS importantes



El código de SISTEMA de la BD de origen no se mantendrá, el código de sistema será el de la BD de destino. Las puertas que han sido importadas deberán ser reinicializadas desde la nueva BD así como también se deberán re editar las llaves de los usuarios importados.

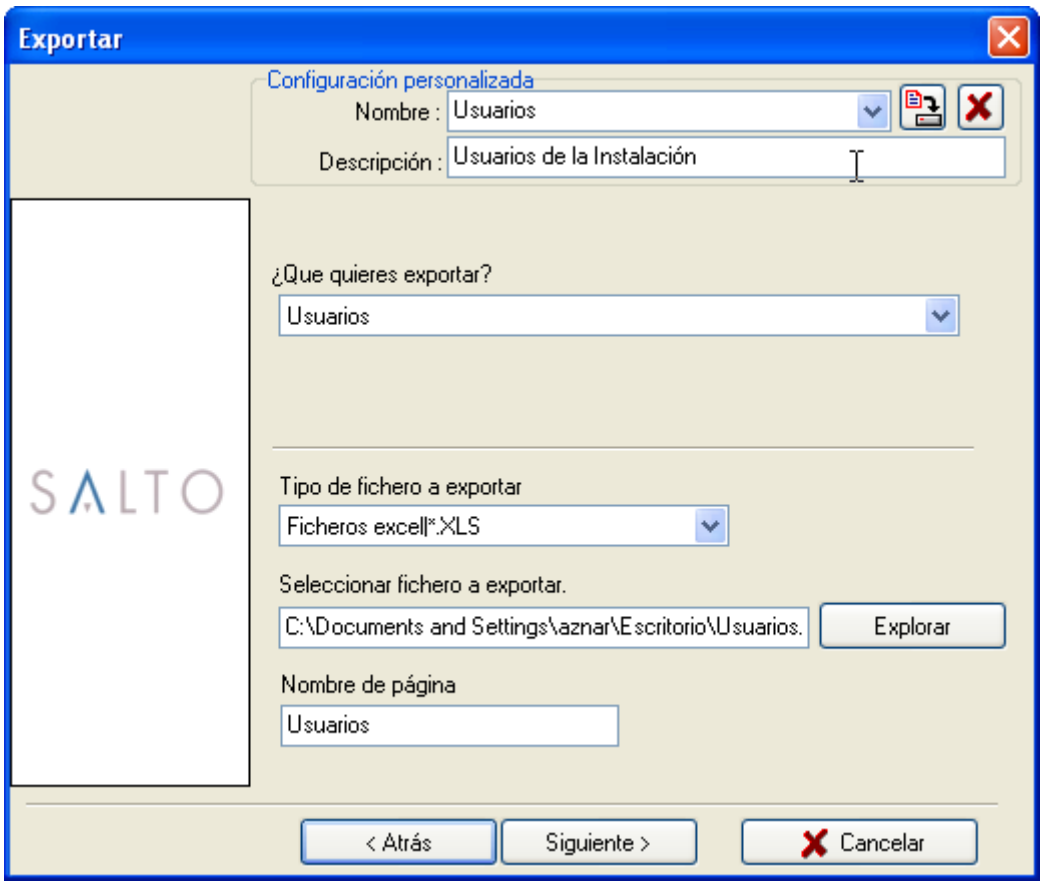
Está opción de importar e unificar bases de datos, no estará visible por defecto. Para activarla, de debe escribir _/d al final de la línea de destino en la acceso directo como se muestra arriba (1) **[...HAMSForService_SQL.exe"_/d]**

Exportar

Para exportar datos de la BBDD a otro fichero tipo txt., xls

Debemos ir al menú despegable FICHERO/ EXPORTAR/IMPORTAR / EXPORTAR.

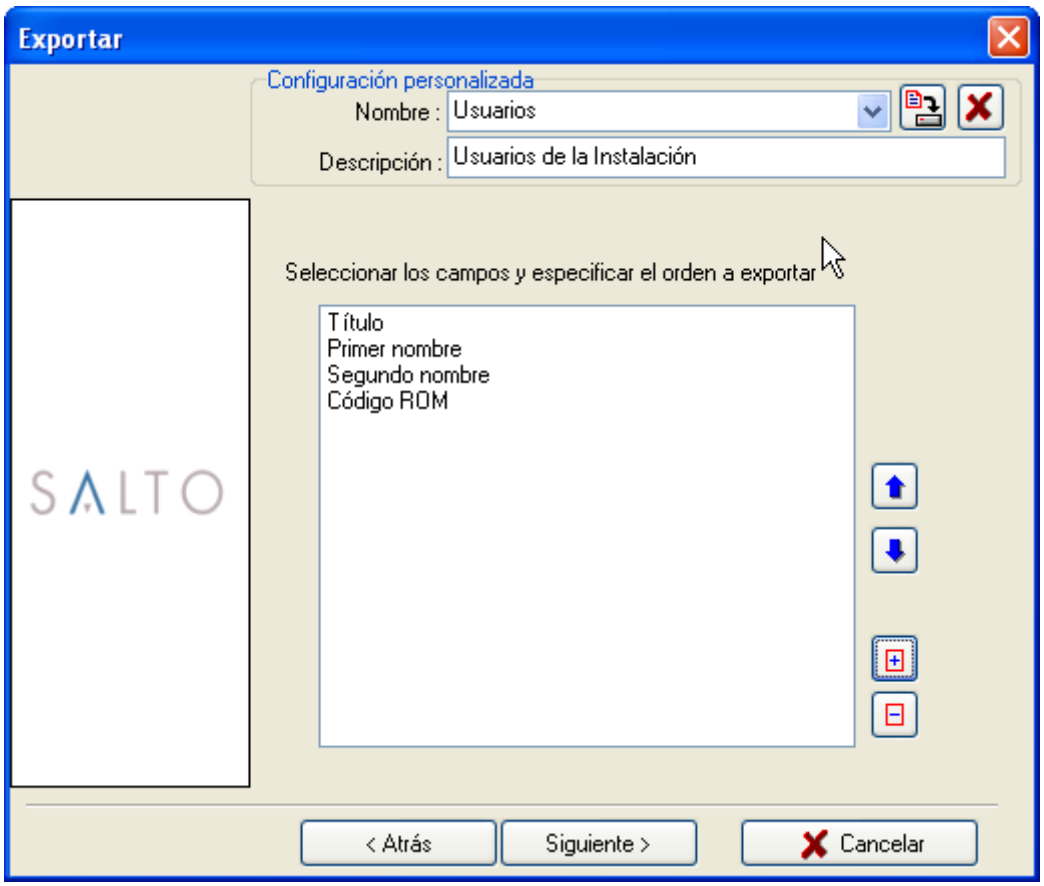
Una vez seleccionada la opción nos aparecerá una ventana de confirmación tras pulsar Siguiente > aparecerá ventana de selección: (Fig.1)



(Fig. 1)

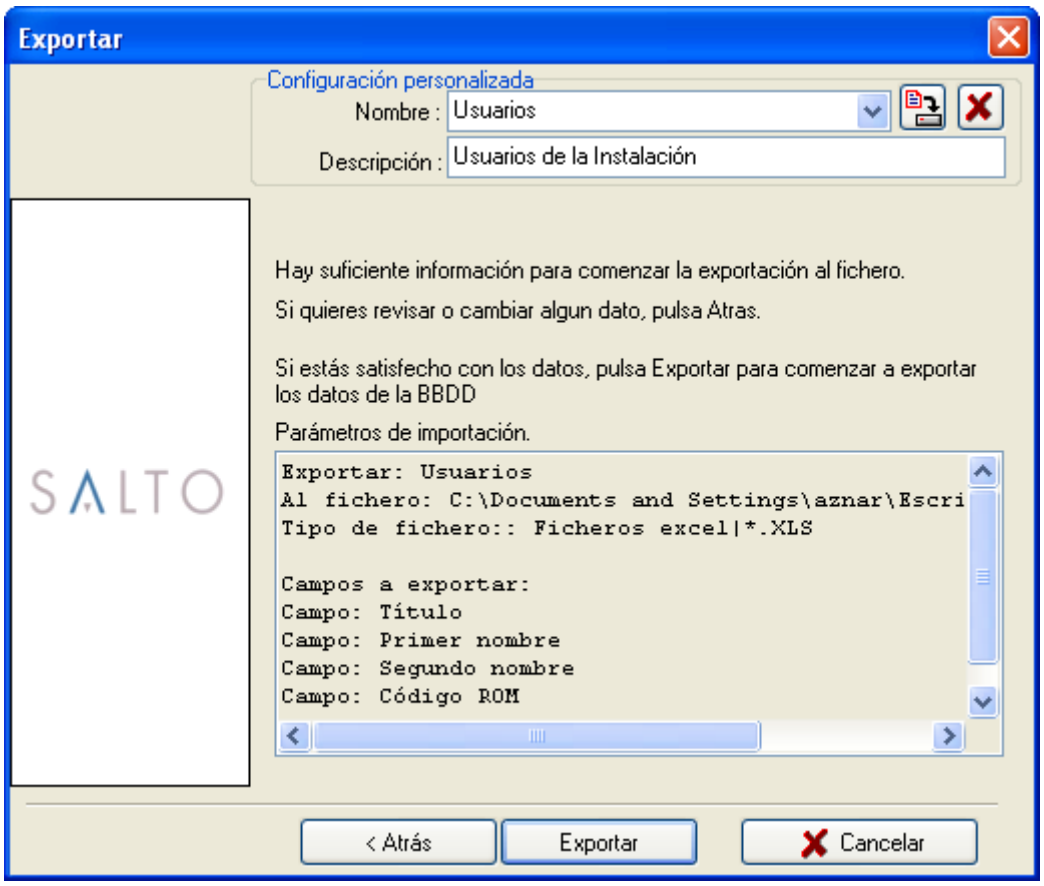
En esta ventana comenzamos dando un nombre y descripción al archivo, seguidamente elegimos qué queremos exportar: Usuarios, Puertas, Grupos y/o Zonas. En la siguiente casilla debemos seleccionar el tipo de fichero al que queramos exportar los datos: txt, xls y/o html. Una vez seleccionado el tipo de archivo,

seleccionamos el fichero al que queramos exportar los datos. Una vez completada la ventana, pulsamos Siguiente >. Aparecerá la siguiente pantalla: (Fig. 2)



(Fig. 2)

En esta ventana debemos seleccionar los campos que queramos exportar y su orden. Pulsamos para añadir campos y para retirar los que no nos interesen. Utilizamos las flechas y para alterar el orden de los campos. Una vez realizada toda la selección, pulsamos Siguiente >. Nos aparecerá la siguiente ventana de confirmación: (Fig. 3)

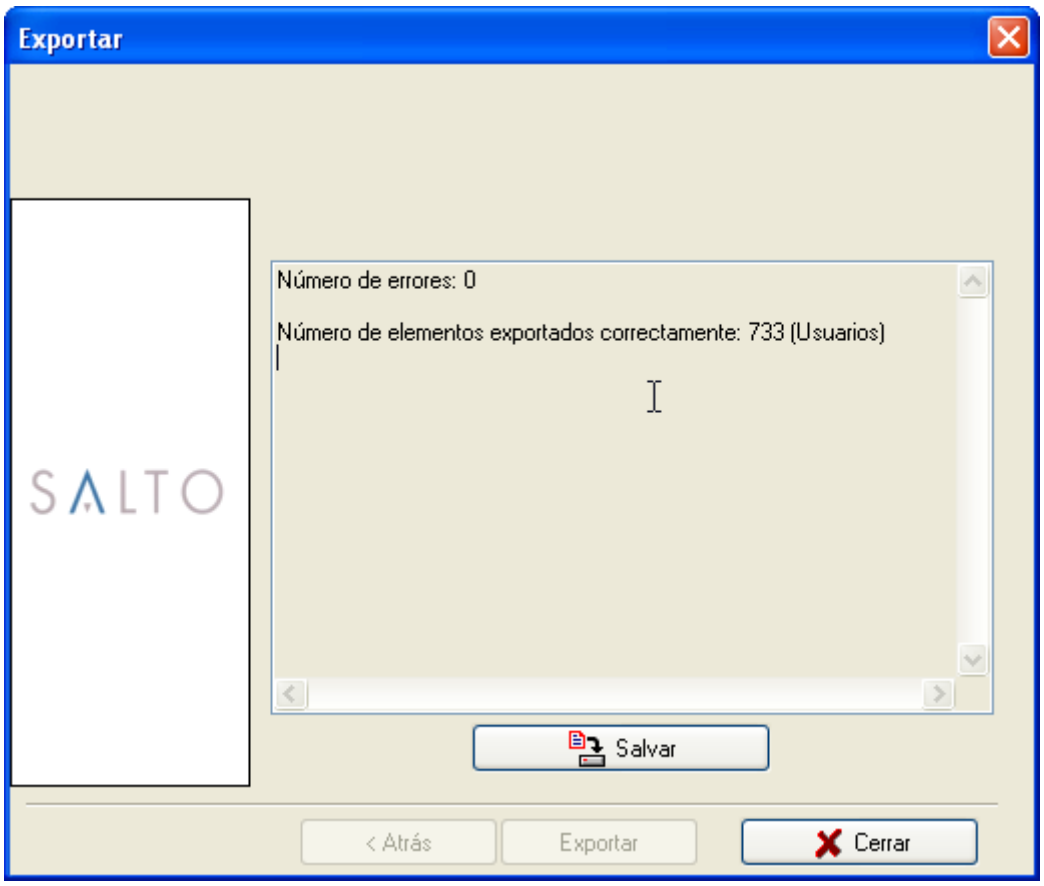


(Fig. 3)

Una vez confirmados todos los datos pulsamos

. Podemos guardar la configuración personal de exportación para futuras aplicaciones pulsando .

Una vez completada la exportación, el software nos mostrará la siguiente ventana: (Fig. 4).


Exportar
SALTO
Número de errores: 0
Número de elementos exportados correctamente: 733 (Usuarios)
Salvar
< Atrás
Exportar
Cerrar

(Fig. 4)

Operador administrador.

Es misión del administrador (o administradores) diseñar el plan de cierre inicial para la instalación y editar las tarjetas que darán acceso a los empleados a las distintas zonas y puertas.

Para explicar cómo se utiliza el software SALTO RW, en este manual, se va a realizar un plan de cierre hipotético que puede servir como ejemplo para ilustrar el método general.

En principio, cabe destacar que, básicamente se pueden realizar todas las operaciones con los iconos de la barra de herramientas. (Excepto los datos estrictamente relativos al hotel). Se pueden ir definiendo los parámetros en cualquier orden, aunque se recomienda seguir el que aparece a continuación:

1. **puertas**
2. **zonas**
3. **horarios**
4. **periodos**
5. **calendarios**
6. **cambio horario**
7. **nivel de accesos de usuarios**
8. **ILocker**
9. **Usuarios y asignación de sus llaves**
10. **Utilizar el PPD**

Primero definiremos las puertas de la instalación. Después agruparemos las puertas por zonas, y definiremos los usuarios del sistema. Agruparemos estos usuarios en conjuntos para después ganar tiempo a la hora de definir sus accesos.

También es necesario definir los horarios, periodos y calendarios, antes de pasar la información al PPD para la inicialización de las puertas. (Excepto para lectores murales Online, que pueden ser inicializados desde el ordenador de control, directamente.)

Puertas

Con esta opción de menú vamos a crear una lista de las puertas que tienen control de acceso en nuestra instalación. (Tanto escudos electrónicos como lectores murales) pero que no son las habitaciones de los clientes.

Hacemos clic con el ratón en el icono de la barra de herramientas que representa a las puertas:

Si es la primera vez que abrimos esta opción, la lista de puertas estará vacía.

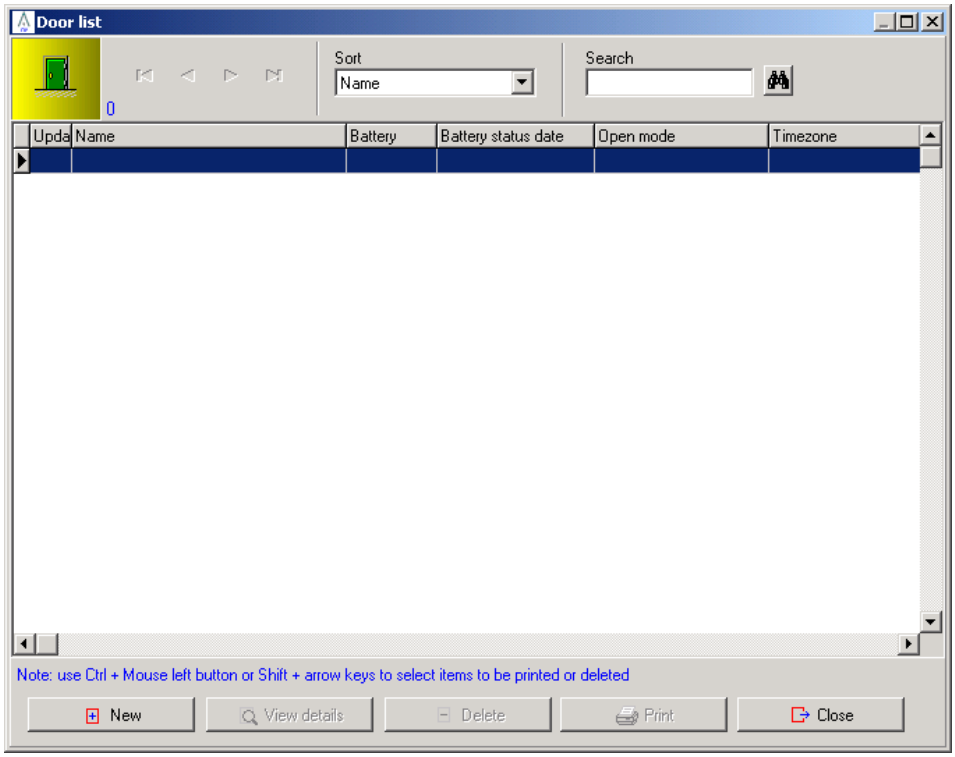


Figura 22

- Pinchamos en el botón llamado *NUEVO* para añadir una primera puerta a la lista.

- En la ventana que se abrirá veremos una serie de campos que iremos rellenando. (A excepción de los usuarios, que no podemos especificar porque todavía no se han definido)

- Escribimos el nombre de nuestra primera puerta.

Después vamos a establecer las características de esta puerta:

ADMITIR LLAVES EXPIRADAS

Las puertas se pueden programar para admitir llaves que lleven expiradas una cantidad específica de días. Esto se podría usar en puertas offline de baja seguridad que se encuentren antes que algún actualizador SVN. Permitiría a los usuarios tener acceso a un actualizador para actualizar su llave.

Esta programación puede ir de 0 a 255 días.

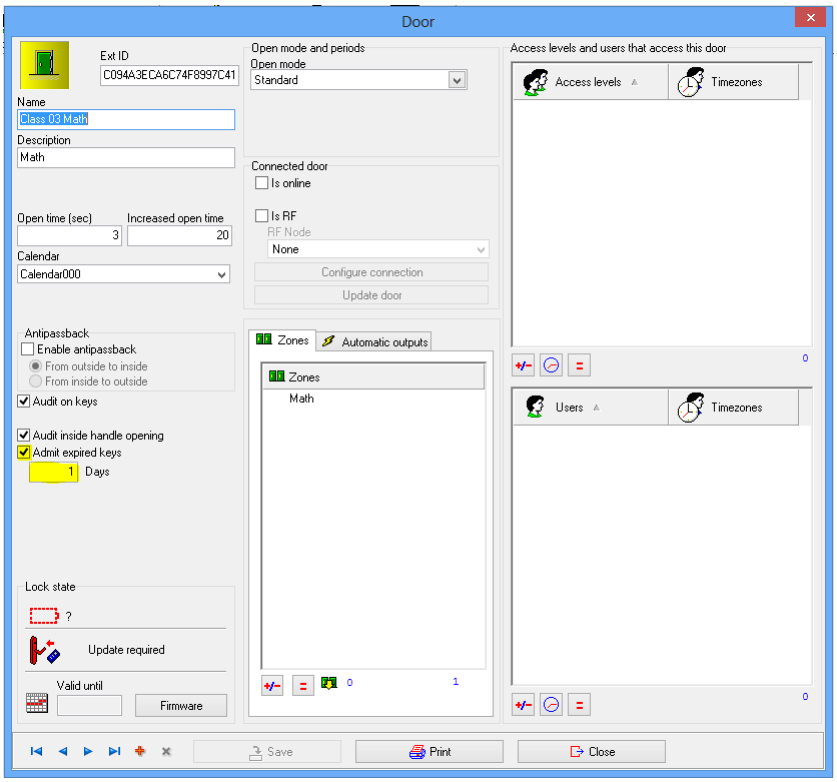


Figura 23

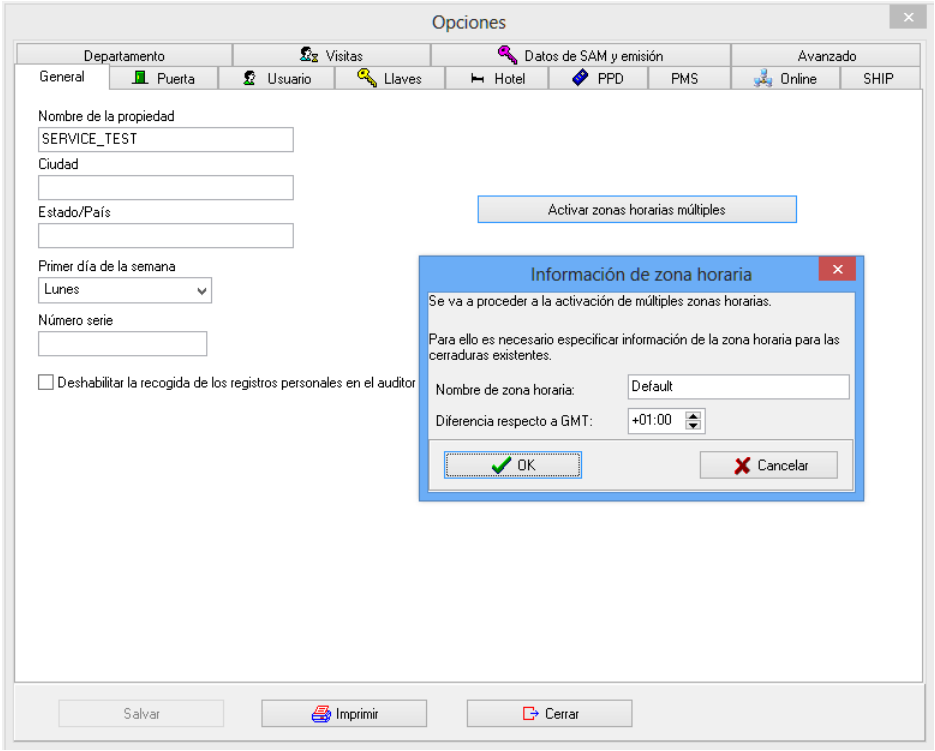
- En el campo TIEMPO DE APERTURA se especifica el tiempo que transcurre desde que un usuario abre la puerta hasta que ésta queda otra vez cerrada por el sistema electrónico. Por defecto, este tiempo es de 10 segundos.

- En el campo TIEMPO AMPLIADO DE APERTURA se especifica un tiempo de apertura más dilatado, especial para usuarios con discapacidades físicas o psíquicas. Por defecto, este tiempo es de 20 segundos.

- Es posible configurar Husos Horarias Geográficos para evitar conflictos horarios en instalaciones que se encuentren en diferentes Husos Horarios y compartan la misma base de datos. Puede suceder en países donde existen varios husos horarios como en Estados Unidos, Canadá, Rusia o Australia. También puede suceder, por ejemplo, entre diferentes países como Reino Unido y Alemania si comparten la misma base de datos.

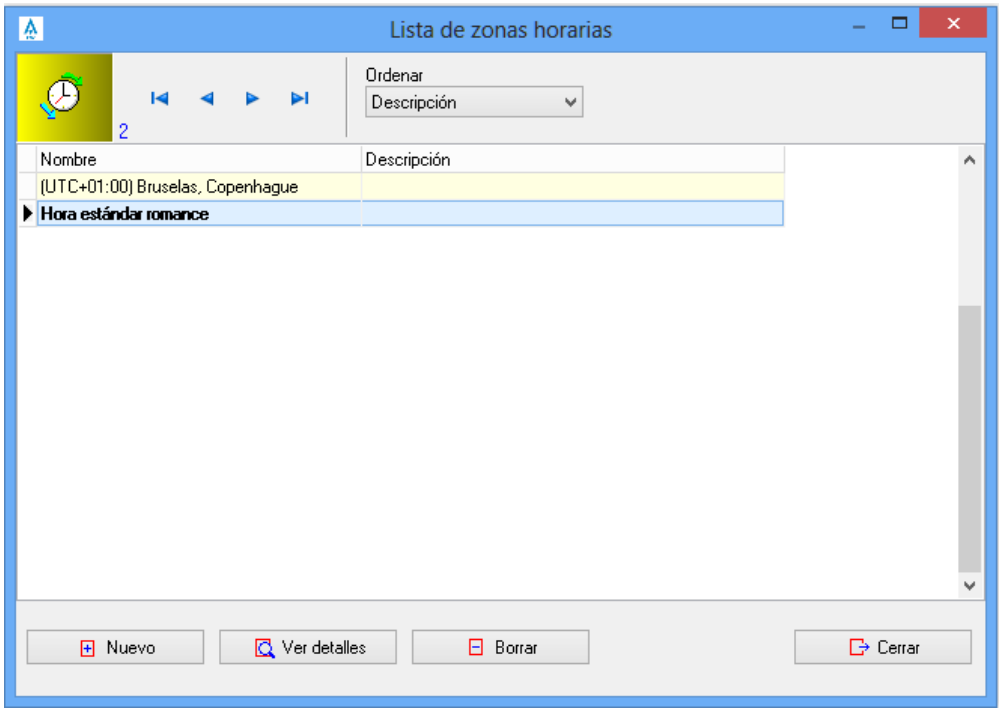
Para el sistema de SALTO es importante usar adecuadamente los períodos temporizados en los puntos de acceso según su zona geográfica, como también es para los usuarios usar los horarios programados con relación al área geográfica donde se encuentren.

Primeramente, la función debe ser activada en las Opciones Generales, pestaña General;

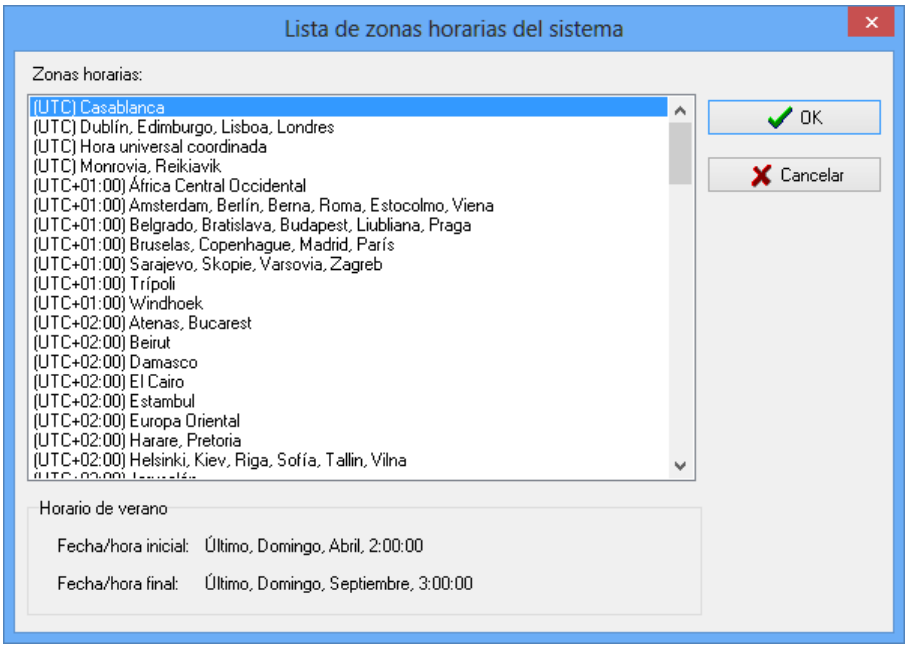


Al activarse la función de múltiples Husos horarios, es necesario seleccionar una Zona Horaria así como la diferencia respecto al GMT.

Si es necesario, es posible crear más Husos horarias en el menú Datos/Zonas Horarias.



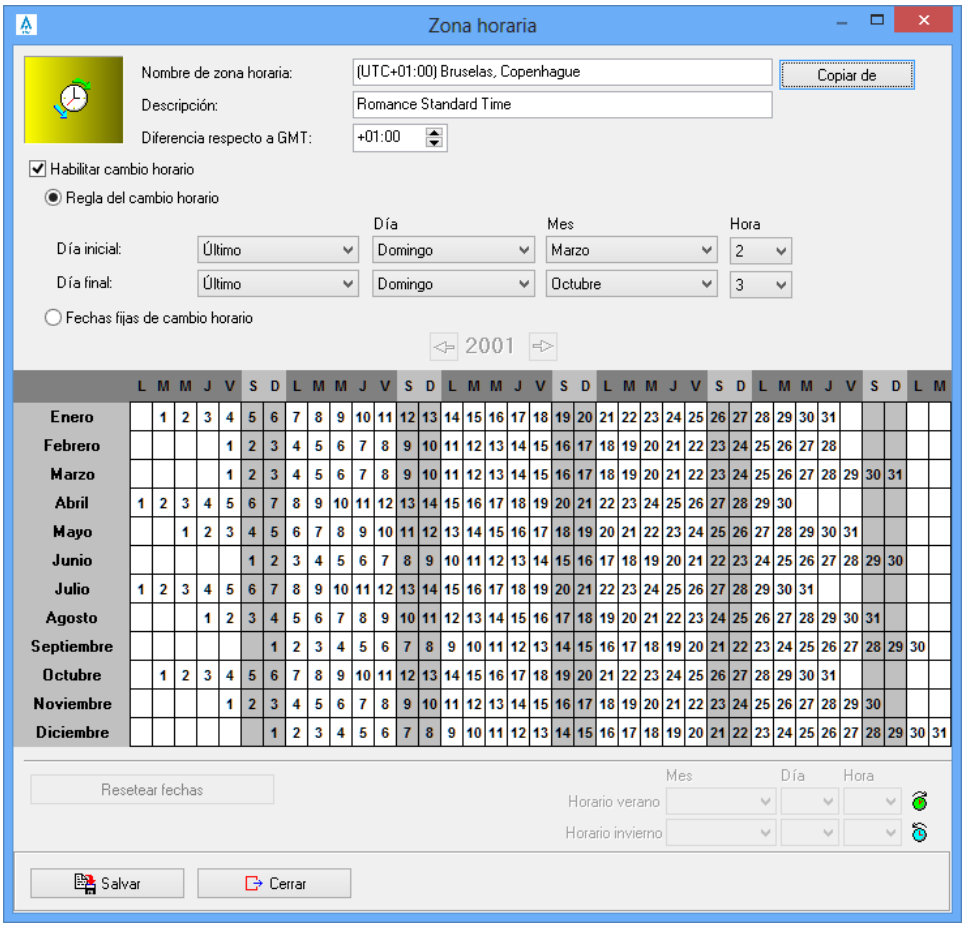
Pulsando "Nuevo" se podrán crear nuevos Husos Horarios. Estos se pueden crear manualmente especificando el GMT y las horas de cambio horario. También es posible utilizar el Huso horario oficial pulsando el botón "Copiar de". Ahí podrá seleccionar cualquier Huso horario de la lista.



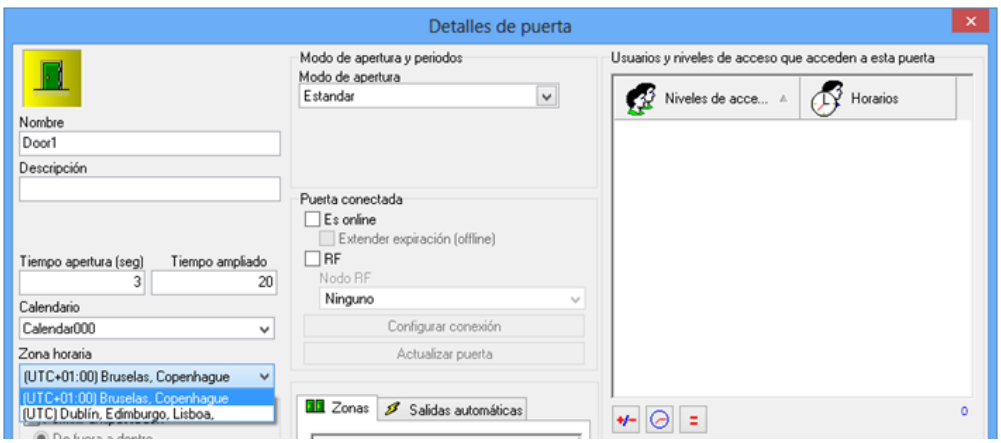
Al seleccionar un Huso Horario, las fechas de cambio horario se pueden habilitar y configurar de las dos formas siguientes:

- Seleccionando la regla de DST estándar.

- Días de DST fijos: seleccionando en el calendario los dos días del cambio para que este se efectúe automáticamente.



En cuanto los diferentes Husos horarios han sido creados podrán ser asignados a los puntos de acceso ubicados geográficamente en diferentes zonas horarias.



- En el campo MODO DE APERTURA especificaremos en qué modo va a trabajar la cerradura electrónica. Se puede escoger uno de los cuatro disponibles:

1. **Standard:** la cerradura sólo se abrirá mediante el empleo de una tarjeta autorizada, dentro de su horario autorizado.

2. **Paso:** la cerradura estará abierta para cualquier usuario que desee entrar. No es preciso presentar ninguna tarjeta autorizada. Para poner el escudo en este modo de funcionamiento, es necesario insertar una tarjeta autorizada y al mismo tiempo, mantener bajada la manilla interior. Repetir esta operación cancelará el modo paso.

3. **Paso temporizado:** el modo de funcionamiento aquí es el mismo que en el apartado anterior, con la diferencia de que sólo se puede poner la cerradura en paso dentro de un intervalo de tiempo determinado, llamado PERIODO. Si se escoge este modo, le asignaremos uno de los varios periodos disponibles, sabiendo que luego es preciso definir dicho periodo, mediante la herramienta PERIODO, de la barra de herramientas. (Se explica más adelante)

4. **Apertura automática:** Semejante al modo anterior, pero con la diferencia de que la puerta se pone en paso automáticamente, sin que sea necesaria la intervención de un usuario. Para este modo de funcionamiento también es preciso elegir un periodo de tiempo, que luego definiremos con la herramienta PERIODO.

5. **Toggle:** En este modo presentando una llave válida el escudo se quedará abierto sin necesidad de bajar la manilla. La siguiente llave válida volverá a dejar el escudo cerrado.

6. **Toggle Temporizado:** Este modo de funcionamiento es igual salvo que hay un periodo de tiempo definido en el que el escudo funciona de esta forma.

7. **Apertura automática+office:** La forma de trabajar es igual a la de apertura automática salvo que en la franja fuera del periodo de apertura está en modo office.

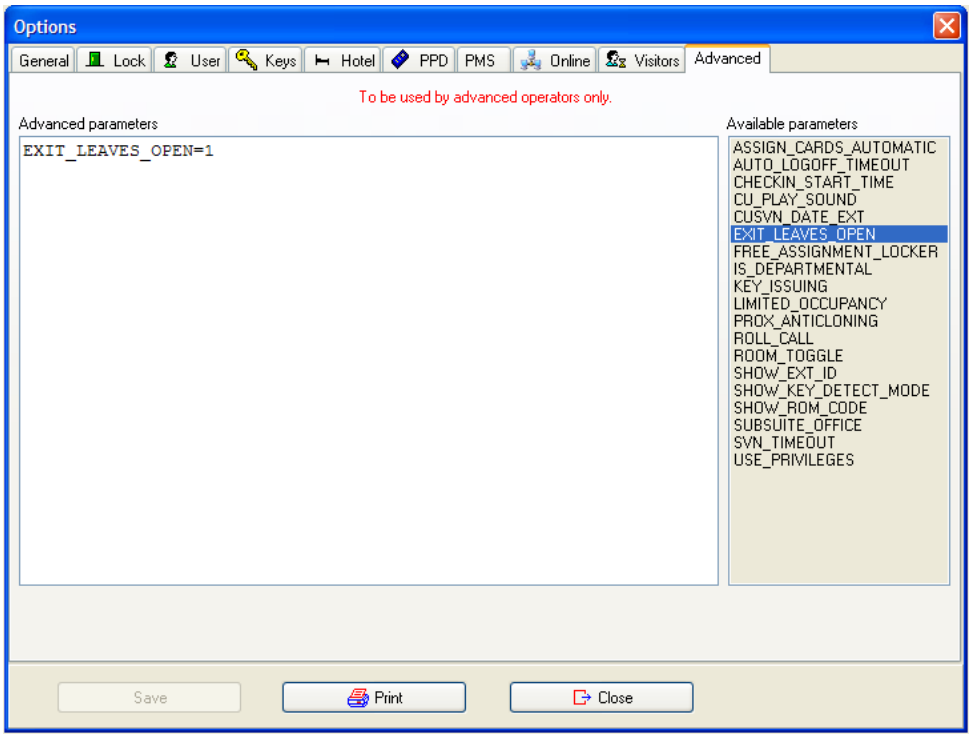
8. **Solo teclado:** Cuando tenemos un teclado conectado al lector podemos configurar la apertura de tal forma que por medio de un código la puerta se abra. El código es único y por tanto común para todos los usuarios. Este código se crea en la ventana de puertas para cada puerta.

9. **Teclado temporizado:** Igual que el anterior pero en este caso en un rango de tiempo especificado. Fuera de este tiempo solo se podrá abrir la puerta con la llave.

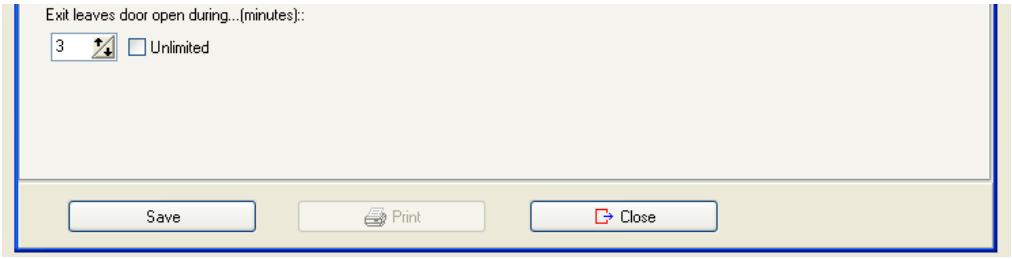
10. **Llave+PIN:** Para poder abrir la puerta además de presentar la llave el usuario ha de insertar su código personal. El código personal se debe crear en la ventana de usuario para cada usuario.

11. **Llave+PIN temporizado:** Igual que el caso anterior pero en un intervalo de tiempo establecido. Fuera de este periodo habrá que presentar la llave para poder abrir la puerta.

12. **Salida deja abierta (requiere la activación en opciones generales del parámetro "exit leaves open"):** La cerradura queda abierta al accionarse la manilla interior.



El tiempo de puerta abierta es infinito por defecto pero puede ser temporizado en minutos desde la pestaña "puerta" dentro de "Herramientas/Configuración/Opciones generales" (ver figura siguiente).



13. **Toggle + Exit leaves open:** se trata de una combinación de estos dos modos. La entrada con tarjeta funciona en modo Toggle (alternancia entre apertura y cierre) mientras que la manilla interior responderá al Exit leaves open.

- La caja titulada ZONAS indica a qué conjunto de puertas pertenece la puerta en cuestión que estamos definiendo ahora. Esta caja permanecerá en blanco hasta que se definan las zonas.

- En la parte inferior izquierda de la ventana, se ven unas flechas que nos servirán para pasar directamente a la puerta inmediatamente anterior o posterior (< >) o bien, ir a la puerta primera o última de la lista.

- En la parte derecha de la ventana se ve una caja titulada ACCESO POR PARTE DE... USUARIOS. Aquí aparecerán los usuarios con acceso a esta puerta, cuando hayamos definido los usuarios.

- La caja titulada ACCESO POR PARTE DE... NIVEL DE ACCESOS, también presentará los niveles de accesos de usuarios con acceso a esta puerta, cuando se hayan definido los niveles de accesos de usuarios. (Más adelante)

- Anti-pass back: Es la opción a través de la cual un usuario no puede pasar 2 veces por la misma puerta hasta que haya salido por la puerta de salida. Esta opción permite evitar que diferentes usuarios puedan entrar utilizando la misma llave.

- En el control de accesos de salto el anti-pass back también se puede configurar con escudos offline. La característica anti-pass back va escrita en la llave del usuario.

- Se tiene que activar la opción anti-pass back en esta puerta. Si se trata de una puerta Online se supone que hay un lector mural a la entrada y otro para salir. Mientras que si se trata de un escudo offline hay que especificar la ruta del antipassback. De tal forma que podemos seleccionar si es hacia fuera o hacia adentro.

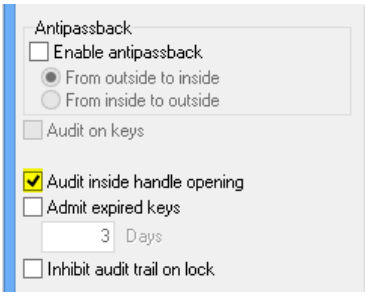
Por seguridad la opción anti-pass back solo es posible para regular la entrada no así la salida.

- Para que la función anti-pass back quede configurada es necesario también activar esta opción en la ficha de usuario.

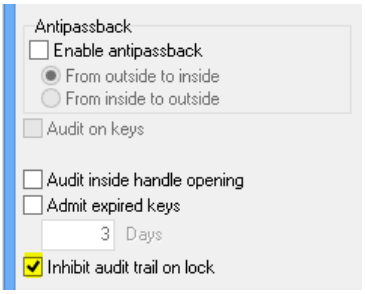
- AUDITAR EN LLAVES, esta opción se tiene que activar si queremos que el registro de por dónde han estado los usuarios quede registrado en la llave. Esto solo es posible para el personal del hotel. Además también tenemos que activar esta opción en la ficha del usuario.

- CALENDARIO, se puede seleccionar cual es el calendario sobre el que trabaje un escudo determinado. Esto es especialmente útil cuando tenemos instalaciones en diferentes zonas geográficas donde cada uno de los escudos se basa en calendarios diferentes.

- AUDITOR APERTURA INTERNA DE MANILLA permite controlar mediante el auditor de cerradura la salida del usuario mediante el giro de manilla interna.



- La opción INHIBIR AUDITOR EN CERRADURA permite deshabilitar la memorización de los eventos de apertura en los puntos de acceso. Ningún evento se registrará en la memoria del dispositivo al presentar una llave. Al activarse esta opción, será necesario actualizar la puerta con el PPD.



Para que esta función aparezca en la lista de puertas es necesario activar el parámetro "PERMITIR INHIBICIÓN DEL AUDITOR" en las opciones generales, pestaña Puertas.

- Las prestaciones online solo están disponibles en PA Connected o superior.

- Cuando hayamos terminado la definición de la puerta, guardamos los cambios y podemos pasar a definir la siguiente puerta pulsando el botón +.

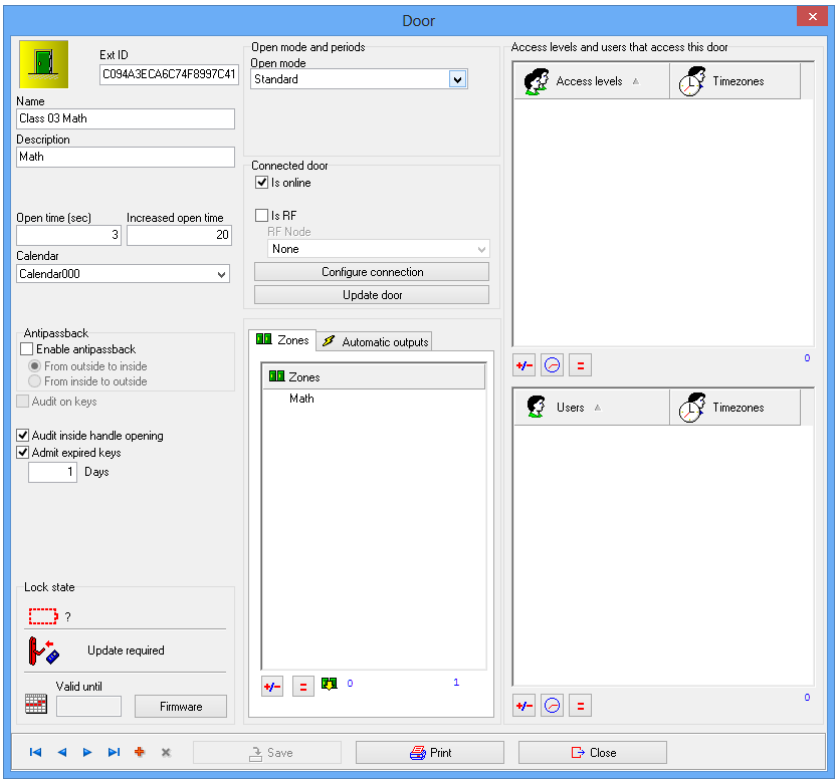


Figura 24

Al terminar de definir todas las puertas de nuestra instalación, podemos tener una lista de puertas como la siguiente:

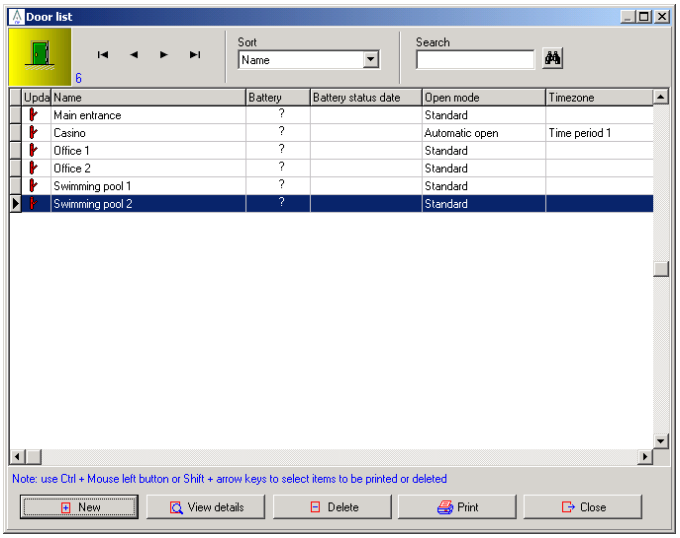


Figura 25

- Cuando tenemos esta ventana activa, y queremos ver las características de una puerta en concreto, lo que tenemos que hacer es seleccionar dicha puerta y pinchar en el botón *VER DETALLES.*

- Si por error, hemos introducido una puerta en la lista que no debería aparecer, simplemente la seleccionamos y pinchamos en el botón *ELIMINAR.*

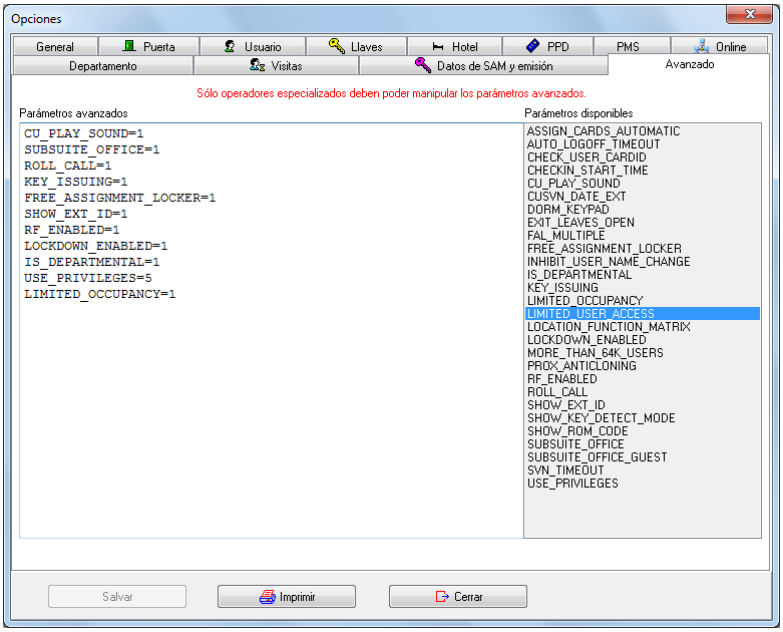
- En la parte superior de la lista se puede ver una caja llamada ORDENADO POR. Pinchando aquí, es posible cambiar el orden en que aparecen las puertas, de manera que aparezcan ordenadas por nombre o por estado de las pilas, o por modo de apertura.

- El botón IMPRIMIR se puede utilizar para obtener un informe en papel de la lista de puertas. Se puede escoger entre imprimir toda la lista de puertas o sólo los detalles relativos a una puerta en particular.

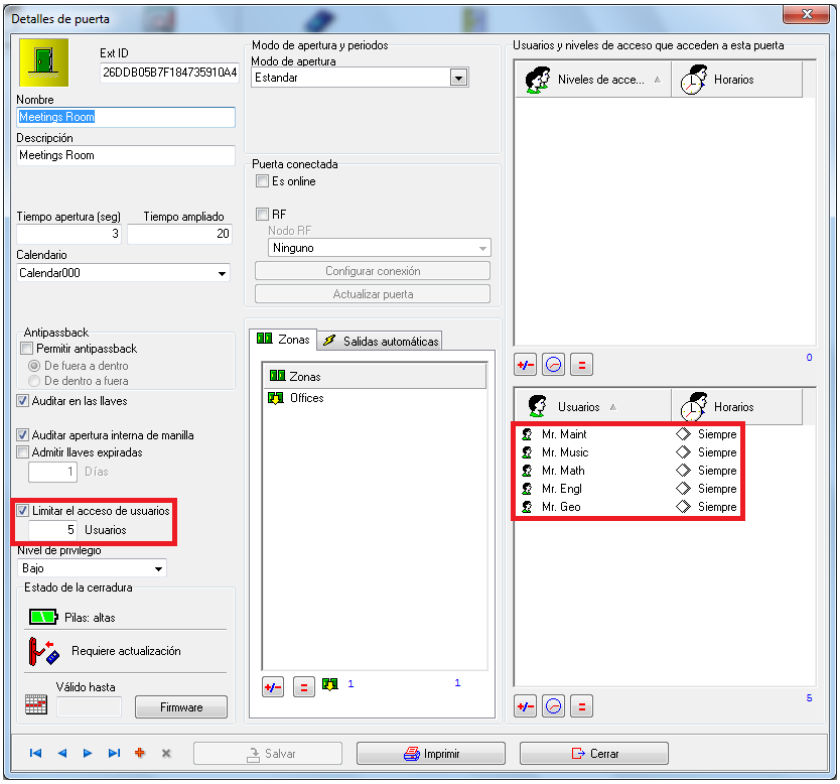
Limitar el Acceso de Usuarios

El software SALTO permite definir una cantidad máxima de usuarios individuales que puede abrir una cierta puerta.

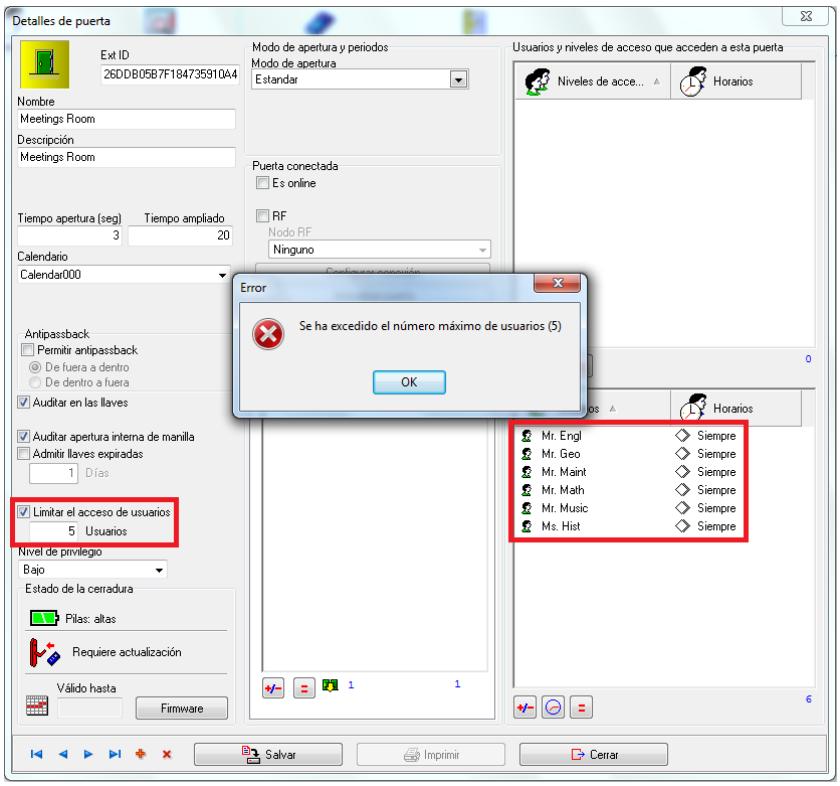
Para poder hacerlo, debe activarse el Parámetro Avanzado LIMITED_USER_ACCESS:



Este Parámetro Avanzado activará una nueva opción en la venta de configuración de las Puertas, la cual permitirá al operador del sistema definir cuantos usuarios pueden asignarse individualmente para abrir la puerta:



En el caso que el operador exceda la cantidad de usuarios especificada en esta opción, el software le avisará de ello cuando los cambios vayan a ser guardados:



NOTA IMPORTANTE: Esta función solo limita la cantidad de usuarios que pueden ser asignados individualmente en la ventana de configuración de la puerta para que puedan abrirla, pero no limita la cantidad total de gente que pueda abrir dicha puerta, por el hecho de poder acceder a una zona que tiene esa misma puerta incluida, o por pertenecer a una nivel de acceso que puede abrir esa puerta.

nas

En este apartado vamos a explicar cómo se crea la lista de zonas. Una zona es un conjunto de puertas que se han agrupado siguiendo un criterio práctico, por ejemplo, primer piso del edificio, segundo piso, etc...

Es importante tener en cuenta que para que un cliente pueda entrar en una puerta que no es su habitación, es necesario que la puerta esté incluida en una zona.

En la barra de herramientas, pinchamos en el icono de *ZONAS*. Se abrirá una ventana como la siguiente:

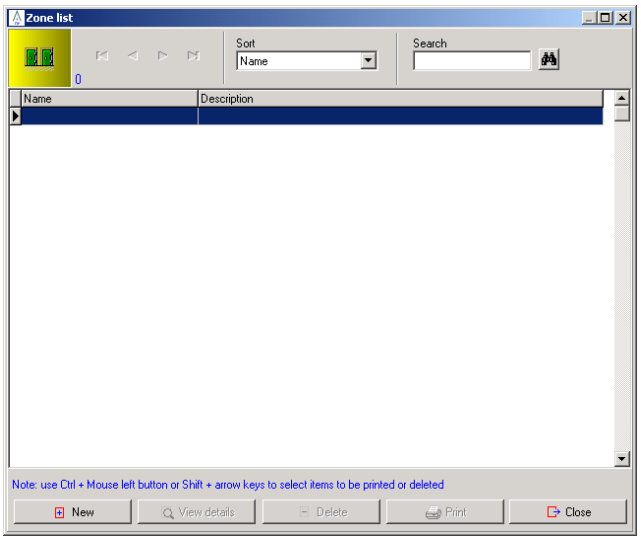


Figura 26

- Pinchamos en el botón llamado *NUEVO* para crear la primera zona de la lista.

- Se abrirá una ventana en blanco como la siguiente:

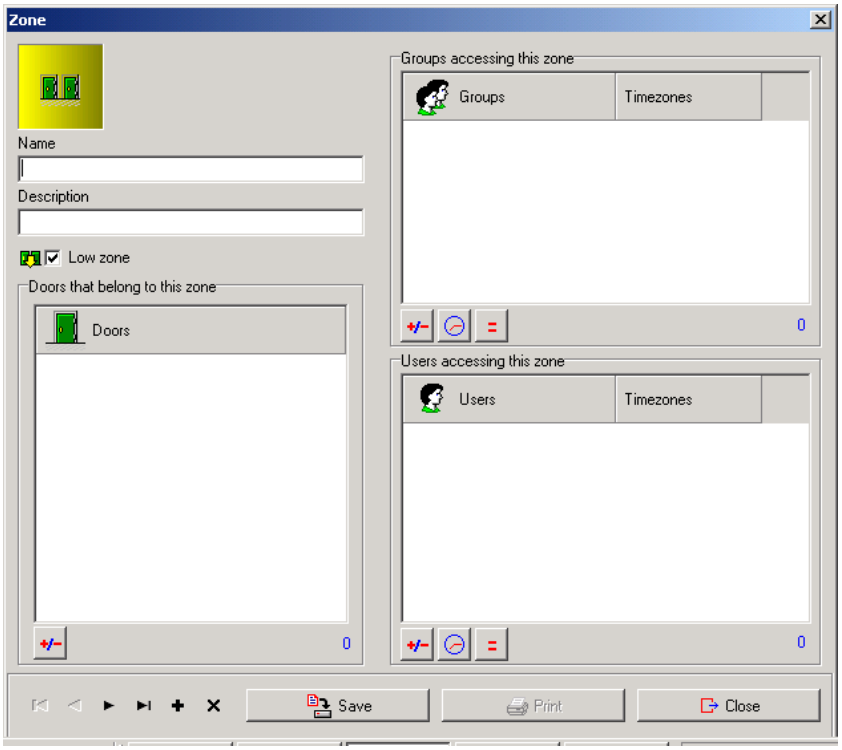


Figura 27

- Primero escriba un nombre para la zona, que sea representativo.

- En el campo DESCRIPCIÓN puede incluir una explicación del criterio que agrupa estas puertas.

- El check box ZONA BAJA se modificará únicamente en caso de necesitarse más de 96 zonas. Las zonas se diferencian en ALTAS y BAJAS en función de la forma en que están se almacenan en la memoria del escudo. Se pueden crear 96 zonas bajas y 928 altas teniendo en cuenta que una cerradura puede pertenecer únicamente a 96 zonas bajas y 20 zonas altas. Una vez cerrada la ventana no se podrá modificar el estatus de la zona.

- La caja titulada PUERTAS QUE PERTENECEN A ESTA ZONA sirve para elaborar el conjunto de puertas que integra la zona. Haga clic con el ratón en el botón +/- para visualizar la lista de puertas y escoger las que pertenezcan a esta zona.

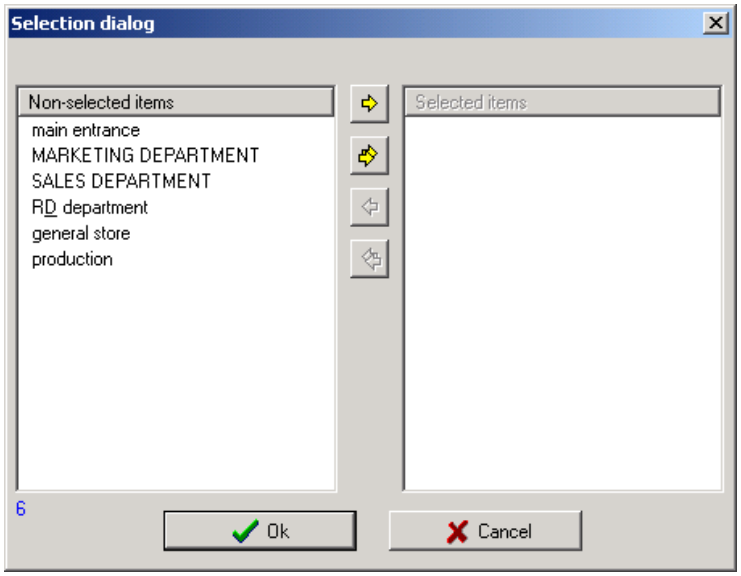


Figura 28

- Seleccione con el ratón la puerta que quiera meter en el conjunto de esta zona, y después pulse la flecha amarilla que indica la columna de la derecha.

- La puerta seleccionada aparecerá en la columna de la derecha como integrante de la zona.

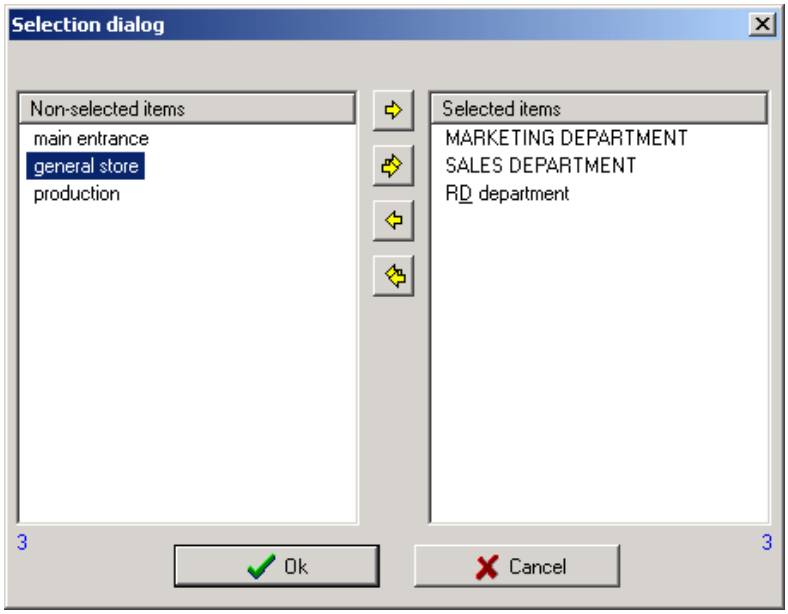


Figura 29

- Repetimos esta operación con cuantas puertas queramos que pertenezcan a esta zona.

- Cuando esté completa la columna de la derecha, según el criterio de selección de esta zona, pulsamos el botón OK.

- Ahora, el conjunto de puertas que integran la zona, aparecerá en la caja de abajo a la izquierda, en la ventana de detalles de la zona.

- La caja titulada CON ACCESO POR PARTE DE,,, USUARIOS , está en blanco porque todavía no hemos definido los usuarios. Cuando los definamos, se puede utilizar esta caja para especificar qué usuarios tienen acceso a esta zona. (y con qué horario).

- La caja titulada CON ACCESO POR PARTE DE... GRUPOS tiene un funcionamiento análogo, sólo que en vez de asignar los accesos a la zona individualmente, lo hacemos por nivel de accesos, con lo cual , se gana tiempo.

- Una vez que hemos cumplimentado todos los campos de la ventana de detalles de esta zona, guardamos los cambios.

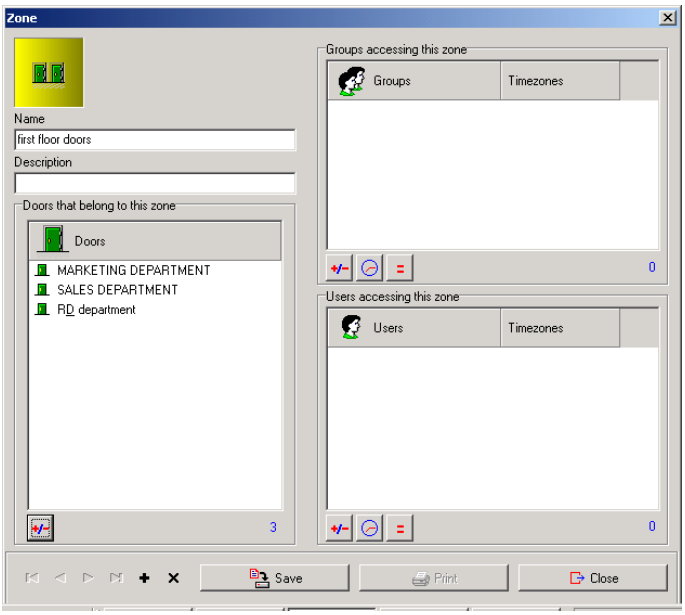


Figura 30

- Pulsando el botón + podemos pasar a la siguiente ventana de detalles, para ir definiendo así todas las zonas de nuestra instalación.

En este ejemplo, se ha definido una zona que engloba las 2 puertas que dan a la piscina. Los clientes de la primera planta tendrán acceso a la piscina, pero los clientes de la segunda planta

no lo tendrán. Esto hace que cada nivel de acceso de clientes esté diferenciado por un régimen de alojamiento diferente.

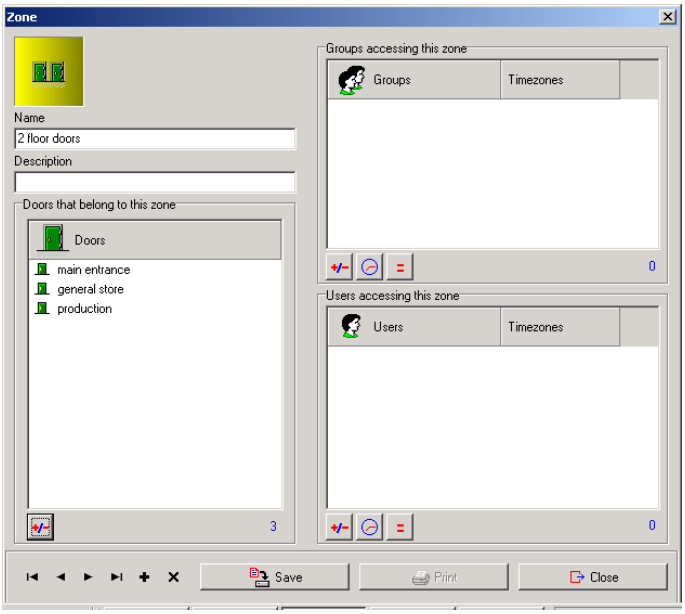


Figura 31

- Al final , podemos tener una lista de zonas como la que se ve a continuación:

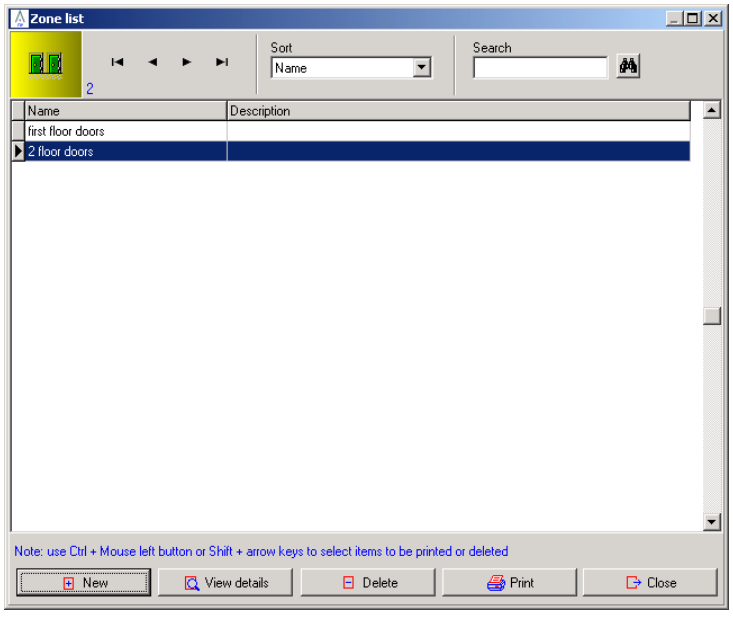


Figura 32

- Si, por error hemos creado una zona que no debería existir, bastará con seleccionarla con el ratón y pulsar el botón ELIMINAR .

- Si después de haber guardado los cambios , queremos ver los detalles de una zona de la lista, la seleccionamos con el ratón y pulsamos el botón VER DETALLES.

- Si queremos seleccionar una zona de la lista , sin utilizar el ratón, también se pueden usar las flechas que aparecen en la parte superior izquierda de esta ventana <> , para avanzar al siguiente elemento de la lista, al anterior, o bien, ir directamente al elemento último o primero de la lista.

- La caja titulada ORDENADO POR sirve para ordenar la lista de zonas alfabéticamente , por nombre de zona , o bien por descripción de la misma.

- El botón imprimir se puede utilizar para obtener un informe en papel de la lista de zonas. Se puede escoger entre imprimir todas las zonas de la lista o sólo los de talles de una zona en particular.

Salidas

Es posible conectar una Unidad de control a una placa de extensión de relés. De esta forma un usuario o huésped podrá activar uno o varios relés en función de los permisos en su tarjeta. En nuestro ejemplo los huéspedes del segundo piso podrán activar los relés que activan el segundo piso y piso cero pero no así el primer piso por ejemplo.

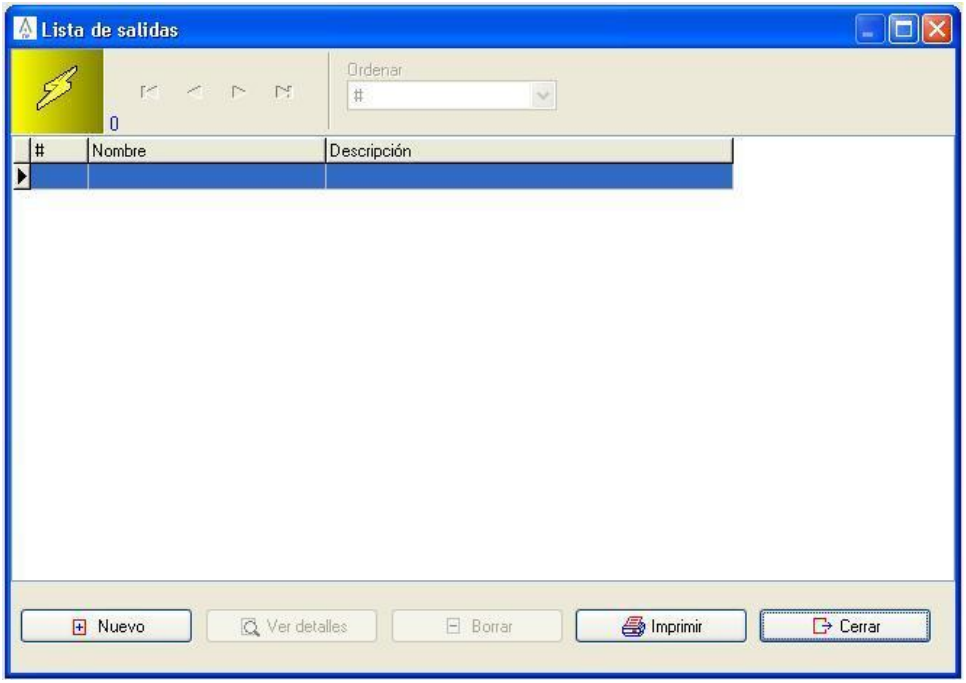
En nuestro caso podríamos tener 2 ascensores y los huéspedes del segundo piso tendrían acceso a las mismas áreas, por lo que las salidas relativas a cada ascensor son las mismas, Salida 1=Piso 1, Salida 2=Piso 2 y Salida 3=Piso cero.

Hay que crear tantas salidas en el software como relés queramos controlar y esas salidas se pueden asignar a usuarios o nivel de accesos de clientes de la misma forma que se asignan las zonas. Es importante tener en cuenta que para que un usuario pueda activar un relé de una CU ha de tener acceso al lector conectado a esa CU.

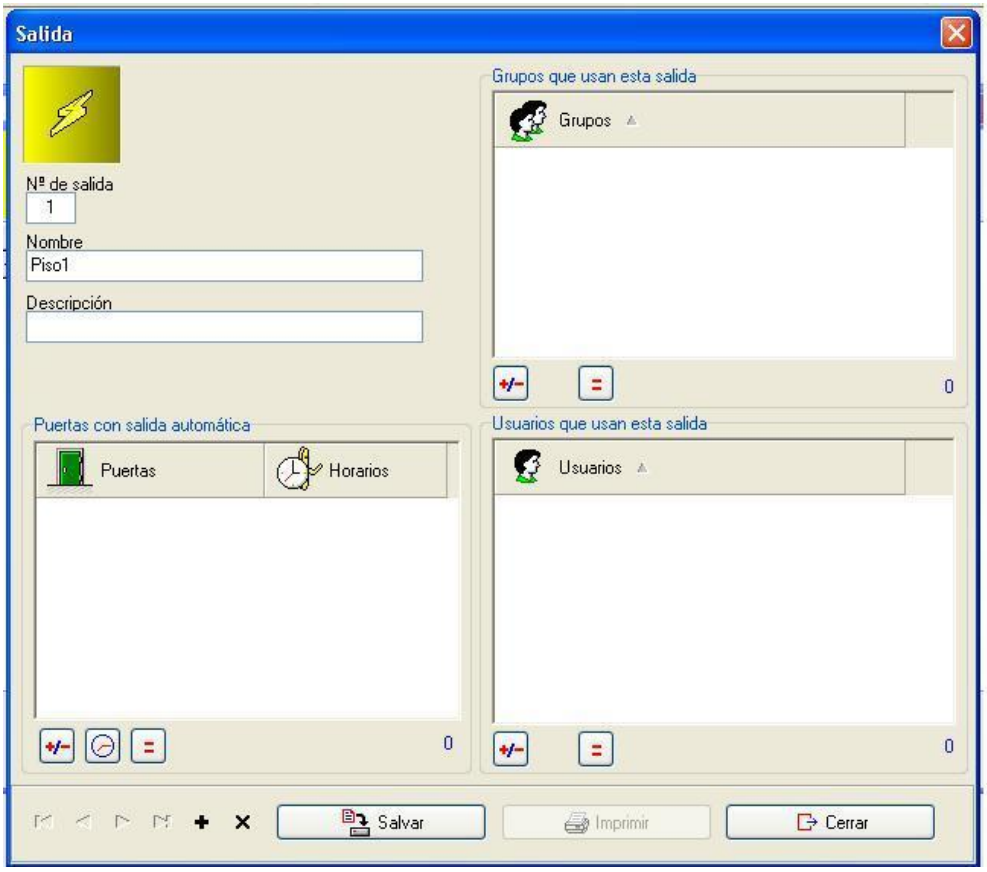
En el siguiente ejemplo vamos a crear 3 salidas para la placa de extensión de relés.

La primera salida será el primer piso(para los ascensores 1 y 2) y la segunda salida será para el segundo piso(ascensores 1 y 2). Hay un lector mural conectado a cada Unidad de control.

Para llevar a cabo nuestro ejemplo vamos a Datos/Lista de salidas:



Aquí se pueden definir los diferentes relés de la placa de extensión de relés y configurar el uso de los relés.

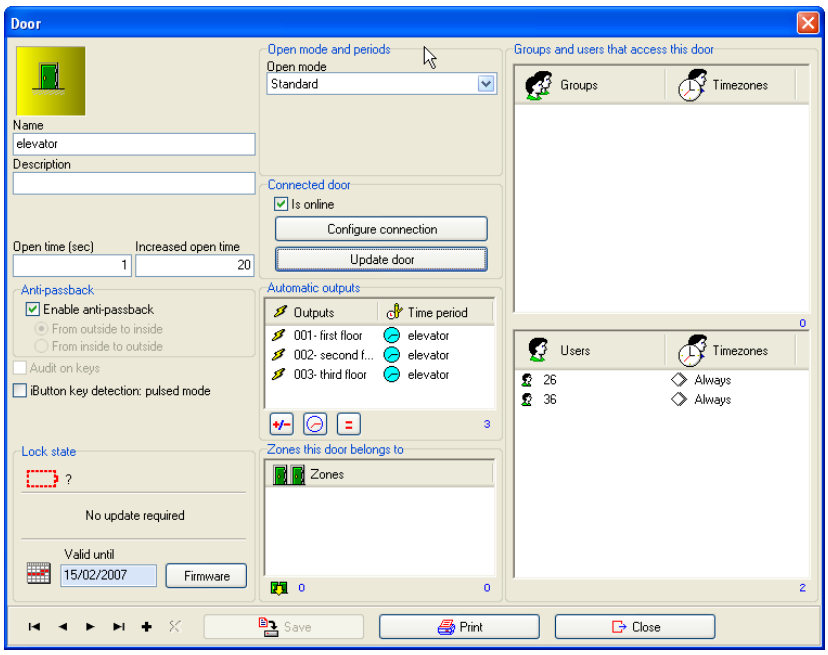


Es importante recordar los números que se asignan a cada relé ya que estos se asignan por medio de las salidas. En nuestro ejemplo la salida 1 se relaciona con el relé 1 de la placa de extensión de relés. En la ventana se puede escribir el nombre y descripción y finalmente salvar los cambios.

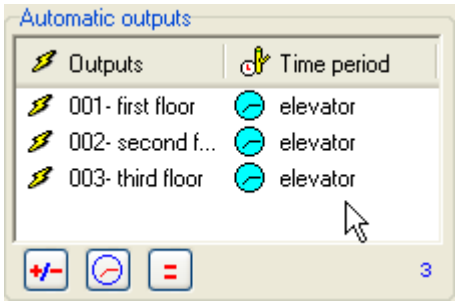
Una vez que ya hemos creado la lista de salidas podremos asignarlos a los usuarios o nivel de accesos de clientes de la misma forma que asignamos las zonas. Es importante no olvidar asignar a esos usuarios accesos a los lectores murales conectados en las unidades de control donde las placas de relés se han conectado.

Salidas automáticas

Si queremos que algunas de las salidas trabajen en apertura automática en un periodo determinado necesitaremos asignar este periodo a las salidas de cada puerta. Para ello hay que ir a la ventana de puertas y en la ventana salidas automáticas añadir las salidas y seleccionar los periodos.



En la ventana salidas automáticas:



Añadir las salidas y seleccionar los periodos en los cuales esas salidas se deben activar de forma automática.

Importante: El máximo de salidas automáticas es 4.

Periodos.

Los periodos son intervalos de tiempo que van asociados con los escudos electrónicos (a diferencia de los horarios, que van asociados con las personas). Un periodo sirve para determinar el espacio de tiempo dentro del cual una cerradura trabajará en un modo especial – paso temporizado, apertura automática.

Si cuando usted definió las puertas , puso un modo de trabajo temporizado para alguna de ellas, ahora tendrá que definir aquí el intervalo de tiempo correspondiente a esa puerta .

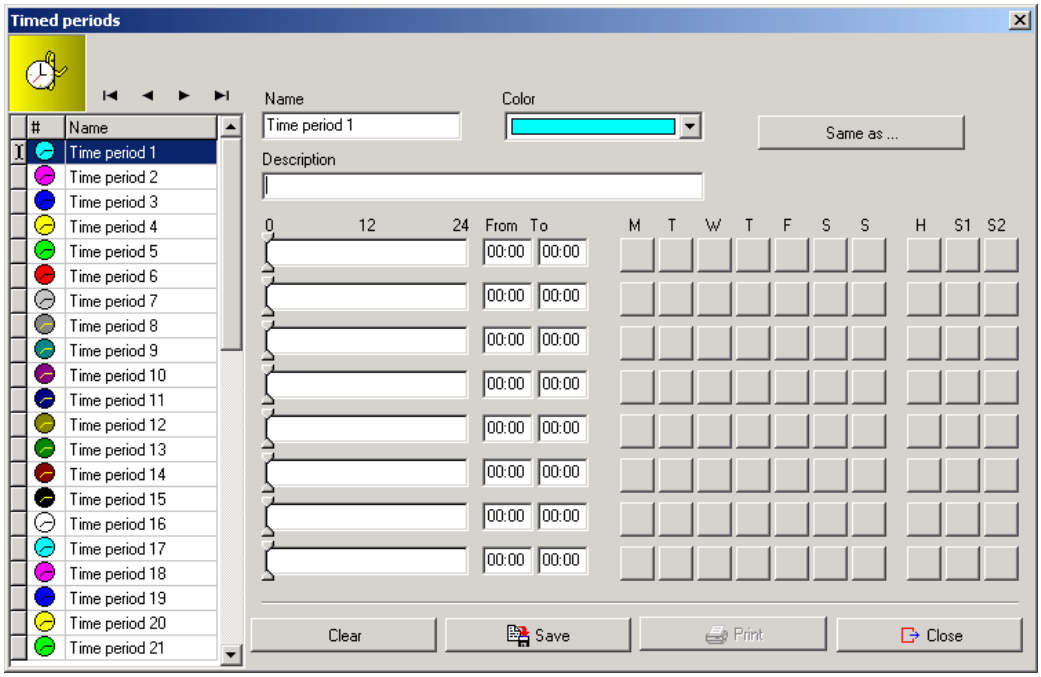


Figura 33

- Hacemos clic en el icono de periodos de la barra de herramientas. Se abrirá una ventana como la de la figura superior.

- Ponemos un nombre al Periodo , y le asignamos un color representativo.

- En la descripción, resulta útil escribir a qué puerta corresponde el periodo que vamos a definir.

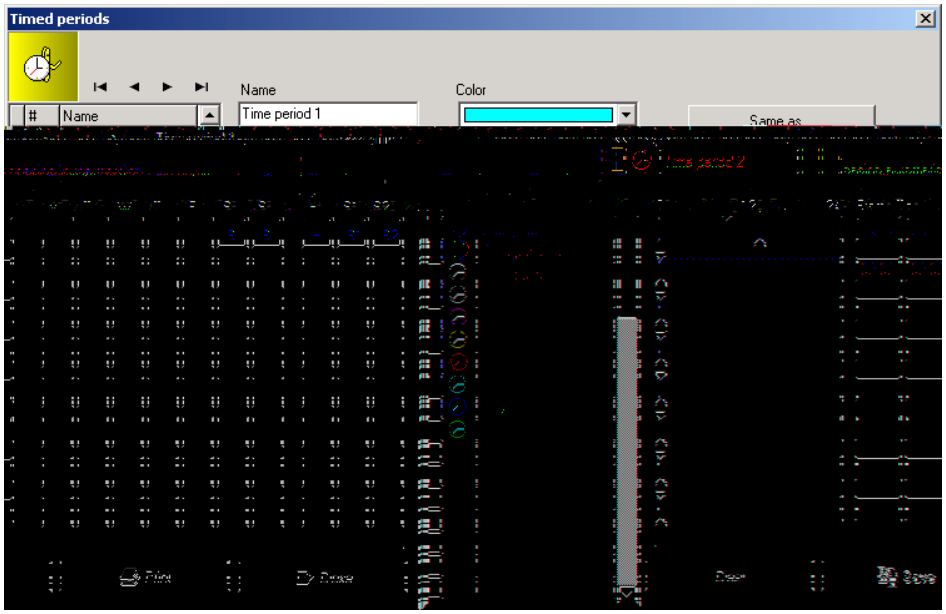


Figura 34

- El intervalo de tiempo se define utilizando el ratón. Haga clic con el ratón sobre el cursor deslizante superior y arrástrelo para establecer el inicio del intervalo.

- Haga clic con el ratón sobre el cursor deslizante inferior para establecer el final del intervalo. La máxima precisión para el tiempo es de 10 minutos.

- Después tendrá que especificar en qué días de la semana se va a aplicar este periodo. También se puede concretar si el periodo va a funcionar en días festivos o especiales. (este dato está relacionado con el calendario 0, ya que en él se determina qué días son festivos o especiales con respecto a los periodos).

- Si el periodo que estamos definiendo tiene varios subintervalos, utilizaremos las líneas que sean necesarias para su definición.

- Al terminar de definir el periodo, guardamos los cambios y podemos definir más periodos, si es que son necesarios en nuestro sistema.

- El botón IMPRIMIR se puede utilizar para obtener un informe en papel de la lista de periodos. Usted puede escoger entre imprimir todos los periodos de la lista o sólo los detalles relativos a un periodo en particular.

- Recuerde asignar el periodo a su puerta correspondiente, si no lo hizo con anterioridad. Para ello, vaya a PUERTAS y

seleccione la puerta que tiene un periodo. Pulse el botón VER DETALLES y verá que el periodo definido por usted aparece en la lista de periodos disponibles. Asigne dicho periodo a la puerta y guarde los cambios.

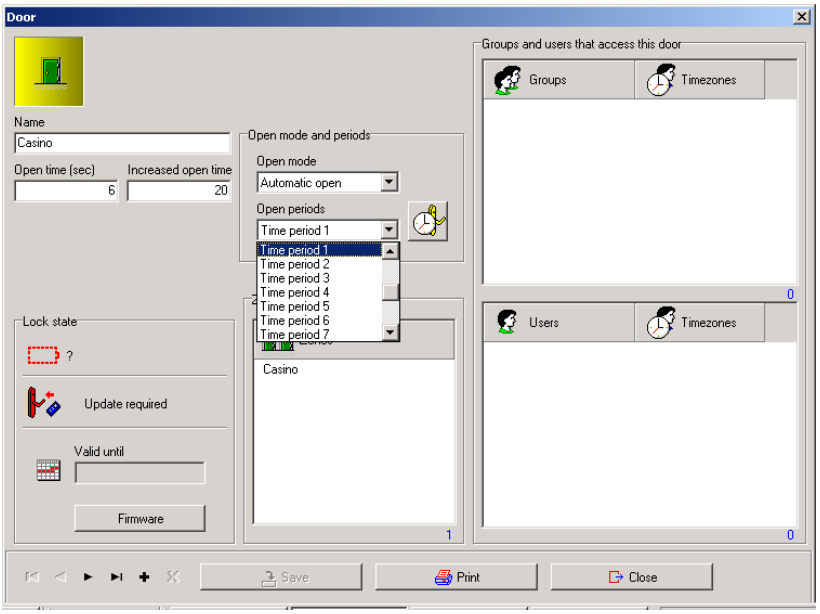


Figura 35

Horarios

Los horarios son intervalos de tiempo que pertenecen a las personas (a diferencia de los periodos que pertenecen a las puertas). Horario es el tiempo dentro del cual, un usuario concreto tiene acceso a una determinada puerta o zona.

- Para definir los horarios, pulsar el icono de HORARIOS de la barra de herramientas.

- Se abrirá una ventana en blanco, como la que viene a continuación.

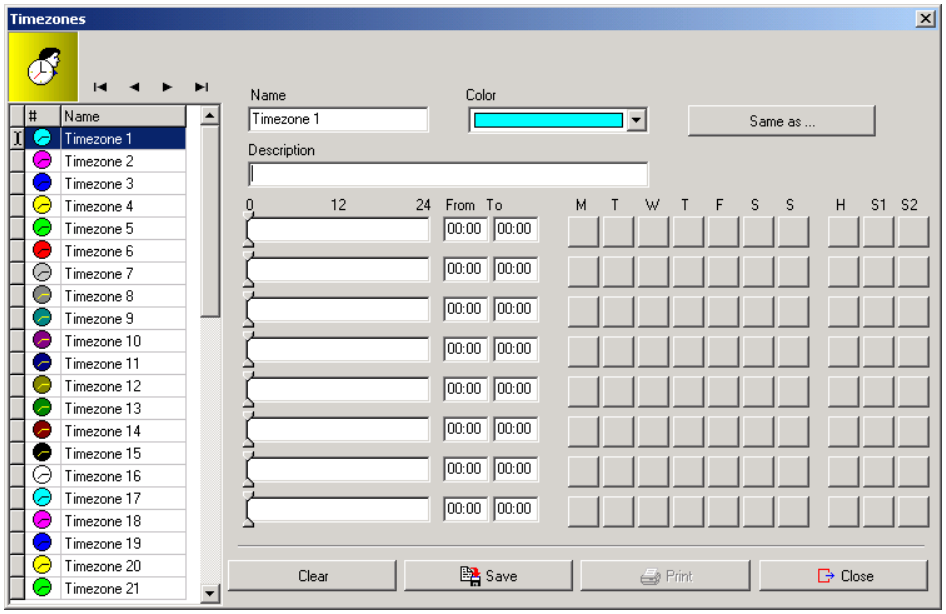


Figura 36

- Escribimos el nombre de nuestro primer horario y le asignamos un color.

- En la descripción, resulta útil escribir el nombre de la persona o nivel de acceso al que corresponde este horario.

- Para la definición del horario, seguimos el mismo procedimiento que para el caso de los periodos, explicado en el apartado anterior.

- No olvide concretar qué días de la semana tendrán el horario en vigor, así como si el horario será válido en días festivos o especiales. Para especificar estos días, basta con pulsar en el cuadrado correspondiente con el ratón.

- El botón IMPRIMIR sirve para obtener un informe en papel de la lista de horarios. Se puede escoger entre imprimir toda la lista de horarios o sólo los detalles relativos a un horario en particular.

- Una vez terminado de definir el horario, guarde los cambios y pase a definir más horarios distintos para otros usuarios o nivel de accesos de usuarios.

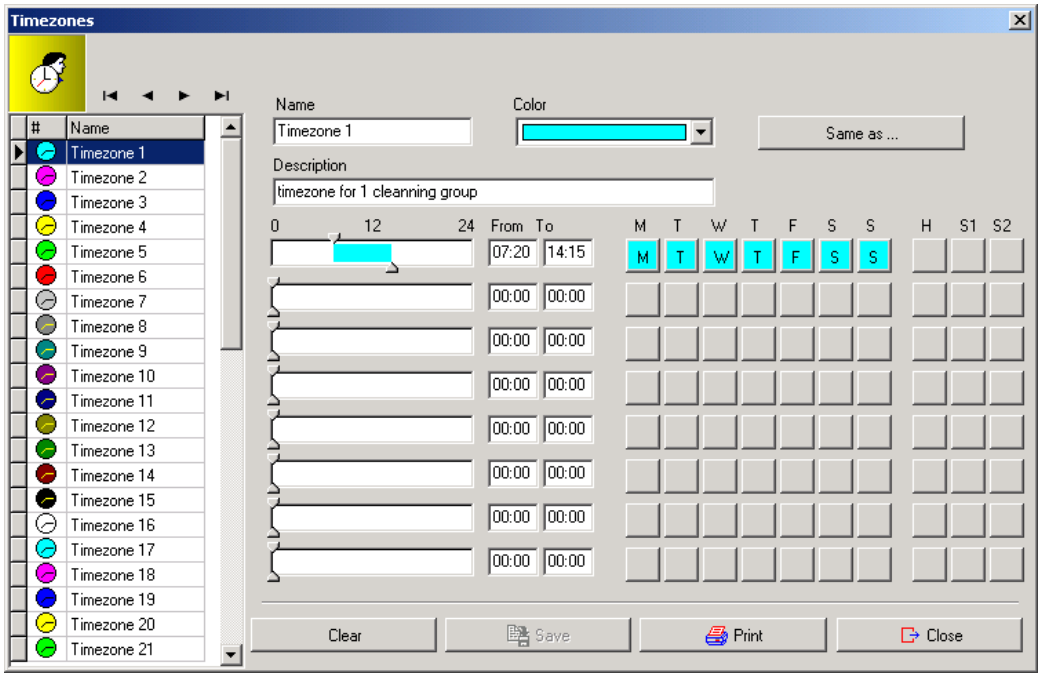


Figura 37

- No olvide asignar el horario a su usuario o nivel de acceso, más adelante se explica cómo se hace, en la definición de los usuarios y nivel de accesos de usuarios.

Calendarios

El rango de calendarios va de 0 a 255 y puede asignarse tanto para usuarios como para escudos.

- Para los escudos los calendarios se usan cuando estos van a trabajar con modos temporizados. Por lo cual se debe definir en qué días se aplican estos periodos.

- De la misma forma son utilizados por los usuarios, para definir en qué días se aplican sus horarios de acceso.

Para definir nuestros calendarios, simplemente hay que pulsar el icono de calendarios en la barra de herramientas.

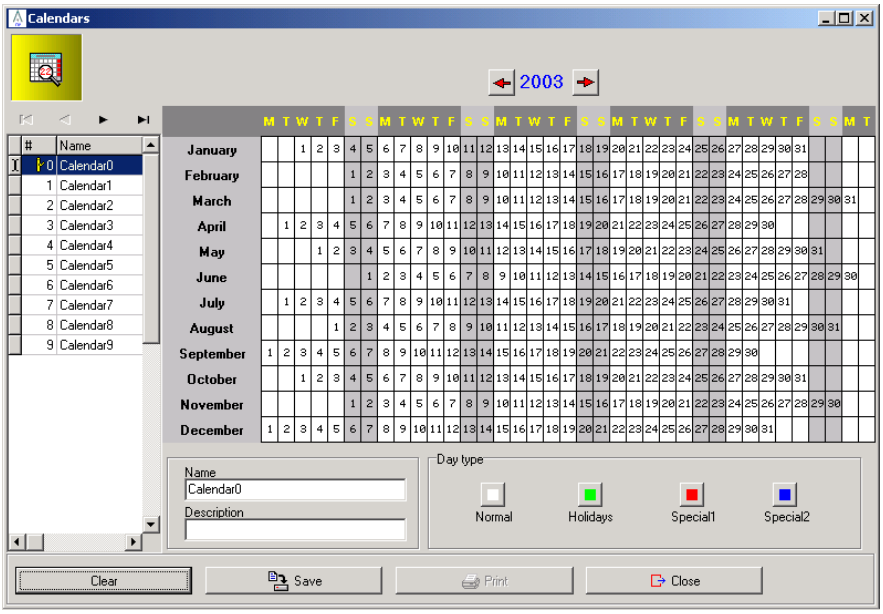


Figura 38

- Se abrirá una ventana como la de la figura superior. podemos dar un nombre a nuestro primer calendario y una descripción, para saber a qué corresponde.

- Se recomienda definir el calendario para el año en vigor y para el año siguiente si es posible. Para pasar al año siguiente basta con pulsar la flecha roja de la parte superior de la ventana, que indica hacia la derecha.

- Hay 4 categorías de días: normal, festivo, especial 1 y especial 2.

- Se puede marcar un conjunto de días del calendario utilizando el ratón y arrastrándolo mientras se mantiene pulsado el botón derecho.

- A continuación pulse el cuadrado de la parte inferior que representa el tipo de día que se quiere asignar a ese conjunto, y verá como los días seleccionados cambian de color de acuerdo con su selección.

- Es importante recordar que el hecho de que un usuario tenga acceso a una puerta en día festivo o de vacaciones, no depende sólo del calendario sino también de que el horario de dicho usuario haya sido habilitado en días festivos o de vacaciones.

- El botón IMPRIMIR sirve para obtener un informe en papel de la lista de calendarios .Se puede escoger entre imprimir toda la lista de calendarios o sólo los detalles relativos a un calendario en particular. El tipo de día se puede reconocer por una pequeña letra , F para Festivos, E para días especiales y N para días normales.

- Cuando haya terminado de definir el calendario , puede tener algo parecido a la figura inferior:

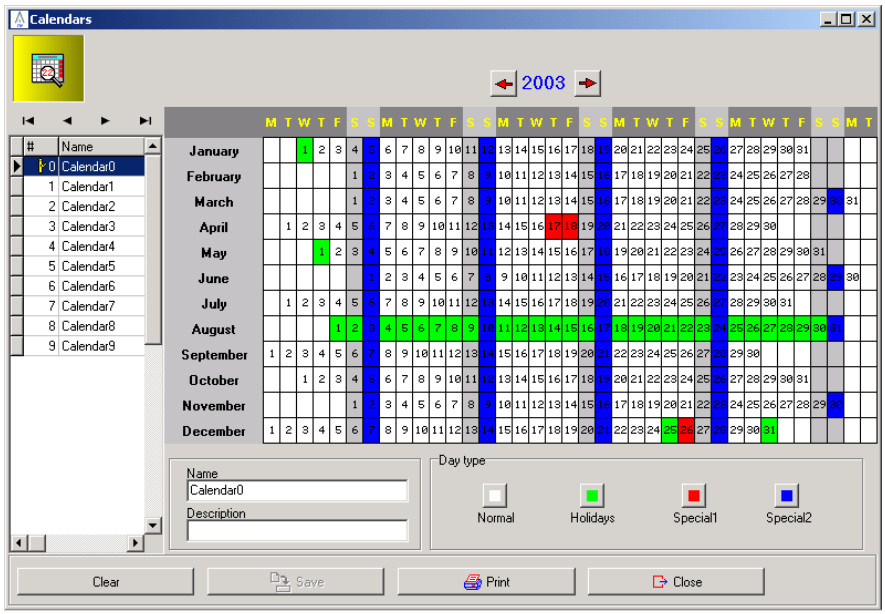


Figura 39

- Guarde los cambios al terminar de definir el calendario y pase a definir el siguiente calendario, si su instalación lo necesita.

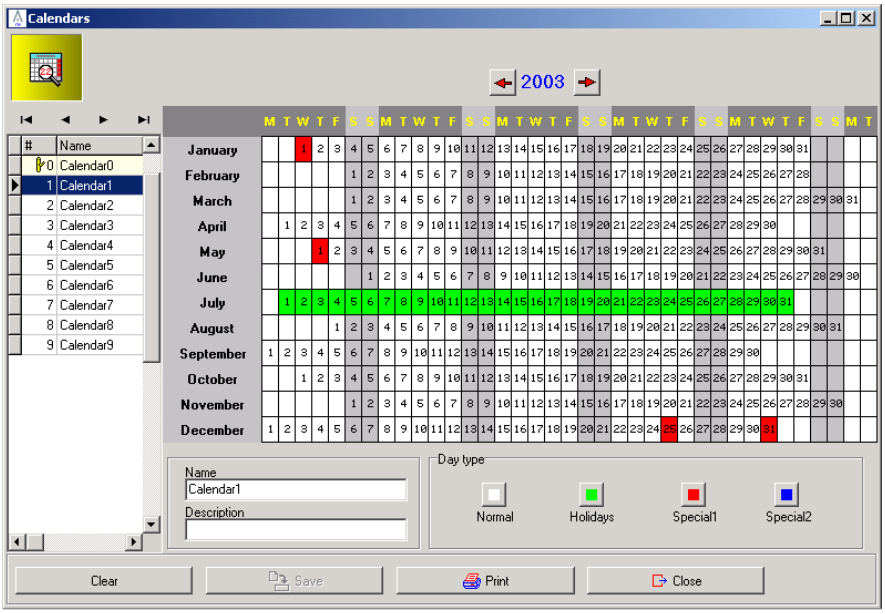


Figura 40

- No olvide asignar los calendarios a sus usuarios , más adelante se explica esta operación , en la definición de usuarios y nivel de accesos de usuarios.

Cambio horario

Las siglas DST vienen del inglés y significan Daylight Saving Time, es decir cambio horario que se realiza con vistas a conseguir un ahorro energético al optimizar el aprovechamiento de la luz solar.

Este cambio se suele realizar poco después de los equinoccios de primavera y otoño, adelantando el reloj en el primero y atrasándolo en el segundo.

Los escudos electrónicos de Salto realizan el cambio horario automáticamente, si así se establece desde el software.

Pulse el icono DST de la barra de herramientas y verá una ventana como la siguiente:

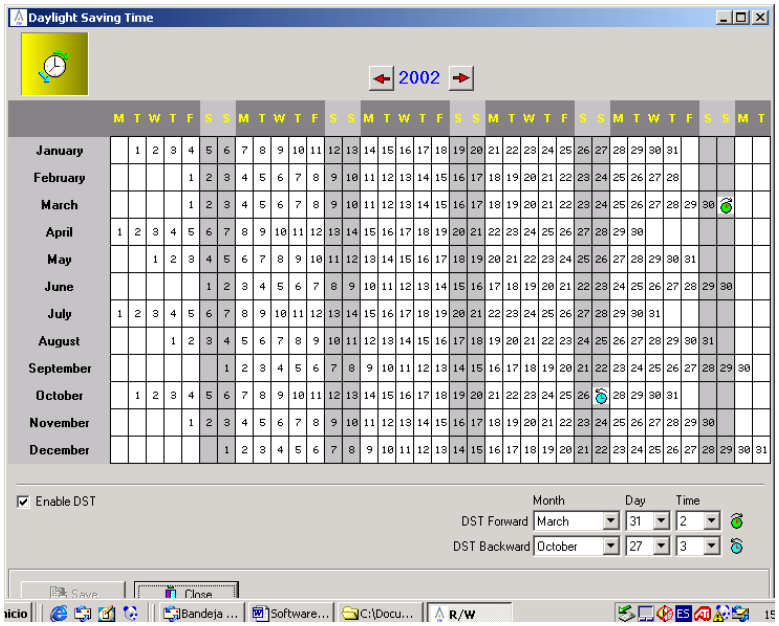


Figura 41

- Usted puede habilitar o no, el cambio horario mediante la "check box" HABILITAR DST que aparece en la esquina inferior izquierda de la ventana.

- También puede cambiar el día y la hora en que se realiza dicho cambio mediante las flechas DÍA y HORA que aparecen en la esquina inferior derecha de la ventana.

- Si usted cambia el día del cambio horario, el símbolo que lo representa se moverá en el calendario de acuerdo con su elección.

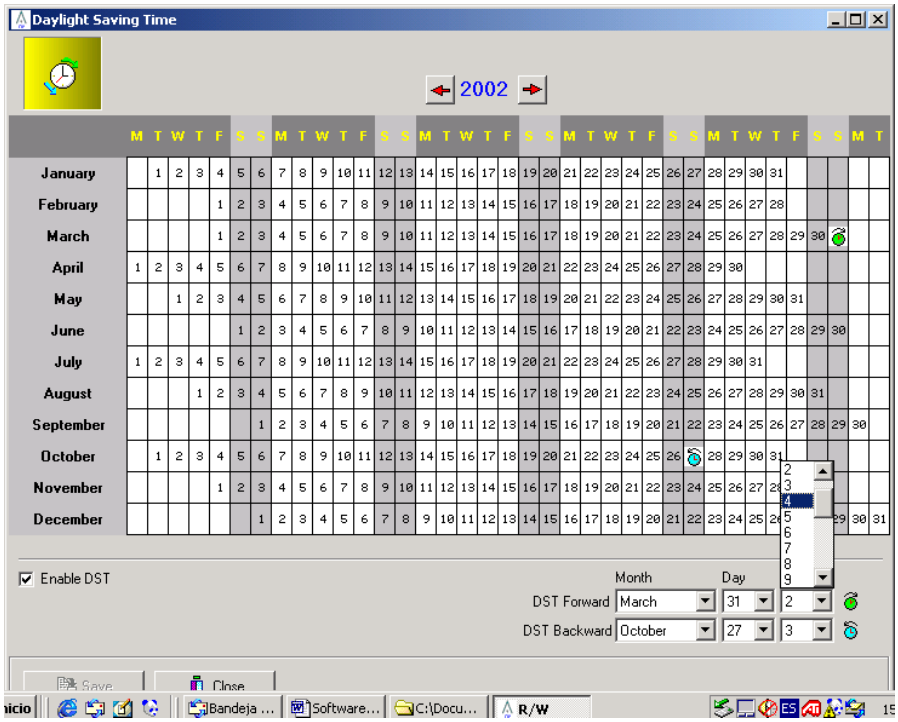


Figura 42

- También se puede planificar el cambio horario para el año siguiente, si lo desea. Pulse la flecha roja (derecha) de la parte superior de la ventana para pasar al año siguiente.

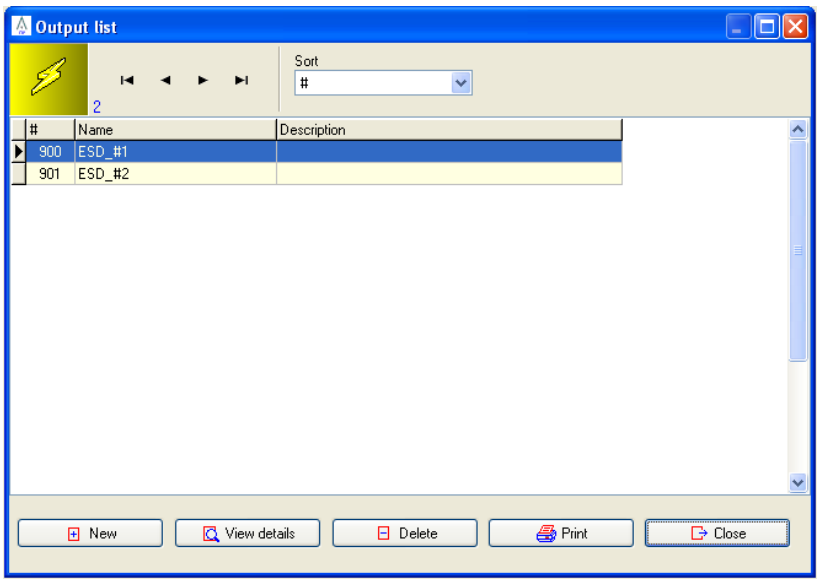
- Guarde los cambios cuando haya establecido los parámetros adecuados para su cambio horario.

- Se recomienda habilitar el cambio horario automático, ya que si no lo habilita por software, tendrá que hacer una actualización con el PPD de todas las puertas de su instalación, en el día previsto para dicho cambio horario.

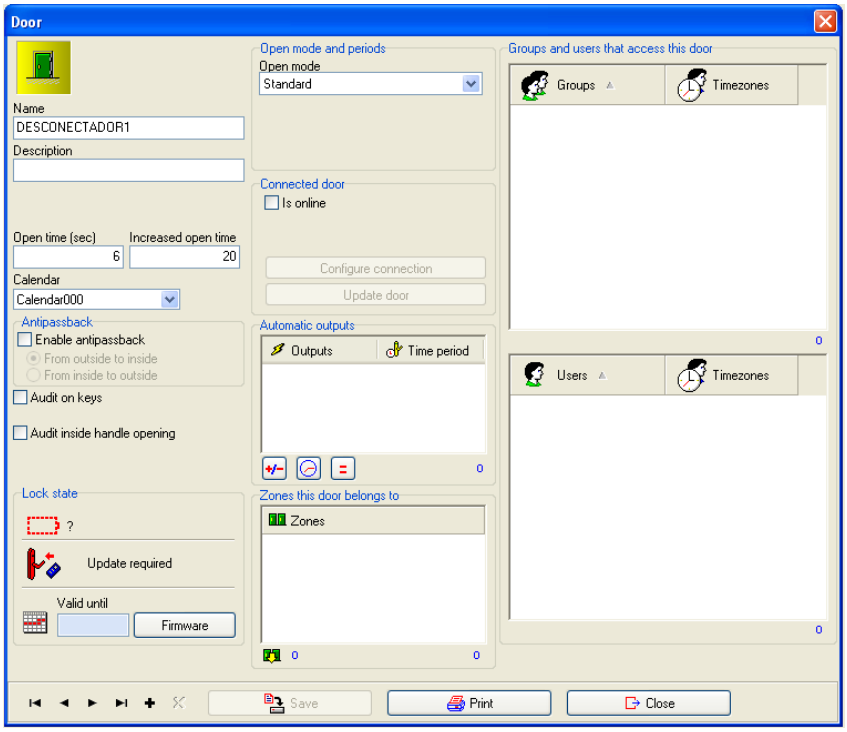
Lista de salidas: utilización de DESCONECTADORES

Es posible utilizar desconectadores de luz mediante el uso de las salidas.

Para ello basta con asignar al usuario deseado una de las salidas (o las 2) disponibles en el menú de salidas. La salida 900 activará el relé1 y la salida 901 el relé2.



El desconectador se crea como una puerta más, configurando únicamente el nombre a asignar (el resto de parámetros no serán enviados).



Cambios temporales automáticos

En esta nueva versión de software se pueden planificar cambios automáticos en los modos de apertura en las CUs. A diferencia de los modos de apertura que hemos dispuesto hasta el momento los cambios automáticos permiten a las CUs modificar sus

modos de apertura en diferentes intervalos de tiempo. Por ejemplo, de 00:00H a 08:00H Modo paso, de 08:00H a 18:00H apertura automática y de 18:00 a 24:00 modo estándar.

Es decir un cambio automático es un intervalo de tiempo en el cual la CU trabaja en diferentes modos de apertura definidos previamente por el usuario. Por tanto los parámetros que definen un cambio automático son: Hora de comienzo, Hora final y Modo de apertura. En un día cualquiera (Normal, Fiesta, Especial1 y Especial2) se pueden planificar hasta 8 cambios automáticos. Para permitir diferentes combinaciones el software agrupa los diferentes tipos de días (con sus cambios automáticos asociados) en 256 tablas.

En resumen, la BBDD de Salto incluye 256 tablas de cambios automáticos donde a su vez cada tabla contiene 10 tipos de días (De Lunes a Domingo, Fiesta, Especial1 y Especial2) y cada tipo de día a su vez puede contener hasta 8 cambios automáticos.

En cuanto al interface gráfico el menú Datos/Periodo de tiempos…muestra ahora 2 subopciones llamadas periodos y cambios automáticos como se puede ver en el figura siguiente:

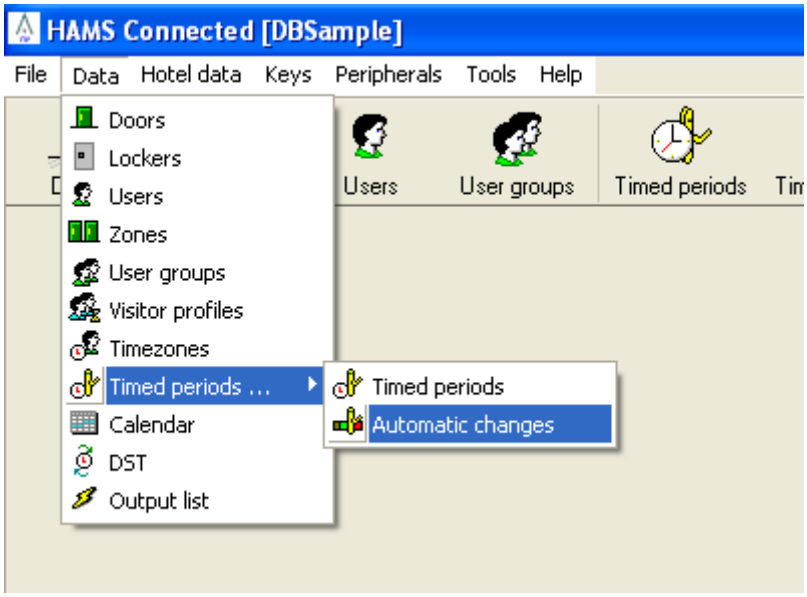


Figura1: Acceso a la ventana de cambios automáticos a través del menú principal.

En la figura de abajo (Fig2) se muestra la ventana que permite establecer los cambios automáticos. En esta ventana se pueden modificar los cambios automáticos de una tabla y tipo de día(a través del botón +/-) como se muestra en la figura3. También es posible copiar cambios automáticos de un día a otro(a través del botón '=') como se puede observar en la figura 4 o incluso copiar toda la tabla en otra (a través del botón '=Copia') como se muestra

en la figura 5. Finalmente se puede hacer que una CU trabaje con cambios automáticos como se puede ver en la figura 6.

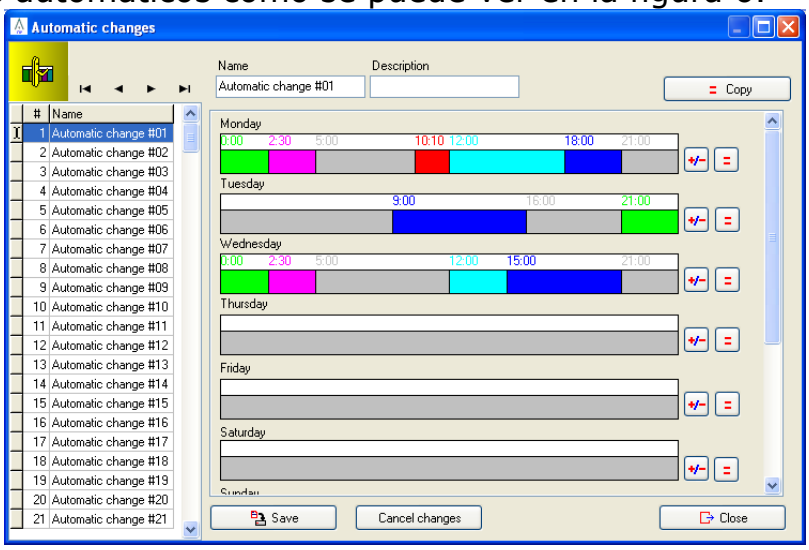


Figura 2: Ventana de cambios automáticos.

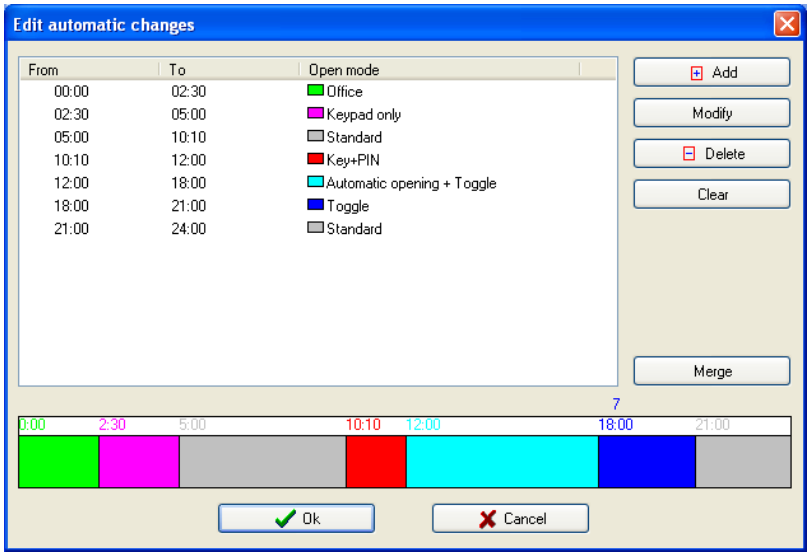


Figura 3: Modificación de cambios automáticos de una tabla dada y día tipo (botón '+/-').

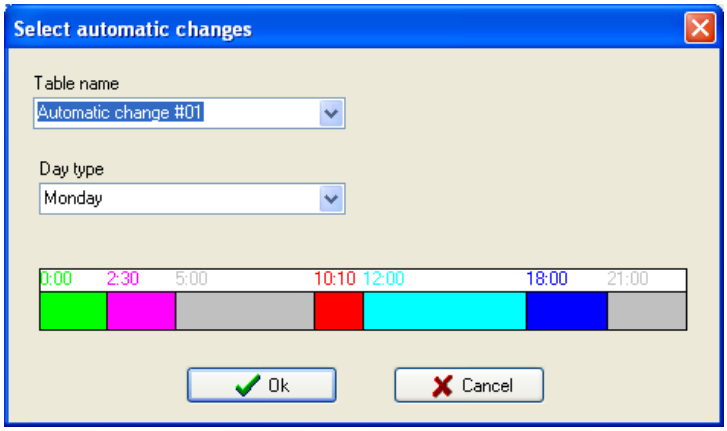


Figura 4: Especificación de la tabla y día tipo desde el cual se quiere que se copien los cambios automáticos (botón '=').

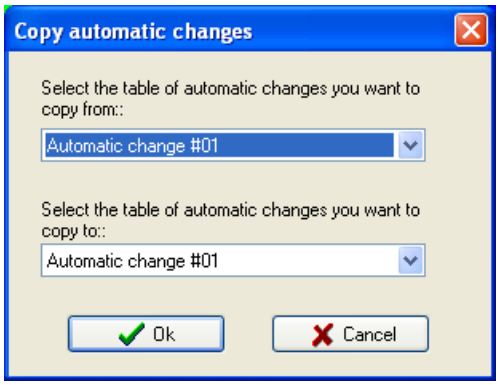


Figura 5: Especificación de la tabla origen y tabla destino para que los cambios automáticos sean copiados (botón '= Copia').

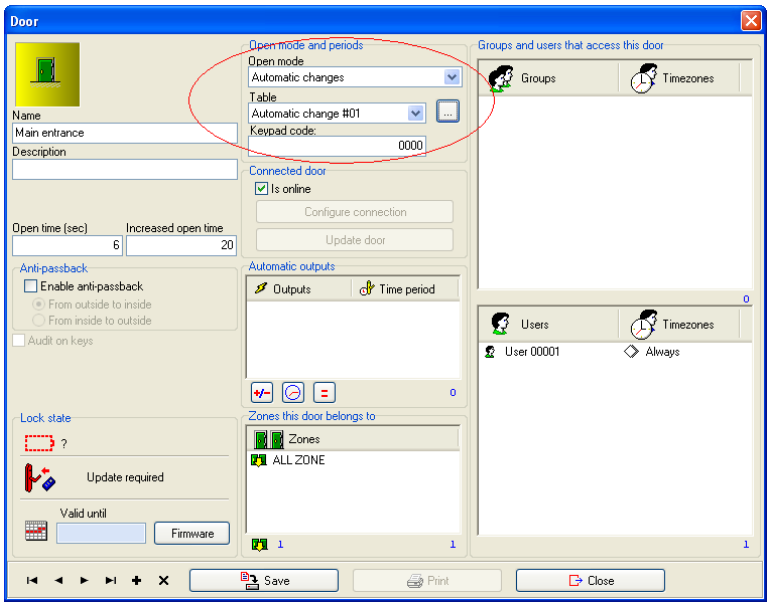
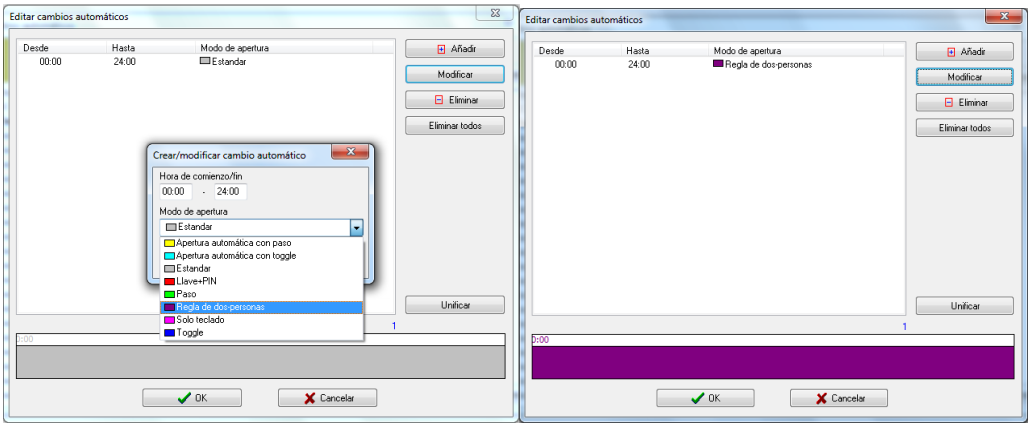


Figura 6: Hacer que una CU trabaje en modo de cambios automáticos.

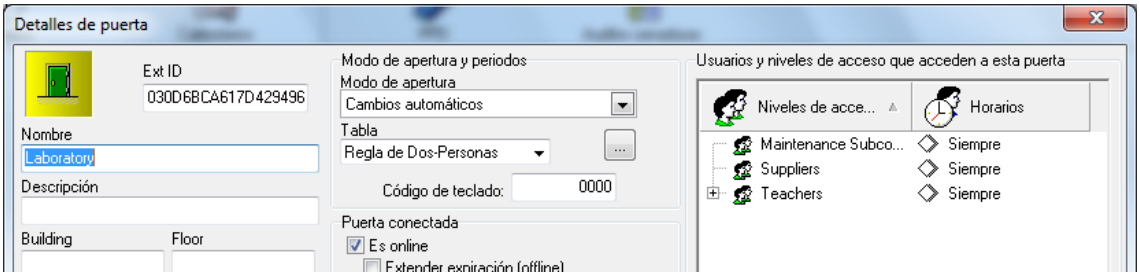
Los Cambios Automáticos incluyen también un modo especial de funcionamiento de cerradura que solo puede activarse en este menú, llamado Regla de Dos-Personas. Cuando se selecciona este modo de funcionamiento, la puerta solo puede abrirse cuando dos personas con acceso válido presentan sus tarjetas una detrás de otra en el dispositivo SALTO que controla el acceso a través de la puerta.

Este modo de funcionamiento por lo tanto solo puede activarse en las cerraduras a través de los Cambios Automáticos.

Como puede verse en los dibujos que viene a continuación, la Regla de Dos-Personas está incluida en la lista de modos de los Cambios Automáticos:



Una vez el Cambio Automático seleccionado se ha configurado, debe elegirse en la configuración de la Puerta, junto con la Tabla correspondiente:



NOTA: Este modo de funcionamiento debe estar disponible también en el firmware del dispositivo al que se quiera asignar. Confirmar por favor la compatibilidad con su contacto de SALTO habitual.

Niveles de Acceso

Conviene recordar que los "usuarios" son los miembros de la plantilla del hotel, nunca los clientes.

Los niveles de acceso son nivel de accesos que podemos definir, los cuales engloban a una cierta cantidad de usuarios que tienen algo en común: Por ejemplo, podemos agrupar a los usuarios por su empleo u ocupación, ya que profesionales de un mismo trabajo suelen tener accesos y horarios comunes.

Haga clic en el icono de NIVELES DE ACCESSO DE USUARIOS en la barra de herramientas.

Se abrirá una ventana como ésta:

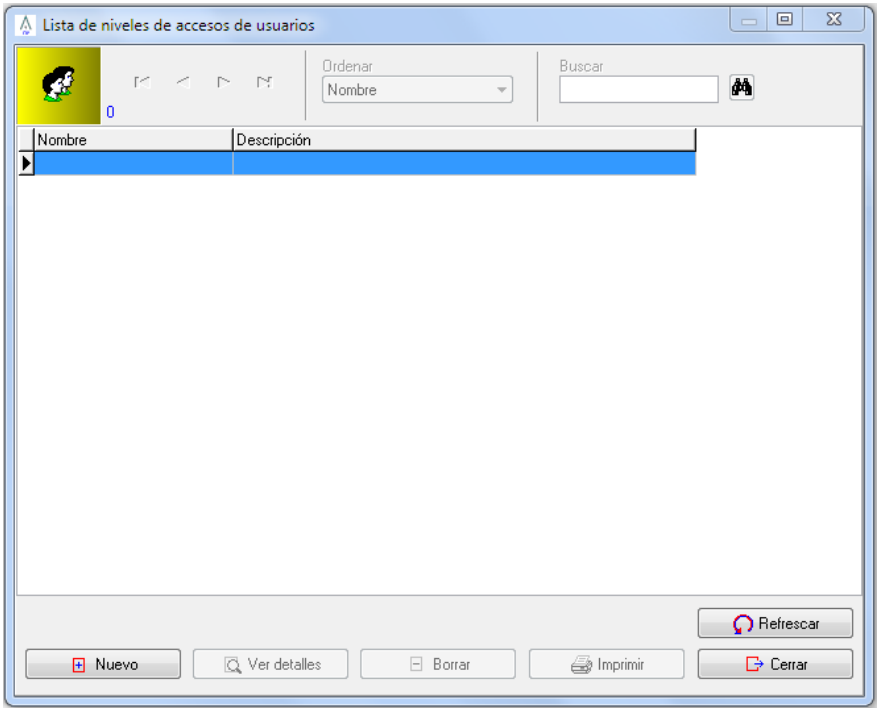


Figura 43

- Como todavía no hemos creado ningún nivel de acceso, la lista está vacía.

- Para crear el primer nivel de acceso, hay que hacer clic en el botón NUEVO.

- Se abrirá una ventana como la que se ve a continuación:

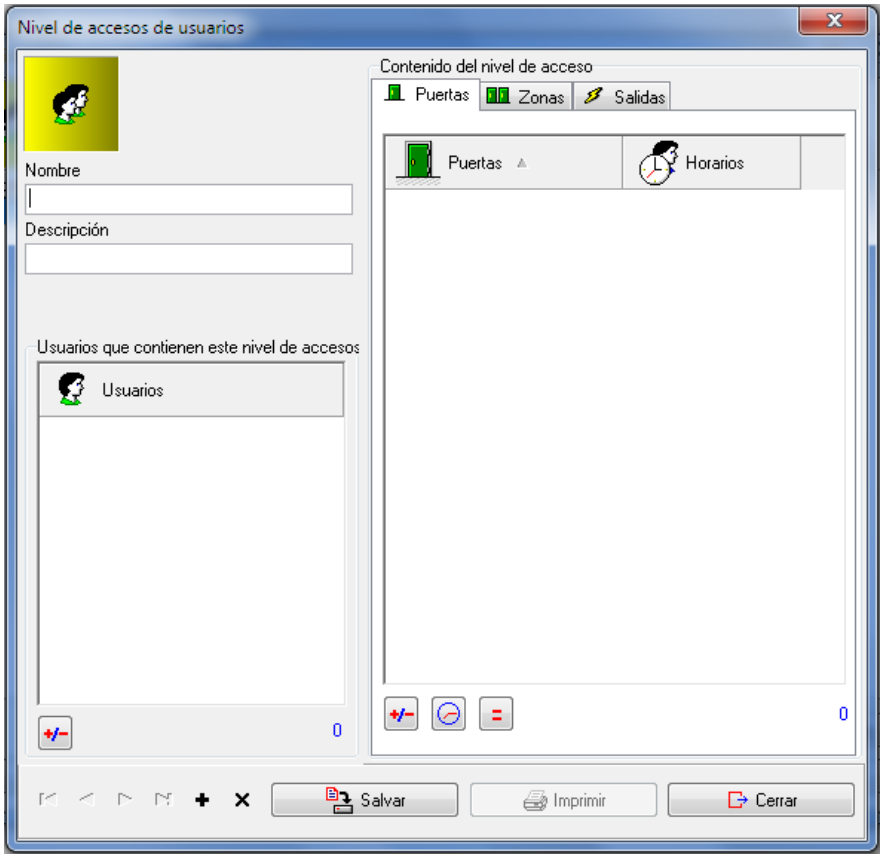


Figura 44

- Primero escribimos el nombre de este nivel de acceso, y debajo una descripción que explique la característica que define al nivel de acceso.

- Como todavía no hemos definido los usuarios, no podemos establecer qué personas pertenecen al nivel de acceso, pero podemos fijar los niveles o accesos del grupo.

- En la ventana llamada "Contenido del nivel de acceso", pulsamos el botón con el símbolo +/- para asignar zonas, puertas o salidas al nivel de acceso.

- Si una persona debe pertenecer a varios niveles de acceso se puede proceder de varias maneras,

1/ En la ficha del nivel de acceso, Figura 44, se añade el usuario usando el botón +/-, en cada uno de los niveles de acceso a los que el usuario debe pertenecer.

2/ En los accesos del usuario, situado en la ficha del usuario, se pueden añadir los diferentes niveles de acceso previamente creados, a los accesos del usuario, como se ve en la figura 44b.

Por otra parte el usuario también podrá tener acceso a puertas independientemente de los niveles de acceso.

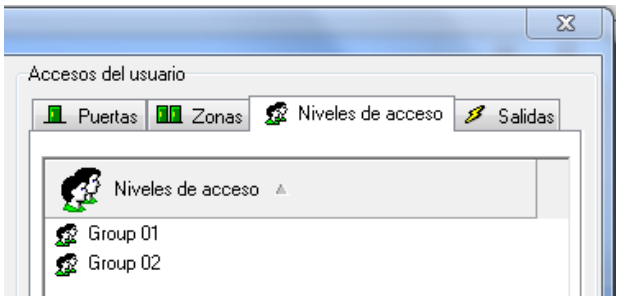


Figura 44b

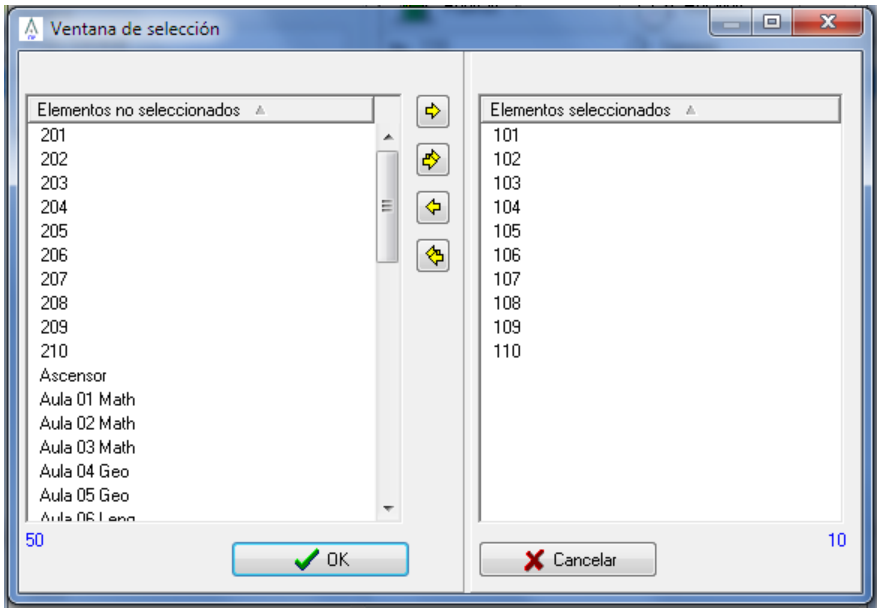


Figura 45

- Tenemos que pasar a la columna de la derecha, las zonas, puertas o salidas a las que van a tener acceso las personas con este nivel de acceso.

- Si por error hemos incluido una zona, puerta o salida, la seleccionamos y pulsamos la flecha amarilla hacia la izquierda, para devolver el acceso a la columna de la izquierda.

- Las dobles flechas amarillas hacen la misma función que las flechas sencillas, pero trasladan todos los usuarios de la columna de origen a la columna de destino en un clic.

- Podemos especificar qué acceso tienen permitido los integrantes del nivel de acceso, pulsando el botón con el símbolo

+/- y también podemos especificar horarios para el nivel de acceso, pulsando el botón que tiene el símbolo de un reloj.

- El hecho de dar acceso a un nivel de acceso, implica que cada persona de ese nivel de acceso puede entrar a cada una de las puertas de la zona, por las puertas individuales o tenga acceso a las salidas.

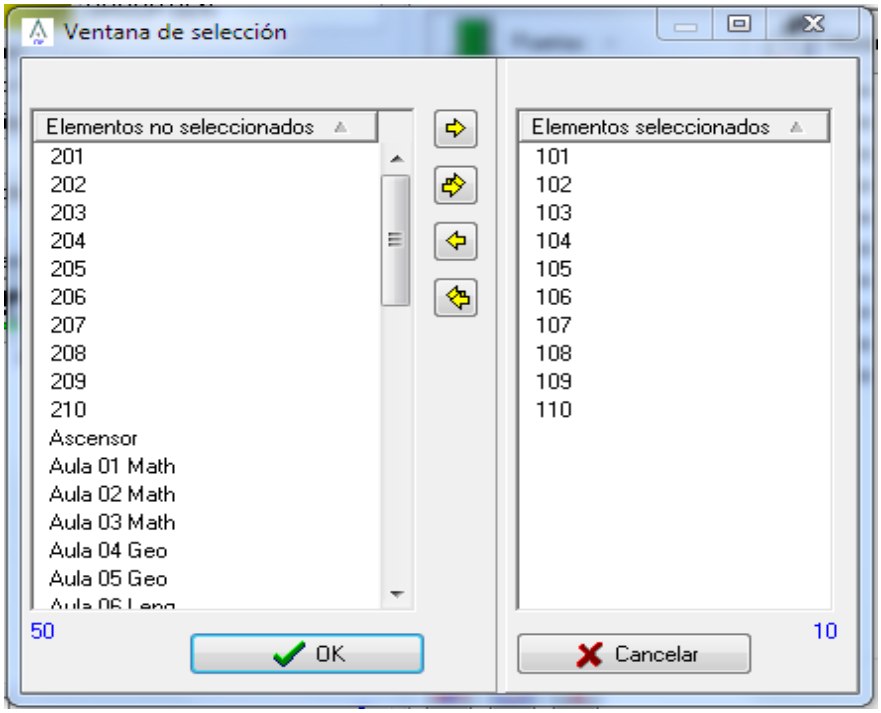


Figura 46

En la ventana de accesos aparece una pestaña titulada PUERTAS y otra titulada SALIDAS. Estas funcionan de la misma manera que la caja ZONAS, pero en vez de asignar accesos por zonas, lo hacemos por puertas individuales. Esta opción se puede utilizar para alguna puerta suelta, pero en general se recomienda gestionar el acceso por zonas para ahorrar tiempo y espacio de memoria. Las salidas permitirán activar los relés a los que se tenga acceso.

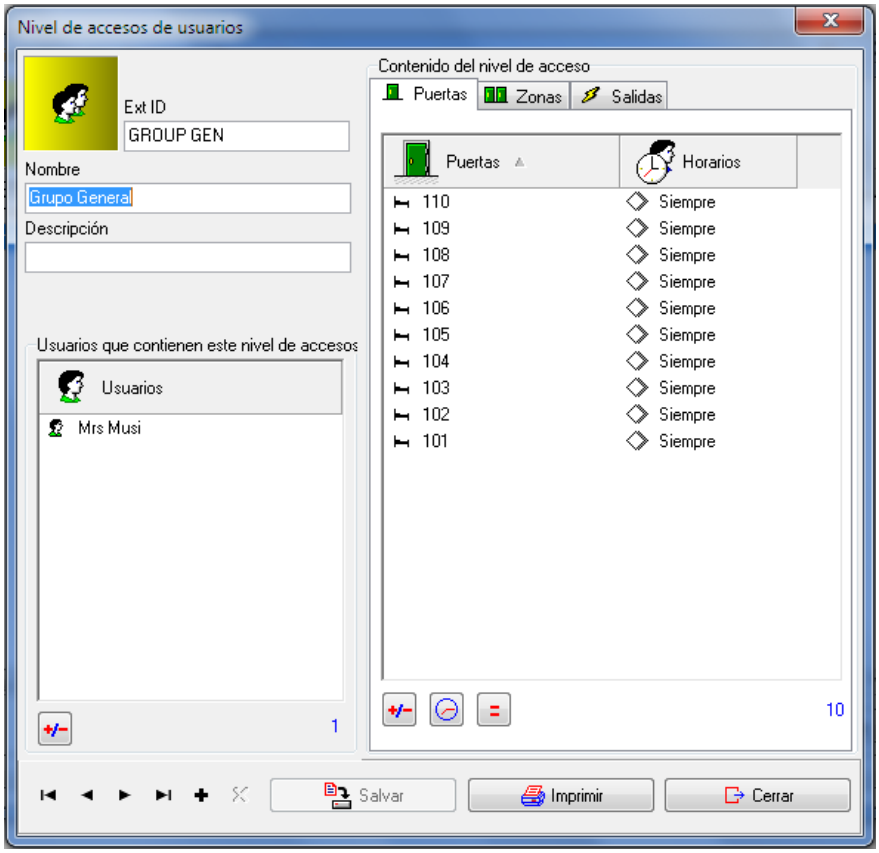


Figura 47

- Cuando haya concretado todas las características del nivel de acceso de usuarios, guarde los cambios y puede pasar a definir el siguiente nivel pulsando el botón +.

- En el ejemplo de la figura 48, se ha establecido un horario para el personal de limpieza. Al asignar las zonas en las que puede entrar el nivel de acceso, podemos también asignarles el horario utilizando el botón que tiene el símbolo de un reloj haciendo sobre clic sobre él.

- Si no se asigna ningún horario para el acceso de un nivel de acceso a una zona, o puerta, el sistema establece por defecto que dicho nivel de acceso tiene un acceso de 24 horas.

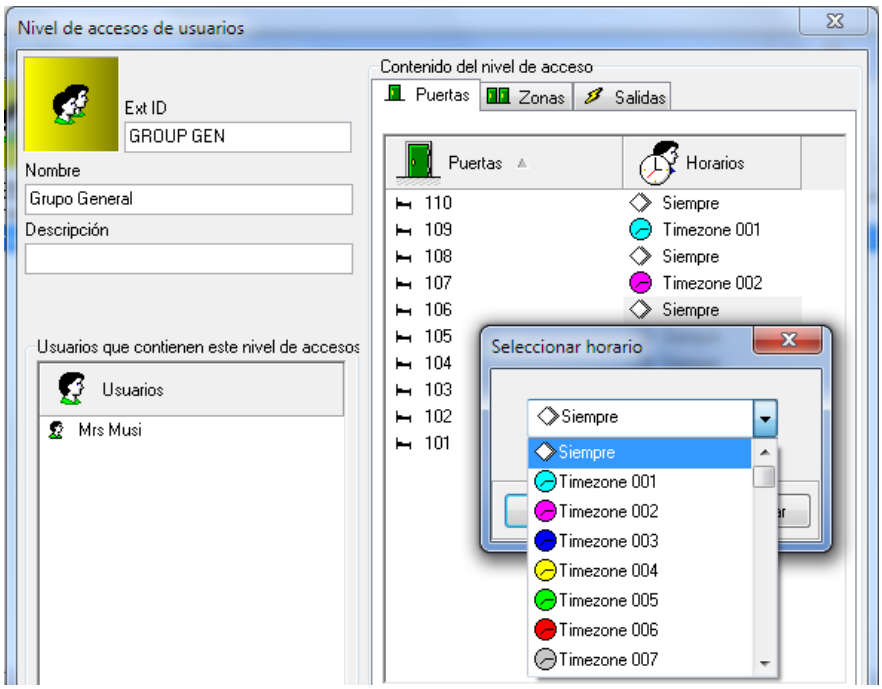


Figura 48

- Al final, tendrá una lista de niveles de acceso de usuarios como la siguiente:

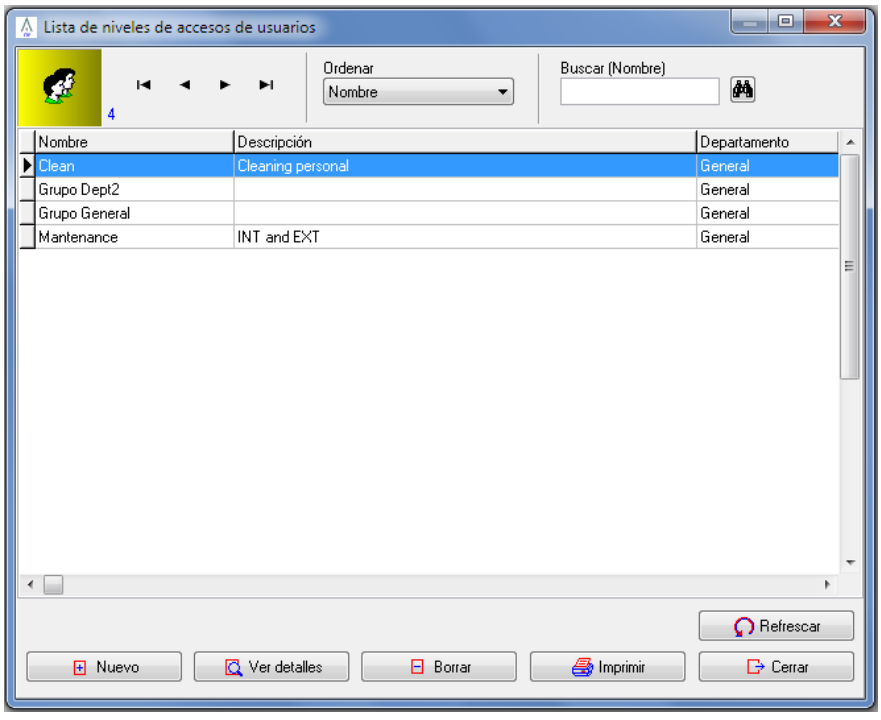


Figura 49

- Si hemos creado un nivel de acceso por error y lo queremos eliminar, lo seleccionamos y pulsamos el botón BORRAR.

- Si en un momento dado, queremos ver los detalles de un nivel de acceso de la lista, bastará con seleccionar dicho nivel y pulsar el botón VER DETALLES.

- Otra manera de seleccionar un nivel de acceso de la lista es utilizando las flechas |< < > >| que aparecen en la parte superior izquierda de la ventana, en vez del ratón.

- La caja que aparece en la parte superior titulada ORDENAR POR sirve para ordenar alfabéticamente la lista de niveles de acceso de usuarios, por nombre o por descripción.

- El botón IMPRIMIR puede utilizarse para obtener un informe en papel de la lista de niveles de acceso de usuarios. Se puede escoger entre imprimir toda la lista o sólo los detalles relativos a un nivel de acceso de usuarios en particular.

ta de Usuarios

En este apartado vamos a definir las características de los usuarios de nuestra instalación. Se definen como usuarios los miembros de la plantilla del hotel pero no se consideran usuarios a los clientes ya que estos son cambiantes.

Pulsamos con el ratón el icono USUARIOS de la barra de herramientas.

Se abrirá una ventana como la siguiente:

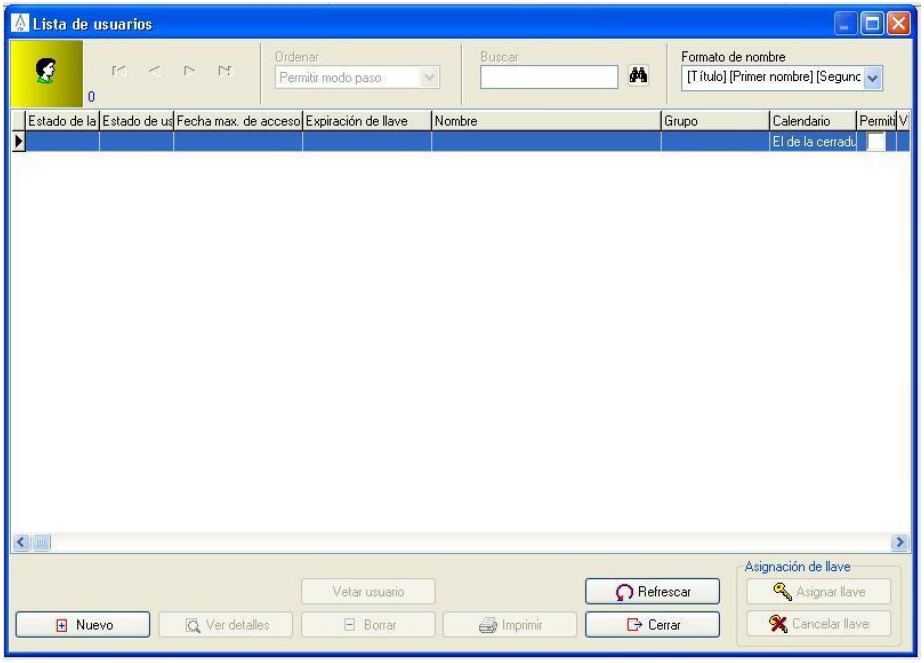


Figura 47

- Como es la primera vez que abrimos la lista de usuarios, la lista está vacía.
- Pulse el botón llamado NUEVO para crear el primer usuario.
- Se abrirá una ventana como la siguiente:

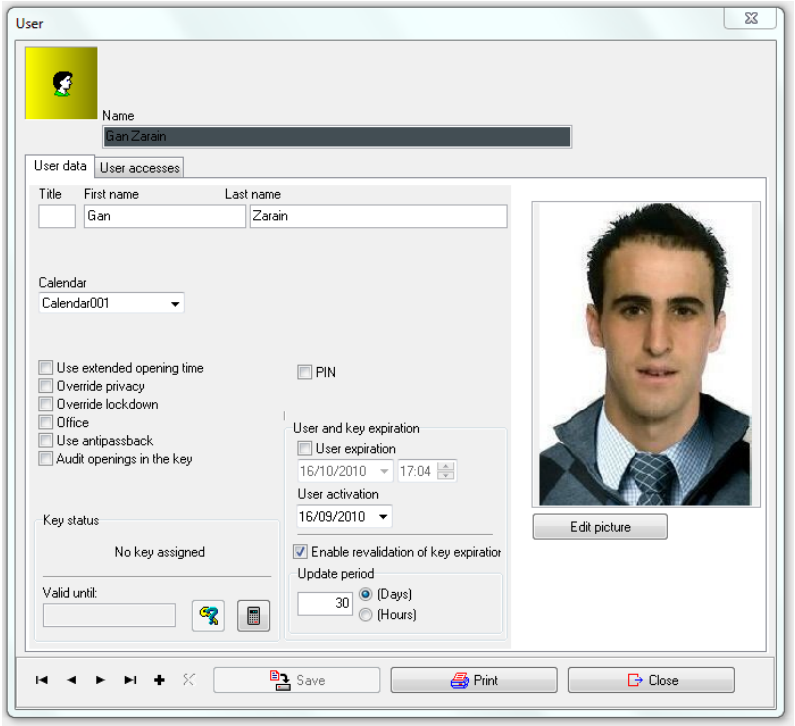
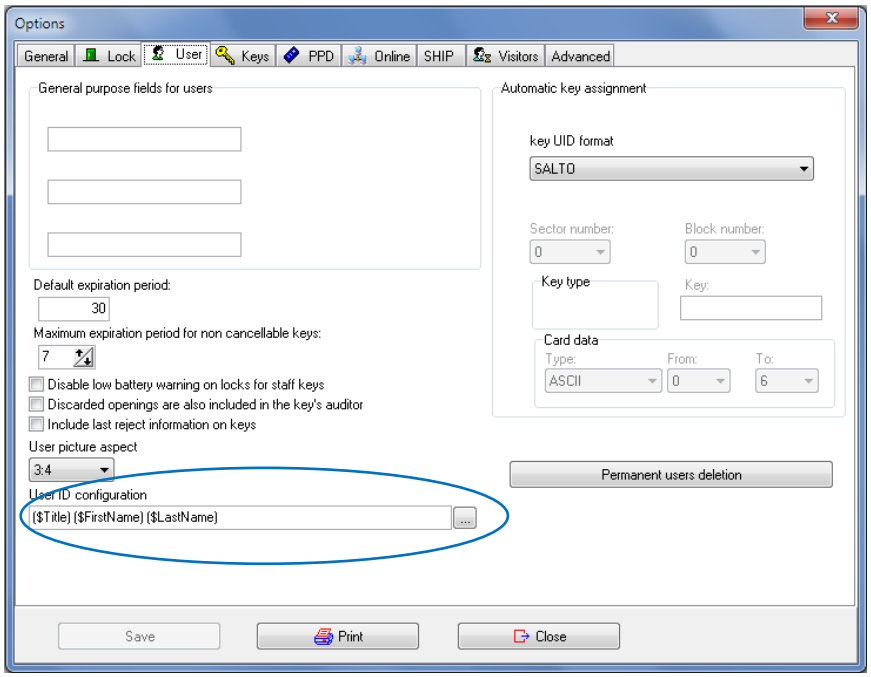
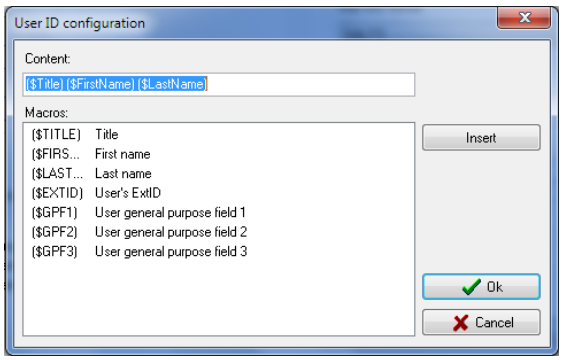


Figura 48

- En primer lugar, escribimos el nombre y apellido de nuestro primer usuario.
  En el caso en que más de una persona tenga el mismo nombre en la misma instalación o base de datos, será necesario definir la composición del identificador de cada usuario. Para hacerlo, vaya a Herramientas/ Configuración/ Opciones generales y la pestaña Usuarios, verá la imagen siguiente.





Como se muestra en la imagen de arriba, el ID de usuario se puede componer con la información de varios campos como;
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.

- Este parámetro INHIBIT_USER_NAME_CHANGE=1 elimina la posibilidad de que un operador pueda cambiar el nombre de un usuario una vez que su llave haya sido grabada. Esto evita que se puedan generar registros falsos en el auditor de cerraduras. Si por alguna razón es necesario un cambio de nombre, se deberá crear un nuevo usuario y volver a grabar otra llave. De esta manera se mantendrá la integridad del auditor de cerraduras.
  Para activarlo, es necesario ir a la pestaña "Avanzado" de las opciones generales.

- Podemos asignar un calendario a nuestro primer usuario, según los calendarios que hemos definido anteriormente.

- Hay que especificar a qué nivel de acceso de usuarios pertenece esta persona. Como antes hemos creado los niveles de accesos de usuarios, ahora tenemos que seleccionar a cuál de ellos pertenece.

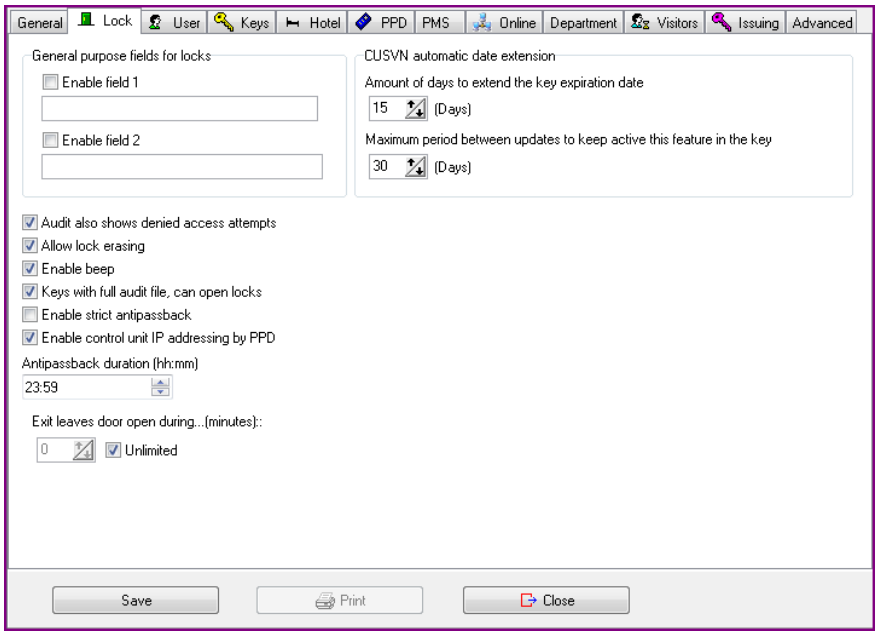
- Vemos una "casilla" titulada UTILIZAR TIEMPO AMPLIADO DE APERTURA. Marcaremos este "casilla" si nuestro usuario es minusválido.

- La "casilla" titulada VENCER PRIVACIDAD sólo debe marcarse para un usuario que tenga el privilegio de entrar en una

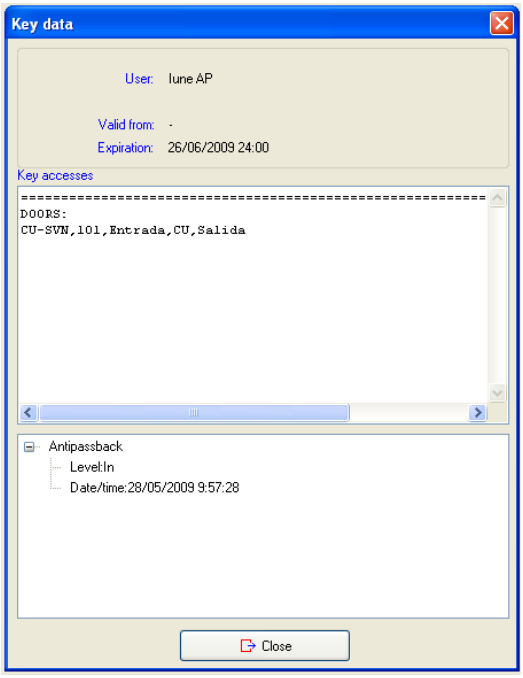
habitación de cliente, a pesar de que éste haya cerrado la palanca de privacidad desde dentro.

- La "casilla" titulada PONER EN PASO puede marcarse para aquellos usuarios que deban poner en paso manualmente las puertas que vayan a trabajar en este modo.

- La "Casilla de selección" titulada USAR ANTI PASS BACK podemos seleccionar si el usuario tendrá el modo anti pass back activado o no. El modo anti pass back, no permitirá al usuario volver a entrar por una puerta si no se ha pasado por la puerta de salida antes. Tanto la puerta de entrada y de salida tienen que estar relacionadas y configuradas como "entrada" y "salida".
  Por defecto, una persona SIEMPRE puede salir.
  Para más detalles sobre el funcionamiento del anti pass back, diríjase a la página 34 de este mismo manual.



Al hacer una lectura de la tarjeta y pulsando sobre el botón de contenido ("Content>>") tendremos acceso a la siguiente pantalla.



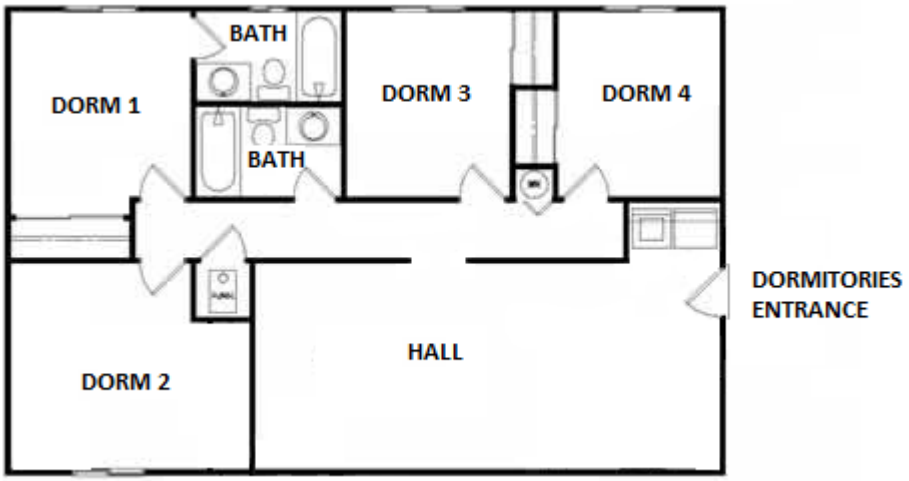
Si la opción de Anti pass back está siendo utilizada se mostrará la información presente en la tarjeta (acceso de entrada en este caso) con la fecha y hora en la que se ha pasado por el primer acceso.

- En la esquina inferior izquierda, se ve la caja titulada ESTADO DE LA LLAVE. En esta caja aparecerán las características de la tarjeta asignada a este usuario, cuando se realice la asignación de tarjetas a los usuarios.

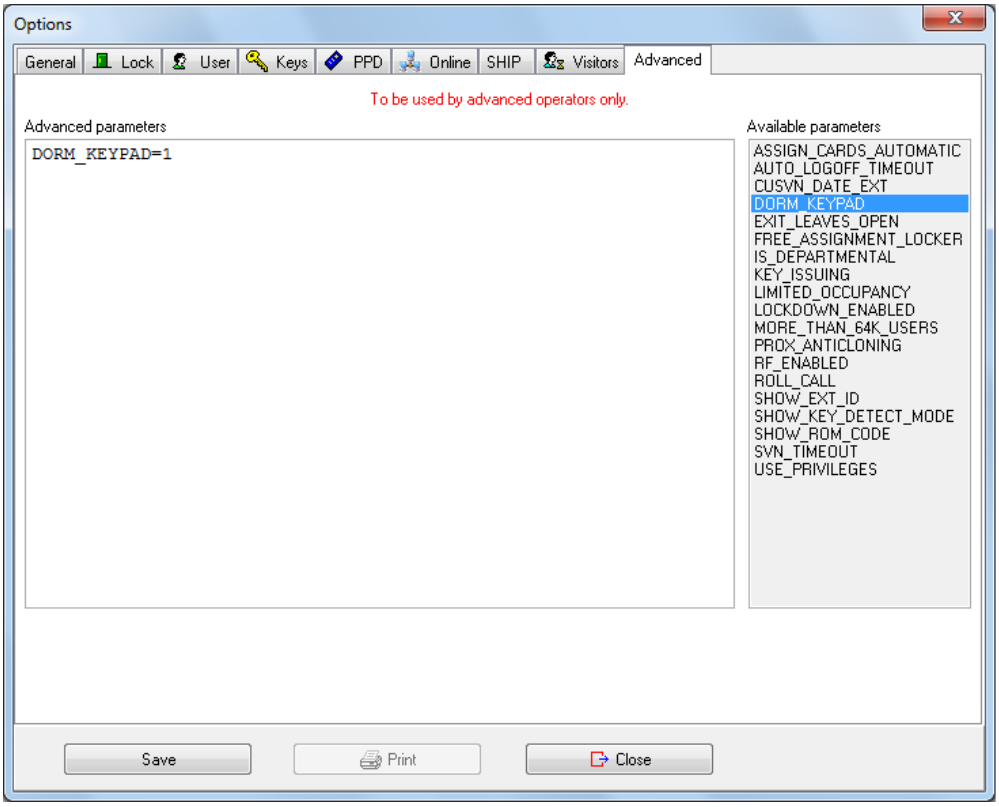
Actualización de clave de teclado a través de SVN

A las puertas que estén funcionando en modo Solo Teclado, se les puede cambiar el código automáticamente cuando un usuario con acceso a esa puerta presente su tarjeta.

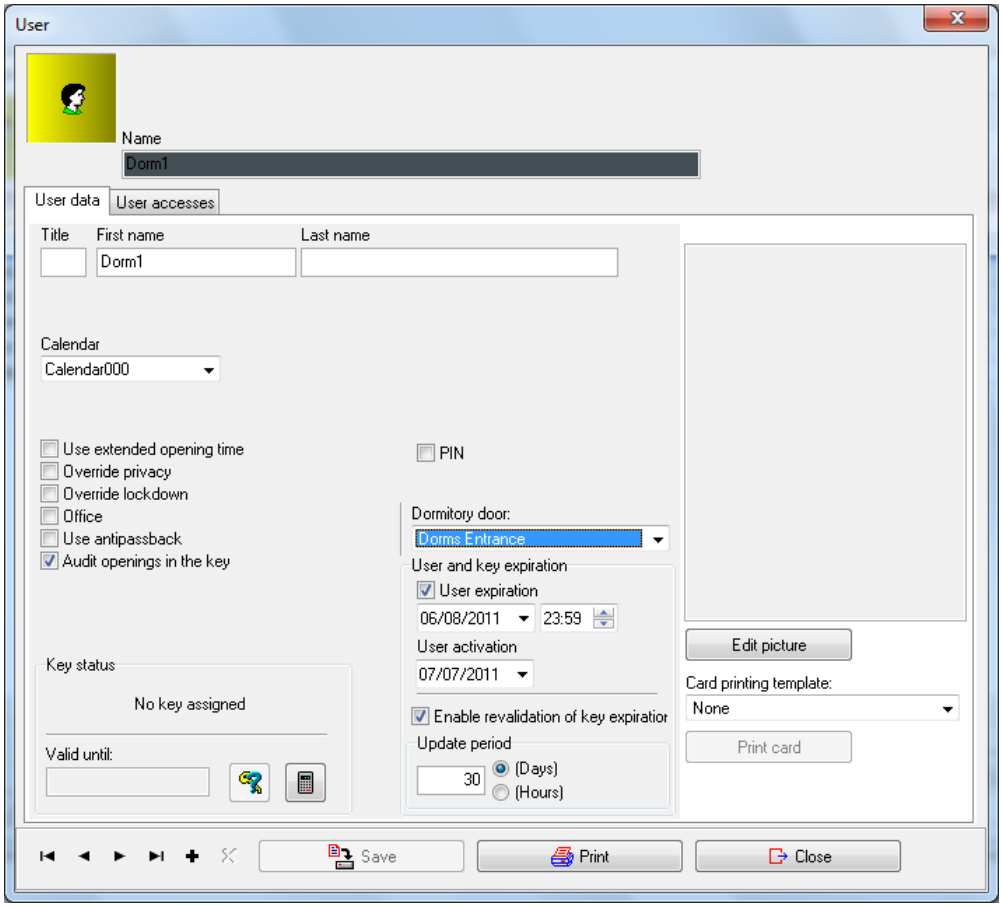
Esta opción es muy útil en puertas que dan acceso a Dormitorios, donde una gran rotación de usuarios requiere el cambio del código cada cierto tiempo, y así evitar problemas de seguridad.



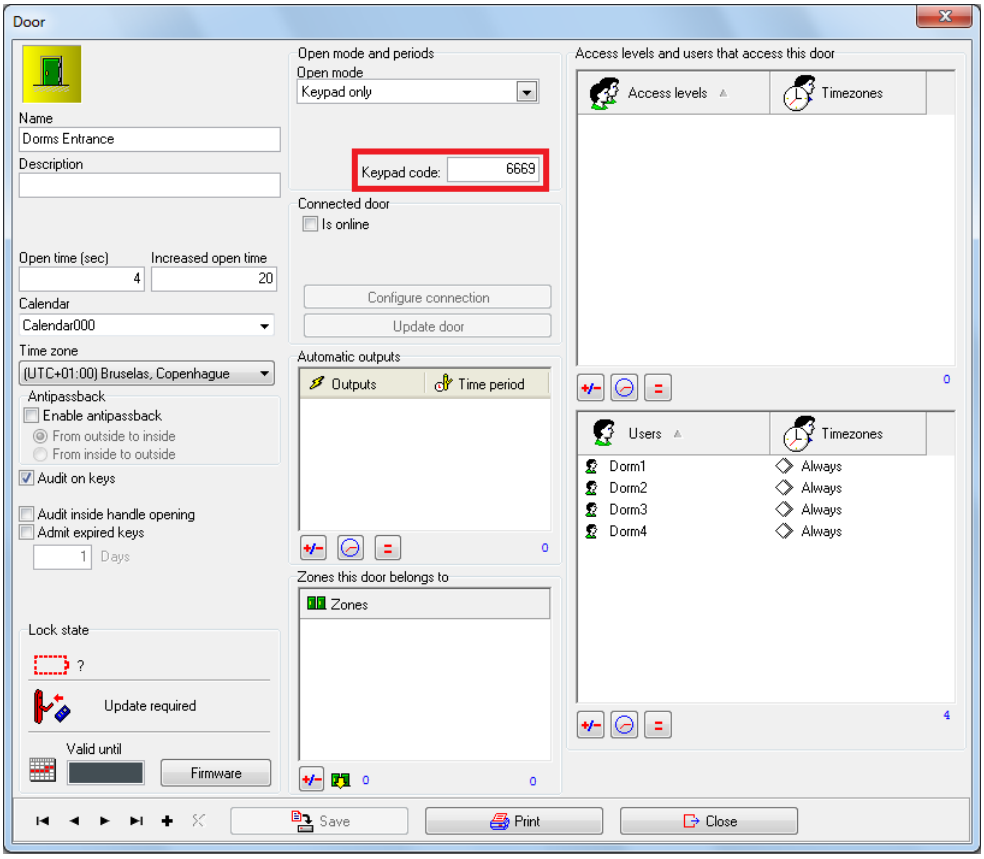
Para tener ésta opción disponible, deberá activarse el parámetro DORM_KEYPAD=1 en el menú de Opciones Generales, en la pestaña Avanzado.



Este parámetro activará la opción "Puerta de Dormitorio" en la ventana de configuración de los usuarios. Cuando una de las puertas de dormitorio es seleccionada en esta opción, el usuario (o usuarios) podrá(n) ser capaces de cambiar el código en dicha puerta.



El código de a puerta deberá cambiarse en su ventara de configuración, simplemente cambiando el código original en la opción Código de Teclado.



Una vez se haya cambiado el código, se les escribirá el nuevo código en la tarjeta a los usuarios con esa puerta seleccionada en la opción Puerta de Dormitorio, cuando presenten su tarjeta en un punto SVN. En cuanto presenten la tarjeta en la puerta, el código de la puerta será cambiado y el anterior código quedará invalidado.

- No es necesario definir los accesos de un usuario, si este usuario pertenece a un nivel de acceso, puesto que la definición de los accesos de los grupos se hizo anteriormente.

- Sólo si el usuario no está englobado en ningún nivel de acceso, entonces se pueden asignar sus accesos en este momento.

- El horario de acceso de un usuario a distintas zonas no tiene por qué ser el mismo.

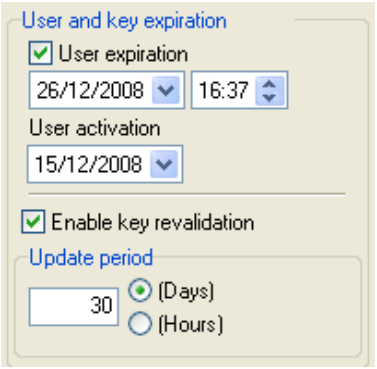
- El hecho de asignar una zona a un usuario, implica darle acceso a todas las puertas incluidas en esa zona.

- Si tenemos algún usuario que no pertenece a ningún nivel de acceso, podemos asignarle sus accesos en esta misma ventana,

siguiendo el mismo procedimiento explicado en el apartado NIVEL DE ACCESOS DE USUARIOS en este manual.

- La caducidad del usuario y su tarjeta se gestionan desde las siguientes opciones

    - **Caducidad usuario** refleja la caducidad máxima del usuario.
    - **Activación usuario** refleja la fecha a partir de la cual la tarjeta será funcional
    - **Habilitar revalidación tarjeta** permite fijar el intervalo de la próxima caducidad de la tarjeta (en días u horas)

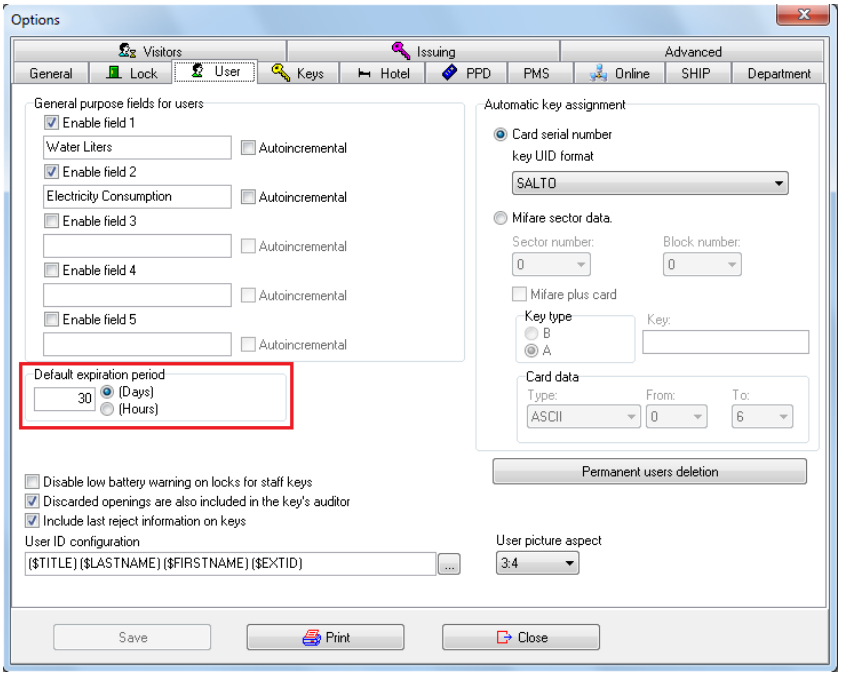


EXPIRACION POR DEFECTO EN HORAS Y DIAS.

El periodo de expiración de usuarios se puede programar en horas y días.

En caso de seleccionar DIAS, tenga en cuenta que el último día de la fecha de expiración tendrá que pasar para que la llave expire. Por ejemplo; si se graba una llave un lunes a las 08:00 y el periodo de expiración por defecto esté programado para 2 días, la llave expirará el miércoles a las 24:00

En caso de seleccionar HORAS, la expiración será precisa, es decir, si se graba una llave a las 16:06 y por defecto el periodo de expiración es de 4 horas, la llave expirará a las 20:06.



- Cuando hayamos terminado de definir las características de la ventana de usuario, se deben guardar los cambios y podemos pulsar el botón + para pasar a definir el siguiente usuario de la lista.

- Cuando hayamos definido todos los usuarios de la instalación, podemos tener una lista como la que se ve a continuación:

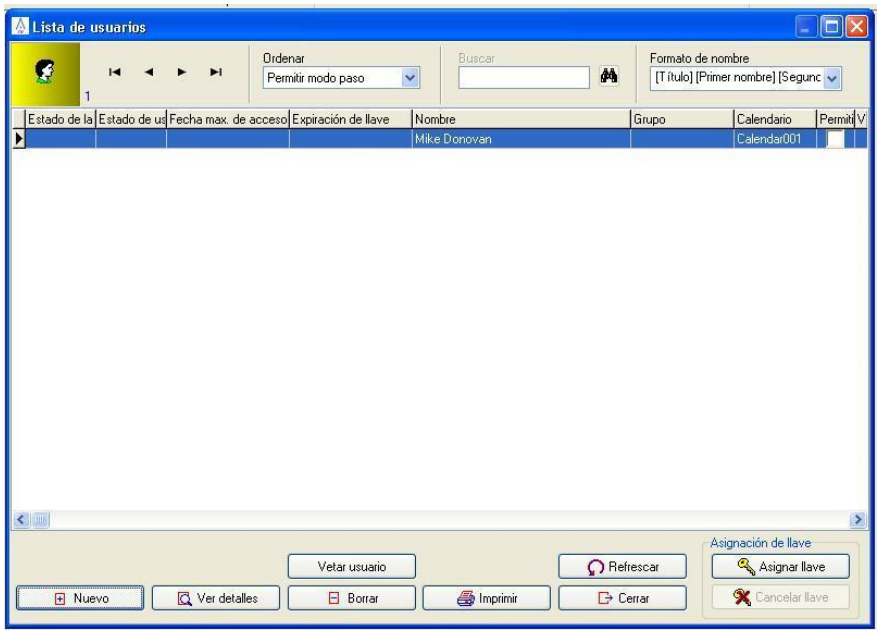


Figura 51

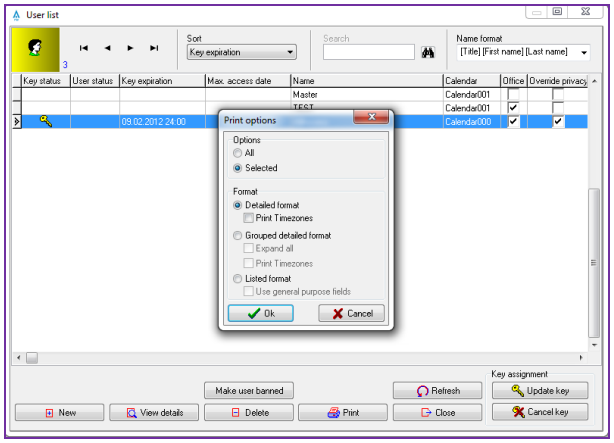
- Si por error hemos introducido un usuario que no debería existir, podemos borrarlo seleccionándolo y pulsando el botón BORRAR.

- Para visualizar la ventana de detalles de un usuario cualquiera, lo seleccionamos y pulsamos el botón VER DETALLES.

- También podemos utilizar las flechas de la esquina superior izquierda para seleccionar un usuario de la lista, en vez de hacerlo con el ratón. <>, con estas flechas pasamos al usuario inmediatamente superior o inferior, o bien al primero o último de la lista directamente |< >|.

- La caja titulada ORDENAR POR sirve para ordenar la lista de usuarios según el criterio que más nos interese, por nombre, por apellido, por calendario, por nivel de acceso, etc...

- El botón IMPRIMIR se utiliza para imprimir un informe en papel de la lista de usuarios. Se puede escoger entre imprimir toda la lista o sólo los detalles de un usuario en particular.



Por defecto están seleccionados, "Seleccionados" y "Formato detallado". Si se desea añadir otros formatos o añadir más detalles, se puede seleccionar según lo propuesto en ventana. Una vez seleccionados los detalles del informe, presionar OK. En la parte de abajo a la derecha podrá fechar y firmar el documento tras haberlo imprimido.

Date: _____

Signature: _____

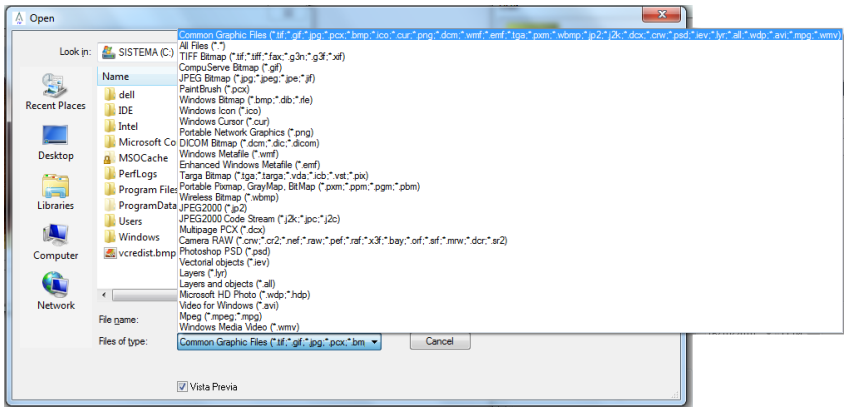
AllAccess

DB: SPICKERT-PC\SALTOSQL\BETA_Version174
10.01.2012 10:48:24 Page 1

- La opción Vetar usuario permite bloquear usuarios. De tal forma que ningún cambio ni modificación puede hacerse en el mismo. En los operadores y permisos se puede configurar que operador tendrá la posibilidad de vetar usuarios. Una vez que un usuario ha sido vetado en cuanto presente su llave a una CU50ENSVN su tarjeta quedará borrada, es decir la llave retendrá el nombre del usuario pero la información relativa al plan de acceso quedará borrada. Si al mismo usuario se le retira el veto en cuanto presenta la llave a la CU50ENSVN la tarjeta recupera el plan de acceso que tiene en ese momento.

- Imagen. Se puede insertar una imagen para identificar al usuario. La foto puede importarse desde cualquier medio de almacenamiento (disco duro, pendrive USB, tarjeta de memoria, ...) o directamente desde una cámara web.

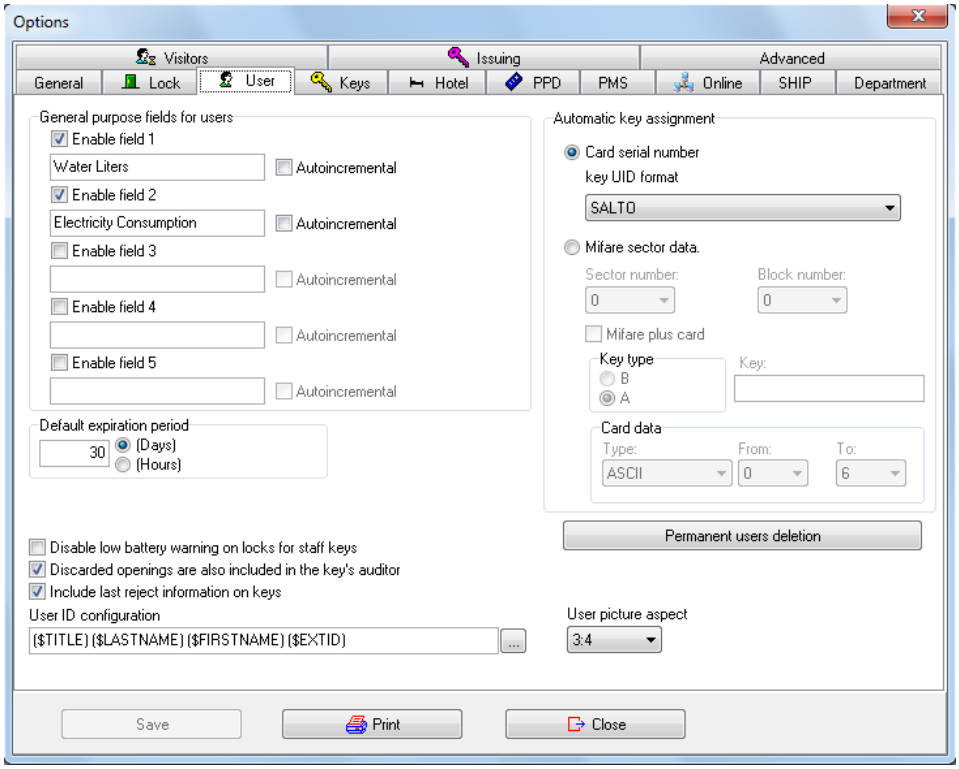
Varios tipos de archivos son compatibles (jpeg, bmp, tif, gif,…).



Aspecto de la foto del usuario

El aspecto de la imagen puede predefinirse desde el menú de Opciones Generales, pestaña Usuario. Las opciones posibles son:

3:4
2:3
1:1



Asignación de llaves a los usuarios

Una vez elaborada la lista de usuarios, podemos dar a cada usuario su llave, que en realidad es una tarjeta chip (Smart Card). Para ello, es necesario conectar el EDITOR al puerto serie de su ordenador. También es necesario alimentar el EDITOR enchufando el alimentador suministrado a una toma de corriente alterna 220-230 V. AC, 50 Hz. E insertando la clavija correspondiente en el cuerpo del EDITOR.

Siga los pasos explicados a continuación para asignar las llaves de usuario:

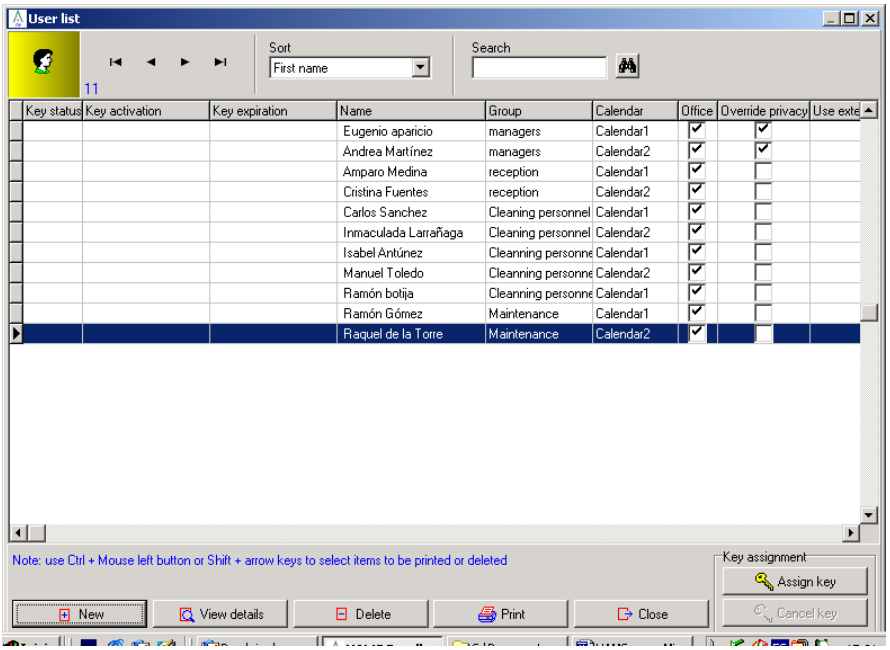


Figura 52

- Desde la lista de usuarios, seleccione un usuario con el ratón. A continuación pulse el botón ASIGNAR LLAVE que se puede ver en la esquina inferior derecha de la ventana.

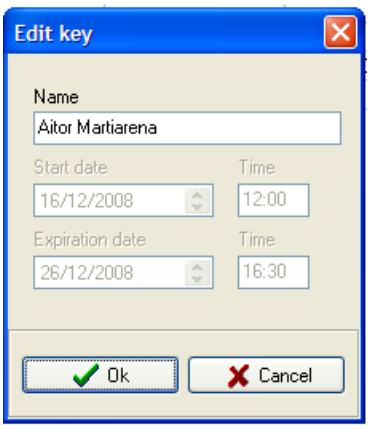


Figura 53

- El sistema le pedirá que introduzca una tarjeta en el EDITOR.

- La codificación es muy rápida. En seguida, el sistema le pedirá que retire la tarjeta.

- Ahora, en la lista de usuarios se puede ver cómo el icono de llave (en amarillo) aparece junto al nombre del usuario que ya la tiene asignada.

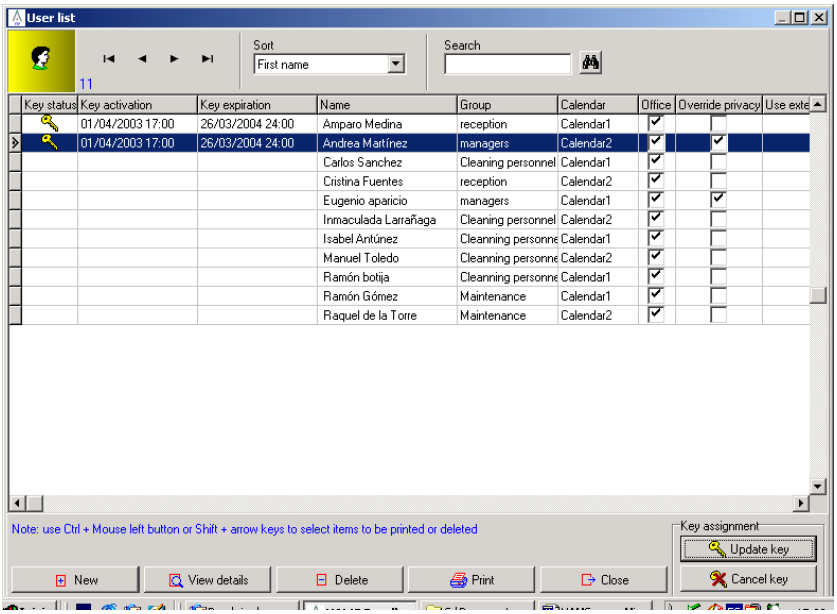


Figura 55

- Se recomienda entregar las tarjetas a sus usuarios correspondientes, inmediatamente.

- Para asignar llaves a otros usuarios, siga el mismo procedimiento.

- Al final, tendrá una lista de usuarios con sus llaves asignadas, como en la figura siguiente:

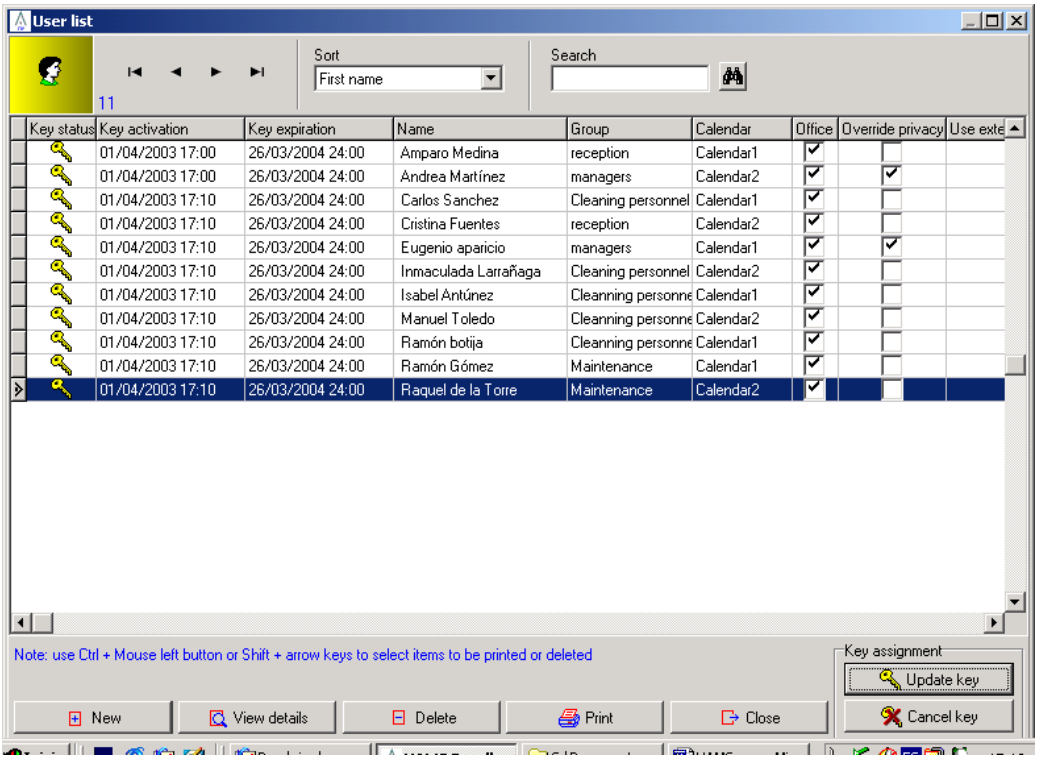


Figura 56

- Si se pierde una tarjeta de usuario, lo primero que hay que hacer es cancelarla en la lista de usuarios. Para ello, marcamos en azul el usuario que ha perdido su tarjeta, y pulsamos el botón CANCELAR LLAVE.

- A continuación, hay que editar una tarjeta nueva para este usuario, con el mismo procedimiento explicado anteriormente. El usuario utilizará la nueva tarjeta a partir de ahora, y si por cualquier razón aparece la tarjeta perdida, ésta ya no abrirá ninguna de las puertas donde antes operaba. (se sobreentiende que todo este proceso funciona realmente así, una vez que los escudos electrónicos han sido inicializados con el programador portátil).

- Si realizamos cualquier cambio en los accesos de un usuario, será necesario actualizar su llave. Para ello, es necesario pedir al usuario que nos de su llave para actualizarla en el EDITOR.

- El color del icono que representa la llave es indicativo del estado de la misma. Así, una llave de color rojo, significa que tiene cambios pendientes por actualizar, una llave de color azul, significa

que se aproxima su fecha de caducidad y una llave de color amarillo con un relojito, significa que ya está caducada.

Taquillas:

SALTO incluye en su software la opción de gestionar también las taquillas. La configuración y uso de éstos es muy intuitiva y similar a la de nuestros escudos y permite además obtener los mismos datos que podemos obtener de nuestros escudos (Aperturas, rechazos, etc.)

Crear taquillas:

Primeramente debemos dar de alta las taquillas. Para ello vamos al menú desplegable: Datos/Taquillas. Aparecerá la siguiente ventana: (Fig. 1). En esta ventana se mostrará la lista de taquillas, el estado (abierta / cerrada), nombre, estado de las pilas, Fecha, Modo de apertura y horario.

En la parte inferior hay un check box que permite visualizar sólo aquellas taquillas que se encuentren cerradas. Así mismo hay una opción de colocar el estado de las taquillas como abiertas. Esta opción es muy útil cuando nuestros usuarios han dejado cerrada alguna taquilla la cuál abrimos posteriormente manualmente con una llave maestra.

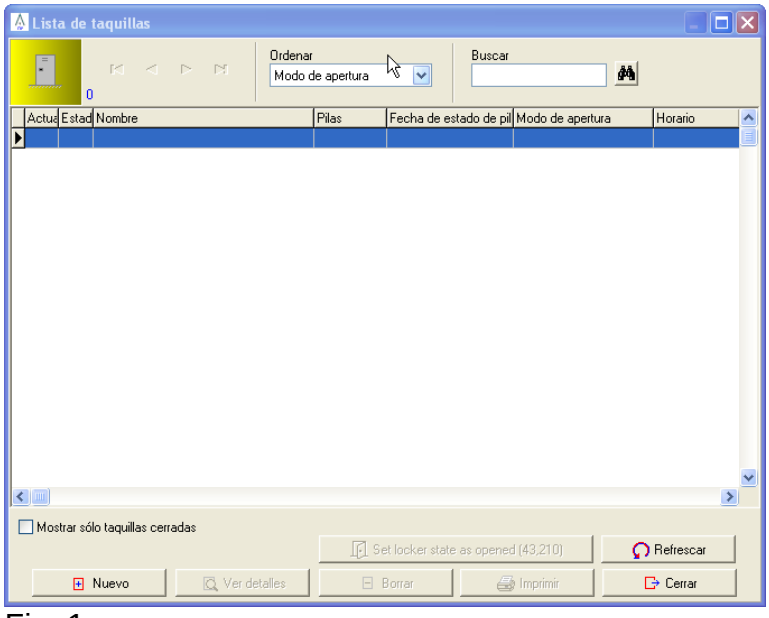


Fig. 1

Pulsamos la opción “Nuevo” y damos de alta a las taquillas. El procedimiento es similar al de crear una puerta nueva puerta: (Fig. 2)

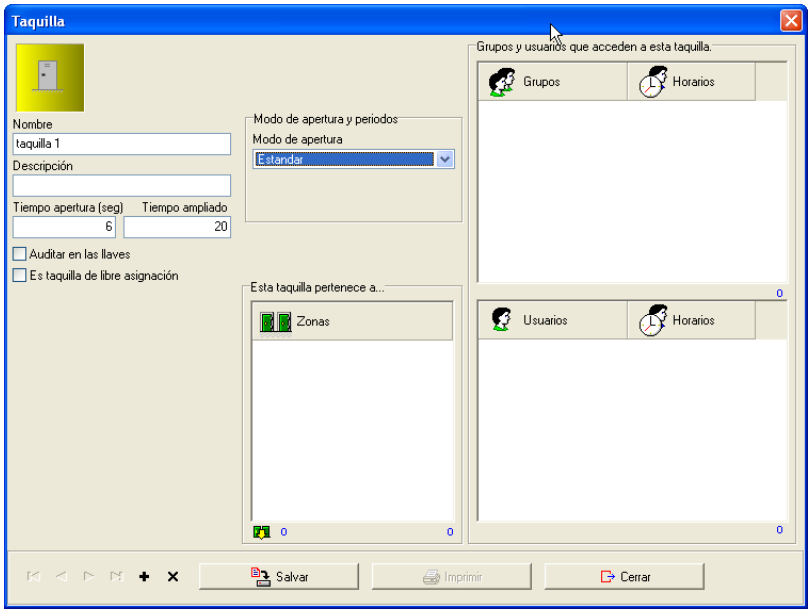


Figura 2

En esta ventana rellenamos los datos teniendo en cuenta que sólo existen dos tipos de modos de apertura para las taquillas: Estándar y Apertura Automática.

Zona de Libre Asignación:

Los accesos a las taquillas pueden asignarse directamente a un usuario (como en los escudos) o también existe la opción de que el usuario elija libremente la taquilla que desea utilizar.

En estos casos debemos colocar todas las taquillas en una zona donde los diferentes usuarios puedan escoger aquella que deseen o este libre y funcionar dependiendo del tipo de llave que hayamos escogido anteriormente. Para ello, debemos crear una “Zona” para estas taquillas, el procedimiento es igual que para crear una zona de puertas.

Crear una Zona de Libre Asignación:

Para habilitar esta opción debemos ir al menú desplegable: Herramientas/ Configuración/ Opciones Generales/ Avanzado y habilitar la opción “Free Assignment Locker”

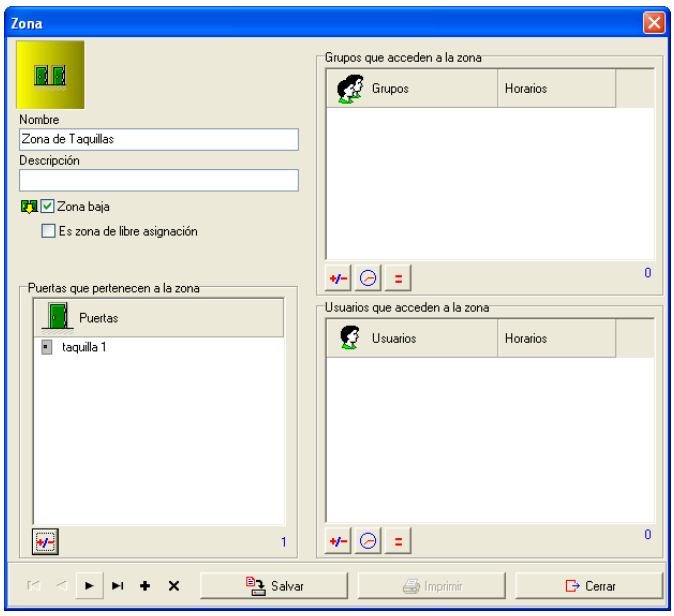


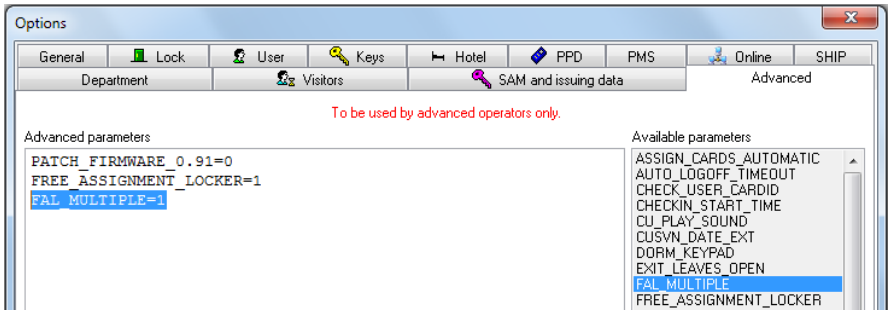
Fig. 4

En este caso debemos marcar el checkbox “Es zona de libre asignación”. **Es importante que previamente hayamos definido las taquillas como taquillas de libre asignación de lo contrario el software mostrará un mensaje de error.**

Múltiples Zonas de libre asignación:

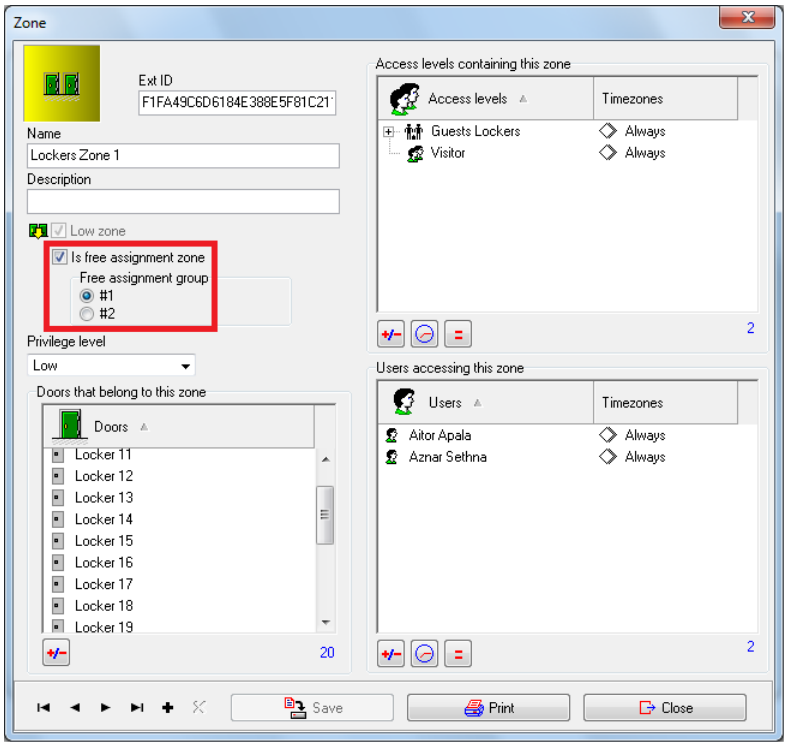
El parámetro avanzado FAL_MULTIPLE permite crear dos zonas adicionales de taquillas, para que un usuario del sistema sea capaz de capturar más de una taquilla con una misma tarjeta, siempre y cuando, esas dos taquillas pertenezcan a una zona diferente de libre asignación.

Para activar dicha función, debe añadirse el parámetro avanzado FAL_MULTIPLE=1 a la lista de parámetros avanzados activados en el software, tal y como se ve a continuación:



Una vez dicha función ha sido activada, aparecerán las siguientes opciones en la ventana de configuración de las zonas:

- Grupo de libre asignación #1.
- Grupo de libre asignación #2.



Dichas opciones estarán activas solo cuando se defina la zona como de libre asignación.

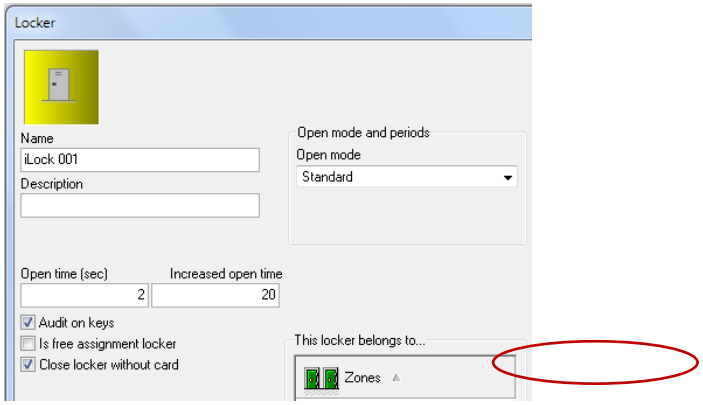
Esto hará que las taquillas de una instalación puedan ser incluidas en uno de los dos grupos de libre asignación. Esta identificación de grupo de la taquilla será escrita en la tarjeta cuando ésta ocupe una taquilla de uno de los dos grupos de libre asignación, imposibilitando la ocupación de otra taquilla en el mismo grupo de libre asignación, pero posibilitando la captura de otra taquilla en el otro grupo de libre asignación.

NOTA IMPORTANTE: Una misma taquilla no debe meterse en ambas zonas de libre asignación.

Cierre libre:

La opción de libre cierre le permite al usuario o a un grupo de usuarios, cerrar una taquilla sin necesidad de usar la llave. Solo sería necesaria la llave para abrir tal taquilla. El botón de la taquilla se queda libre de cierre mientras la taquilla está abierta. Para trabajar de esta manera la llave tiene que configurarse en modo llave “Estática”. Por ejemplo, esta configuración podría

ser útil para el uso común de taquillas de farmacia o en tiendas donde se guardan componentes concretos y donde varios usuarios deben tener acceso.



Tipos de Llaves:

En el menú desplegable Herramientas / Configuración / Opciones Generales/ Llaves. Aparecen las distintas opciones para las llaves que podemos definir. (Fig. 3):

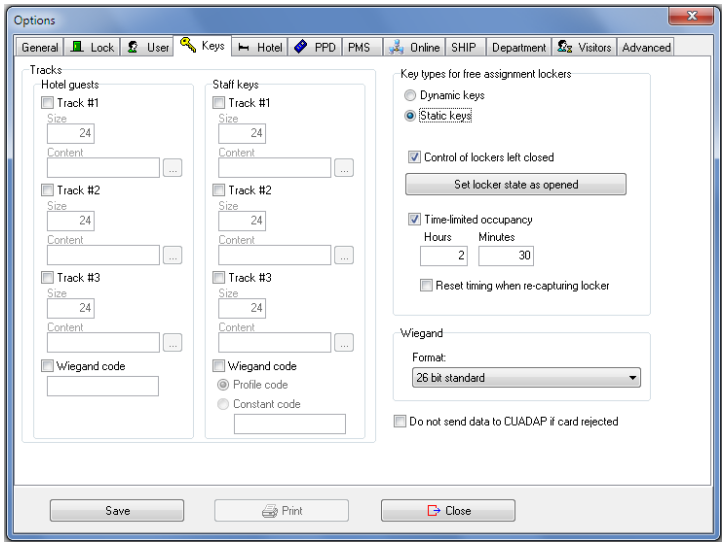


Fig. 3

- **Llaves Dinámicas:** Si seleccionamos este tipo de llave nos permite capturar cualquier taquilla de una zona de libre asignación utilizarla y una vez liberada poder coger cualquier otra taquilla de la zona.

- **Llaves Estáticas:** En este caso podemos escoger cualquier taquilla de la zona de libre asignación. No obstante, una vez liberada no podremos escoger cualquier otra taquilla de la zona de libre asignación* sino esa misma.

Cambiar estado de taquilla a abierta cuya función es la misma que la que aparece en la "Lista de Taquillas" checkbox "Control de taquillas cerradas"*

Ocupación de taquilla limitada:

Esta opción limita el tiempo de captura de la taquilla. Se debe definir este tiempo en Horas y Minutos rellenando las casillas.

Nota: Si el tiempo de ocupación expira sólo una llave maestra podrá abrir la taquilla.

Reiniciar la temporización al volver a capturar:

Esta opción permite capturar otra taquilla y reiniciar el tiempo de uso si se ha sobrepasado el tiempo de uso de la primera.

* "Control de taquillas cerradas: Ver apartado Taquillas & Visitas.

Taquillas & Visitas:

En el menú desplegable Herramientas / Configuración / Opciones Generales y en la pestaña de Llaves hay un checkbox "Control de las taquillas cerradas". Esta opción nos permite comprobar en el momento de efectuar un Check out de Visitas si el visitante se ha dejado la taquilla cerrada impidiendo de esta forma su uso para un nuevo visitante.

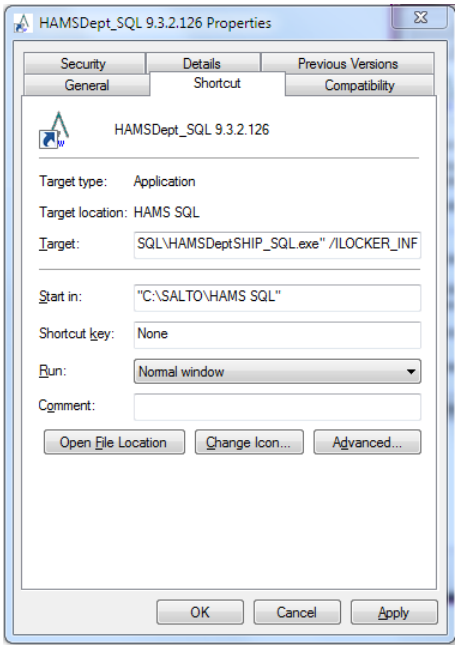
Inicialización de Taquillas:

La inicialización se realiza siguiendo el mismo procedimiento que para la inicialización de un escudo. Se selecciona las taquillas a inicializar y se cargan al PPD. Una vez inicializadas se vuelve a descargar la información a la base de datos.

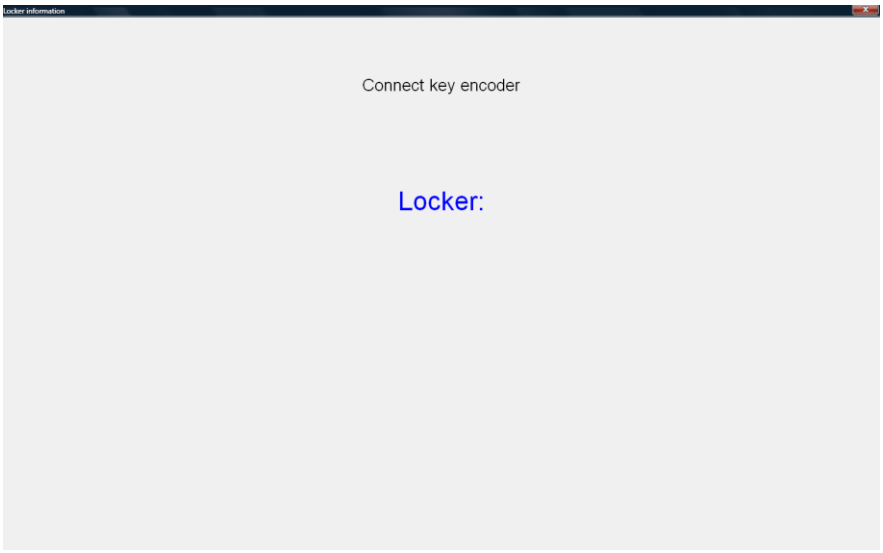
Información del número de la Taquilla capturada:

Existe la opción de obtener información sobre el número de la taquilla que ha sido capturado con una llave.

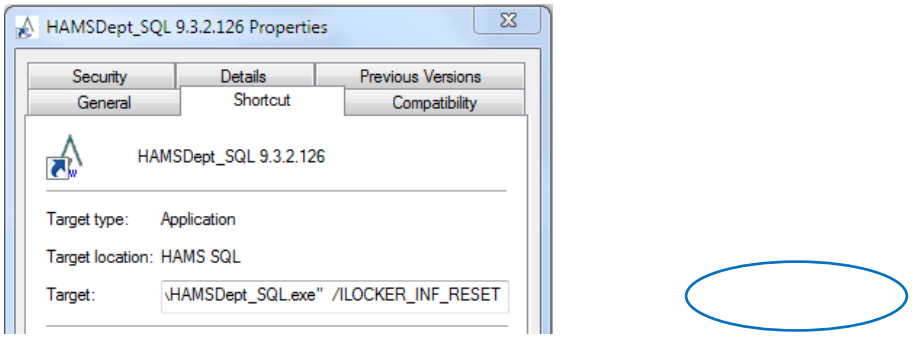
Para esto es necesario dedicar un PC y una pantalla además de un editor de tarjetas Salto. En las propiedades del acceso directo de la aplicación Salto, se debe escribir "…exe" **/ILOCKER_INF** al final de la línea.



Saldrá una ventana como se ve a continuación que solamente indicará el número de la taquilla capturada al presentar la llave ante el editor conectado.



Por otra parte, también es posible además de visualizar el nombre de la taquilla, aprovechar la operación para resetear el contador de la llave en caso de que esta se haya corrompido o no abra. Para esto en las propiedades del acceso directo de la aplicación Salto, se debe escribir "…exe" **/ILOCKER_INF_RESET** al final de la línea como se ve en la siguiente imagen.



Después del reseteo, podrá volver a abrir su taquilla y también cualquier otra taquilla desocupada.

CUIDADO: En caso de que capture otra taquilla por error, no podrá abrir la taquilla que era suya previamente. Por otra parte, solo podrá leer qué taquilla tiene capturada la primera vez, porque después del reseteo desparecerá de la llave la información relacionada con la taquilla.

Visitas:

El software permite asimismo la gestión de visitas, definimos como visitas aquellas personas no incluidas dentro del sistema y que van a tener unos accesos temporales al sistema por diversas razones. Para activar las visitas debemos primeramente ir al menú desplegable HERRAMIENTAS y pinchamos en CONFIGURACIÓN y luego OPCIONES GENERALES. Pinchamos sobre la ficha de **Visitas.** (Figura 1)

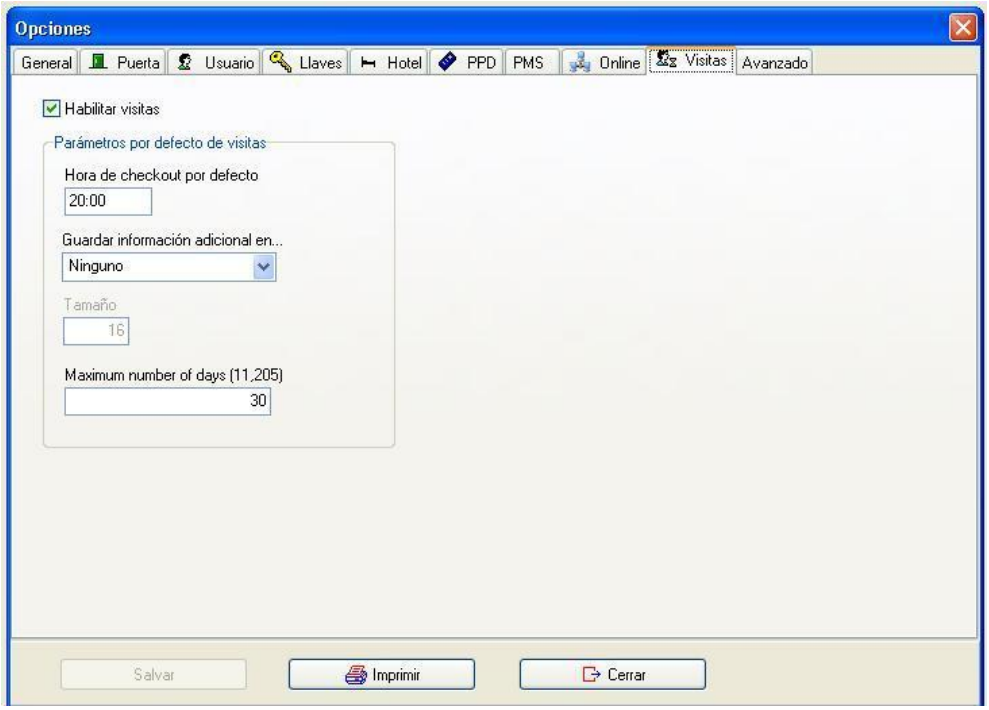


Figura 1

Habilitamos el check box "Habilitar Visitas". La siguiente casilla establece la hora del check out por defecto. Ésta hora puede luego modificarse al hacerse el check in. La segunda casilla indica si se quiere guardar información adicional en cualquiera de las Pistas posibles (Pista1, Pista2, Pista3) y el número de caracteres que se quieren habilitar para cada pista. Finalmente nos encontramos la opción de establecer el máximo número de días por defecto a asignarle a una visita, de tal forma que al hacer el check in de la visita no podremos superar ese número.

Una vez habilitadas las visitas debemos definir los perfiles de visitas. Para ello debemos ir al menú desplegable DATOS y seleccionar el PERFIL DE VISITAS. Nos aparecerá una ventana de "Lista de Grupos de Visita", debemos crear un nuevo grupo. El método es similar al de crear un nivel de acceso de usuarios. Hay que definir los accesos y horarios así como si estos accesos son opcionales. Esto es importante ya que de hacerlos opcionales aparecerán como tales en el Check-in y si no los definimos como opcionales vendrán dados por defecto (Figura 2)

Tener en cuenta por favor, que la cantidad de puertas máxima que puede asignarse a una tarjeta de usuario es de 96, lo cual no limita la cantidad de puertas opcionales que pueden asignarse al grupo de visitas.

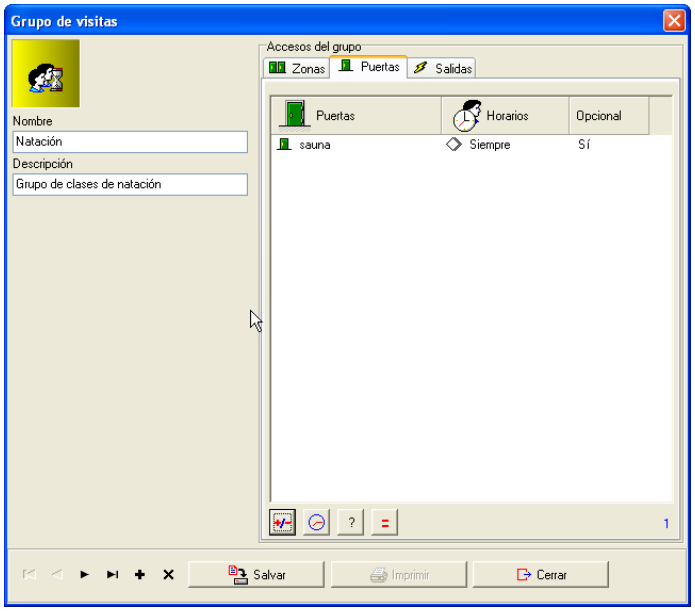


Figura 2

Check in de visitas:

Para hacer un checkin de un visitante hay que ir al menú desplegable LLAVES o pulsar F10. (Figura 3)

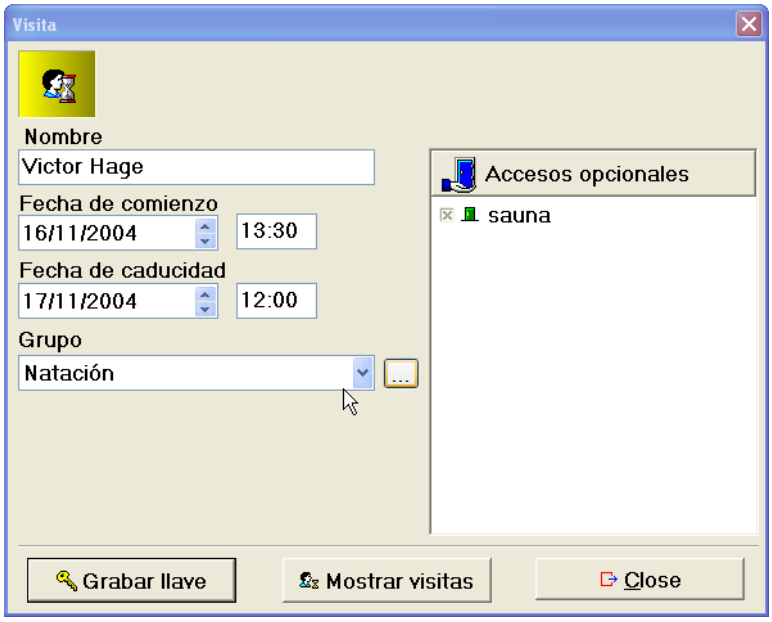


Figura 3

Para hacer el check-in debemos rellenar los siguientes campos:

- Nombre
- Fecha y hora de comienzo
- Fecha y hora de caducidad
- Grupo al que pertenece el visitante
- Marcar si queremos darle algún acceso opcional.
- Finalmente grabaremos la llave.

En esta ventana hay una opción de "Mostrar Visitas" Esto nos permite ver todas las visitas activas que tenemos. (Figura 4)

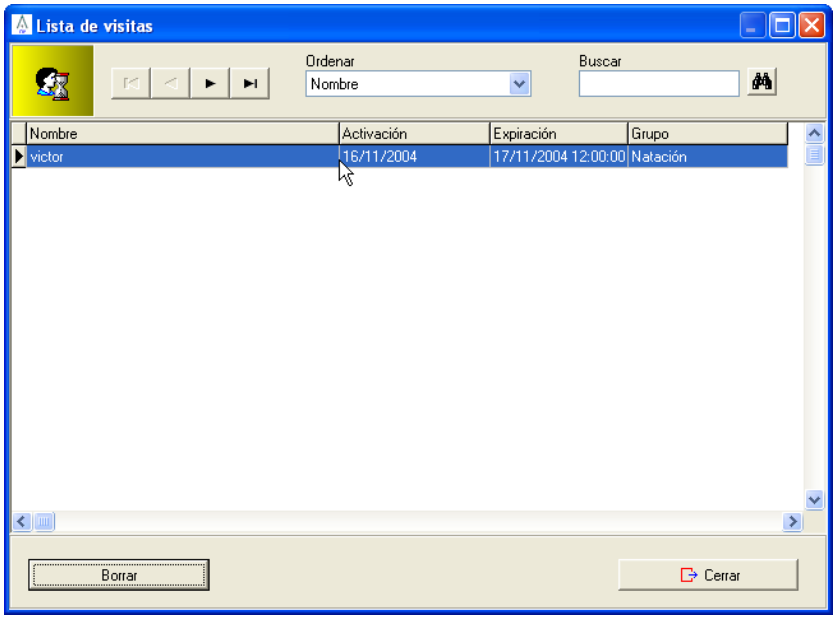
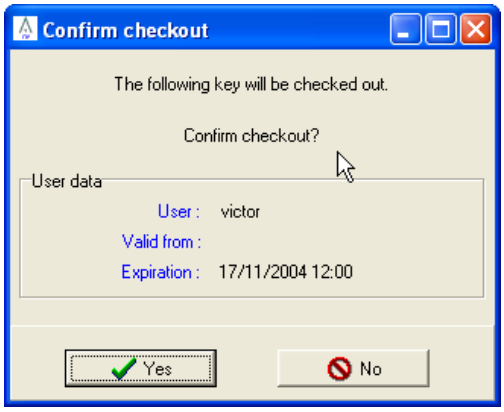


Figura 4

Checkout:

Para hacer el check out es necesario ir al menú desplegable "LLAVES" o pulsar F11 y luego presentar la llave en el editor.



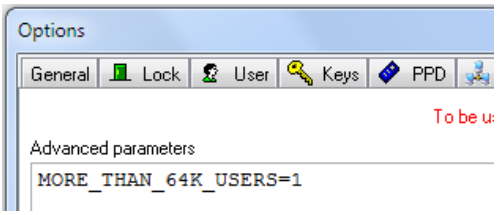
Lista Negra

La lista negra es una lista virtual donde se alojan los códigos de llaves de usuario que han sido canceladas. Una vez una llave es cancelada, el código de esta será enviado a través de la red virtual de Salto llamada SVN. Todos los lectores online SVN, actualizarán las llaves de los usuarios con la información de la lista negra. Estas llaves de usuario a su vez actualizarán la lista negra de todos los escudos en los que sus llaves se presenten, de esta manera la información de la llave cancelada será propagada por todas las llaves que contengan la información de la lista negra.

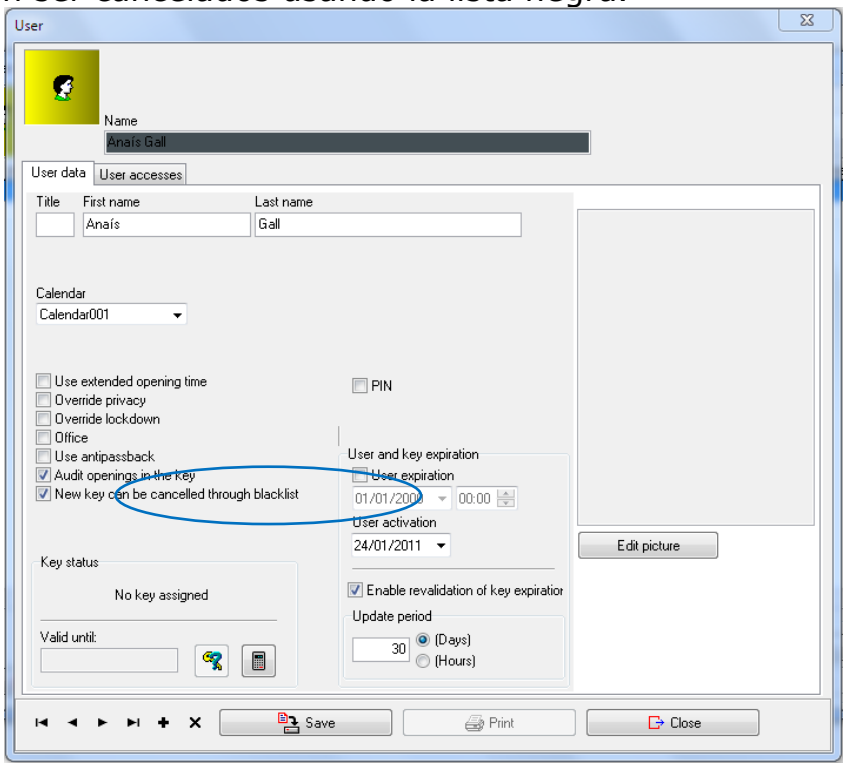
Configuración de Lista Negra

El software permite la creación de una cantidad ilimitada de usuarios, una cantidad máxima de 4 millones de llaves de usuario, pero solo un total de 64000 llaves podrán ser canceladas por lista negra. Una vez la lista negra llegue al máximo de 64000 llaves canceladas, la lista negra ya no será enviada a las llaves a través de la red virtual SVN, por eso es IMPORTANTE entender su concepto para que su gestión se haga de la mejor manera posible.

Por defecto, todos los usuarios son enviados a la lista negra en cuanto son cancelados pero el software permite seleccionar si un usuario será colocado en lista negra o no al ser cancelado. Para esto tendrá que seleccionar en las opciones avanzadas el parámetro avanzado MORE_THAN_64K_USERS=1, como se muestra en la imagen siguiente;



Una vez salvado el parámetro, en la lista de usuarios aparecerá una opción que le permitirá seleccionar qué usuarios podrán ser cancelados usando la lista negra.



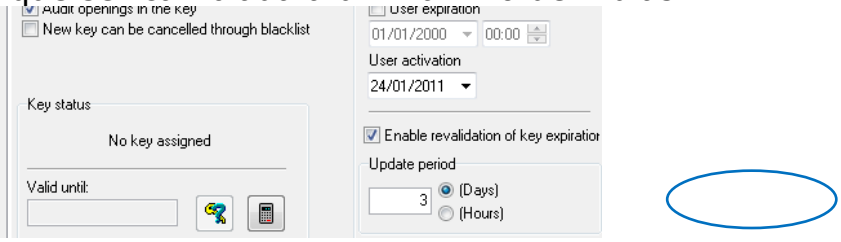
En el caso de tener la opción seleccionada, al ser cancelado el usuario será enviado a la lista negra y la información será propagada a todas las unidades de la instalación.

En el caso en el que NO se seleccione esta opción, la llave no será enviada a la lista negra. Es importante saber que solo hay 2 maneras para que esta llave cancelada deje de funcionar;

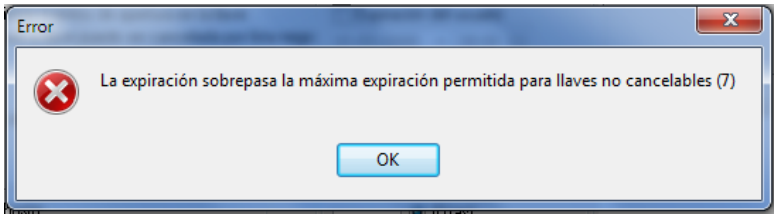
1/ Que sea presentada ante un lector mural online SVN y este lector borrará la llave cancelada al instante, de esta manera se impedirá que la llave pueda abrir tanto puertas online como offline.

Pero, este lector no actualizará las llaves de los otros usuarios con la información de la llave cancelada para que estos propaguen la lista negra.

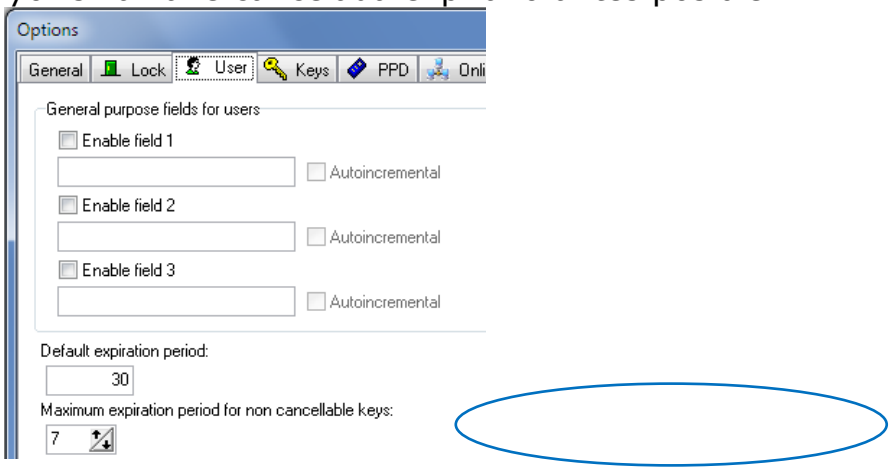
2/ Que la llave expire. Por esta razón, al deseleccionar la opción de envío a lista negra del usuario, la revalidación de la llave tendrá que ser cambiada a un máximo de 7 días.



Si se deselecciona esta opción y el tiempo de revalidación es superior al planeado, por defecto 3 días, un mensaje de error lo mostrará.

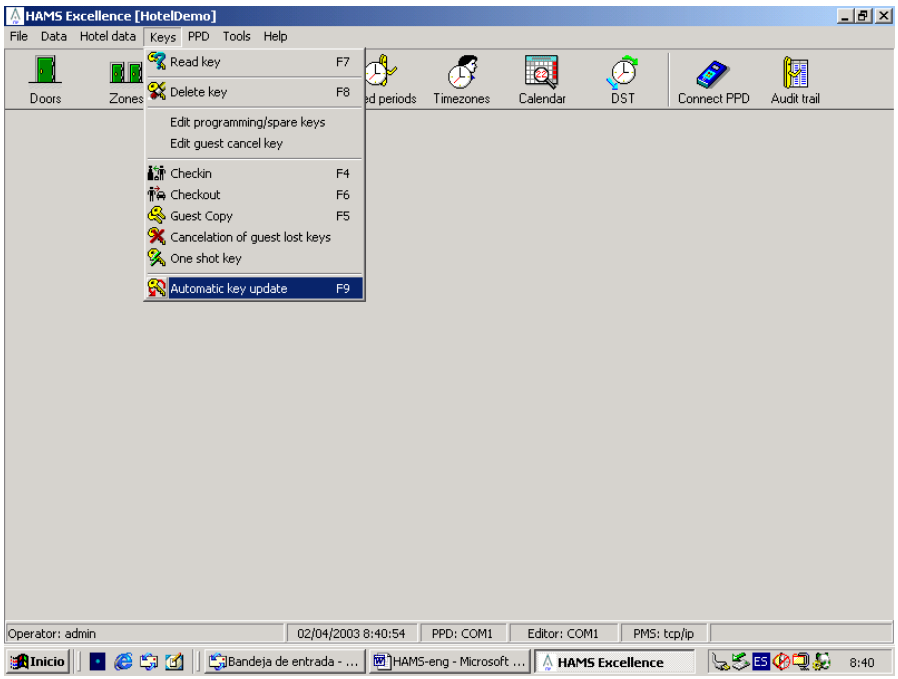


La cantidad máxima de días de revalidación permitida es de 7, como se ve en la siguiente imagen, aunque por defecto esta se configura a 3 días por el hecho de que la seguridad de la instalación es mayor si la llave cancelada expira lo antes posible.

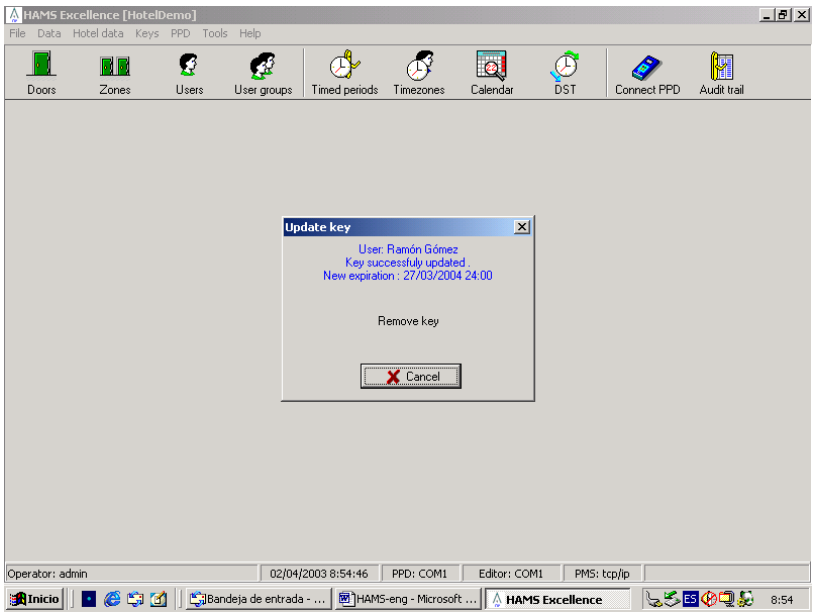


Actualización automática de llaves

Hay una opción en el menú de llaves, llamada ACTUALIZACIÓN AUTOMÁTICA DE LLAVES, que nos permite actualizar la llave de un usuario en el editor sin necesidad de ir a la lista de usuarios y seleccionar a este usuario de la lista.



La nueva fecha de caducidad para esta llave será la que hayamos especificado en HERRAMIENTAS / OPCIONES / GENERAL (en días). Al utilizar la función de actualización automática de llave, el editor entrará en un estado de solicitud continua de llave, y actualizará todas las tarjetas de usuario que sean insertadas en él, no importa en qué orden se inserten. Si hay algún cambio reciente en el perfil de acceso del usuario, esta información será editada en la llave. Así como los códigos de las últimas llaves canceladas (lista negra).



Utilizar el PPD .Inicializar

El programador portátil es un dispositivo que se utiliza para comunicarse con un escudo y transferirle toda la información procedente del PC donde hemos diseñado nuestro plan de cierre. Si tiene cualquier duda sobre el manejo de este dispositivo, por favor, consulte el manual de usuario del PPD Smart que encontrará en el mismo CD-ROM donde viene el software RW.

Menú principal

A continuación se puede ver un esquema de las opciones de menú del PPD. Es importante destacar que no siempre van a aparecer todas las opciones y esto depende de que las hayamos habilitado o no, desde el ordenador de gestión. Por defecto, aparecerán siempre las opciones DIAGNÓSTICO y RECOGIDA DE APERTURAS aunque no hayamos habilitado ninguna en el ordenador.

Inicializar las puertas:

Cuando tengamos nuestro plan de cierre terminado, tenemos que pasar toda esa información desde nuestro ordenador hasta el programador portátil.

Inicializaremos cada una de las puertas dándoles un nombre, que será definitivo a partir de ese momento.

Asegúrese que su ordenador tiene el reloj correctamente ajustado, es decir , que no adelanta ni atrasa, ya que la hora con la que van a funcionar los escudos electrónicos es la hora que tiene su ordenador, donde se ha diseñado la base de datos.

- Para cargar el programador portátil con la información de nuestro plan de cierre, conectamos el dispositivo a nuestro ordenador mediante el cable serie, y vamos al menú principal del programa. Pinchamos en el icono *PPD.*

- Si es la primera vez que utiliza el PPD para descargar un plan de cierre, puede que le salga un mensaje de error. pulse el botón *SI* para confirmar que, a partir de ese momento, el PPD será para uso exclusivo de su instalación.

- Se abrirá una ventana como la que tenemos a continuación, en ella vemos que ya aparecen seleccionadas todas nuestras puertas que están pendientes de inicializar.

- No es obligatorio inicializarlas todas a la vez, pero se recomienda para no dejar ninguna pendiente.

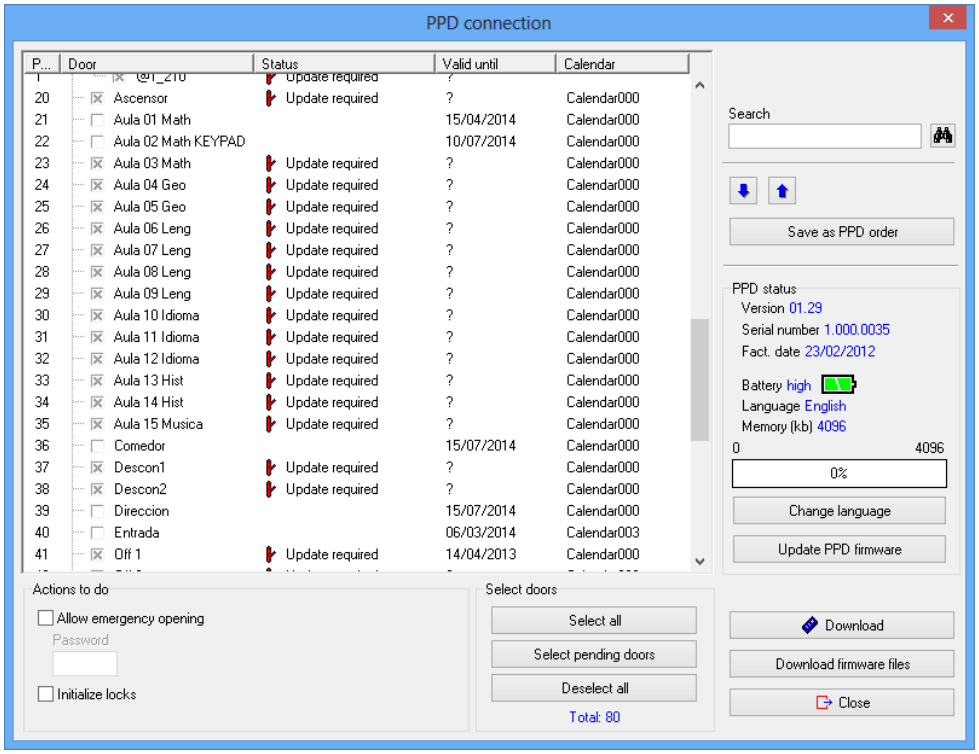


Figura 63

Vemos en esta ventana, abajo a la izquierda, un recuadro llamado *ACCIONES A REALIZAR.* En este recuadro vamos a marcar qué acciones vamos a realizar con el PPD.

1. **Si marcamos *PERMITIR APERTURA DE EMERGENCIA, esta* opción aparecerá después en el menú del PPD.**

2. **Si marcamos *INICIALIZAR CERRADURAS*, esta opción aparecerá después en el menú del PPD. Esto es lo que vamos a hacer ahora.**

Para estos dos posibles "tics", tenga en cuenta que no sólo es suficiente con marcar la acción a realizar sino también marcar con un aspa la puerta o puertas en las que quiera, realizar dicha acción.

- Si no marcamos ninguna de estas dos opciones, lo único que podremos hacer será: Actualizar cerraduras.

- Podemos cambiar el idioma de los mensajes que aparecen en la pantalla del PPD. Para ello, pincharemos en el botón *CAMBIAR EL IDIOMA.*

- Cuando tengamos las puertas en el orden deseado, pinchamos la opción *CARGAR AL PPD.*

- El trasvase de datos desde el ordenador hasta el PPD tardará unos segundos. Observe la pantalla del ordenador y cuando vea que llega al 100% la barra de progresión de la ventana activa, sabrá que ha terminado la transferencia.

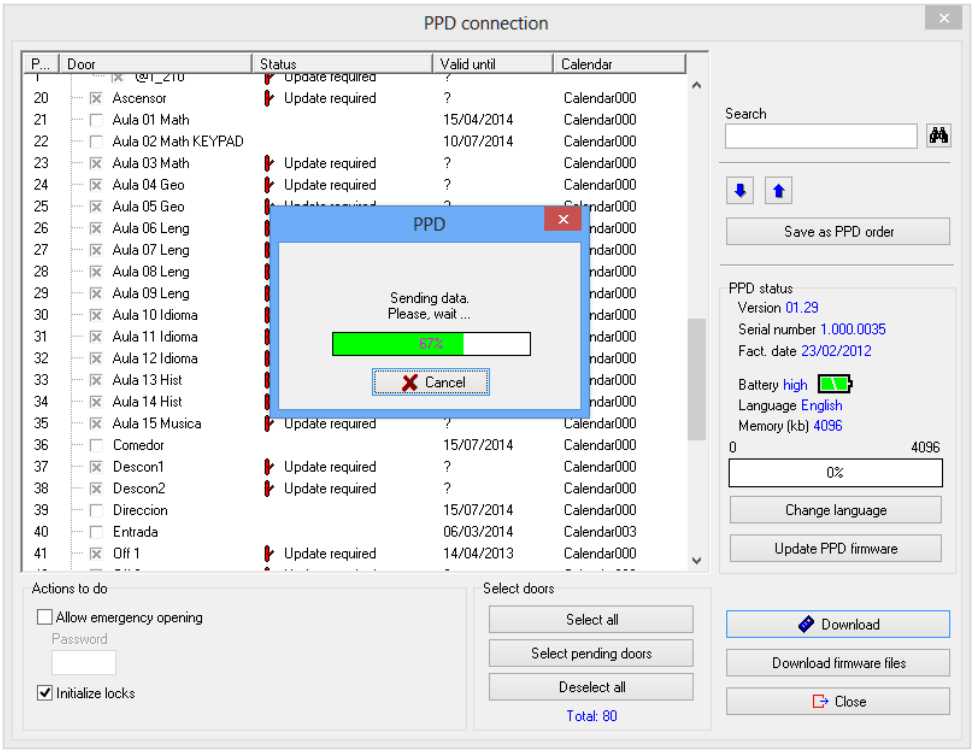


Figura 64

- Ahora puede desconectar el cable serie, y desplazarse hasta cada una de las puertas para inicializarlas.

- Conecte al PPD el cable terminado en una tarjeta especial que tiene 3 contactos eléctricos. (por el otro extremo verá un conector telefónico RJ11)

- Acérquese a la primera puerta de su sistema, enchufe el cable de comunicación y encienda el PPD.

- Desde el menú principal, seleccione la opción *INICIALIZAR.* Verá una lista de puertas, donde usted tendrá que seleccionar la puerta con la que está trabajando en este momento. Tenga especial cuidado en la realización de este paso, pues la asignación de la identidad de una puerta es fundamental.

- Cuando tenga en pantalla el nombre de la cerradura que va a inicializar, pulse el botón OK del PPD, y el dispositivo le pedirá que lo conecte a la cerradura.

- Verá en la pantalla del PPD el mensaje *CONECTAR CON CERRADURA.* Inserte en el lector de la cerradura el extremo del cable de comunicación (que es una tarjeta especial) y observe la pantalla del PPD. Verá una barra de progreso y escuchará un sonido agudo que indica que se está produciendo la transferencia de datos.

- Si por error, esta comunicación se interrumpe durante más de tres segundos, tendrá que volver a realizarla.

- Repita estos pasos con cada una de las puertas de su instalación. Tenga en cuenta que los nombres de las puertas no van a desaparecer de la lista de puertas contenida en la opción INICIALIZAR por el hecho de haber inicializado ya esa puerta. Esto es para que usted pueda volver a inicializar una puerta en caso de haberse confundido al darle el nombre.

- Cuando haya terminado la ronda de inicialización, vuelva a conectar el PPD a su ordenador mediante el cable serie, y pinche el icono CONECTAR PPD. Esto es para actualizar la información del software con respecto a los valores reales de estado de pilas, y actualizaciones pendientes. En este momento, la opción de menú INICIALIZAR CERRADURAS desaparecerá del menú de su PPD.

Opciones avanzadas

En este apartado se van a explicar algunas funciones, que en algunos casos no son imprescindibles, pero en general resultan muy importantes para el diseño de nuestro plan de cierre.

Identificar su instalación

Vamos al menú desplegable *HERRAMIENTAS* y pinchamos en la opción *OPCIONES GENERALES:*

- En la primera ficha que se nos presenta, veremos el nombre que dimos al principio a nuestra base de datos, en la casilla NOMBRE DE LA PROPIEDAD.

- Veremos dos casillas más, llamadas CIUDAD y ESTADO/ PAÍS. Por favor, rellene estos campos de acuerdo con las características de su instalación.

- Es importante rellenar también el campo llamado PRIMER DIA DE LA SEMANA, este dato afecta a la estructura de los calendarios.

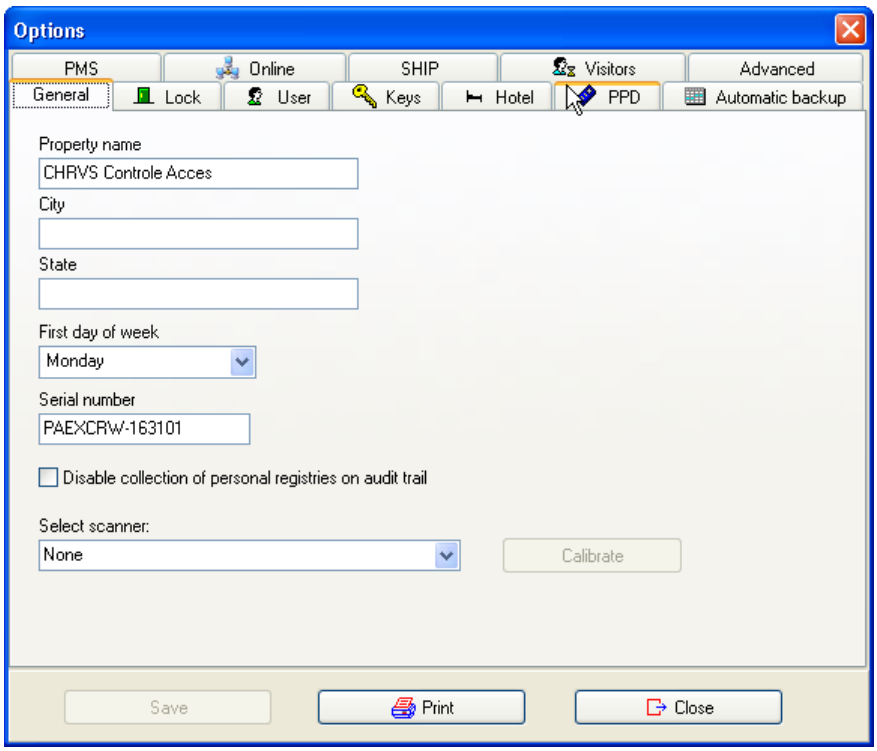


Figura 65

- El campo NÚMERO DE SERIE muestra el número de serie del software, número que se escribió al crear la base de datos por primera vez.

- El botón IMPRIMIR se puede utilizar para obtener un informe en papel de todas las ventanas de OPCIONES. Se recomienda utilizar esta opción cuando se haya terminado de diseñar la base de datos, de manera que todos los campos están rellenos con información real.

- La casilla DESHABILITAR LA RECOGIDA DE REGISTROS PERSONALES EN EL AUDIT TRAIL se puede marcar si queremos filtrar la información guardada en el audit trail, de manera que los operadores del software sólo puedan visualizar las actualizaciones de llaves y puertas pero no las aperturas hechas por personas.

- Guarde los cambios antes de pasar a las fichas siguientes.

Estado del PPD.

Vamos al menú desplegable *HERRAMIENTAS* y pinchamos en la opción *OPCIONES.* Esta vez vamos a escoger la ficha titulada PPD.

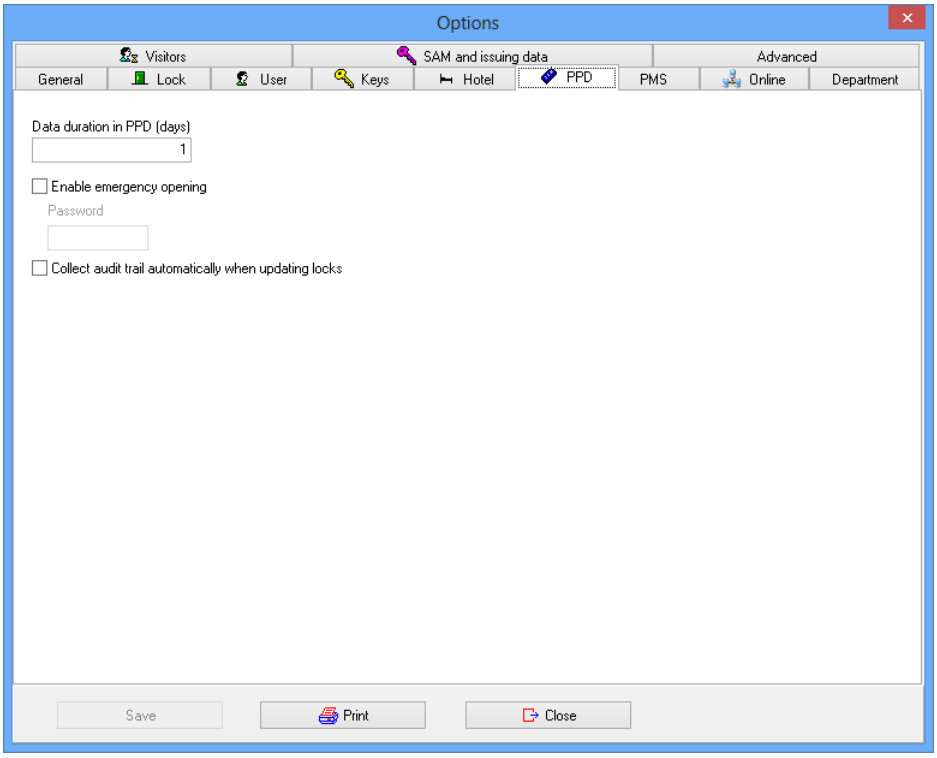


Figura 66

- La primera casilla se refiere a cuánto tiempo van a durar los datos transferidos al PPD desde el ordenador, hasta que éstos expiran. Por defecto, el sistema establece un tiempo de un día, pero usted puede aumentar esta duración.

A continuación se ven dos campos que pueden ser marcados o no, según quiera usted definir la configuración por defecto del PPD.

- Si usted marca HABILITAR APERTURA DE EMERGENCIA, esta opción seguirá apareciendo en el menú del PPD incluso después de la caducidad de los datos.

NOTA: tenga cuidado con esta opción, ya que si usted habilita la apertura de emergencia de manera permanente, el PPD se convierte en una llave maestra que abre todas las puertas de su instalación, si cae en manos de una persona no autorizada.

- Si usted marca EN LAS ACTUALIZACIONES DE CERRADURAS, RECOGER AUTOMÁTICAMENTE APERTURAS el PPD recogerá el auditor de cerraduras de cada puerta, cada vez que usted haga una actualización de dicha puerta.

Opciones Locales

Desde el menú desplegable HERRAMIENTAS/ OPCIONES LOCALES escoja se le abrirá una ventana como ésta:

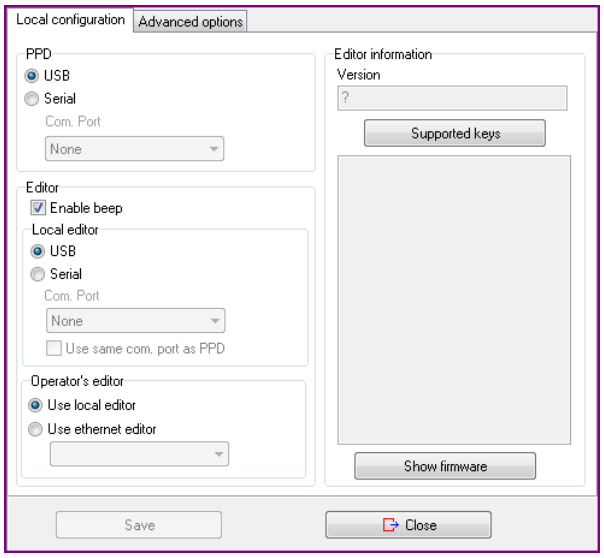


Figura 67

Puede seleccionar comunicar con el PPD a través del puerto **USB**. Al instalar el programa, los controladores se instalarán y no hará falta ninguna otra configuración.

En el recuadro "PUERTO DE COMUNICACIÓN", seleccione el puerto **SERIE** de su ordenador, a través del cual quiere comunicar con el PPD (COM 1, COM 3).

También, es posible utilizar un puerto serie para el editor y otro puerto serie para el PPD. Esto se explica en el apartado EDITOR.

De la misma manera que con el PPD USB, también se puede usar el puerto USB para comunicar con un editor.

Estado del Editor.

Desde el menú desplegable HERRAMIENTAS / OPCIONES LOCALES escoja la ficha del EDITOR. Se le abrirá una ventana como ésta:

Figura 67

- En esta ventana, aparecerá el número de versión del editor de tarjetas, desde la primera conexión del mismo al puerto serie de su ordenador.

- También es posible ver qué tipos de tarjetas pueden ser utilizadas por el editor. Pulse el botón TARJETAS ADMITIDAS.

- La casilla titulada HABILITAR SONIDOS se puede marcar o no dependiendo de si usted quiere que el editor emita señales acústicas.

- La caja MISMO PUERTO SERIE DEL PPD se utiliza para especificar si vamos a utilizar el mismo puerto serie para el PPD y el editor, o, por el contrario, vamos a utilizar un puerto serie distinto

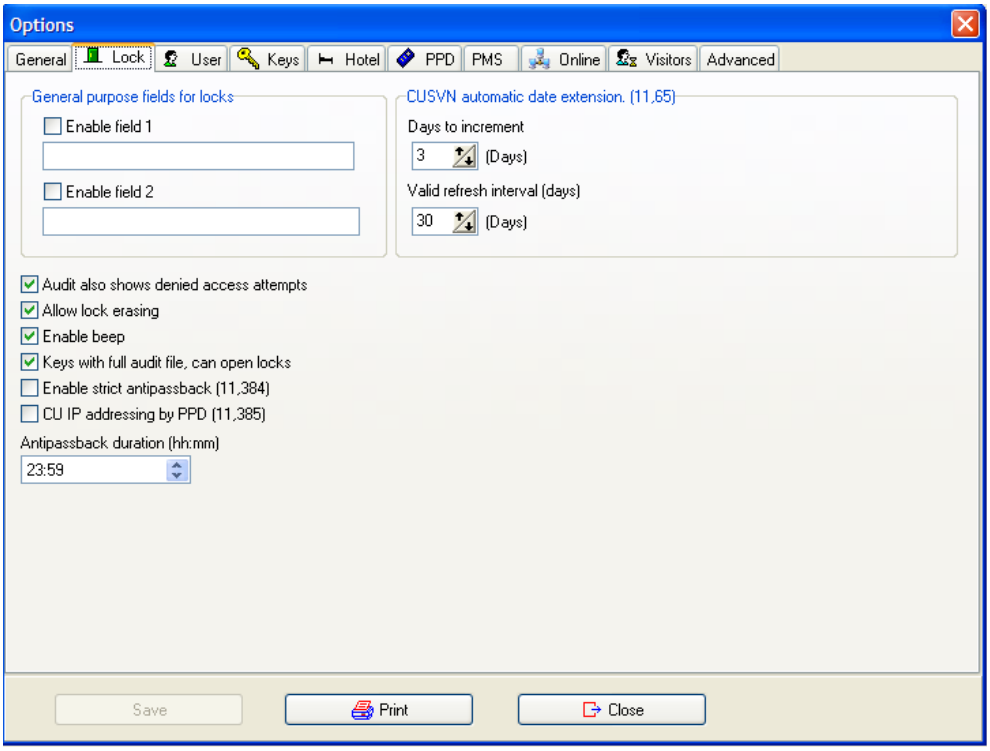
para cada dispositivo. En el segundo caso, tendrá que seleccionar el puerto utilizado para la comunicación con el editor (para trabajar de esta manera es necesario tener al menos, 2 puertos serie disponibles en el ordenador).

- Es muy importante entender completamente los siguientes dos conceptos para evitar confusión: El editor serie local y el Editor del operador. El Editor del operador se refiere al Editor real que va a ser usado por cualquier usuario que va a trabajar localmente en el software Salto. Podría ser cualquier Editor que se ha ajustado al sistema serie o Ethernet. Si se selecciona la opción Ethernet hay que elegir uno entre los diferentes Editores Ethernet disponibles.

- Por otro lado el Editor serie local se refiere al editor conectado a la máquina a través de un puerto serie o USB. Este editor se puede utilizar por medio del servidor Salto-PMS o el servidor Salto-Ship cuando se solicita emitir llaves en el editor local. De la misma forma este editor local puede ser usado por cualquier operador que ha entrado en el sistema siempre que el parámetro 'Operador Editor' haya sido establecido para usar el Editor local serie.

Estado de las puertas

En esta ventana vamos a concretar ciertas características de funcionamiento de los escudos y lectores.



- La casilla AUDITAR TAMBIÉN RECHAZOS EN CERRADURAS se puede marcar o no dependiendo de si usted desea ver en el Auditor de Eventos los intentos fallidos de traspasar una puerta.

- PERMITIR BORRADO DE CERRADURA: si usted habilita esta opción, se puede resetear la cerradura .No recomendamos habilitar esta opción, por razones de seguridad. (a no ser que tenga la plena seguridad de que los escudos electrónicos van a ser usados para más de 1 plan de cierre distinto , a lo largo de su vida).

- **Nota:** si en algún momento usted quiere habilitar el borrado de un escudo en particular, tendrá que volver a inicializar el escudo que quiera resetear. No es suficiente con actualizarlo.

- La casilla HABILITAR SONIDOS se puede marcar o no, dependiendo de si usted quiere que los escudos electrónicos emitan sonidos de señalización durante su empleo.

- LLAVES CON EL AUDITOR LLENO ABREN CERRADURAS. Si se quita esta opción, las llaves dejarán de abrir una vez la memoria de la tarjeta esté llena forzando así la descarga en un lector SVN.

- HABILITAR ANTIPASSBACK ESTRICTO.

- DIRECCIONAMIENTO IP CU POR PPD. Al chequear esta opción, el PPD asignará la dirección IP a la CU en el momento de su inicialización. Esta opción resulta útil cuando dicha CU se encuentra en una red de rango diferente a la del maestro de comunicaciones.

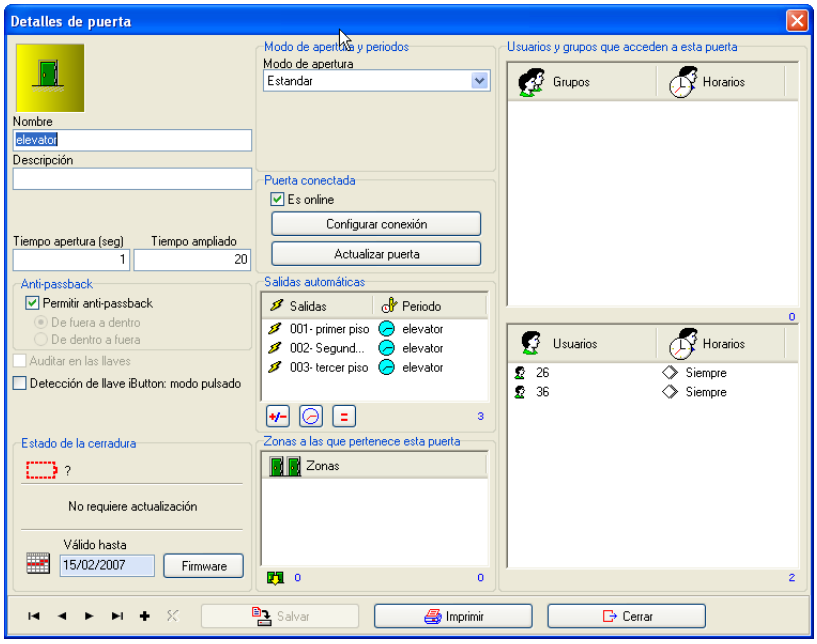
- PERMITIR INHIBICIÓN DEL AUDITOR añadirá una opción en la ventana de puertas. El habilitar dicha opción, en la lista de puertas, deshabilitará la memorización de eventos de apertura en la memoria de la puerta en concreto. Esto significa que aun usando el PPD no se recogerán eventos puesto que estos no habrán sido creados.

- CUSVN AUTOMATIC DATE EXTENSION. Esta función regula el modo de funcionamiento de un actualizador SVN cuando por alguna razón se encuentre trabajando en modo off-line. De esta manera, el actualizador seguirá revalidando las tarjetas de acuerdo a los siguientes parámetros:

  - Días a incrementar: número de días a revalidar.
  - Intervalo válido para refresco: límite máximo de revalidación desde la última actualización on-line.

Salidas temporizadas

Si queremos que ciertas salidas de una puerta trabajen en un periodo específico en modo de apertura automática. Para ello debemos ir a ver los detalles de la Habitación/Puerta:



En la siguiente ventana añadiremos las salidas y su periodo.

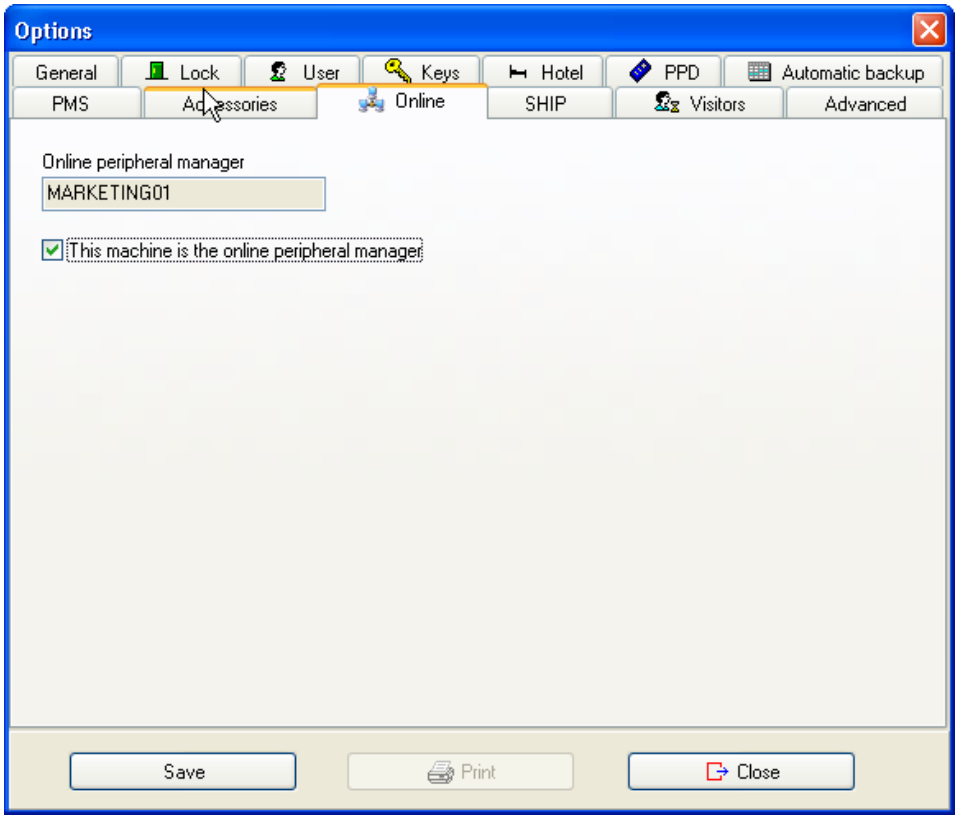
NOTA: El máximo número de salidas temporizadas son 4.

On Line

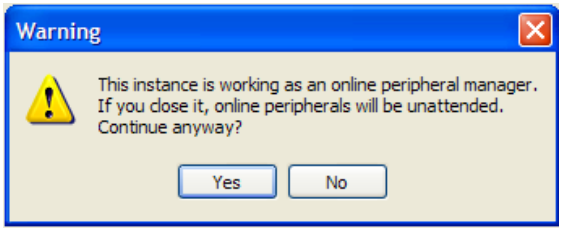
Esta tarjeta muestra información sobre el ordenador que sea el maestro de comunicaciones para dispositivos On line (unidades de control On line y actualizadores).Si estamos trabajando en una red de área local , con varios puestos de trabajo contra la misma base de datos , sólo uno de estos ordenadores puede ser el maestro de periféricos.

El campo MAESTRO DE PERIFÉRICOS ON LINE muestra el nombre de este ordenador en la red de área local.

La check box ESTE ORDENADOR ES EL MAESTRO DE PERIFÉRICOS ON LINE Sólo puede estar marcada para un puesto de trabajo, debe estar en blanco para los otros puestos de trabajo LAN.



El maestro de comunicaciones debe estar encendido constantemente para asegurar una buena sincronización de los elementos cableados. El siguiente aviso se mostrará cuando se intente cerrar la aplicación.



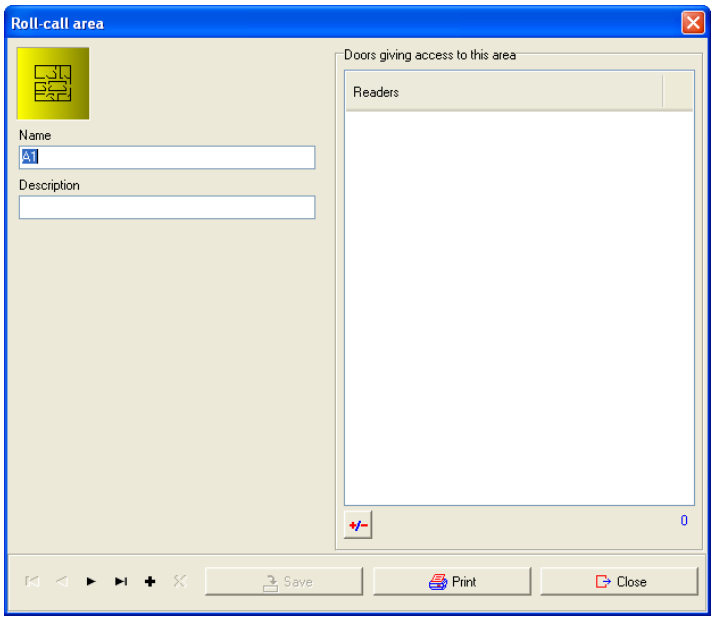
Roll-Call:

Esta opción permite conocer cuántos usuarios y qué usuarios se encuentran en un área "Roll-Call" en cada momento. Los datos de las áreas Roll-Call se actualizan automáticamente cada minuto.

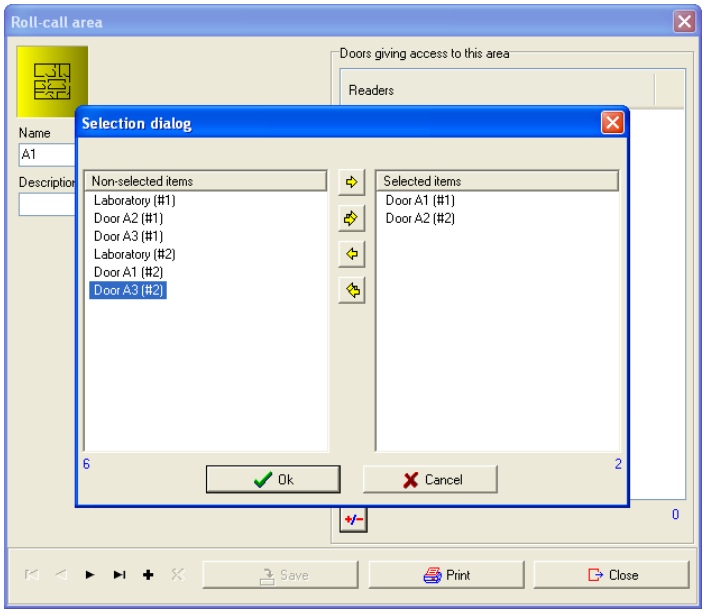
Esta opción se activa desde el menú desplegable: HERRAMIENTAS/CONFIGURACIÓN/ OPCIONES GENERALES/ AVANZADO/ ROLL-CALL.

Crear Áreas Roll-Call:

Para definir un área Roll-Call vamos al menú deplegable DATOS/ ÁREAS DE ROLL-CALL.



Para cada área Roll-Call debemos definir los lectores online que dan acceso. Para ello pulsamos el botón +/- y aparecerá una pantalla de selección donde para cada puerta online aparecen sus dos lectores (#1 y #2). (Ver Fig. 2)



Debemos asegurarnos de elegir cuál de los dos lectores es el de entrada al área y pasarlo al otro lado en la ventana de selección.

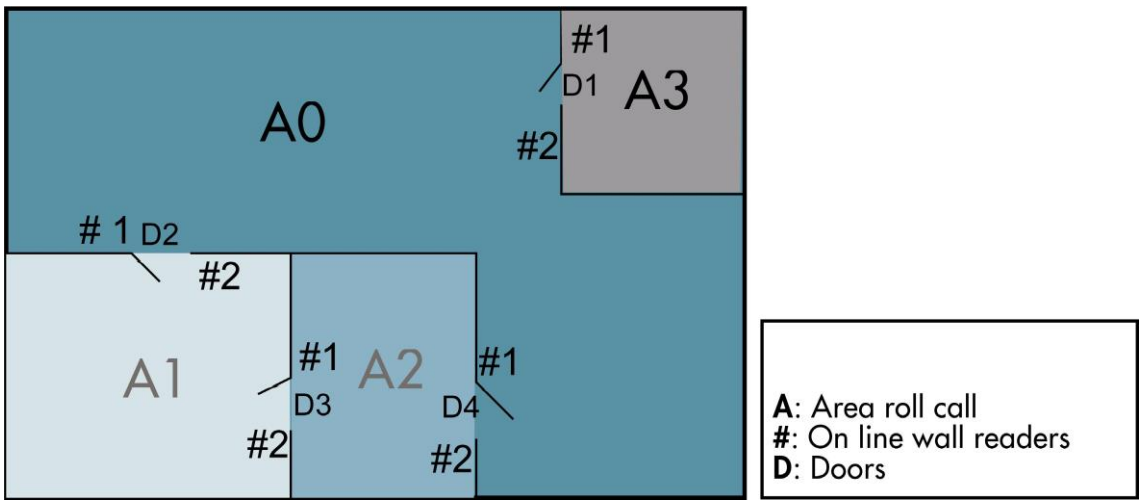
Nota: Una vez creadas todas las áreas que queremos controlar debemos crear un área más.

Área Externa:

Este área será la referencia en donde localizaremos a los usuarios cuando no están dentro de ninguna de las áreas anteriores. En esta función del software hay un concepto muy importante: "El usuario no sale de un área sino que entra en otra". Si no creamos este área el software no podrá interpretar la salida de un área al no ser que esta salida sea entrada a otro área.

Para crear esta área debemos seleccionar todos aquellos lectores online que den salida a las anteriores áreas Roll-Call y que no sean entrada a otro área ya creada.

Ejemplo:



En el ejemplo de la figura hemos definido las distintas áreas Roll-Call que queremos controlar (A1, A2, A3):

A1: lectores de entrada: D2 (#1), D3 (#1)
A2: lectores de entrada: D3 (#2), D4 (#1)
A3: lectores de entrada: D1 (#2)

Una vez definidas estas áreas Roll-Call es necesario crear un nuevo área A0. Este área nos mostrará cuántos y qué usuarios no se encuentran dentro de las zonas A1, A2 y/o A3.

A0 tendrá la siguiente configuración:

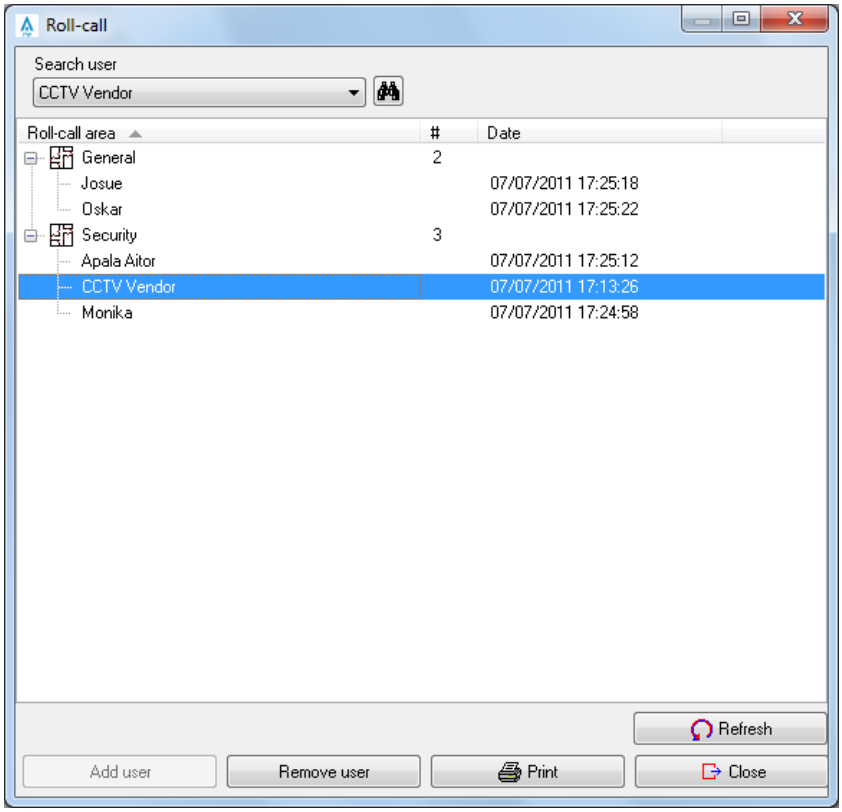
A0: lectores de entrada: Puerta A1 (#2), PuertaA3 (#1)

MONITORIZACIÓN DE LAS ÁREAS ROLL-CALL

(Estado de las áreas y Control de presencia):

Para acceder a la información que nos proporcionan las áreas Roll-Call debemos ir al menú desplegable PERIFÉRICOS/ ROLL-CALL. (Fig.3)

La ventana de Roll Call muestra la cantidad de usuarios y visitas en cada zona definida de Roll Call, incluyendo sus nombres y la fecha y hora en la que entraron en dicha área.



(Fig. 2)

Como puede verse en la figura superior, si quiere localizarse a un usuario o visita, su nombre puede buscarse con el botón de búsqueda, seleccionando a la persona en la lista desplegable. Una vez encontrado, su nombre aparecerá remarcado en azul.

En esta pantalla obtendremos la información del número de usuarios o visitas que tenemos en cada área así como el detalle de quien y a qué hora accedió al área.

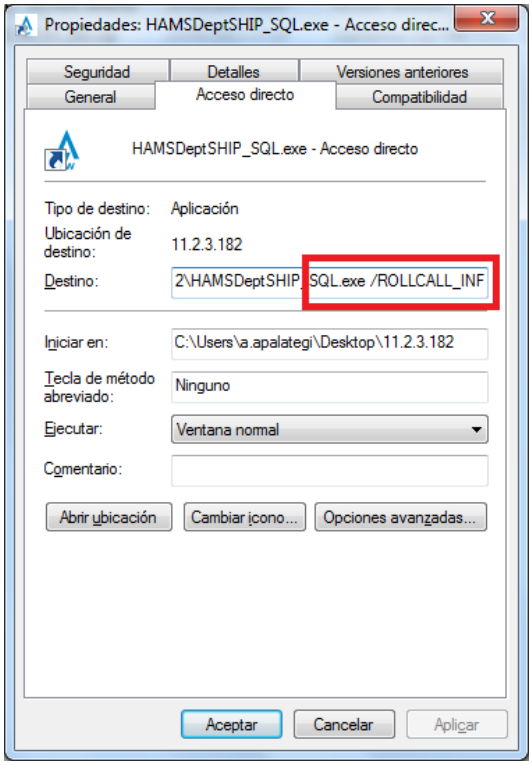
Podemos también buscar un usuario o visita escribiendo su nombre en la casilla superior. El software automáticamente lo localizará.

Hay una opción de añadir o eliminar usuarios y visitas manualmente. Para ello, hay que pulsar los botones de la parte inferior.

Nota: El correcto funcionamiento de esta opción del software depende del buen control de las puertas del edificio, sin este hardware (tornos) es difícil obtener un informe Roll-Call correcto ya que los usuarios pueden entrar y salir en nivel de accesos sin presentar sus identificadores.

El software Pro Access / HAMS permite al usuario del sistema ejecutar el software de manera limitada, para que solo se muestra la venta de monitorización de la función Roll Call, y así poder ver en qué lugar de la instalación se encuentran los usuarios.

El parámetro avanzado ROLLCALL_INFO debe añadirse al comando del campo Destino en el acceso directo del software:

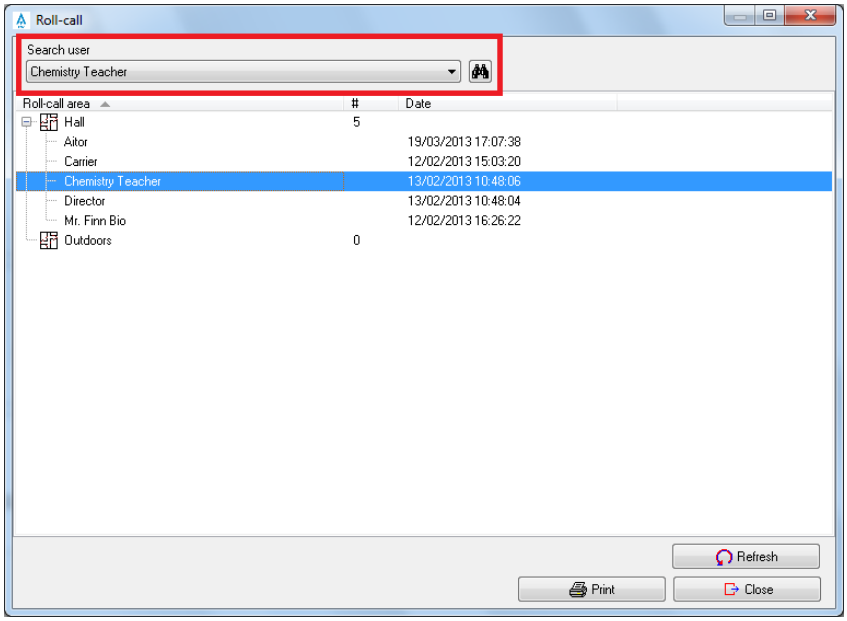


(Fig. 3)

El parámetro avanzado hará que el software se ejecute como una simple ventana de monitorización a pantalla completa de la función Roll Call al hacer doble click sobre el acceso directo del software.

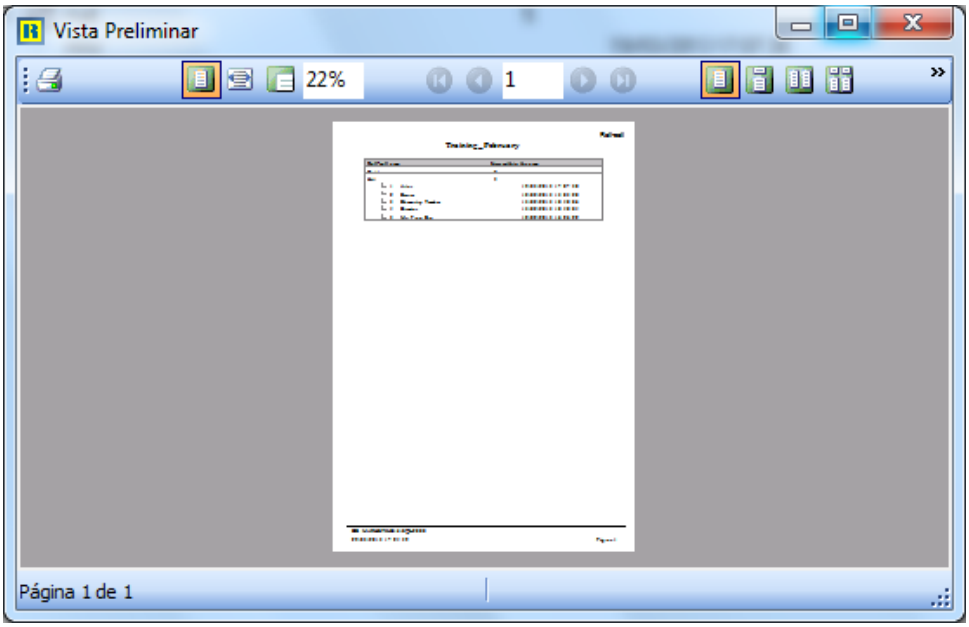
Este modo permite accede de manera reducida a las opciones del Roll Call normal incluido en el software Pro Access / HAMS.

La localización de un usuario específico puede encontrarse seleccionando el nombre del usuario de la lista y seleccionando el botón de los prismáticos:



(Fig. 4)

El botón Imprimir permite imprimir un informe que incluye la localización de todos los usuarios del sistema, como puede verse en el siguiente dibujo:



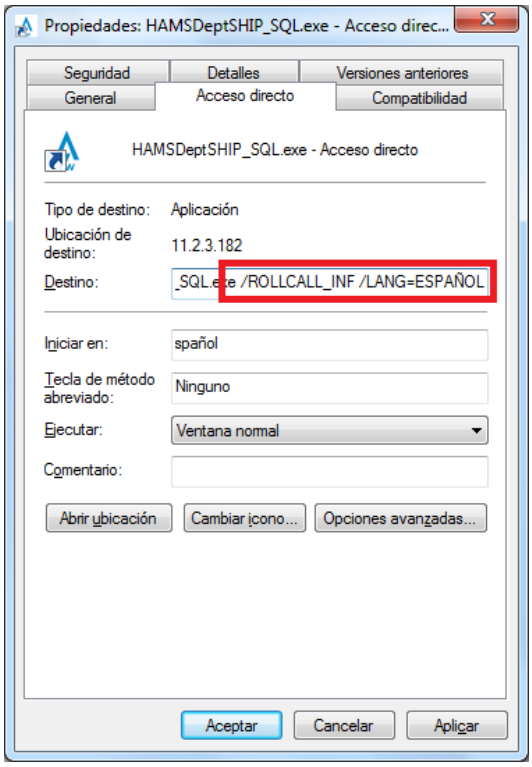
(Fig. 5)

Finalmente, el botón Cerrar cerrará la venta de monitorización Roll Call, al igual que el software.

Notas Importantes: La función Roll Call debe activarse en la pestaña de Herramientas / Configuración / Opciones Generales / Avanzado para poder ejecutar este modo específico de Roll Call.

Ejecutar este modo de Roll Call no precisa de ninguna contraseña. Se mostrará directamente al ejecutar el acceso directo del software.

Este modo de monitorización Roll Call puede ejecutarse eligiendo cual es el idioma predeterminado, añadiendo el parámetro /LANG=idiomaseleccionado, tal y como se ve en la figura siguiente:



(Fig.6)

Limitación de accesos (Parking):

Por medio de esta opción vamos a poder crear diferentes zonas y nivel de accesos. En los niveles de accesos a su vez podremos limitar el número máximo de usuarios. Es decir podremos crear diferentes niveles de accesos con diferentes restricciones en cada uno de ellos.

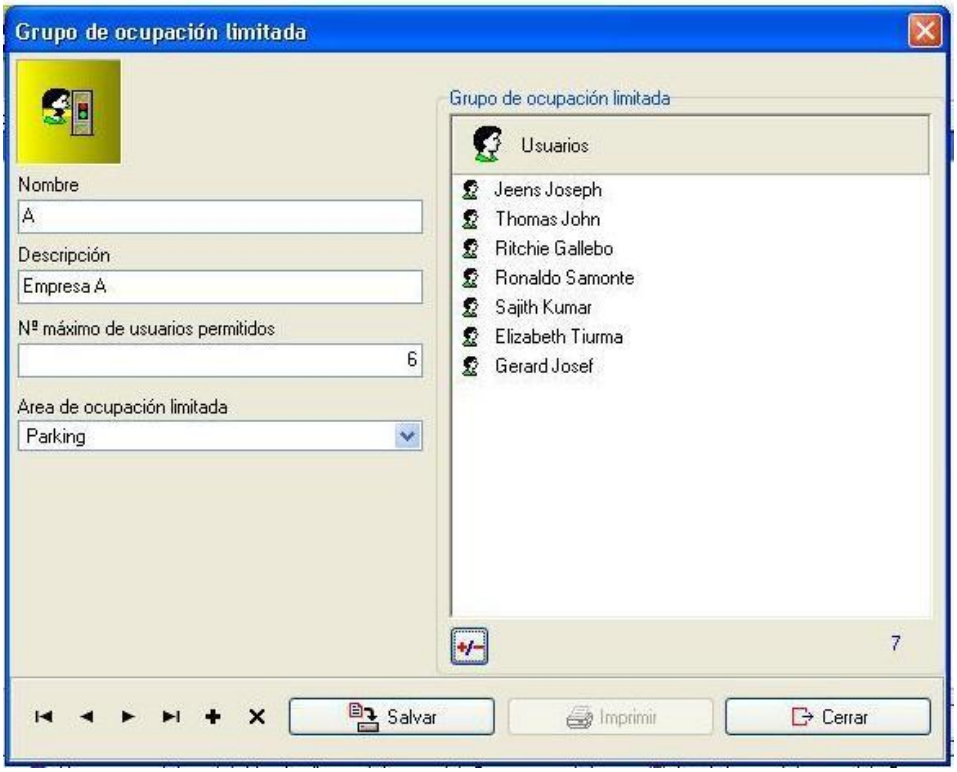
Para poder utilizar esta prestación es necesario tener una CU50EN o CU50ENSVN.

El caso o ejemplo más común de esta aplicación sería un parking al que diferentes compañías tendrían acceso. Por ejemplo la compañía A podría tener un máximo de 6 usuarios con acceso de

forma simultánea y la compañía B 8. En el software crearíamos 2 nivel de accesos A y B con un máximo de 6 y 8 usuarios respectivamente. Por tanto cuando el usuario 7 del nivel de acceso A quiera entrar deberá esperar hasta que alguno de los 6 usuarios (del nivel de acceso A) que están en el parking salgan del mismo.

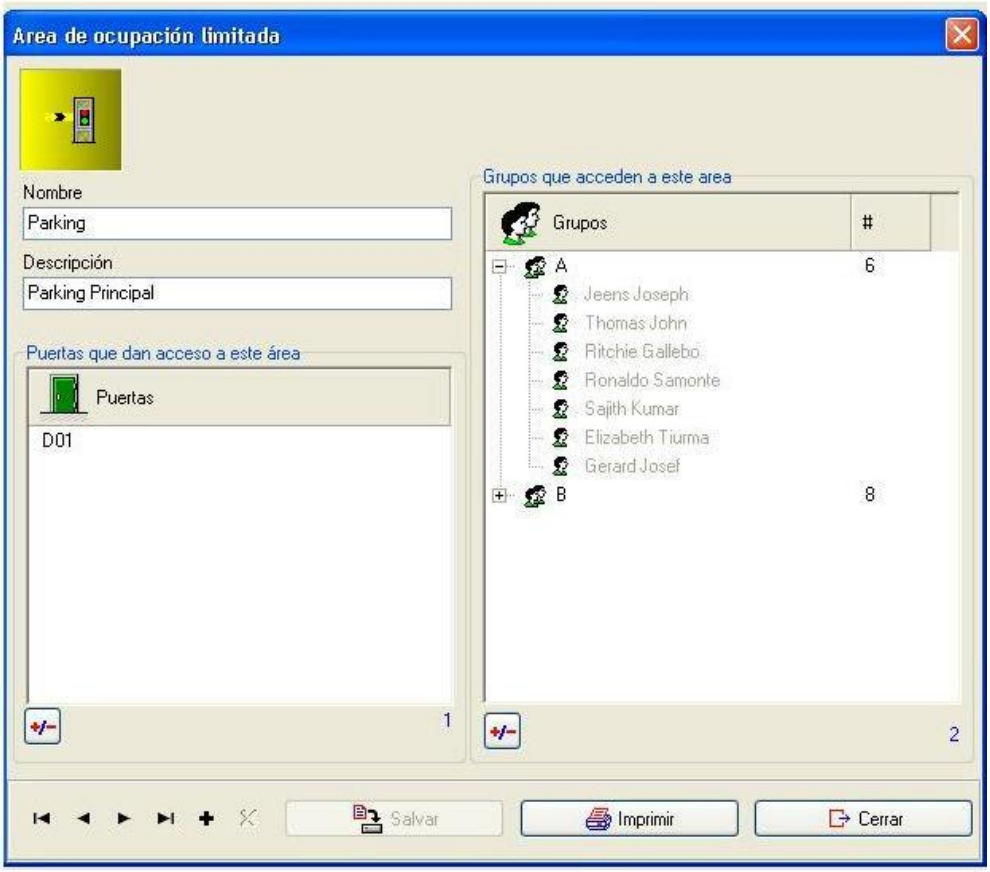
Para configurar esta opción hay que ir a herramientas/Opciones generales/Avanzado y activar la opción de Limited occupancy.

Entonces en datos podremos ver la opción ocupación limitada activa. La primera cosa que tenemos que hacer es crear un nuevo nivel de acceso:



En la ventana superior se puede crear el grupo, el máximo de usuarios que pueden acceder de forma simultánea, los usuarios que pertenecen al nivel de acceso y el área a la que tienen acceso.

El siguiente paso será crear la zona:

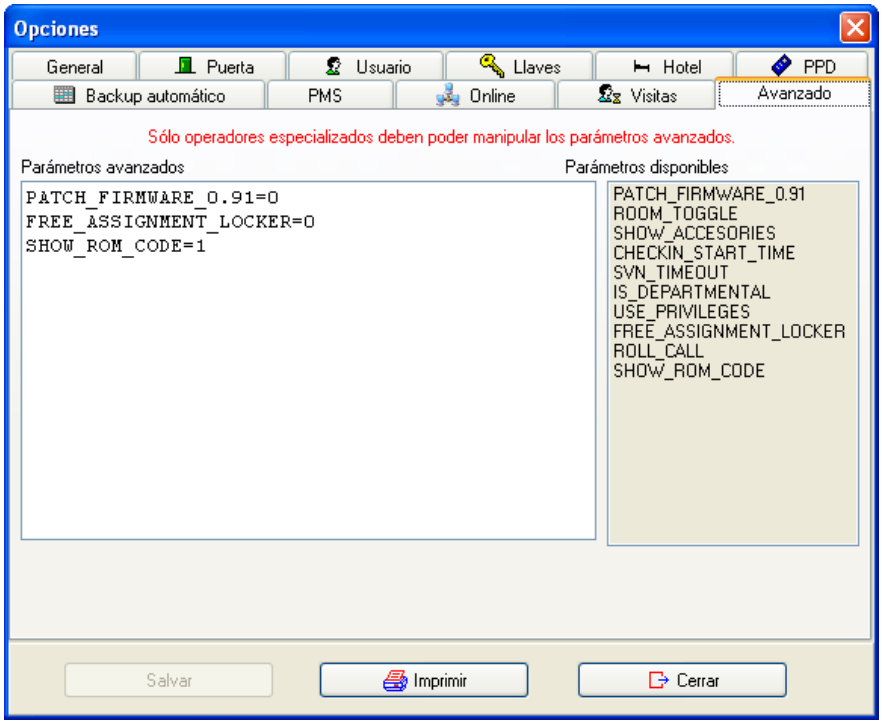


De la misma forma se tiene que especificar la puerta Online que delimita la zona y los nivel de accesos que acceden a esa zona.

Algo importante a tener en cuenta es que todos los usuarios que pertenecen a esos nivel de accesos y que tienen acceso a esas zonas han de tener acceso a la puerta Online que delimita esa zona. En este ejemplo todos estos usuarios deberán tener acceso a la puerta D01 que delimita la zona Parking.

Mostrar el código ROM:

Para activar en el software esta opción debemos ir al menú despegable HERRAMIENTAS/ CONFIGURACIÓN/ OPCIONES GENERALES y pulsar la pestaña "AVANZADO" (Fig. 1):



(Fig. 1)

Debemos pasar a la ventana de Parámetros avanzados la Opción: "SHOW_ROM_CODE".

El código ROM lo visualizaremos al leer una llave en su contenido. Así mismo, el código ROM aparecerá cada vez que exportemos usuarios o exportemos el Auditor de cerraduras.

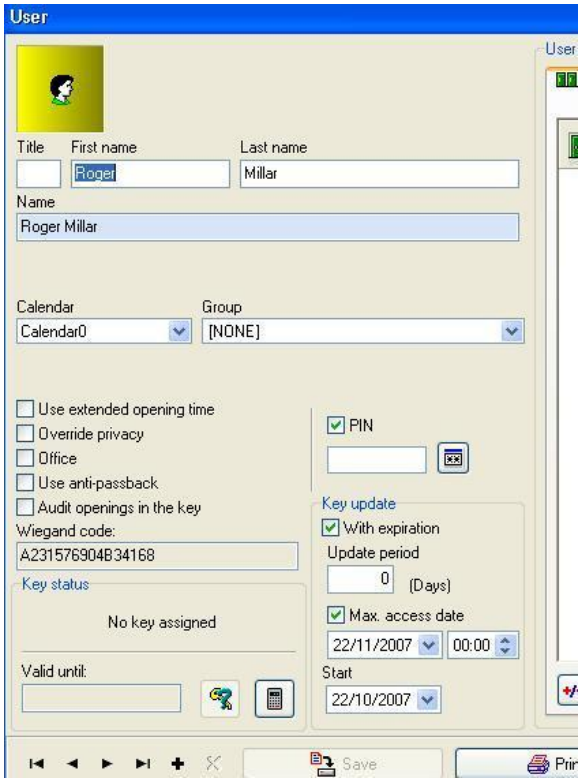
Mostrar el código Wiegand:

Para algunas aplicaciones externas como T&A, POS, podría ser interesante recibir el código Wiegand del usuario. En algunas ocasiones estas aplicaciones externas necesitan el código Wiegand para poder trabajar.

Por medio de esta herramienta vamos a poder escribir este código en la tarjeta y enviarla a la otra aplicación a través e un WRAdaptor, CUAdaptor o Desktop reader.

Para activar esta opción hay que ir a herramientas/opciones generales/Llaves y aquí activar la opción Wiegand. Una vez activada esta opción en las opciones generales podremos ver en la ventana de usuario como un nuevo campo se muestra con el código Wiegand en su descripción. Este nuevo campo no se puede rellenar de forma directa, de hecho para insertar el código Wiegand hay que hacerlo a través de la sincronización de BBDD. A la hora de ajustar la sincronización hay una columna para asignar el código Wiegand a cada usuario.

Una vez que el código se inserta en la BBDD ya puede ser escrito en la tarjeta de usuario y por tanto ser enviado a otra aplicación.



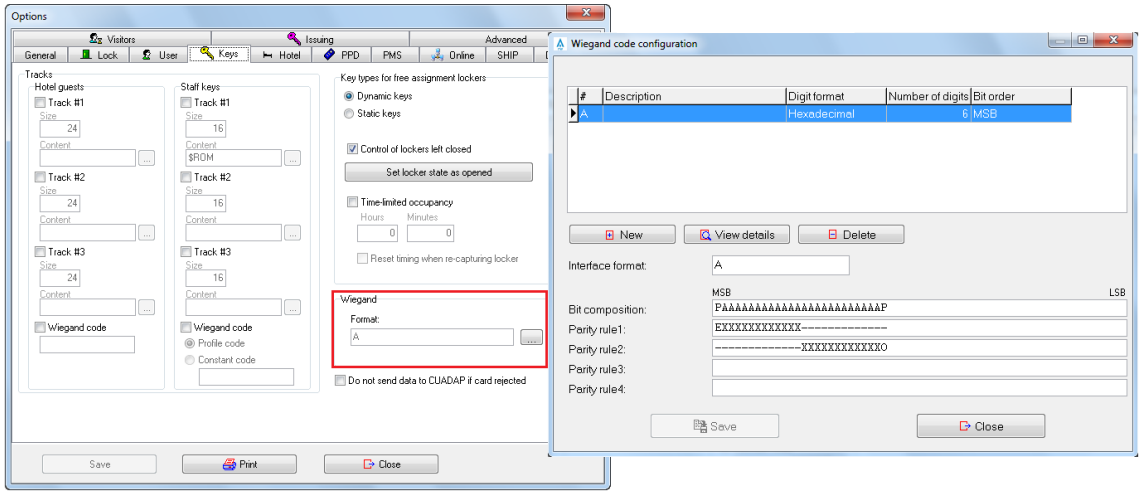
En esta ventana se puede observar como el código Wiegand se ha registrado en este usuario.

Si se le **deniega** el acceso a un usuario, su código Wiegand no será exportado a la aplicación tercera.

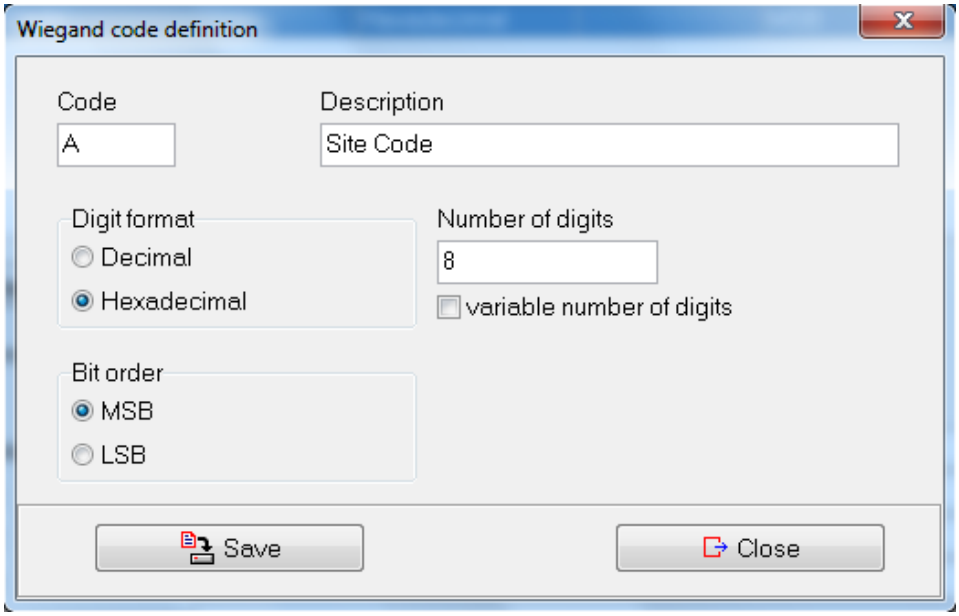
GENERADOR DE FORMATO WIEGAND FLEXIBLE

La pestaña de Llaves en Opciones Generales permite configurar el formato de las tarjetas Wiegand que se vayan a grabar. Esta opción permite adaptarse al formato Corporate 1000 de HID y al igual que a otros formatos Wiegand diferentes del clásico de 26 bits.

Tal y como puede verse en la imagen inferior, el software permite definir la composición de los bits del Wiegand, al igual que el formato de los datos.



Primero se definen los códigos que conformarán el código Wiegand final. Seleccionando el botón Nuevo, se pueden crear las diferentes partes del código Wiegand, al igual que sus características.



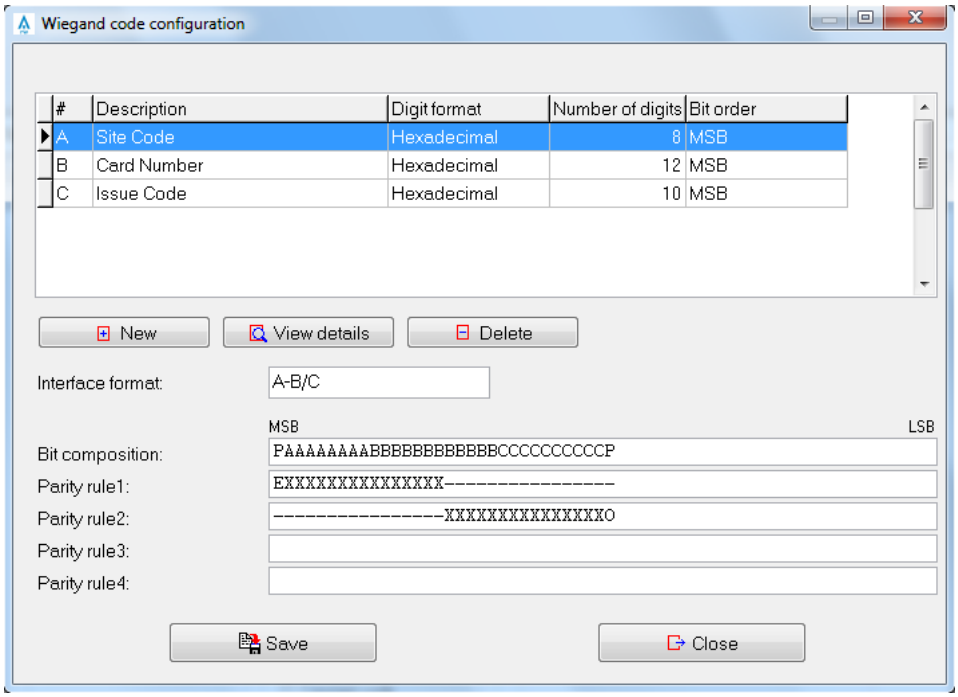
Dichas partes o códigos serán identificados internamente por letras, como por ejemplo la A en el ejemplo de la figura superior. Cualquier letra puede ser usada para ello, exceptuando la P, ya que esta se usa para identificar la Paridad de los códigos al principio y al final del código Wiegand.

La inclusión de una pequeña descripción del código ayudará posteriormente a identificar su significado.

El formato de los dígitos puede ser configurado como Decimal o Hexadecimal, al igual que el número de dígitos que contendrá ese

código. También se puede configurar el número de dígitos del código como variable.

Los bits pueden ordenarse empezando por los de mayor significado (MSB) o menor significado (LSB).



Una vez los códigos han sido creados, el Formato del Interface (Interface Format) indica el orden en que aparecen los códigos en la base de datos, y si se incluyen literales (caracteres de cabecera, separadores…).

En el ejemplo de la figura superior, el código A se separa del B con un guión (-) y este a su vez del C con una barra ascendente (/).

Una tabla muestra la composición de los bits del Wiegand a partir de los códigos anteriores, especificando en la parte superior de la tabla cuál el bit más significativo (MSB), y cuál es el menos significativo (LSB).

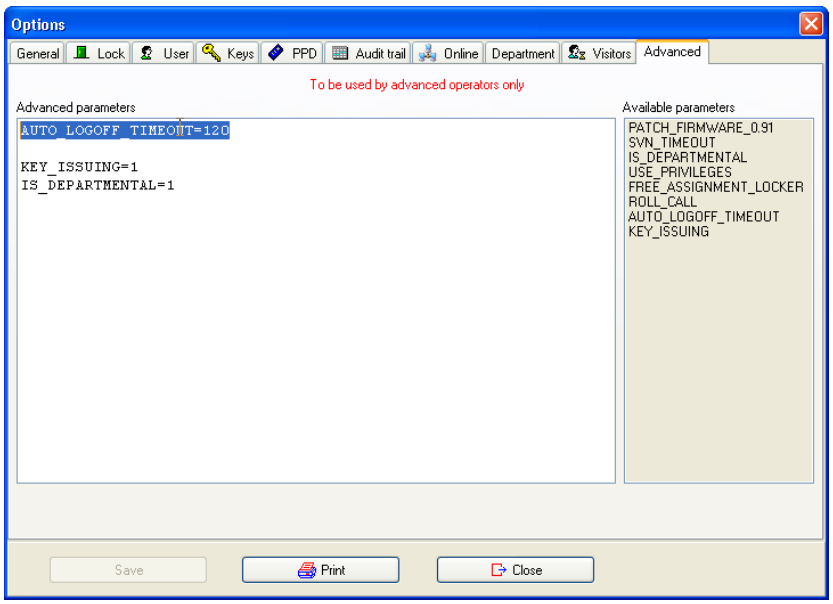
La Composición de los Bits (Bit Composition) debe mostrar cómo se va a componer el código Wiegand, empezando y terminando con la Paridad (P).

Las Reglas de Paridad 1 y 2 indican cómo se calcula uno de los bits de Paridad, siendo la E la Paridad Par, y la O la Paridad Impar. La X indica con qué bits se calcula la paridad y el guión (-) indica cuáles no se tienen en cuenta.

Las paridades se calculan en el orden indicado por las líneas. Es importante porque una paridad puede ser calculada teniendo en cuenta el bit de paridad resultado de otra anterior.

Auto Logoff

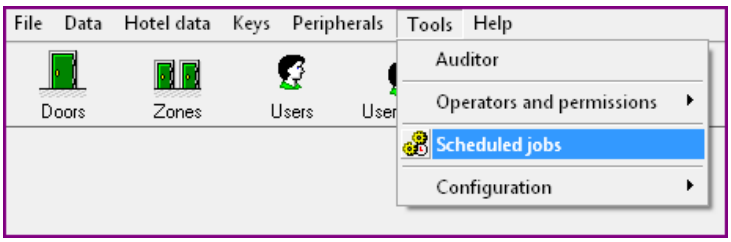
Tenemos dentro de los parámetros avanzados la opción de activar esta opción. Podemos por medio de este comando hacer logoff automático un tiempo después de que ninguna operación se haya hecho en el software.



Simplemente añadimos los segundos que queremos que se contabilicen antes del logoff automático desde la última operación realizada en el software.

Purgado automático

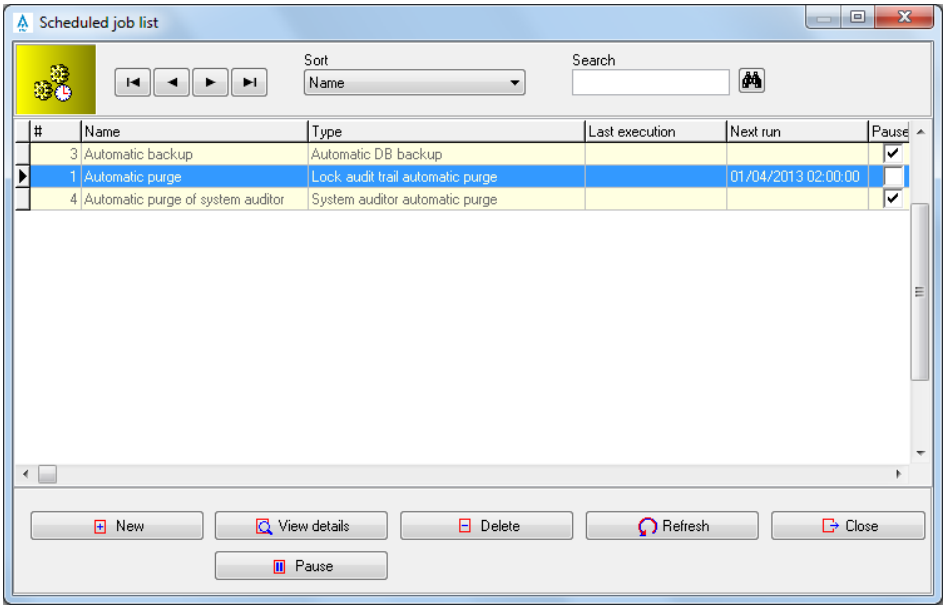
Por medio de esta opción se puede programar el purgado del auditor de cerraduras y del sistema.



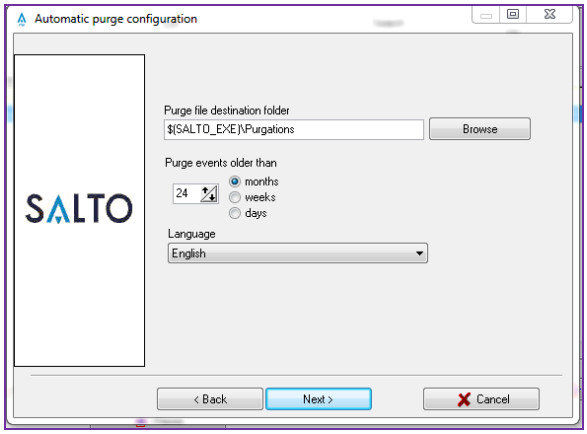
Los eventos purgados se volcarán en un fichero plano de texto para su posterior consulta.

En la siguiente figura se muestra las opciones del purgado automático. Número de eventos a purgar, % del auditor a purgar, frecuencia del purgado y la dirección donde se quiere colocar el fichero TXT.

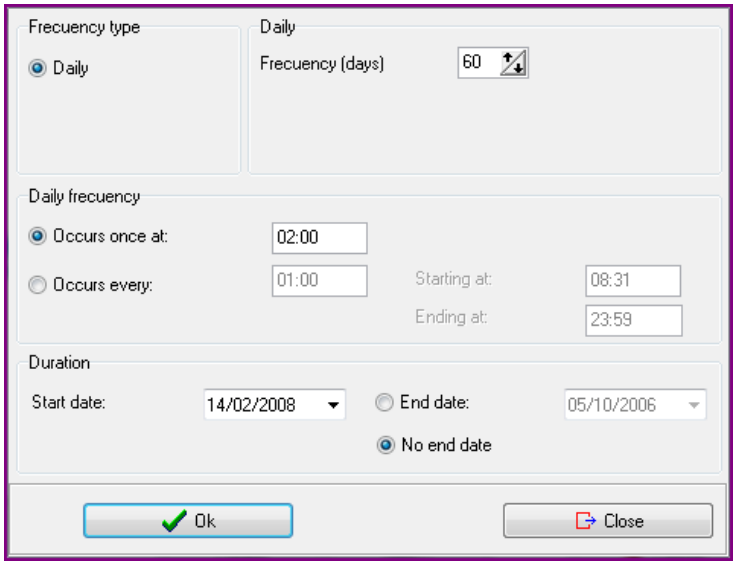
La siguiente ventana muestra las líneas disponibles para realizar el purgado.



Haga doble clic en la línea deseada.

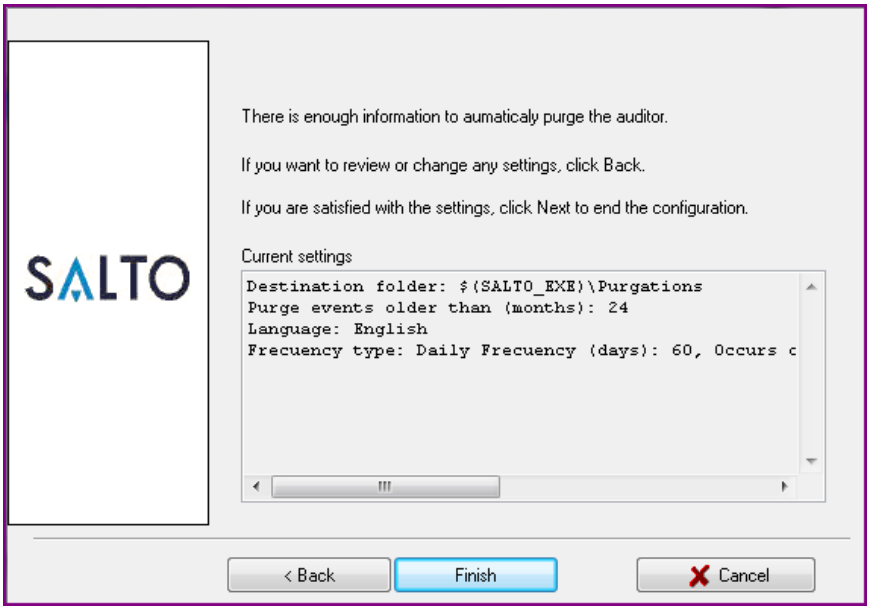


La siguiente ventana muestra la frencuencia de dicho purgado.



Aquí se puede indicar la frecuencia en días, la frecuencia en horas durante el día y el comienzo y fin de la tarea. Según el ejemplo de la lámina de arriba, la tarea se lanzará cada 60 días, a las 02:00 comenzando el 14/02/2008.

Seleccione “Siguiente” y en la siguiente ventana se indicará que hay suficiente información para hacer el purgado además de un resumen de lo programado.



Usuario

El CAMPO DE PROPÓSITO GENERAL PARA USUARIOS se puede habilitar si queremos que aparezca un campo adicional en la ventana de detalles de usuario. Este campo se puede utilizar para introducir un número adicional, por ejemplo el número de pasaporte.

La casilla AUTOINCREMENTAL debe marcarse si queremos que este número se incremente en una unidad, cada vez que creamos un usuario nuevo.

- El PERIODO DE EXPIRACIÓN POR DEFECTO es el tiempo de caducidad dado a un usuario por defecto en su ventana de detalles.

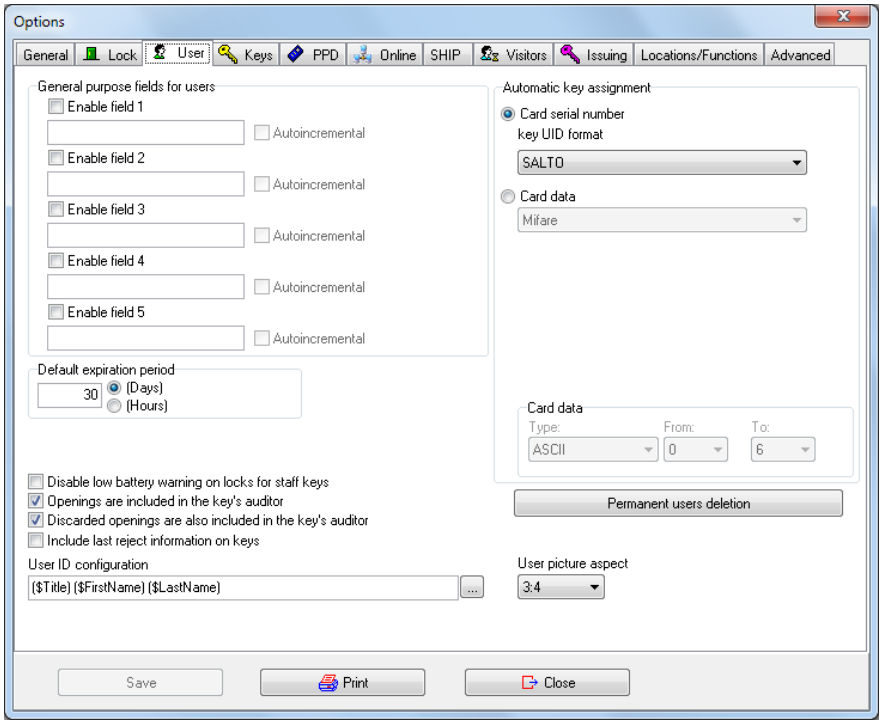
- La casilla DESHABILITAR AVISO DE PILAS BAJAS A LOS USUARIOS se puede marcar si no queremos que las cerraduras den este aviso acústico a los usuarios, porque podemos estar informados del estado de las pilas a través del auditor personal de las llaves.

- La casilla INCLUIR RECHAZOS EN EL AUDITOR DE LAS LLAVES se puede marcar para que en el audit trail personal aparezcan también los rechazos y no sólo las aperturas.

- La casilla INCLUIR INFORMACIÓN SOBRE EL ÚLTIMO RECHAZO se puede habilitar si queremos saber por qué una llave concreta no puede abrir una puerta. Es posible leer la información sobre el último rechazo, leyendo la llave y pulsando el botón CONTENIDO.

Puede seleccionar si los registros de apertura se almacenarán, o no, en el auditor de la llave, así como también si se quieren almacenar los registros de rechazo de apertura. Por defecto, el registro de aperturas está siempre seleccionado.

Disponible en el menú Herramientas/ Configuración/ Opciones Generales / pestaña Usuarios



Escribir información adicional en las pistas

Escribir información adicional en las pistas 1, 2 o 3 para llaves de usuarios:

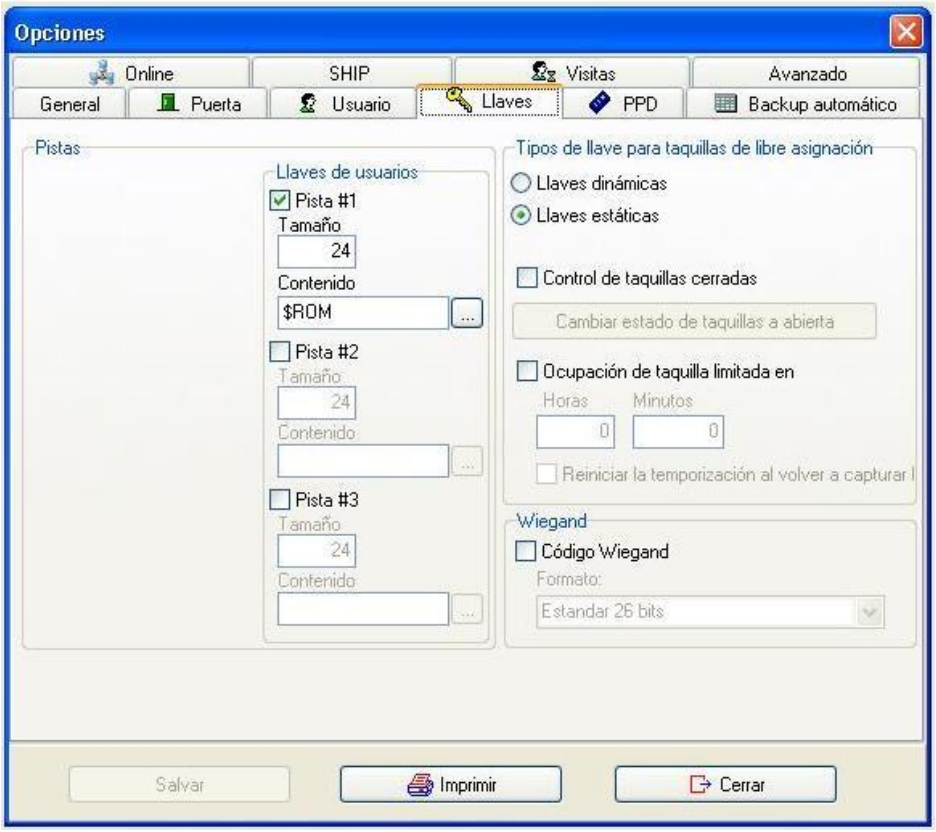
El software incluye la posibilidad de escribir en las pistas 1, 2 o 3.

Para activar el campo donde escribir en la pista, deberemos en un primer lugar ir al menú:

HERRAMIENTAS/ CONFIGURACIÓN/ OPCIONES GENERALES y en la opción llaves veremos las casillas para activar las pistas donde queremos escribir y el número de caracteres o tamaño que le queremos asignar.

Escribir información extra en las llaves de usuarios/clientes.

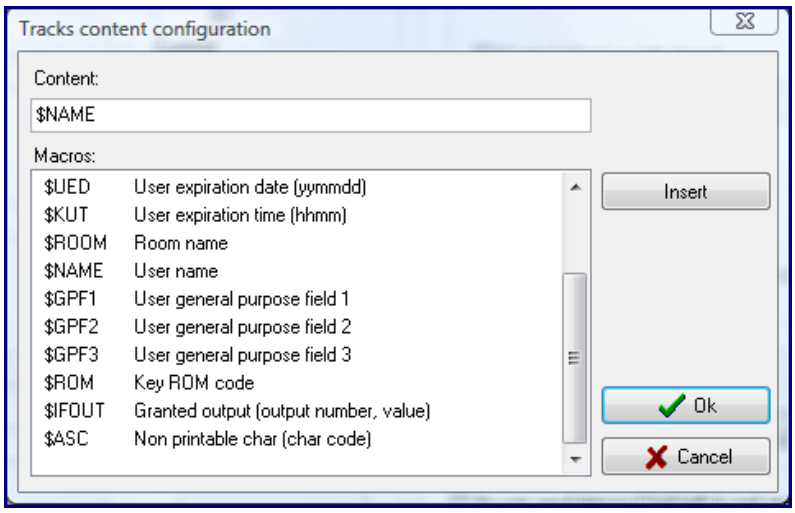
Para escribir información extra en cualquiera de las pistas de la tarjeta debemos ir al menú desplegable HERRAMIENTAS/ CONFIGURACIÓN/ OPCIONES GENERALES/ LLAVES. Nos aparecerá la siguiente ventana (Fig. 1):



(Fig. 1)

En esta ventana podemos seleccionar la pista en la que queramos escribir, el tamaño así como si queremos hacerlo en las llaves de clientes y/o en las llaves de los usuarios del hotel. Además debemos definir el tamaño (número de bytes) que queremos reservar para cada pista.

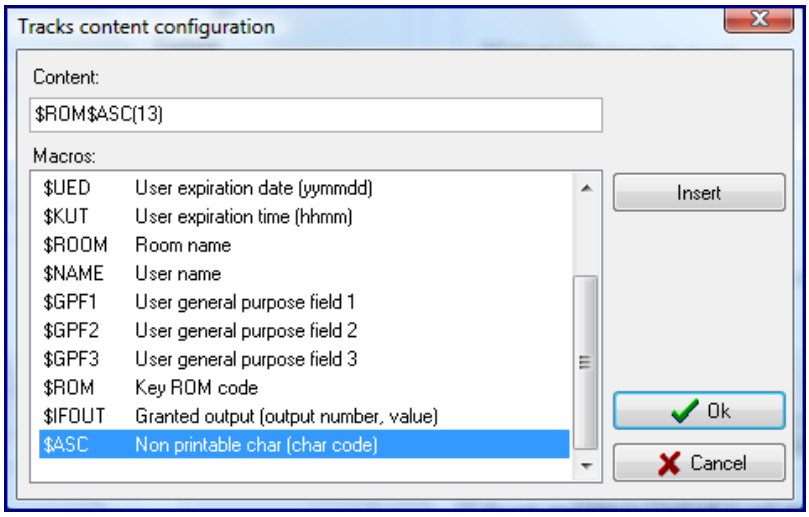
El siguiente paso es seleccionar qué queremos que se escriba en la pista. Para ello pulsamos . Nos aparecerá la siguiente pantalla (Fig. 2)

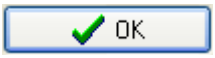


(Fig. 2)

En esta pantalla seleccionaremos el macro o macros que queramos que se escriban por defecto cada vez que se edite una nueva llave. El software nos permite también escribir un valor constante delante o detrás de cada macro. Para ello, lo escribiremos antes o después del macro en la ventana de contenido.

Se ha añadido una nueva macro para poder introducir caracteres ASCII como el "ENTER".



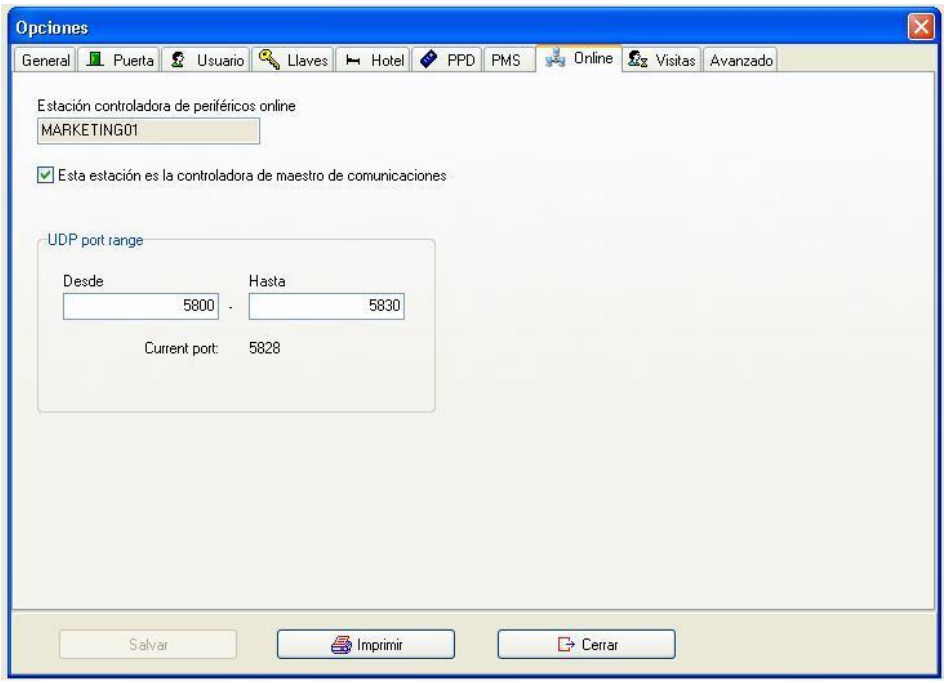
Finalmente pulsamos 

. A partir de este momento, cada vez que emitamos una llave aparecerán escritos estos macros en la pista o pistas seleccionada.

Rango de puertos

Por defecto PA puede trabajar en un rango de puertos que van de 5000 a 10000. Ocurre que por razones de seguridad en la red hay que limitar el rango de esos puertos.

En el software Salto es algo muy fácil de configurar. Ir a herramientas/Configuración/Opciones generales/Online:



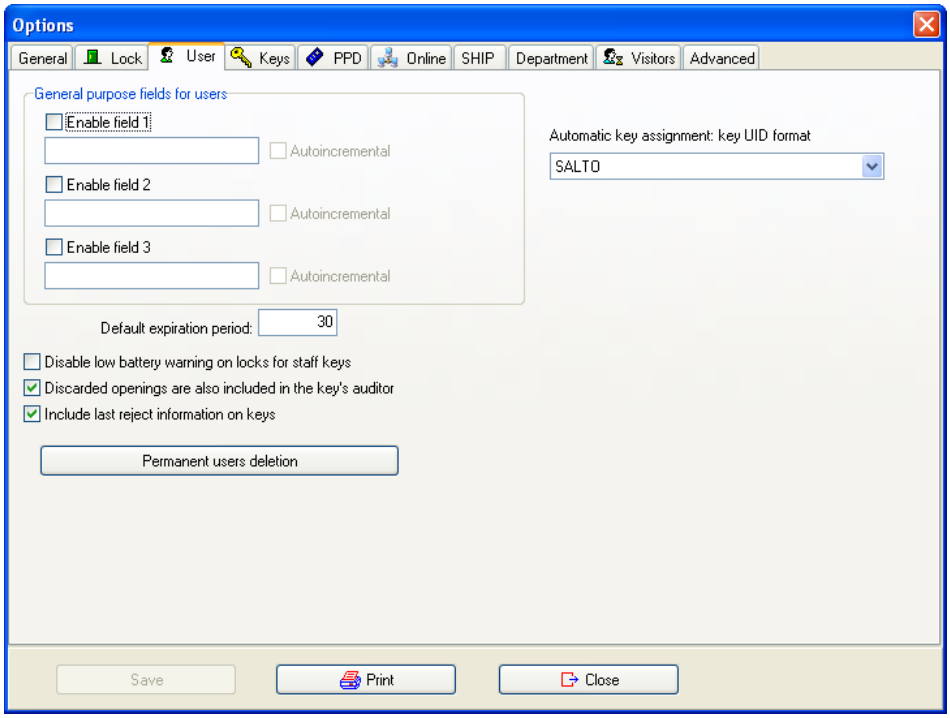
En los campos UDP podemos delimitar los rangos de los puertos en los cuales queremos que trabaje la aplicación. Incluso si hiciera falta podríamos trabajar con un puerto específico escribiéndolo en ambos campos.

Eliminación de usuarios permanentes

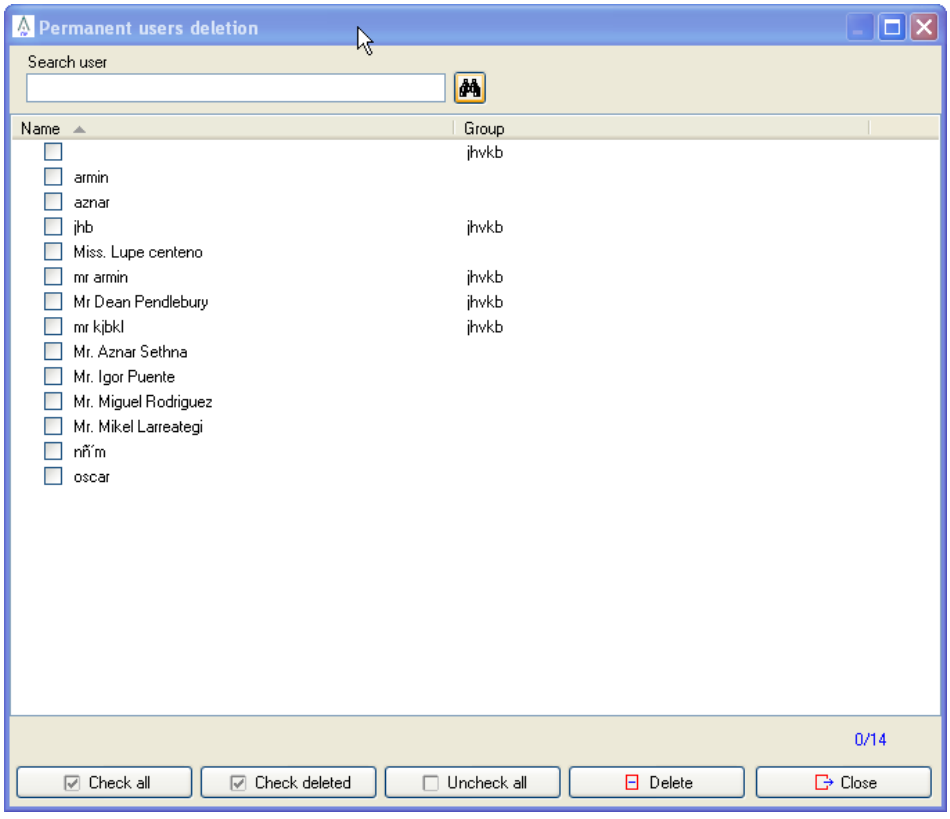
Por medio de esta opción podemos eliminar usuarios de forma permanente a los que nunca se les ha asignado una llave.

Para activar esta opción hay que ir a:

Herramientas/Configuración/Opciones generales e ir a la ventana de usuarios y pulsar la opción "Eliminar usuarios permanentemente"



Entonces la siguiente ventana se mostrará:



Aquí se muestran los usuarios que nunca han tenido asignada una llave, por lo cual serán los podrían ser permanentemente

eliminados. Simplemente hay que seleccionar los que queremos eliminar.

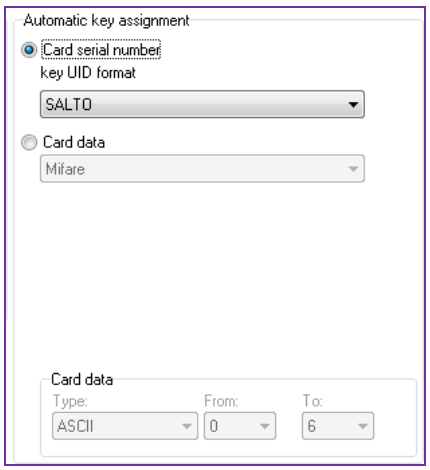
Asignación automática de usuarios

Por medio de esta prestación el sistema podrá asignar llaves de forma automática a los usuarios. Para ello es necesario, por medio de la sincronización de bases de datos, asignar el código ROM/UID de la tarjeta.

Entonces, se puede elegir el formato UID de la tarjeta. (Salto, Mifare, Desfire, HID)

También es posible usar un código diferente al código ROM/ Serie. Se puede usar cualquier otro código que se alojará en un sector concreto en la llave especificado por el fabricante o el propietario de la llave.

En las opciones avanzadas, pestaña Usuario, se puede ver una ventana como la siguiente donde se puede seleccionar qué UID se quiere utilizar para la asignación automática, número de serie de la llave o un dato pregrabado en la llave.

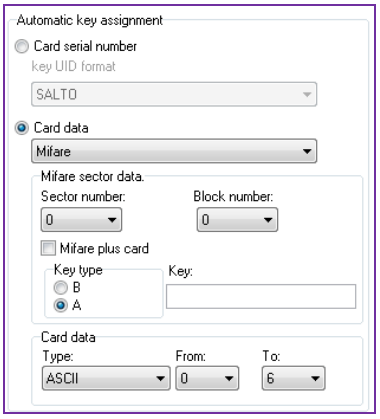


Al usar el UID de la propia llave, a continuación, se deberá seleccionar el formato del UID dependiendo de la tecnología. (SALTO, Mifare, DESfire o HID)

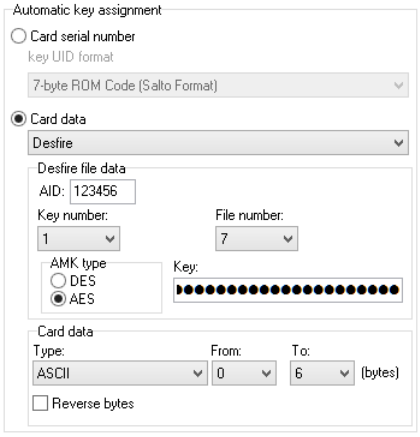
Si se usan tecnologías como Mifare y DESfire y además se va a usar un código diferente del UID, entonces se deberá seleccionar "Datos en tarjeta"

En la parte "Sector de datos Mifare" es necesario seleccionar el sector y el bloque donde se encuentra el código. Si el sector está protegido, será necesario introducir el tipo de clave y la clave de

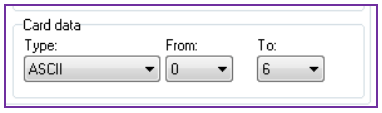
desbloqueo pudiendo ser la clave A o la B. En caso de usar tarjetas Mifare Plus, seleccionar la opción "Tarjetas Mifare Plus"



Para la tecnología DESFire, es necesario introducir el AID, identificación de la aplicación de la llave. A continuación, introducir el número de clave y el número de fichero en caso de que la aplicación use más de uno. Seleccionar el tipo de clave AMK, DES o AES e introducir la clave.



En "Datos de tarjeta" debe introducir la localización exacta del código, es decir, a partir de qué byte y hasta qué byte se encuentra el código.



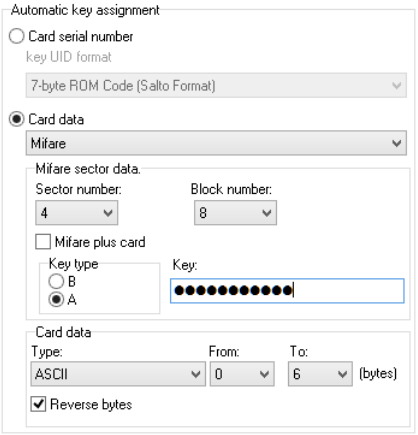
Los "Datos en tarjeta" especifican el formato de la información según lo siguiente:

- ASCII
- WIEGAND (HEX)
- WIEGAND (HEX SWAP) - Nibble swap

Esta información debe ser suministrada por el sistema a integrar.

Diferecia entre los formatos Wiegand:

- Wiegand (HEX): 1A2B3C4D
- Wiegand (HEX SWAP): A1B2C3D4



Además de los distintos tipos, también se puede utilizar la opción de "Invertir bytes" para adaptarse a las necesidades de la integración.

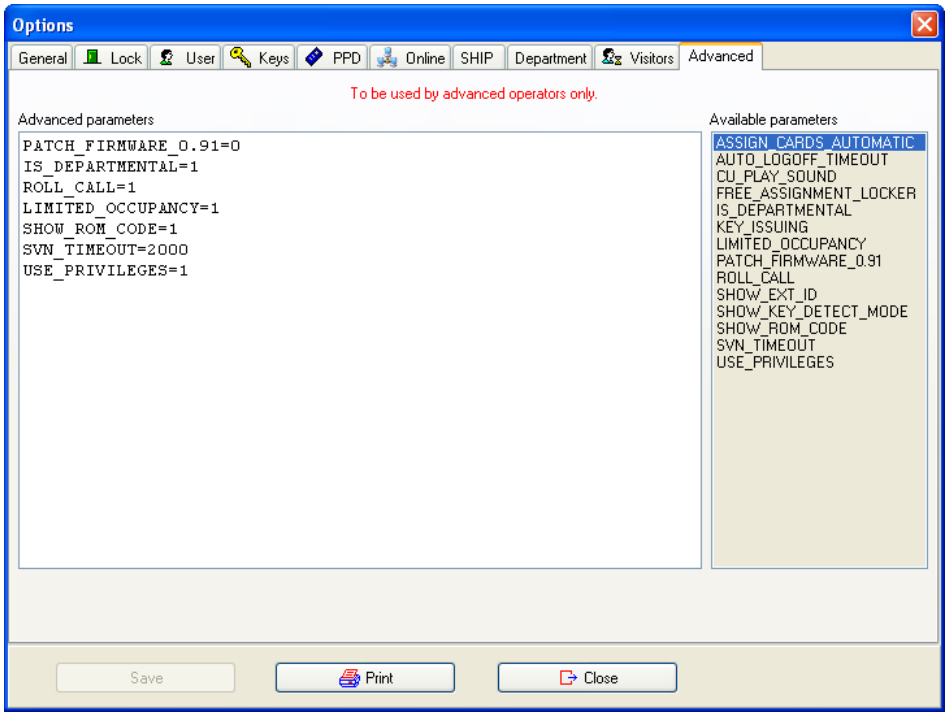
Ej.

- Wiegand (HEX): 1A2B3C4D
- Wiegand (HEX) + Invertir bytes: 4D3C2B1A

Para activar esta prestación en el software hay que ir a Herramientas/Configuración/Opciones generales y en los parámetros avanzados activar la opción "ASSIGN_CARDS_AUTOMATIC"

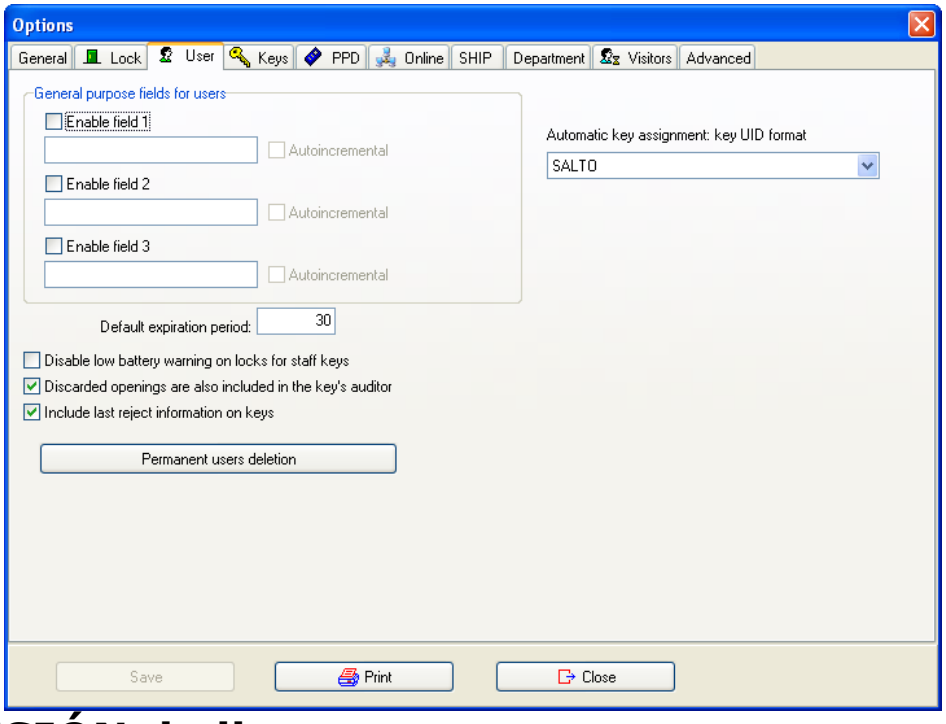
Para utilizar la asignación automática, se puede presentar una llave vacía ante un editor o también ante un lector mural. En caso de usar un editor, este deberá programarse como actualizador. No hay necesidad de programar ningún modo especial para los lectores murales, el estar en modo actualizador SVN será suficiente.

La versión mínima de FW debe ser la siguiente;
Ethernet: versión **01.41** o superior.
CU5000: versión **02.02** o superior.
WR: versión **02.65** o superior.



Entonces hay que elegir el formato UID de la tarjeta. (Salto, Mifare, Desfire, HID)

Para ello hay que ir a Herramientas/Configuración/Opciones generales/ Usuarios. En esta ventana se puede seleccionar el formato UID de la tarjeta:



EMISIÓN de llaves

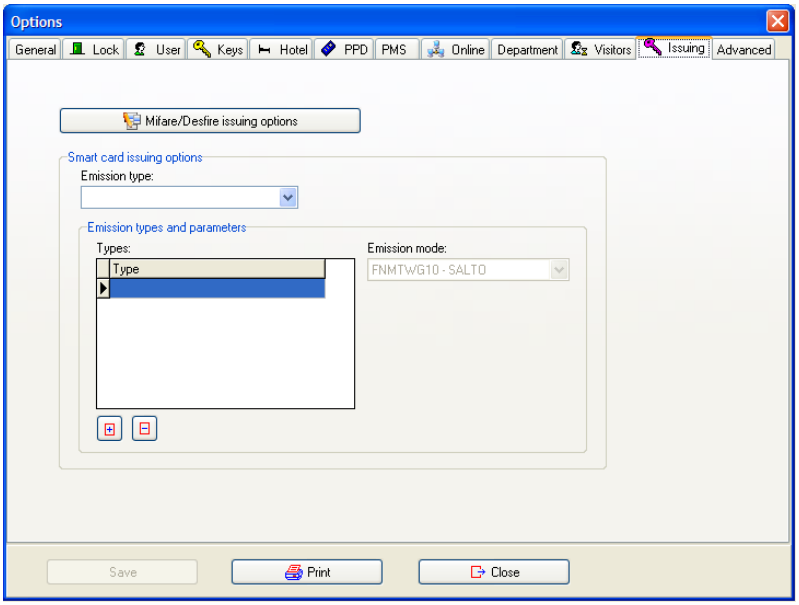
La emisión de la llave se define al proceso de configurar una nueva llave para su posterior utilización en el sistema Salto. Normalmente los usuarios reciben las llaves ya emitidas por Salto (como las azules, rojas y amarillas Smart o iButtons). Estas llaves se pueden utilizar en cualquier instalación.

Sin embargo ciertas instalaciones requieren que sus llaves sean emitidas en la instalación de acuerdo a algunas especificaciones. Una vez emitidas estas llaves en la propia instalación ya no podrán ser usadas en otra distinta. El RW software ofrece ahora la herramienta para poder emitir la llave.

Actualmente se pueden emitir los siguientes tipos de llaves:

- Smart (consultar referencias)
- Picopass
- Mifare
- Desfire
- Mifare Plus
- Legic

Una vez activada la opción KEY_ISSUING=1 en los parámetros avanzados, se mostrará una nueva pestaña con el nombre de "Emisión" (ver figura siguiente).



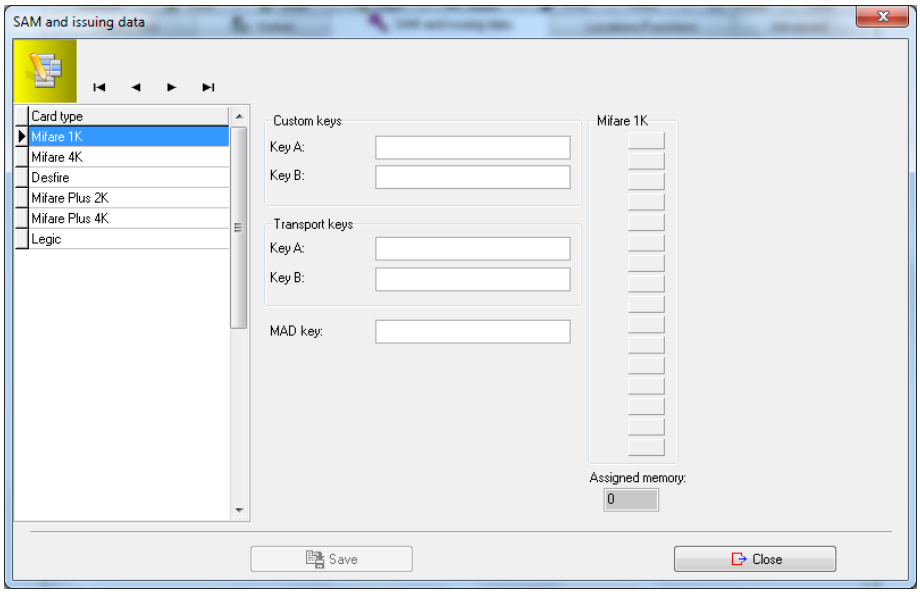
En el caso de tarjetas Mifare/Desfire, se debe disponer de un SAM kit con su correspondiente tarjeta y claves.

ATENCIÓN: la modificación de los siguientes parámetros se tiene que llevar a cabo únicamente bajo la supervisión de

un técnico certificado por SALTO Systems. SALTO Systems no se hará responsable de los posibles daños causados por una mala utilización de esta herramienta.

Llaves MIFARE

Para acceder al menú de configuración de parámetros pulsar sobre el botón "Opciones de emisión Mifare/ Desfire".



Seleccionar el tipo de tarjeta utilizado en la instalación:

- Mifare 1K
- Mifare 4K
- DESfire
- Mifare Plus 2K
- Mifare Plus 4K
- Legic

En el campo "Claves propias" copiar las claves suministradas por Salto junto con el SAM kit.

Los campos "Claves de transporte" son opcionales y contendrán las posibles claves del propio suministrador de las llaves.

La clave MAD se utiliza para desbloquear dicho sector en el caso que una aplicación externa necesite utilizarlo.

La casilla situada debajo de la clave MAD se debe activar en el caso de que se quiera gestionar automáticamente la selección de sectores si los seleccionados se encuentran ocupados.

El botón LEER TARJETA SAM se utiliza para capturar las claves desde la tarjeta SAM (de la misma manera que se hace con el software SAM).

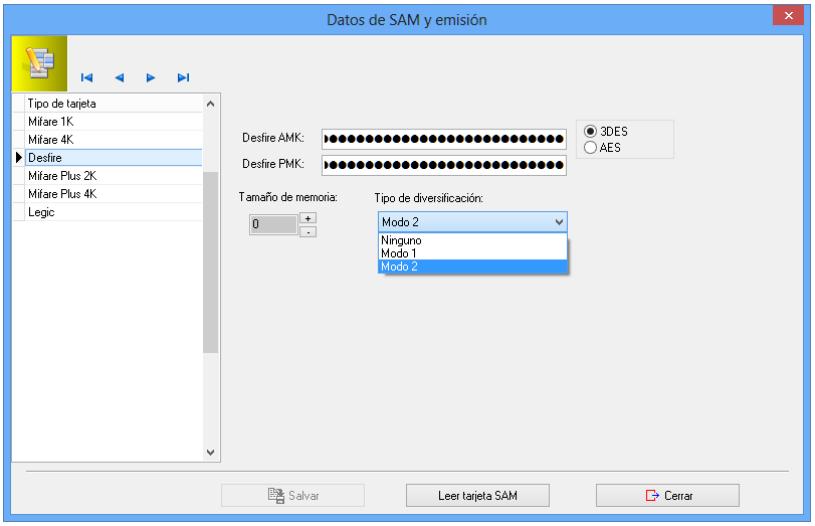
Por razones de seguridad, las claves se ocultarán al pulsar el botón SALVAR.

AUMENTO DE SECTORES EMITIDOS

Al usar emisión de llave desde el software de Salto, es posible aumentar la cantidad de sectores emitidos después de la emisión inicial. Esta operación es posible solo si se poseen claves SAM distribuidas por Salto y usando llaves de terceros.

Para añadir más sectores a una llave, desde la pestaña "Emisión" de las opciones generales, se deben seleccionar los sectores que se desean añadir. Para que el cambio tenga efecto en la llave es necesario actualizar la llave desde la opción Llaves/ Emitir llaves.

DESFire Evolution 1



En esta versión se incluye la posibilidad de trabajar con este tipo de tecnología. Con capacidades de 4kbytes y 8kbytes estas tarjetas utilizan encriptación AES128bits mucho más compleja y segura que la ya robusta 3DES.

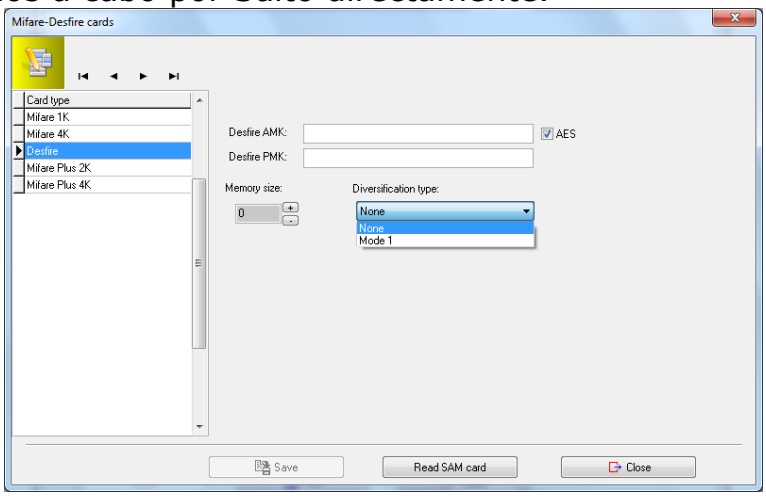
La opción AES se activará en el caso de ser necesario este nivel de encriptación (*). Salto suministrará una PMK ligada a este tipo de tecnología.

(*) Las tarjetas DESFire EV1 pueden utilizarse igualmente junto con una encriptación 3DES.

PMK diversificada

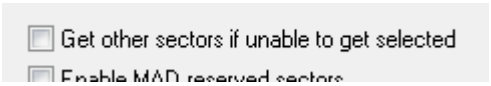
Cuando vayan a usarse tarjetas Desfire, puede seleccionarse el Tipo de Diversificación en la pantalla de configuración de las tarjetas Desfire, como puede verse en la figura superior.

Nota: Esta opción solo se usará en proyectos específicos llevados a cabo por Salto directamente.



MIFARE PLUS

Como puede ver en la imagen de arriba, se pueden seleccionar tarjetas Mifare Plus 2k o 4K. La opción "Capturar otros sectores si los seleccionados están ocupados" no está disponible en Mifare Plus en comparación con Mifare 1K y 4k.



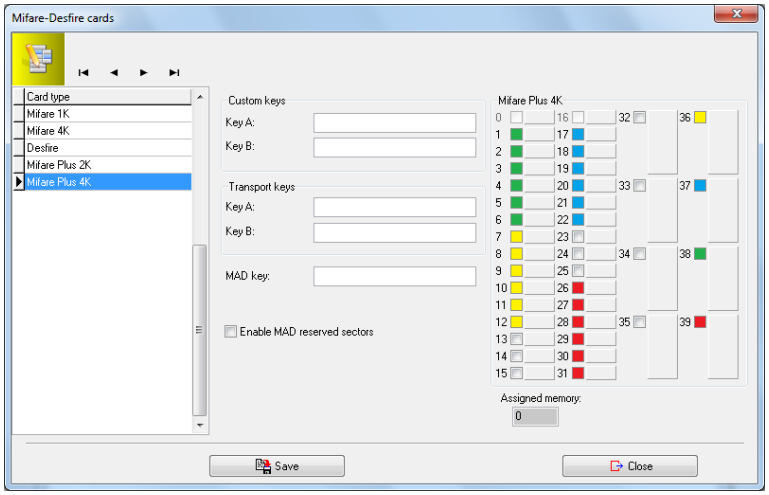
Esta es una limitación de la tarjeta, obliga saber la distribución de los sectores que se quieren usar, necesario para saber qué sectores están disponibles, para ser asignados o configurados en el software.

En este caso, hay que tomar en cuenta de que no se puede usar la auto-detección.

En el caso de que sea necesario emitir sectores para varias instalaciones en la misma llave, hay que tener en cuenta de que las CLAVES SALTO ORIGINALES no podrán ser usadas.

En caso de que una instalación vaya a usar la misma llave, tenga en cuenta que los últimos 4 sectores de las llaves DEBEN ser asignados para cada instalación, siendo 4 el máximo de instalaciones posibles en una llave.

El ejemplo de abajo muestra la combinación de los sectores con diferentes colores. Tenga en cuenta de que deferentes instalaciones puedan necesitar más o menos memoria que la seleccionada en la imagen y que los sectores seleccionados no tienen que estar uno al lado del otro obligatoriamente.



LEGIC PRIME y ADVANT

STAMPS

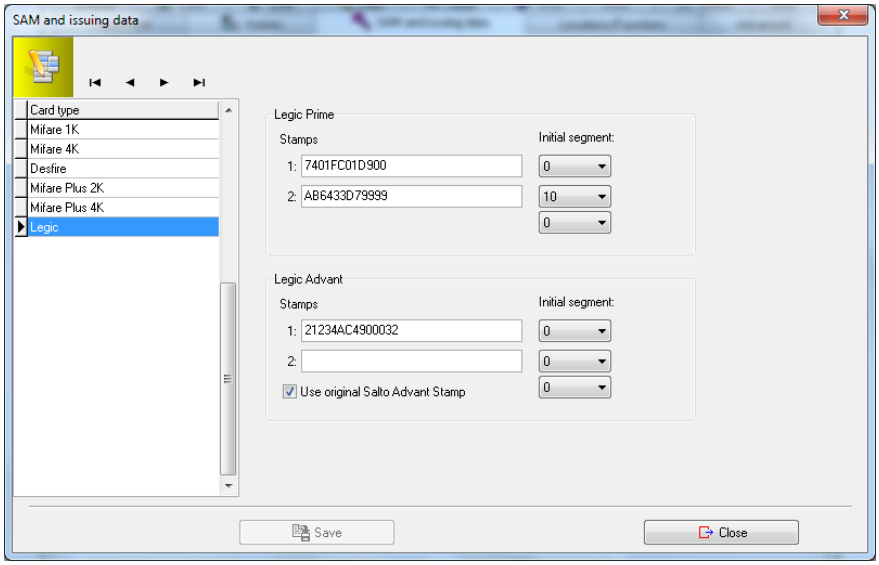
Los dispositivos Legic de SALTO se suministran con el stamp SALTO original. Los stamps forman parte del proceso de SAMeo y personalización.

Ir a "HERRAMIENTAS/CONFIGURACIÓN/OPCIONES GENERALES/DATOS DE SAM Y EMISIÓN".

Rellenar los campos dependiendo del tipo de tarjeta que se vaya a utilizar: STAMPS de Legic Prime (6 bytes hex) o Advant (7 bytes hex).

Los lectores de Salto pueden contener hasta 3 STAMPS diferentes:

- STAMP 1
- STAMP 2
- STAMP Original Salto



Los lectores SOLO podrán leer UNO de los segmentos de una misma tarjeta.

Si se usa un STAMP original Salto, cualquier llave Legic original de Salto podrá utilizarse.

SEGMENTO INICIAL

En "Segmento Inicial" seleccionar a partir de donde empezará la búsqueda del STAMP de Salto. Si se desconoce, dejar el valor a **0.** De esta manera, los lectores sabrán donde se encuentra la aplicación y acelerarán el proceso de búsqueda.

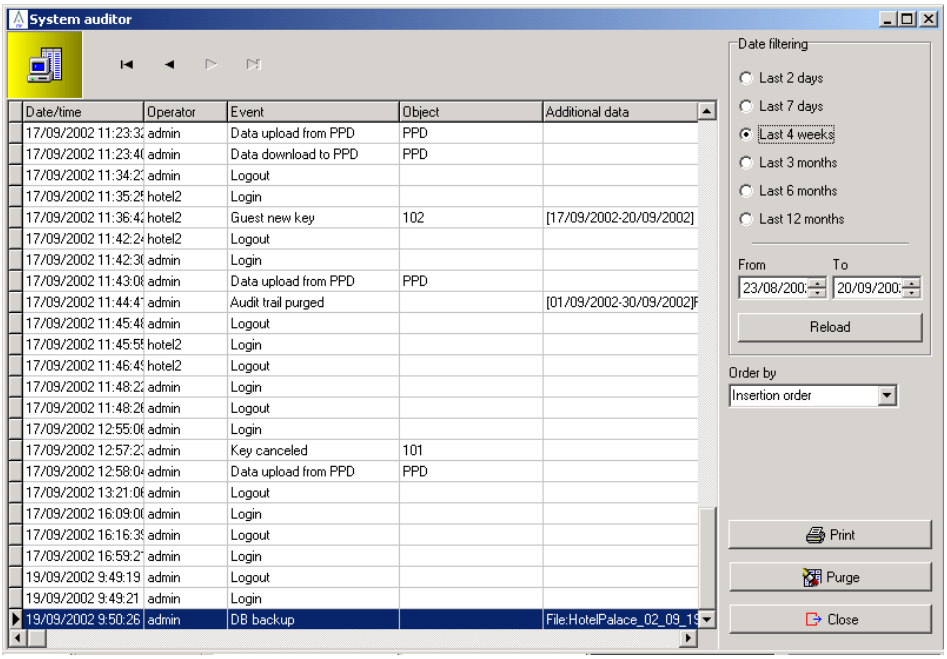
Si el parámetro seleccionado es erróneo, el lector podría no encontrar la aplicación en la tarjeta.

Los segmentos podrían compararse a carpetas donde la entidad que emite las llaves colocará las diferentes aplicaciones. Existen 128 segmentos, desde el 0 al 127.

Para más información, dirigirse al manual "Legic Prime and Advant SAMING Process".

Auditor

El menú HERRAMIENTAS presenta algunas opciones más que resultan muy prácticas. Si se pincha la opción AUDITOR se abrirá una ventana como la siguiente:



En esta ventana se indican todas las operaciones que han sido realizadas por los operadores del software.

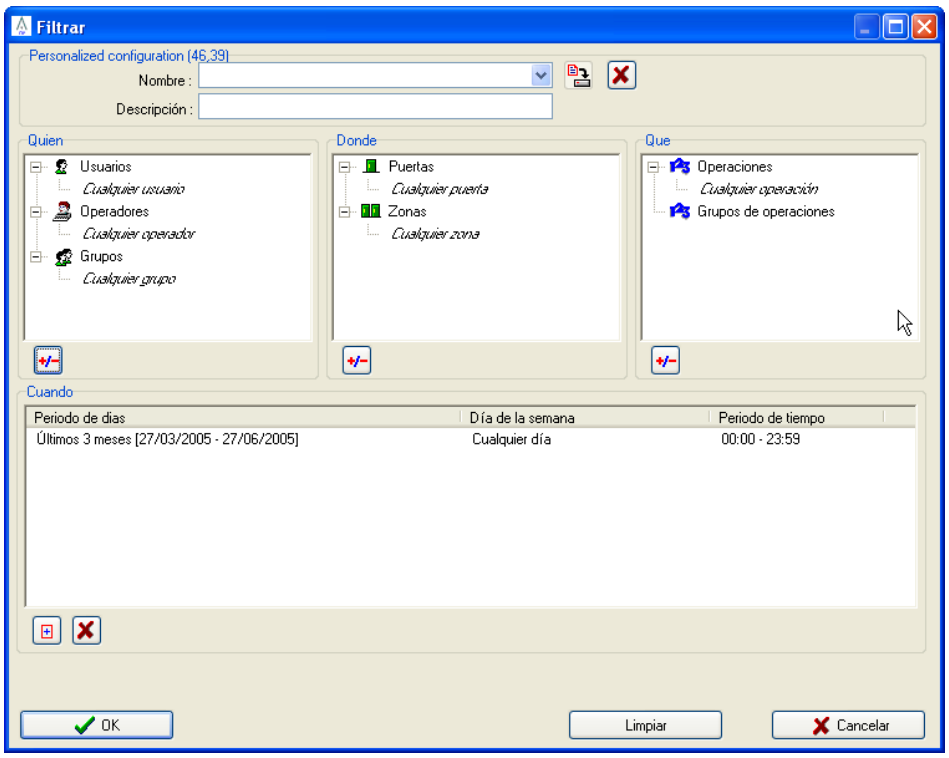
El orden en que aparecen puede ser modificado para ser visualizadas por operador, por operación, etc... Para ello haga clic en el botón ORDENAR POR.

Si usted quiere una copia en papel de este informe, bastará con pulsar el botón IMPRIMIR siempre que tenga una impresora conectada y en línea con el ordenador.

Cuando pasa mucho tiempo y la lista de AUDITOR es muy larga, empieza a ocupar demasiado espacio de memoria. Para liberar memoria, pulse el botón PURGAR y así limpiará los registros más antiguos.

Filtro avanzado

Para realizar y guardar filtros especiales debemos pulsar el botón "Filtrar" en la ventana del Auditor de Cerraduras. Una vez pulsado nos aparecerá la siguiente ventana (Fig.1):

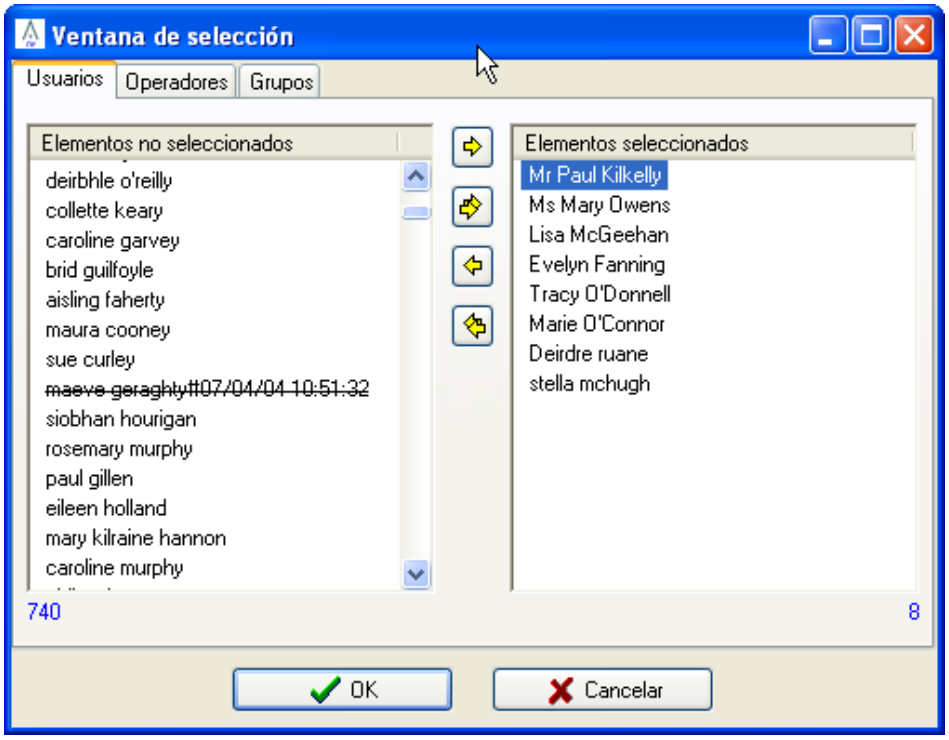


(Fig 1)

Este filtro permite filtrar los eventos por Quién (usuario, operador y/o nivel de acceso) lo ha realizado, Dónde (Puerta, Zona) lo ha realizado, Qué operación o tipo de operación ha realizado y Cuándo la ha realizado.

Crear un filtro nuevo:

Debemos seleccionar quién o quienes queremos filtrar para ello pulsamos el botón de la parte inferior de la ventana Quién. Nos aparecerá la siguiente ventana de selección: (Fig. 2):

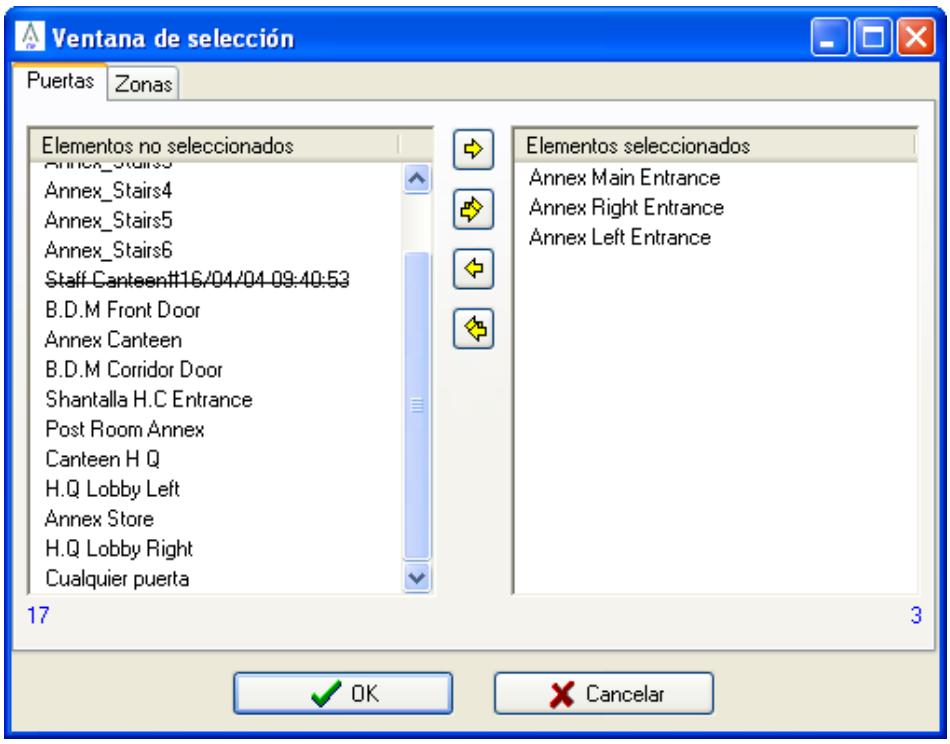


(Fig. 2)

Seleccionamos aquellos usuarios que queramos filtrar, de la misma manera seleccionaremos los operadores y/o nivel de accesos de usuarios que queramos filtrar.

Nota: Si queremos que aparezcan todos los usuarios, operadores, nivel de accesos dejaremos al lado derecho de la ventana la opción cualquier usuario, cualquier operador y/o cualquier nivel de acceso.

La siguiente selección es la de Dónde. Esta ventana nos permite seleccionar las Puertas y/o Zonas que queramos filtrar. Volvemos a apretar el botón para seleccionar las puertas y/o zonas que queramos filtrar. (Fig. 3)



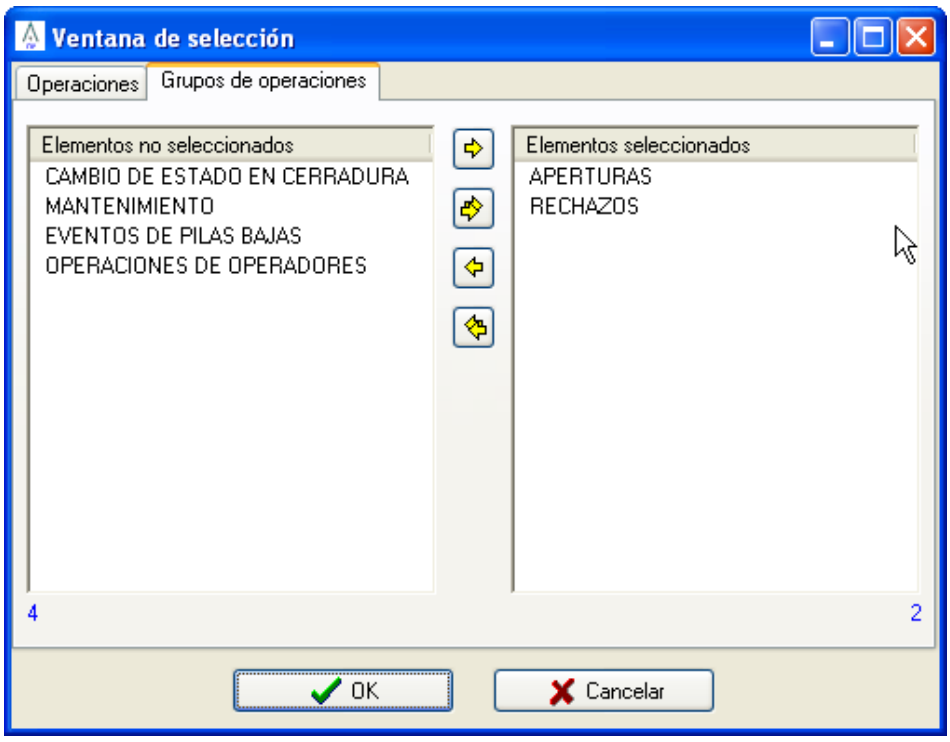
(Fig 3)

De la misma manera incluiremos las zonas que queramos filtrar.

Nota: Si queremos mostrar los eventos en todas las puertas y/o zonas seleccionaremos la opción "cualquier puerta", "Cualquier zona".

El filtro permite además seleccionar la operación o nivel de acceso de operación que queramos filtrar. Para ello, pulsamos de nuevo el botón

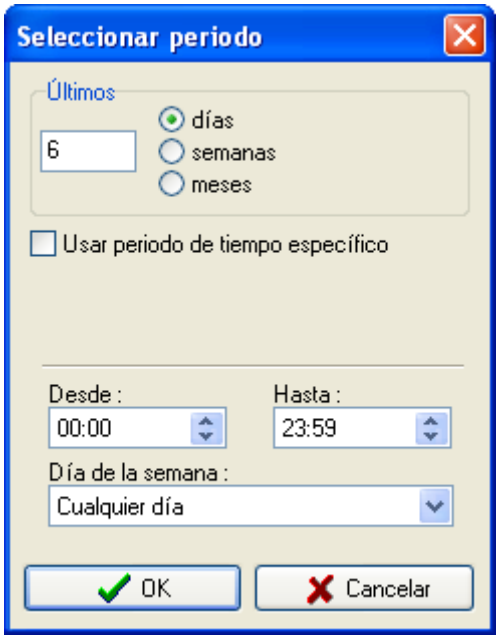
y seleccionamos la operación o nivel de acceso de operaciones que queramos filtrar. (Fig 4)



(Fig. 4)

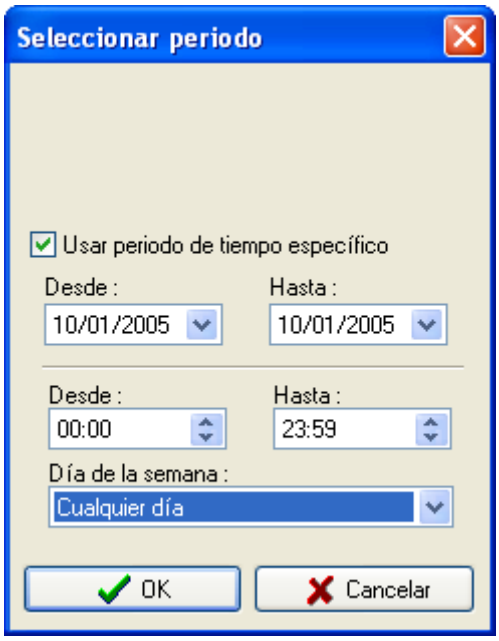
Nota: Si queremos ver todas las operaciones que han realizado estos usuarios seleccionaremos "Cualquier operación"

Por último, podemos seleccionar las fechas de nuestro filtro. Para ello pulsamos el botón y nos aparecerá la siguiente ventana (Fig 5):



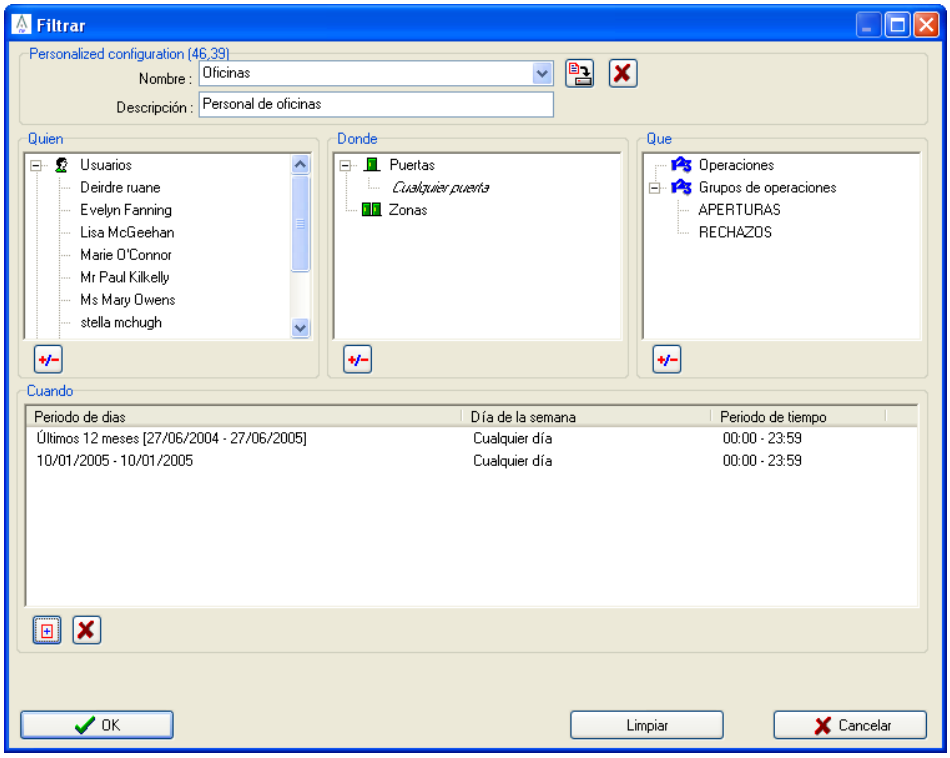
(Fig. 5)

Esta ventana nos permite definir el periodo del filtro: seleccionando los últimos días, semanas y/o meses o por otro lado seleccionar el periodo entre dos fechas (activando la opción "Usar periodo de tiempo específico" Fig. 6) así como el día o días de la semana que nos interese filtrar.



(Fig. 6)

Una vez realizada la selección completa del filtro, Nos aparecen todas nuestras selecciones en la pantalla: (Fig. 7)



(Fig. 7)

Para ver el resultado de nuestro filtro pulsamos el botón

El filtro seleccionado se podrá exportar a un fichero txt. , xls.. Pulsando la opción exportar.

Guardar el filtro:

El software permite además guardar estos filtros para futuras ocasiones. Para ello pulsar el botón . Debemos rellenar los campos nombre y descripción.

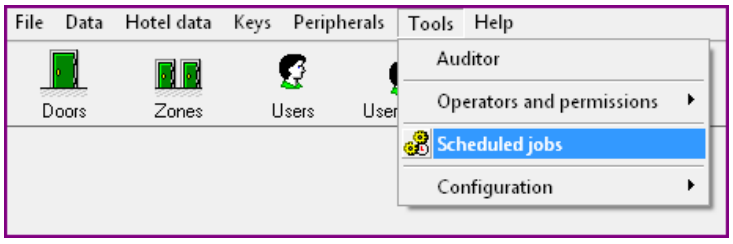
Exportación automática del Auditor de cerraduras

(solo software para Servicio)

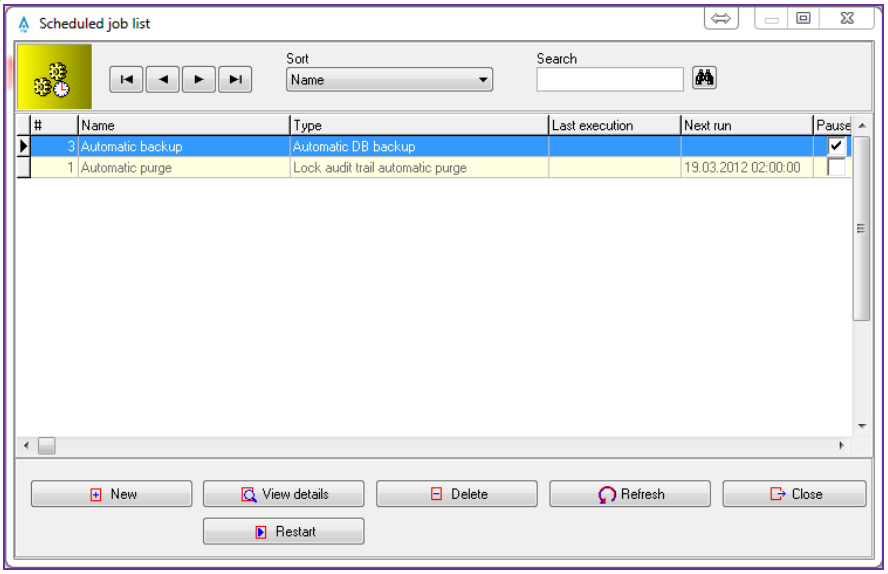
Es posible configurar el programa de Salto para hacer exportaciones automáticas del auditor de cerraduras a ficheros CSV. Esta operación exportará el auditor sin borrar los datos el programa, de esta manera será posible consultar el auditor desde el propio programa de Salto. Esta exportación permitirá entregar las diferentes operaciones de apertura a cualquier programa de terceros, como por ejemplo, para un reloj de fichar.

Hay que tener en cuenta que en cuanto se purguen los datos del auditor de cerraduras, la auto exportación dejará de funcionar por el hecho de que no hay dato que exportar.

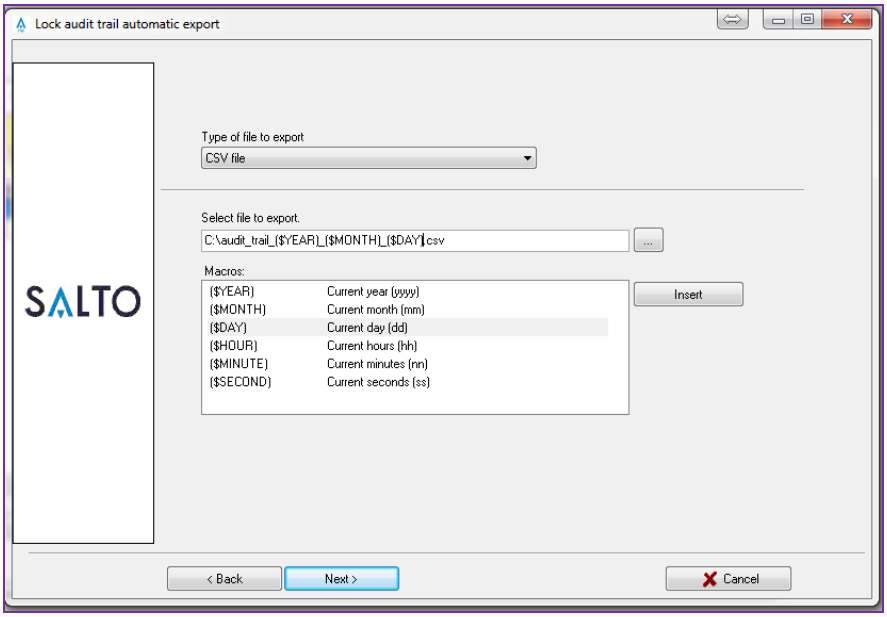
Para activar la auto exportación, es necesario abrir las "Tareas Programadas" del menú "Herramientas".



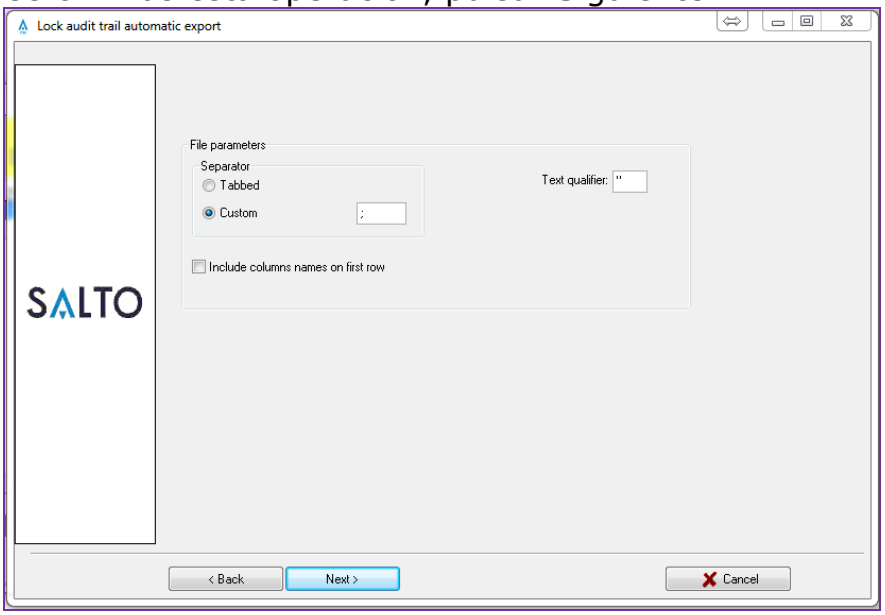
En la lista, se verán las demás tareas programadas ya creadas en el sistema. Para activar la exportación automática, crear una nueva tarea, y seleccionar desde el menú desplegable "Exportación automática del auditor de cerraduras" y al presionar OK, el menú de configuración comenzará.



Aparecerá el configurador donde podrá seleccionar donde colocar el fichero con los eventos exportados así como su nombre.

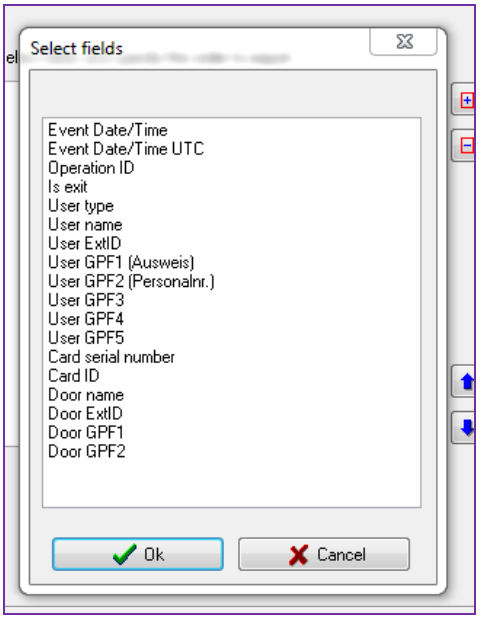


En el ejemplo de la pantalla anterior, el fichero se guardará en C:\ y su nombre será "audit_trail_($YEAR)_($MONTH)_($DAY).csv". Esto significa que si la exportación se hace el 24/01/2012, el nombre del fichero será "audit_trail_2012_01_24.csv". Al usar los MACROS a la creación del fichero, se evitará la sobre-escritura y pérdida de ficheros anteriores. Para añadir el macro, colocar el cursor en la posición deseada en el campo del nombre y presionar en "Insert". Tras esta operación, pulsar Siguiente.

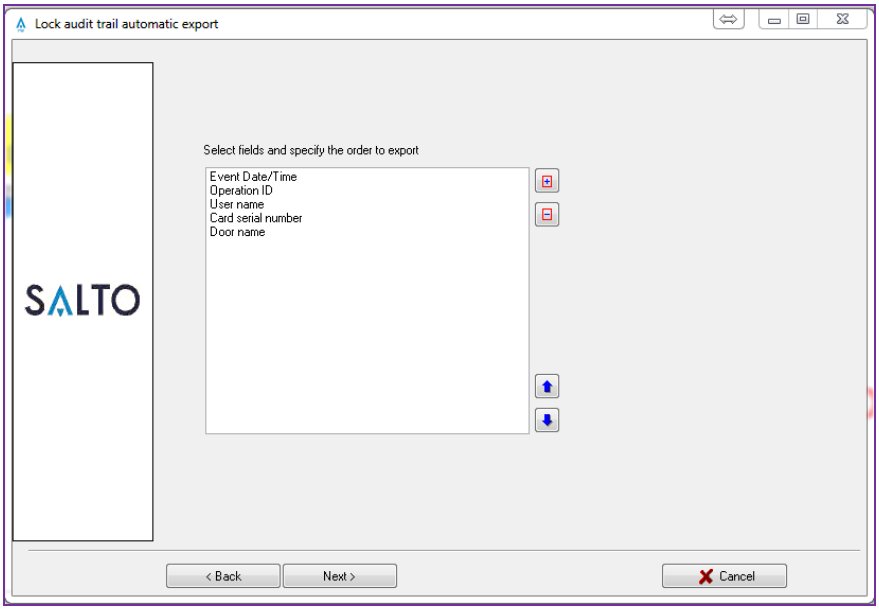


En la siguiente ventana se especifica cómo se ordenará el texto en el fichero. Se puede seleccionar qué separador se usará entre columnas, el cualificador de texto y también si se quiere añadir el nombre de las columnas en la primera línea cada columna exportada. Por defecto, el separador usado es ";" y cuando el nombre contiene un espacio, el cualificador de texto "". Presionar siguiente para continuar.

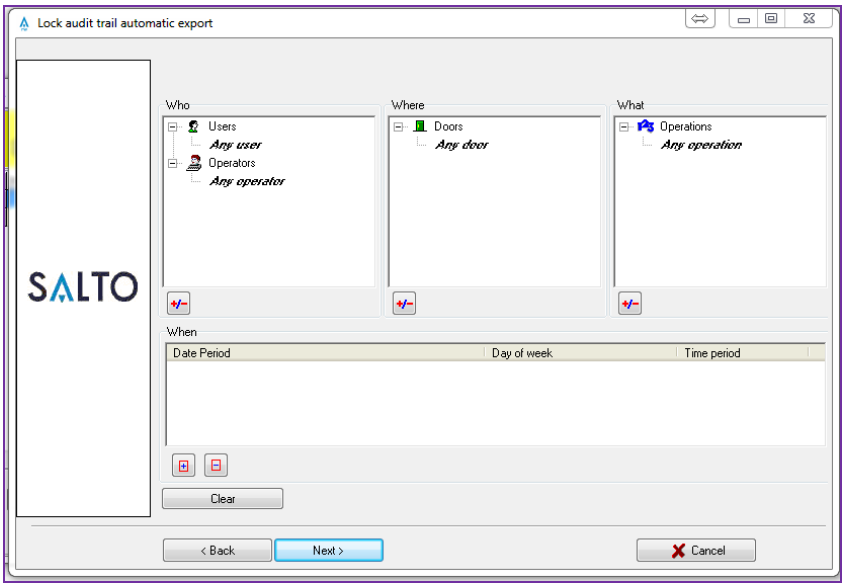
En este punto podemos seleccionar, QUÉ queremos exportar y en qué orden. Al presionar en +, se añadirán los valores a la lista. Para más información sobre el significado de cada valor, ver el documento "SALTOAutomaticExportOfAuditTrail_1_0.pdf" o versión posterior. Si es necesario, contactar con el departamento técnico de SALTO.



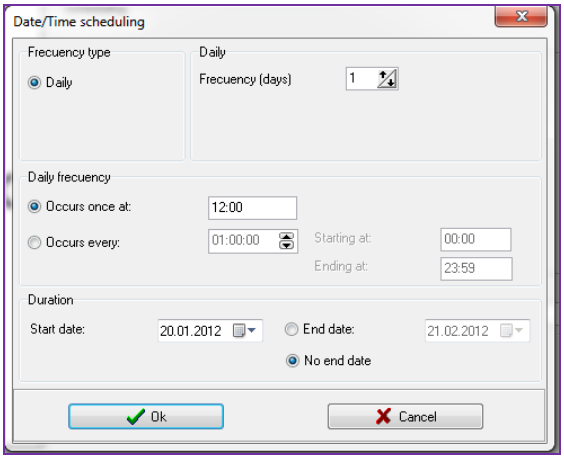
Una vez seleccionados los campos, presionar en OK. En la imagen de abajo, se ve un ejemplo de los campos más comunes.



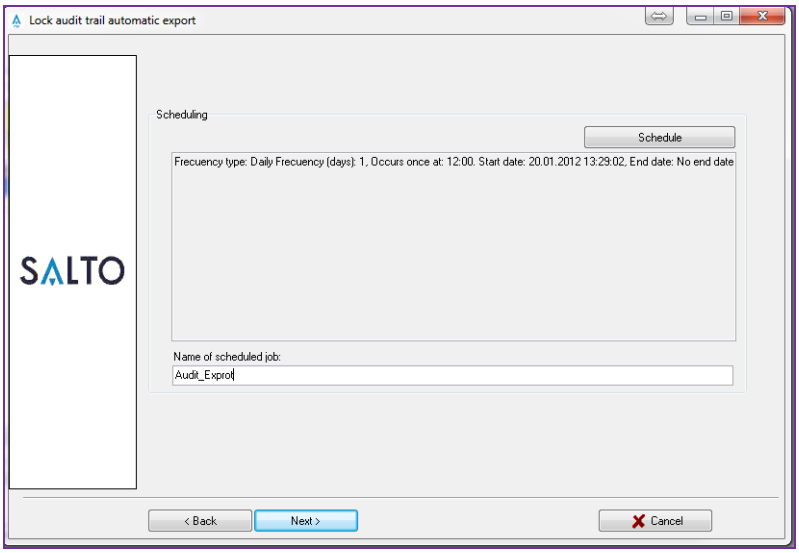
A continuación, se puede filtrar las partes deseadas a exportar. Si se deja como viene por defecto, se exportarán todos los usuarios, todas las puertas, todas las operaciones y qué periodo del auditor desea exportar, como el último mes por ejemplo. Siguiente para continuar.



En la última parte del configurador, se debe planear CUANDO la tarea se lanzará. Presione en "Planificar". En la siguiente pantalla se puede seleccionar la frecuencia en días, en qué momento del día o cada cuanto se lanzará la tarea.



En el ejemplo de arriba, la tarea se ejecutará cada día a las 12:00 a partir del 20/01/2012 sin fecha de conclusión. Mientras la tarea esté activa, la ejecución de la tarea se lanzará. También es posible pausar la tarea o borrarla.



Finalmente, aparecerá en pantalla, un breve resumen de la configuración de la tarea. Presionar en Finalizar para salvar la programación y la tarea se lanzará según el periodo programado. La primera tarea puede demorarse unos minutos hasta que el servicio se actualice. Aquí debajo, se puede ver un ejemplo de un auditor exportado:

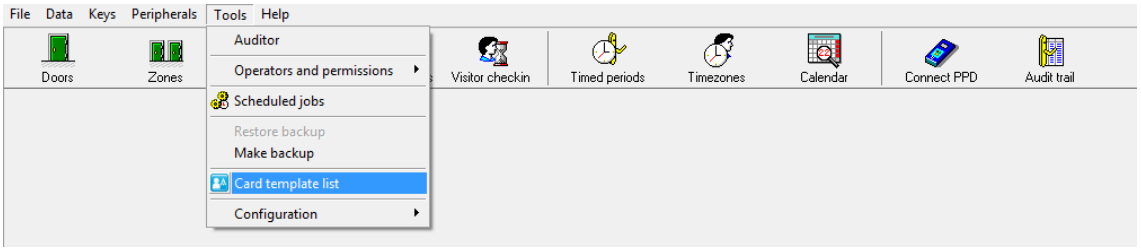
2012-01-19T09:50:36	79			Online_Koffer
2012-01-19T09:50:42	28	admin		Online_Koffer
2012-01-19T09:52:34	79			Online_Koffer
2012-01-19T09:53:10	79			Online_Koffer
2012-01-19T09:55:36	72			Online_Koffer
2012-01-19T09:55:56	17	Dr. Max M 1234	4E4C3A53000000	Online_Koffer
2012-01-19T09:56:06	17	Dr. Max M 1234	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

Para más detalles o información más técnica, ver el documento "SALTOAutomaticExportOfAuditTrail_1_0.pdf"

Badging

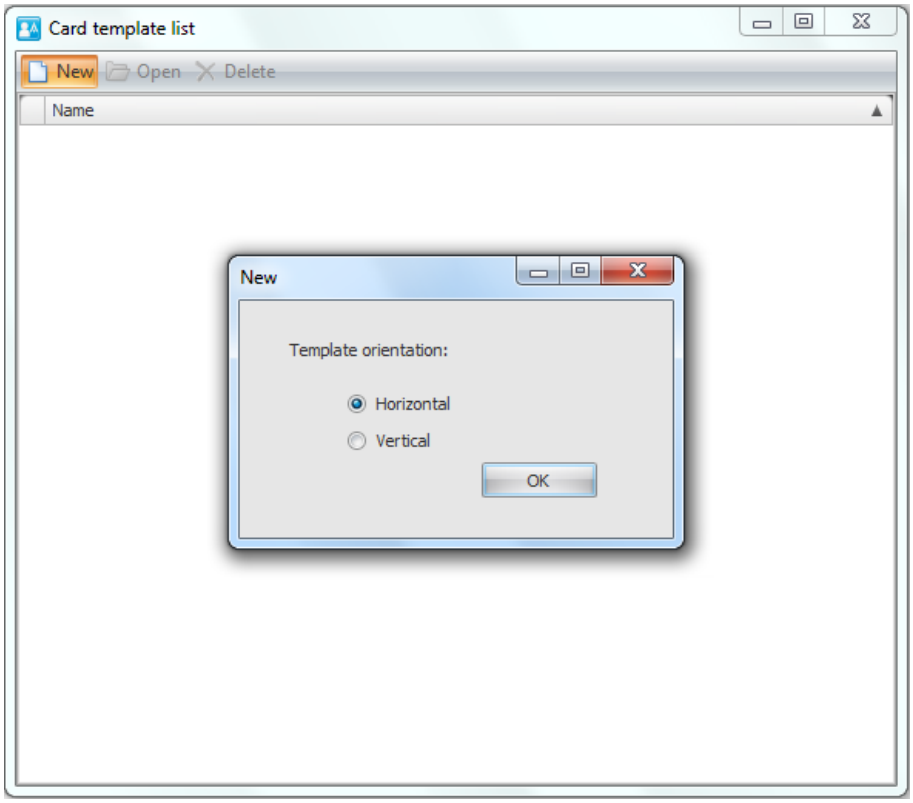
(solo PA para servicio)

El software SALTO permite crear diferentes plantillas de tarjetas, para poder imprimir tarjetas personalizadas. Dichas plantillas pueden incluir textos y dibujos o fotos, y pueden crearse seleccionando la opción "Lista de Plantillas de Tarjeta", en el menú "Herramientas", como puede verse en el dibujo de abajo.



La opción ejecutará automáticamente una aplicación paralela que se basará en el Servicio SALTO para coger la información relativa a los usuarios del sistema de la base de datos.

Para crear una plantilla de tarjeta, seleccionar la opción "Nueva" y elegir entre las opciones de diseño horizontal o vertical.



Una vez la orientación ha sido elegida, el resto de opciones de diseño, al igual que las opciones generales de programa, aparecerán disponibles.

En la comuna de la izquierda, se sitúan las opciones de diseño generales que permiten añadir elementos al diseño de la tarjeta:

TEXTO:

Esta función permite definir las típicas características de Texto, como son Color, Fuente, Localización y Tamaño

El texto puede ser definido en la columna de la derecha como Texto Constante o Dinámico, en la opción Tipo de Dato.

Un Texto Constante es un texto fijo que no cambia.

Un Texto Dinámico cambia dependiendo de la configuración que se le asigne, y de la información del Usuario en la base de datos del programa SALTO.

Como puede verse en el dibujo de la izquierda que viene a continuación, cuando el Texto se configura como Constante, el texto fijo se puede definir en la opción TEXTO, marcada en azul en el dibujo.

Por otro lado, si se elije Texto Dinámico en la opción Tipo de Dato, se activa la opción Campo de Datos, en la cual se puede elegir entre la siguiente información de Usuario de la base de datos: Primer Nombre, Segundo Nombre, ID del Usuario, ExtID del Usuario, Fecha de Activación, Fecha de Caducidad, y Campos de Propósito General. Ver dibujo de la derecha.

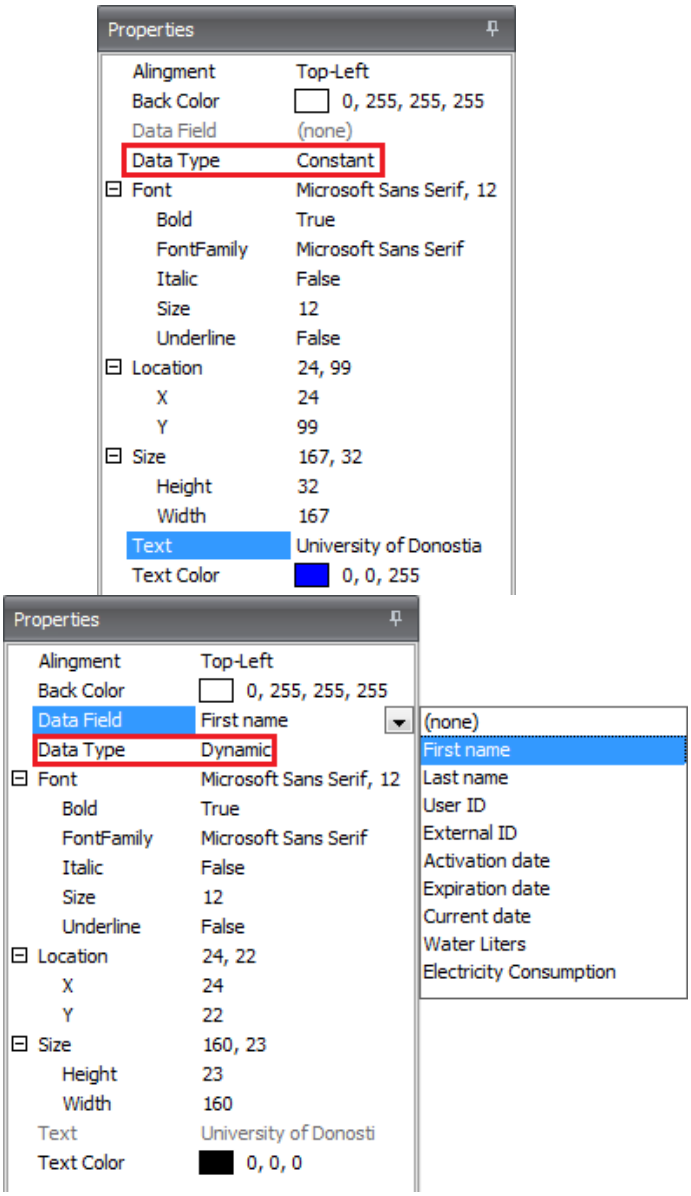
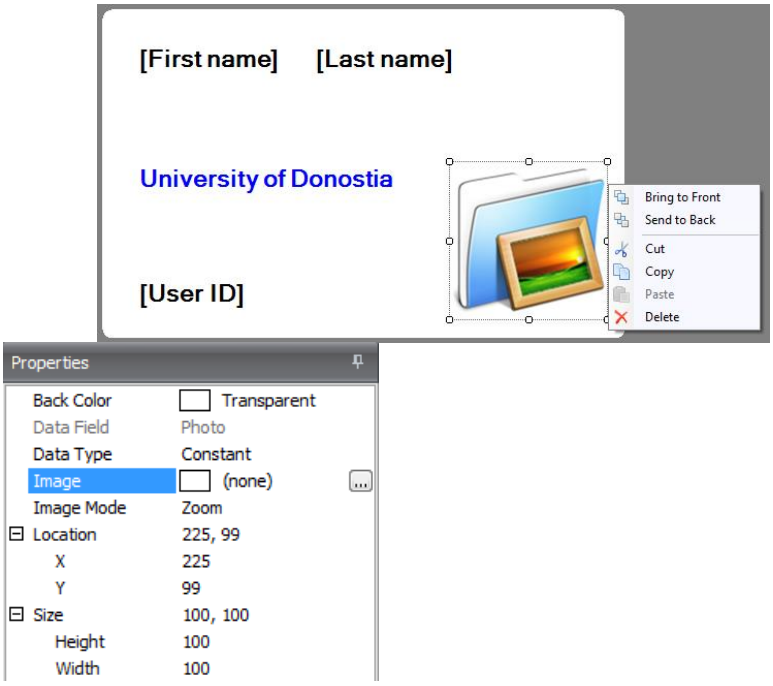


IMAGEN:

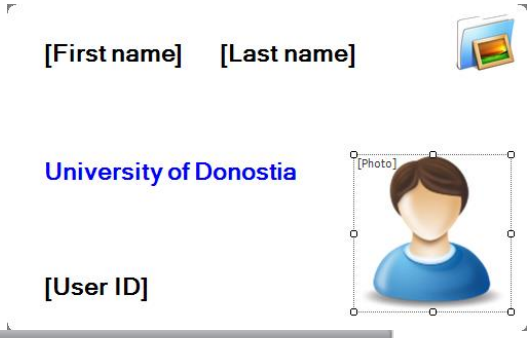
Se pueden importar imágenes en el diseño de la tarjeta usando esta opción. Al igual que con la opción de Texto, las imágenes pueden ser Constantes o Dinámicas.

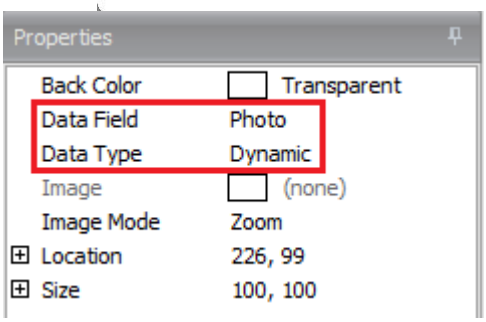
En caso de seleccionar el tipo Constante, se debe elegir una imagen que aparecerá en todas las tarjeta impresas con esta plantilla, con solo pulsar el botón de los tres puntos, a la derecha de la opción Imagen.



La imagen puede colocarse en los planos Anterior o Posterior de la tarjeta, pulsando sobre la imagen con el botón derecho del ratón, y seleccionando una de las opciones "Llevar al Frente" o "Enviar al Fondo". También puede elegirse entre las opciones Cortar, Copiar, Pegar y Eliminar.

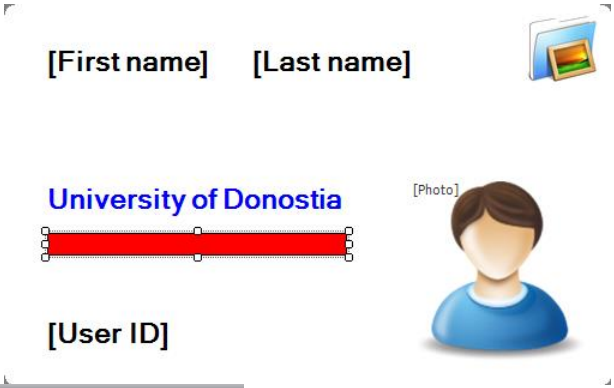
Si se elije la opción de imagen Dinámica, la imagen que se cargará en el diseño de la tarjeta será la imagen o foto cargada en la ficha de usuario de la base de datos del programa SALTO.

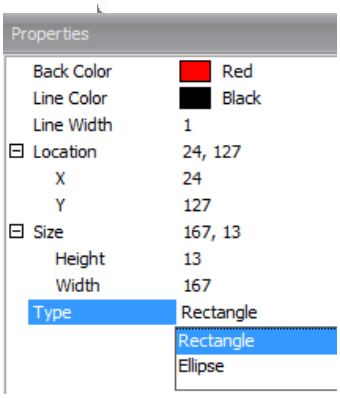




FORMA:

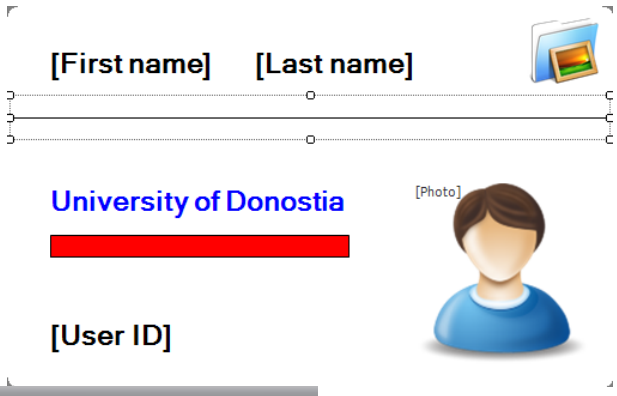
Pueden cargarse también unas Formas especificas en el diseño de la tarjeta. Estas formas son el Rectángulo y la Elipse, especificando los colores del fondo y de la línea, as igual que el grosor de la línea.

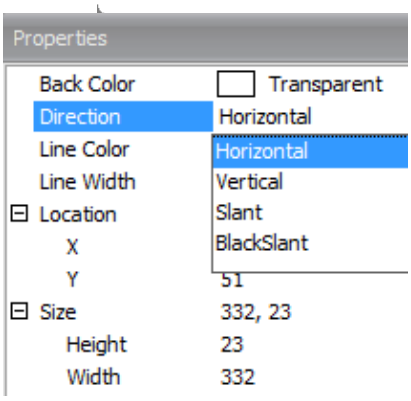




LÍNEA:

Pueden también añadirse Líneas al diseño de la tarjeta, seleccionando diferentes posiciones como Horizontal, Vertical, Línea Ascendente o Descendente.





En caso de que se quiera añadir elementos de diseño en ambos lados de la tarjeta, pulsando sobre la pestaña Frente con el botón derecho del ratón, podrá añadirse una pestaña para el diseño de la parte posterior de la tarjeta.

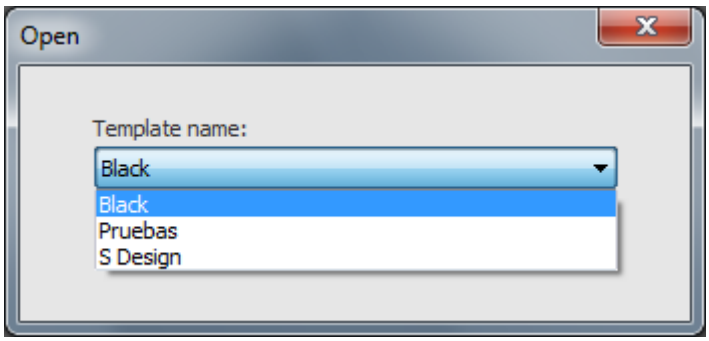
Las herramientas a utilizar para diseñar la parte posterior de la tarjeta, al igual que las opciones disponibles, serán las mismas que para el Frente de la tarjeta. Revisar las explicaciones de arriba para diseñar la parte posterior.

Una vez el diseño se ha completado, este debe guardarse.

La parte superior izquierda del programa contiene las opciones generales para manejar el diseño de las tarjetas, como Nueva, Abrir, Guardar, Guardar Como, Imprimir, Rejilla y Tamaño (de la Rejilla).

La opción Nueva permite crear nuevas plantillas.

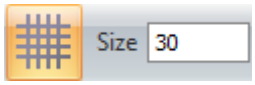
La opción Abrir permite abrir diseños de tarjeta que han sido creados anteriormente, para que así puedan ser modificadas:



La opción Guardar permite guardar el diseño realizado.

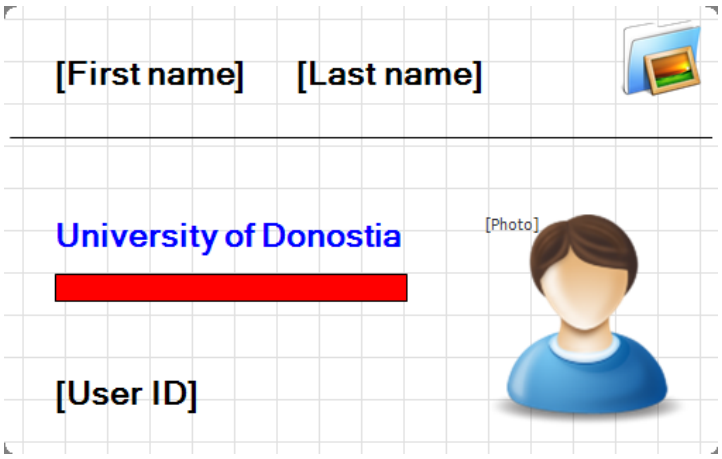
La opción Guardar Como permite guardar un mismo diseño con diferentes nombres, en el caso de que sea necesario llevar a cabo diferentes modificaciones sobre una misma base de diseño.

Los diseños realizados pueden imprimirse en cualquier impresora de tarjeta, siempre y cuando se disponga de los drivers necesarios para el sistema Operativo utilizado.



Se puede añadir una Rejilla a la tarjeta durante el proceso de diseño para así tener referencia de donde colocar los diferentes elementos.

El tamaño de la rejilla puede especificarse en el Campo de Tamaño.



Menú de periféricos

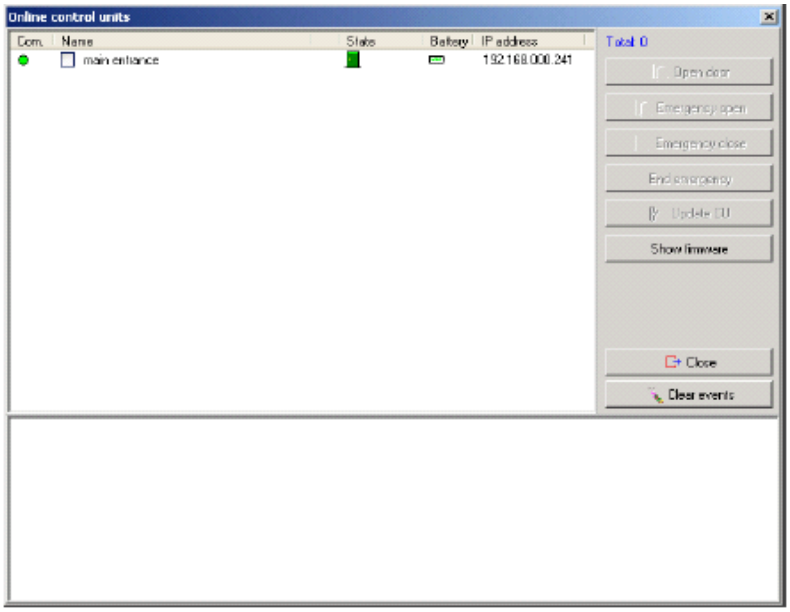
Este menú tiene 2 opciones importantes, MONITORIZACIÓN DE UNIDADES DE CONTROL ON LINE y LISTA DE PERIFÉRICOS:

Monitorización de unidades de control online

Esta ventana nos permitirá controlar en tiempo real el estado de las unidades de control online, y realizar algunas operaciones especiales, como forzar el modo cerrado en emergencia o abierto en emergencia.

Una de las mejores ventajas de la unidad de control online es que la lista negra se transmite a esta puerta automáticamente, sin necesidad de visitar la puerta con una tarjeta de usuario recién actualizada.

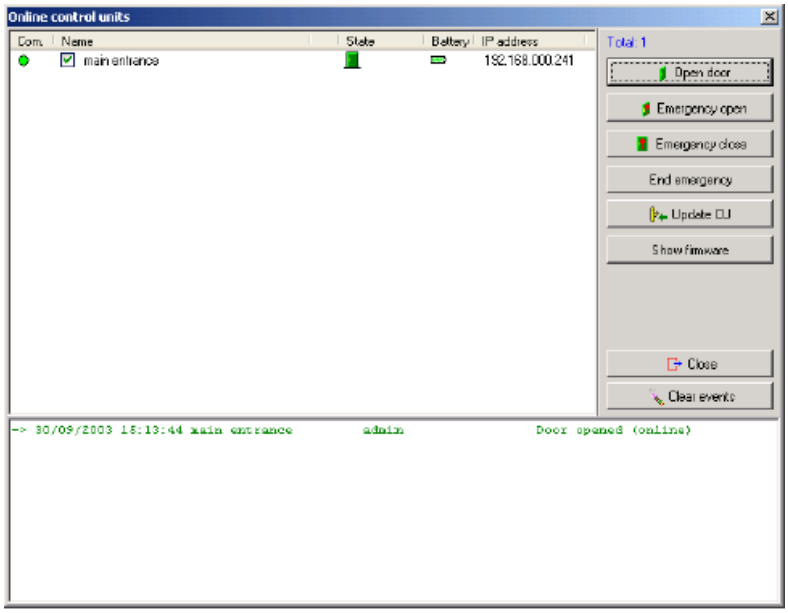
Esta lista negra se transmitirá en tiempo real si estamos trabajando con el ordenador maestro de comunicaciones. Si estamos en otro puesto de trabajo, esta transmisión puede tardar varios minutos.



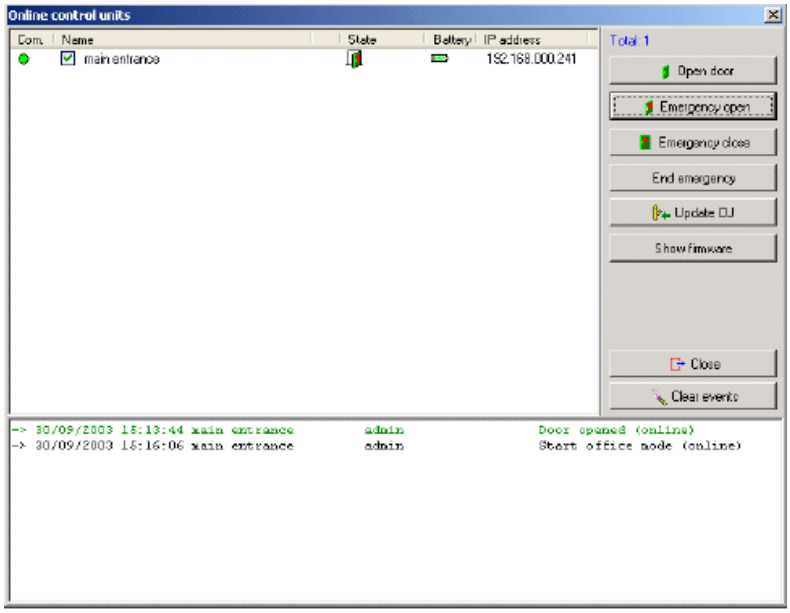
- Marque la casilla junto al nombre de la unidad de control, para activar los botones del software.

- El botón ABRIR PUERTA puede ser utilizado para realizar una apertura remota, si estamos trabajando con el ordenador maestro de comunicaciones.

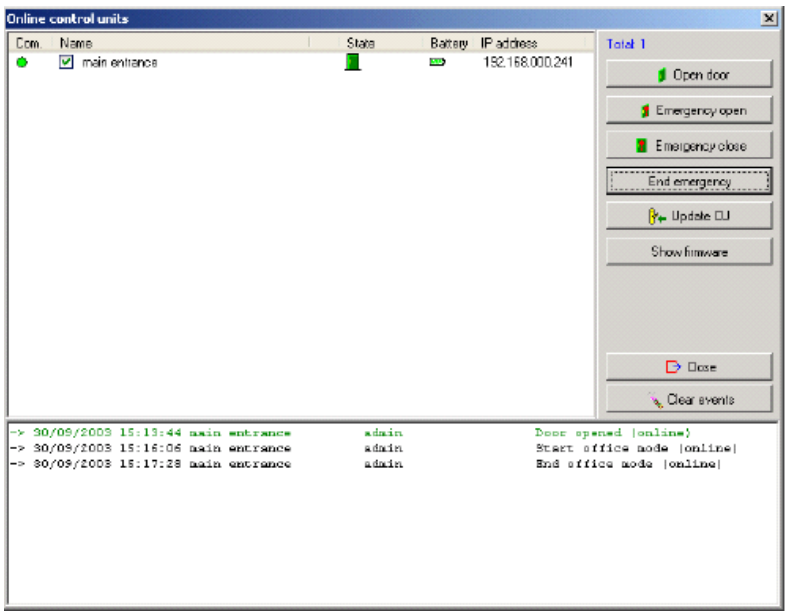
- Con este botón se pueden abrir varias unidades de control remotamente.



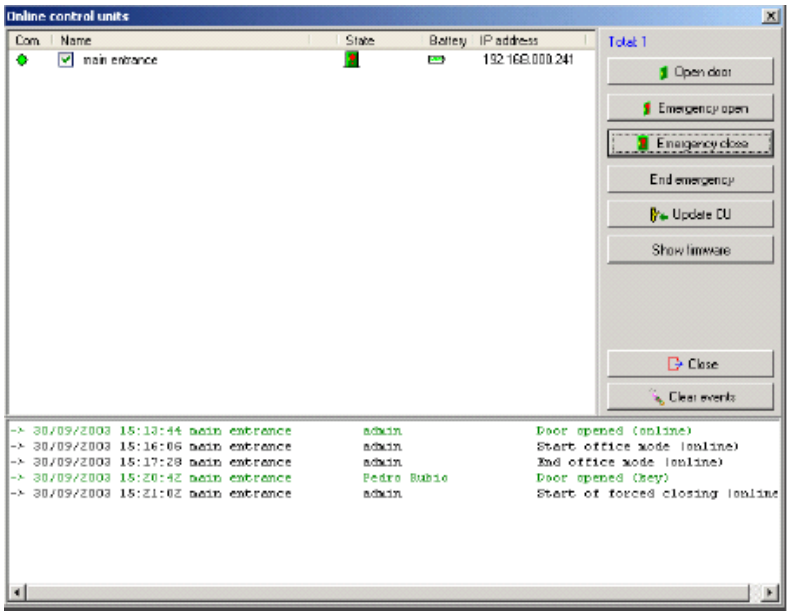
- El modo ABIERTO EN EMERGENCIA puede activarse si queremos que la puerta quede abierta por algún tiempo, sin importar quién pueda entrar durante ese tiempo Esto no tiene nada que ver con el modo paso o la apertura automática. Para terminar este modo de trabajo especial, pulsamos el botón FIN DE EMERGENCIA.



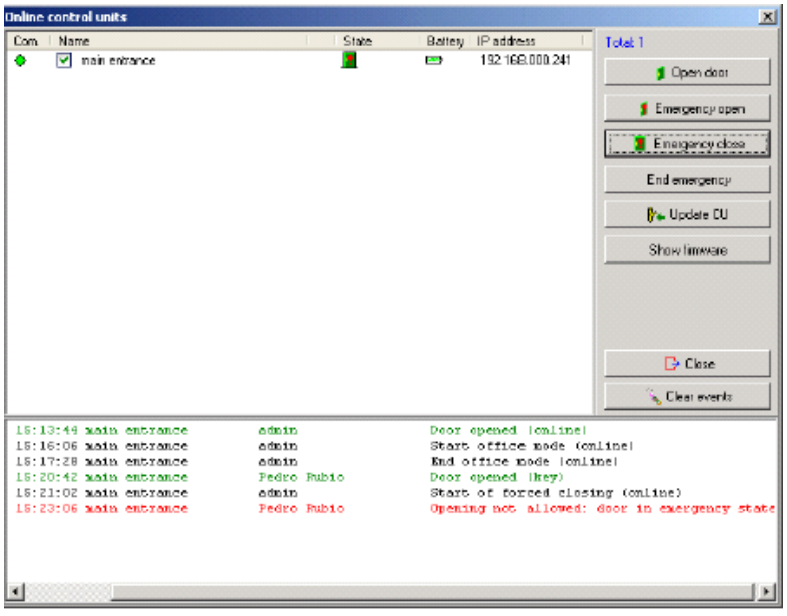
- Después de pulsar el botón FIN DE EMERGENCIA la puerta volverá a su funcionamiento normal.



- El modo CERRADO EN EMERGENCIA puede utilizarse si queremos dejar la puerta cerrada durante un tiempo, de manera que nadie podrá entrar, ni si quiera los usuarios autorizados. Este modo especial terminará pulsando la tecla FIN DE EMERGENCIA.

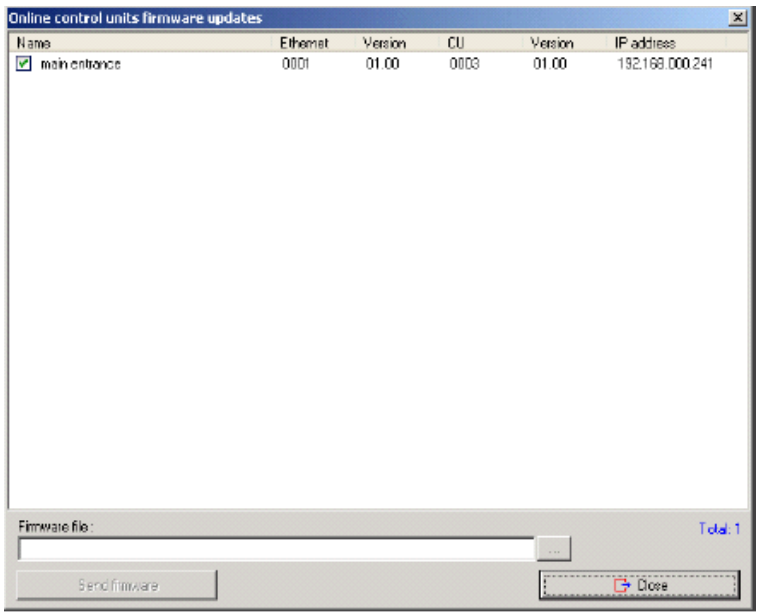


En la imagen superior podemos ver como un usuario autorizado puede entrar. Pero después de forzar el modo CERRADO EN EMERGENCIA (2 minutos después) Pedro Rubio ya no puede volver a entrar, debido al modo CERRADO EN EMERGENCIA (imagen inferior).



- El botón ACTUALIZAR CU se puede utilizar para transmitir información a la unidad de control, cuando hayamos hecho un cambio en la base de datos, que implique una actualización de esta puerta.

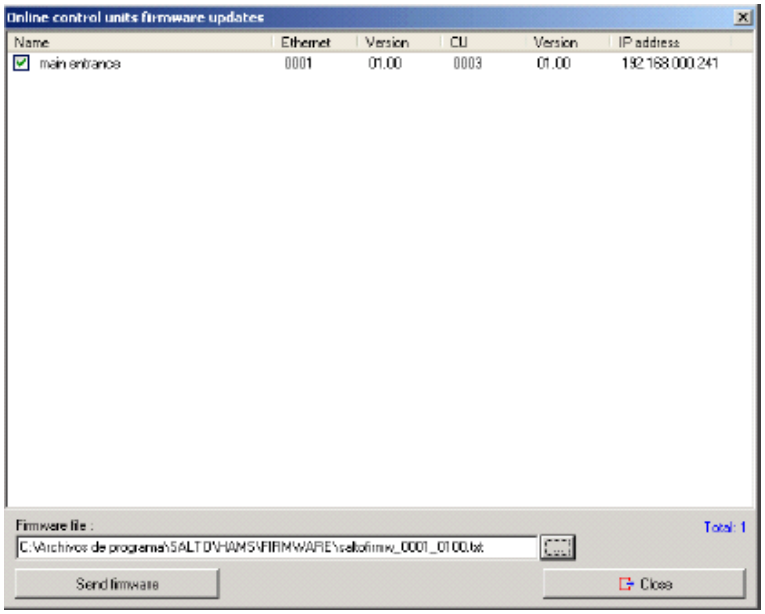
- El botón MOSTRAR FIRMWARE se puede utilizar para ver la versión de firmware de la unidad de control.



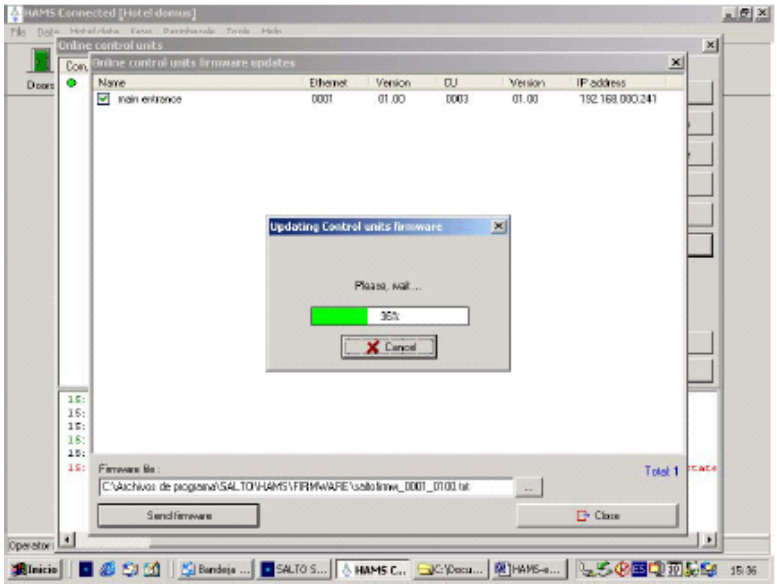
- Una unidad de control online se compone de 2 elementos, la placa Ethernet y la placa base. La placa Ethernet EN (online) se muestra como dispositivo 0001, la placa Ethernet SVN como dispositivo 0002 y la placa base CU5000 es el dispositivo 0003.

- A veces es necesario actualizar la versión de firmware, para dar a la unidad de control nuevas características. Salto SYSTEMS informará a los clientes cuando esta operación sea necesaria. Para descargar un nuevo firmware en una unidad de control online, siga estas instrucciones.

- Seleccione la ruta donde el fichero de firmware está guardado, en su disco duro. Esto es posible pulsando el pequeño botón con 3 puntos situado a la derecha del campo FIRMWARE FILE.



- En el ejemplo, el archivo seleccionado tiene 2 números: el primero se refiere al dispositivo (placa Ethernet) y el segundo es el número de versión. Ahora, pulse el botón ENVIAR FIRMWARE para transmitir el nuevo firmware.



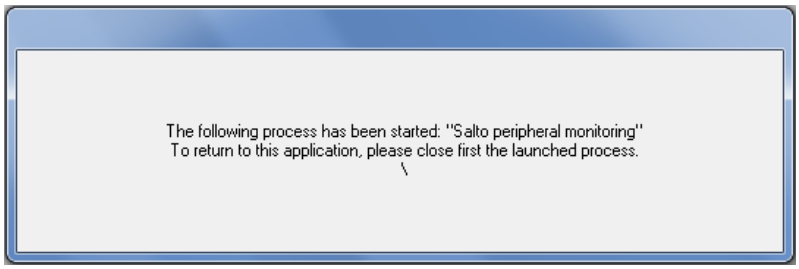
Esta operación tardará algunos segundos. Al final de la transmisión, usted recibirá un mensaje de confirmación, para asegurarle que la operación ha terminado con éxito. Es posible enviar el archivo de firmware a varias unidades de control al mismo tiempo.

Ahora, usted puede repetir esta operación con el archivo de firmware para el dispositivo 0003 que es la placa base. Estos archivos serán suministrados por Salto cuando sea necesario.

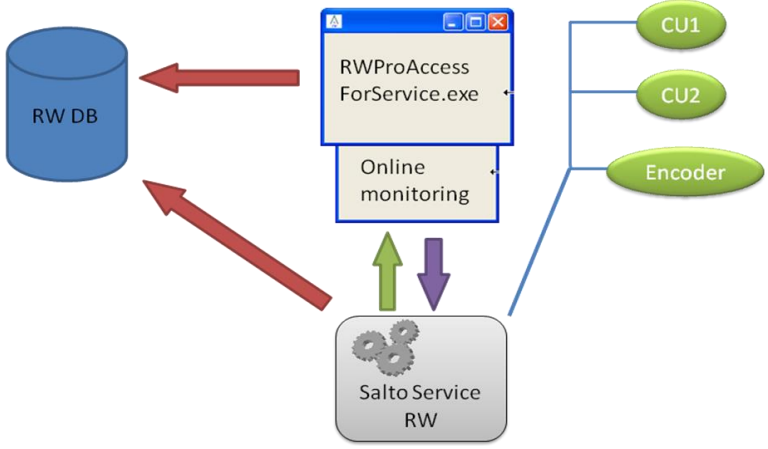
Monitorización Múltiple online

(solo para servicio)

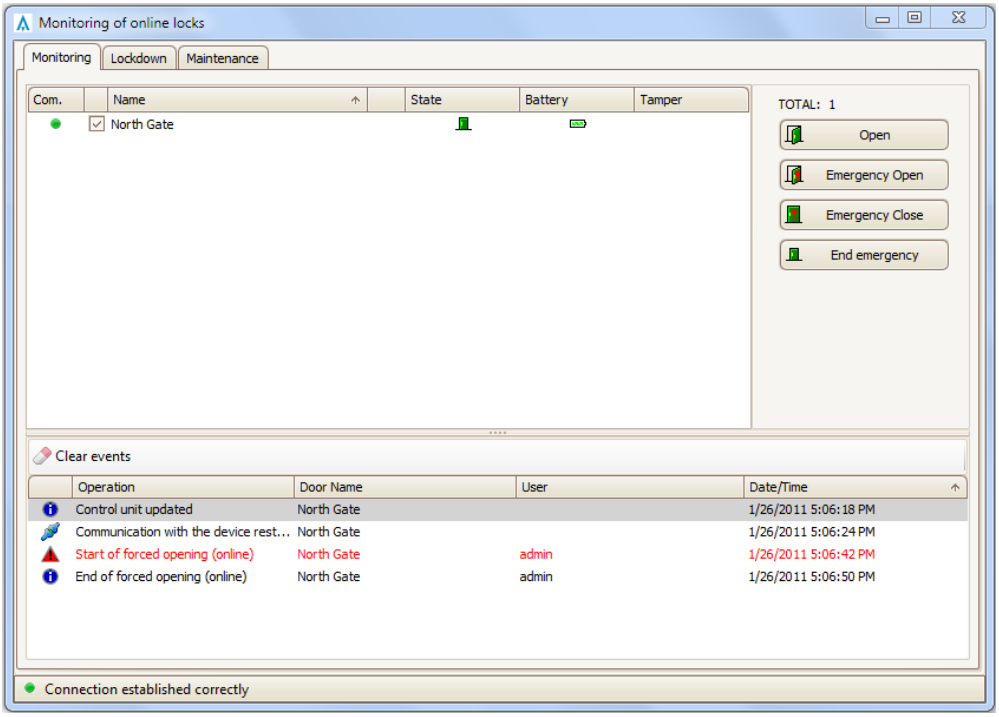
Al arrancar la ventana de monitorización desde periféricos, aparecerá una ventana, como la siguiente, indicando que se inicia la comunicación entre el módulo de monitorización, el servicio y el software.



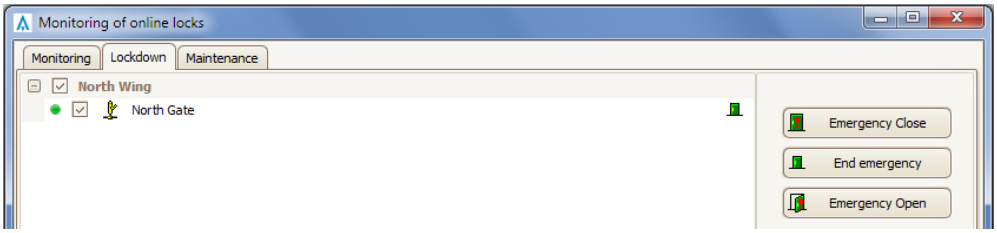
Como se puede apreciar en el diagrama a continuación, los periféricos están todos en comunicación con el **Servicio de Salto** y este a su vez en comunicación con la base de datos. De esta manera, todos los clientes de Salto podrán conectarse a la ventana de monitorización aunque no sean el maestro de comunicaciones.



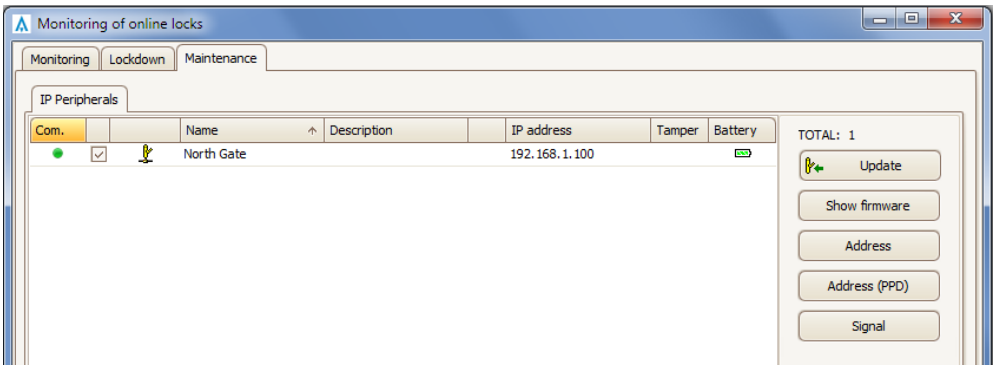
La ventana de monitorización le permitirá abrir la o las puertas seleccionadas a través de la red online, dejar las puertas abiertas o cerradas en emergencia y finalizar la emergencia.



Después de haber creado zonas de Lockdown, podrá desde la pestaña Lockdown abrir y cerrar en emergencia estas zonas seleccionadas.



En el software para servicio, al momento de inicializar las unidades online, será necesario acceder a esta ventana de monitorización, pestaña Mantenimiento. Podrá actualizar, direccionar o actualizar las versiones de firmware.



Actualización del firmware de editores & PPD

Nota: Esta opción del software está exclusivamente limitada a los sistemas E6000, E7000, EH y E9000 y únicamente para la edición de tarjetas de un sistema nunca anteriormente utilizado en SALTO.

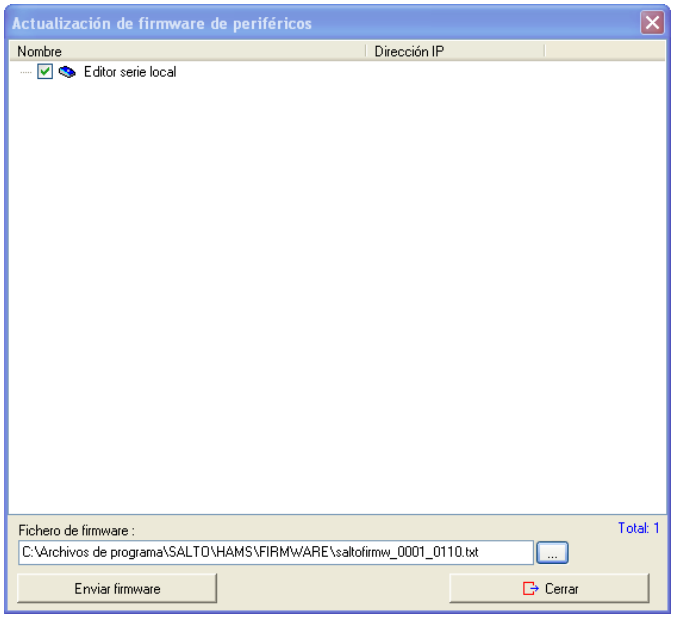
El software permite además actualizar el software de los editores de llaves, tanto los editores serie como los editores Ethernet. Para actualizar el firmware de un editor deberá ir al menú desplegable: HERRAMIENTAS/ CONFIGURACIÓN/ OPCIONES LOCALES y pulsar "Mostrar Firmware".

A continuación se mostrará una pantalla (Fig. 1) en la que aparecerán los diferentes Editores que tengamos en nuestro sistema.

Seleccionaremos el editor/es que queremos actualizar.

Seleccionamos la ruta hasta donde alojado el fichero de firmware en nuestro disco duro. Esto es posible pulsando el pequeño botón con tres puntos situados a la derecha del campo Fichero de Firmware.

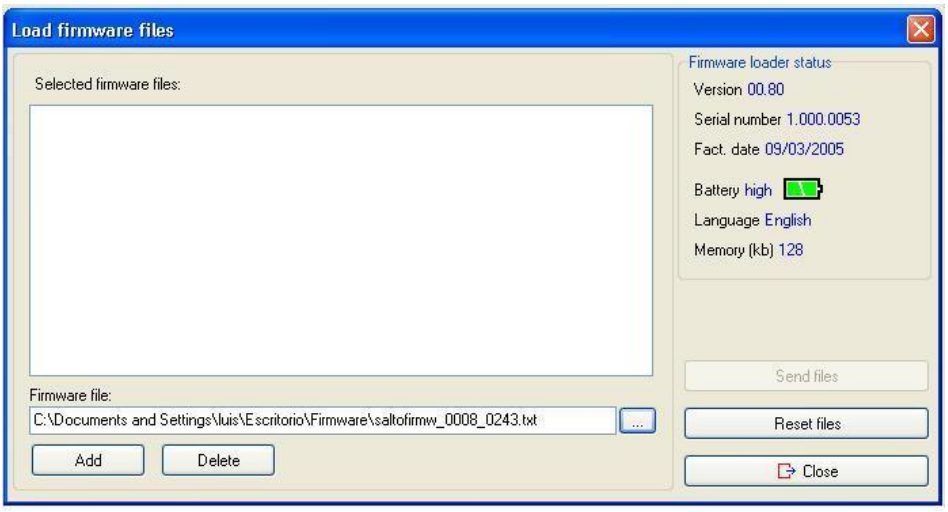
Para transmitir el fichero pulsaremos "Enviar Firmware"



Actualización de lectores:

Importante: Comprobar la referencia y número de lote del escudo y contactar a su distribuidor para saber si se puede actualizar el firmware. Los escudos E6000, E7000, EH y E9000 podrían ser actualizados.

El software presenta una opción para actualizar los lectores de un sistema E6000. Para ello necesitaremos un PPD especial suministrado para estos casos. Al pulsar entonces el botón PPD se mostrará una ventana especial para cargar los ficheros firmware al PPD. Estos son los que habrá que cargar al PPD y a continuación pasar este por todos los lectores.

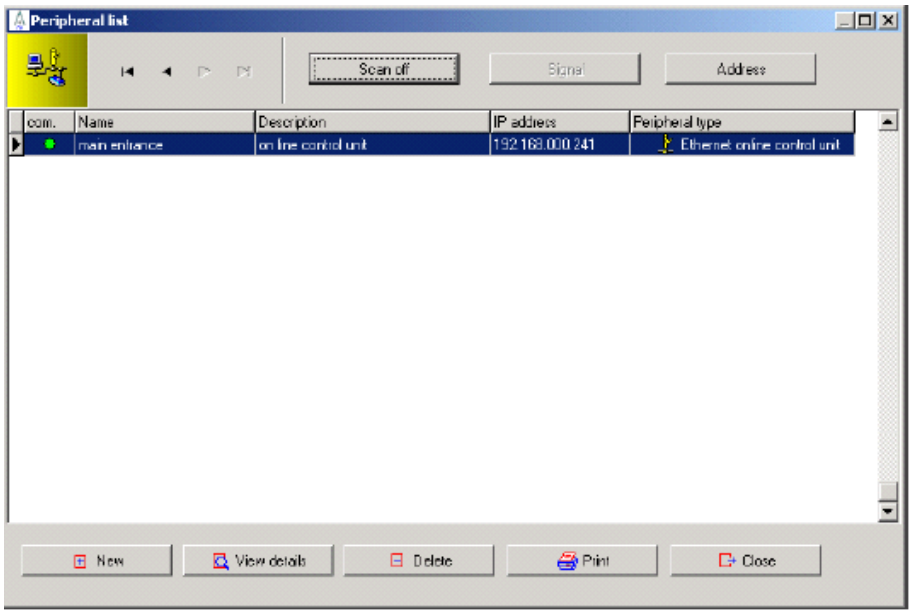


El nuevo modelo de PPD (*) (ver imagen) incluye la función de carga de archivos de firmware permitiendo el almacenamiento de varios ficheros. La actualización de dichos archivos se realiza de manera automática al detectarse una en el dispositivo una versión inferior a la cargada en el PPD.

(*) Versión firmware PPD 1.16 o superior

Lista de periféricos

Esta lista tiene 2 funciones: crear dispositivos online como lectores murales y actualizadores, y asignar la dirección IP a estos dispositivos. En nuestro ejemplo, la "entrada principal" ya está creada como PUERTA, previamente.



Los botones superiores tienen las siguientes funciones:

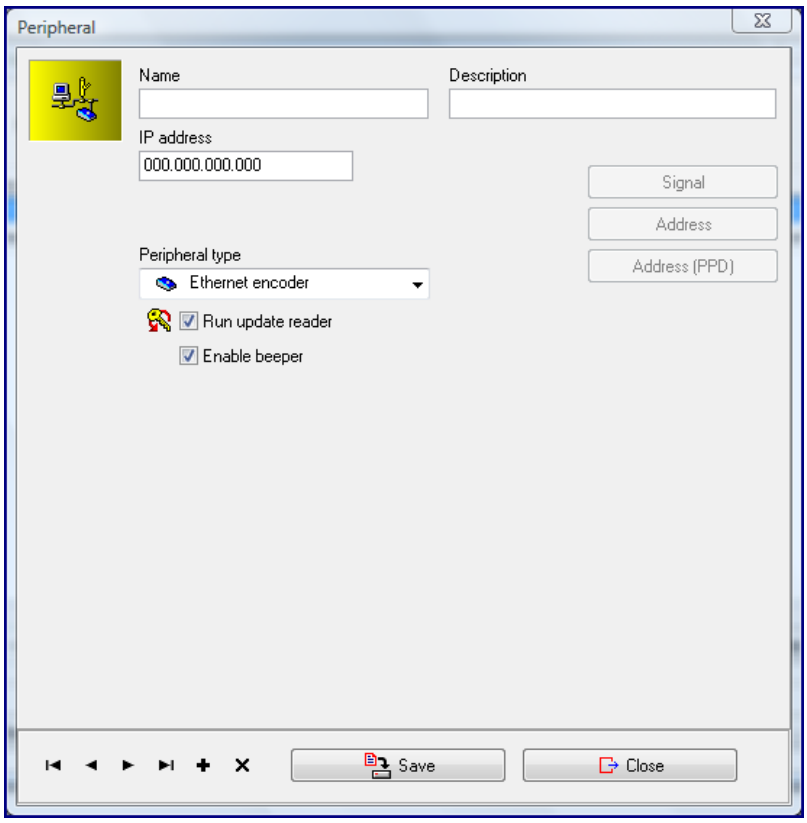
- MONITORIZAR: se puede utilizar para lectores murales y actualizadores. Informa al operador sobre el estado de la comunicación entre el PC y el dispositivo online. Un icono verde significa que hay buena comunicación, un icono rojo significa que hay algún problema.

- SEÑALIZAR: este botón sólo puede utilizarse para los actualizadores, no sirve para las unidades de control online. Hace que el actualizador emita sonidos y parpadee por unos segundos, para localizarlo en caso de haber olvidado su ubicación física.

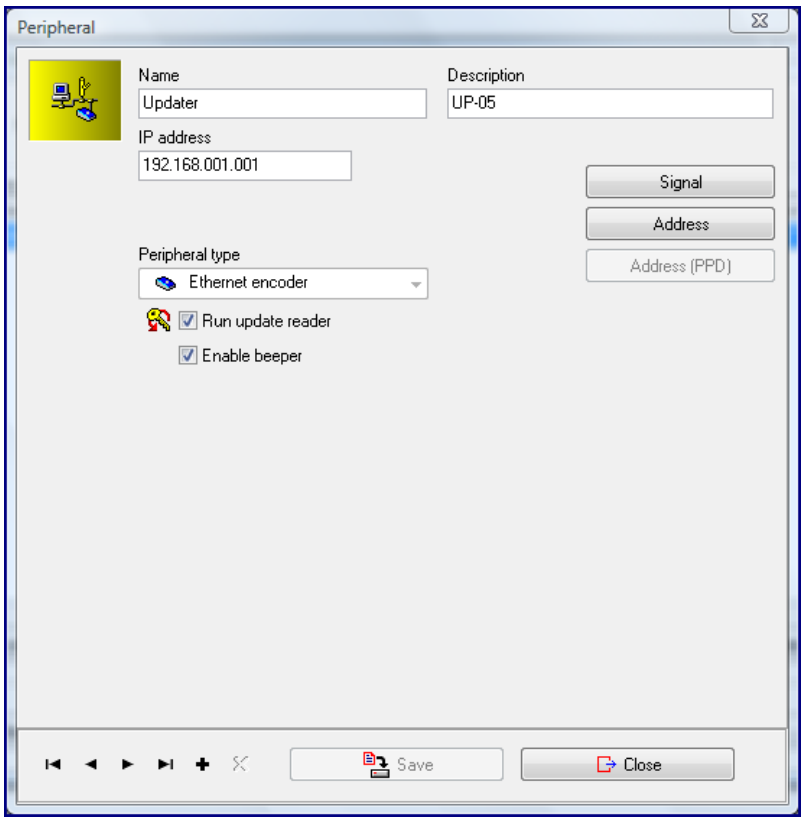
- DIRECCIONAR: este botón se utiliza para lectores murales y actualizadores. Después de pulsar el botón CLR del dispositivo durante unos segundos, (mientras el LED verde parpadea) es necesario pulsar el botón DIRECCIONAR del software, de manera

que la dirección IP seleccionada será capturada por el dispositivo online. Si no recibimos un mensaje de error a continuación, se supone que la dirección IP ha sido correctamente asignada al dispositivo.

- Asegúrese siempre que la dirección IP está libre y no está siendo usada por otro dispositivo, cuando vaya a asignarla.



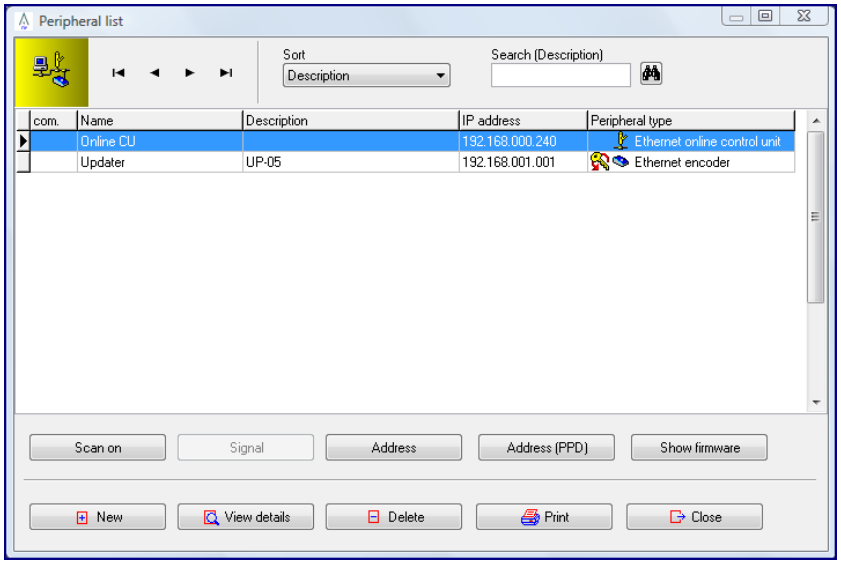
En nuestro ejemplo, vamos a crear un actualizador. Esta operación sólo puede realizarse si estamos trabajando con el ordenador maestro de comunicaciones. (HERRAMIENTAS / OPCIONES / ON LINE). Pulse el botón NUEVO de la lista de periféricos y dele un nombre al dispositivo. También es necesario escribir la dirección IP que se le va a asignar, y decidir si es un Ethernet editor (actualizador) o es una unidad de control online. (Lector mural).



Es necesario marcar la casilla RUN UPDATE READER, si estamos creando un actualizador.

Si queremos que el actualizador emita sonidos durante su funcionamiento, marcaremos la casilla HABILITAR SONIDO. Después hay que guardar los cambios para poder asignar la dirección IP.

El actualizador funcionará de manera continua, y actualizará cualquier tarjeta de usuario (staff) que sea introducida, dándole una nueva fecha de caducidad que es la fijada en HERRAMIENTAS / OPCIONES / USUARIO. El actualizador también transmite la lista negra, de los códigos de tarjetas perdidas o canceladas.



Inicialización de Periféricos

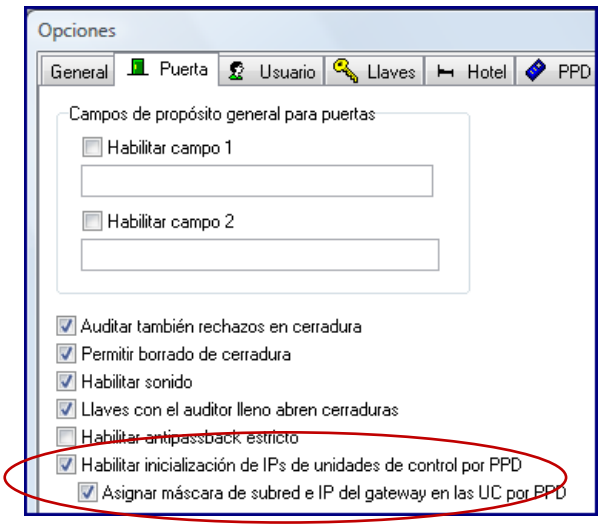
Para la inicialización del periférico es necesario pulsar el botón CLR en el circuito por unos 4 segundos hasta que el LED empieza a parpadear. Entonces pulsamos el botón DIRECCIONAR (ADDRESS) del software y esperamos unos segundos. Al comunicar, el icono de la columna "COM" en la ventana de periféricos, pasará de rojo a verde.

También es posible direccionar una CU situada en una LAN diferente usando un PPD. Será necesario cargar el PPD con la información de las unidades online e inicializar las puertas manualmente.

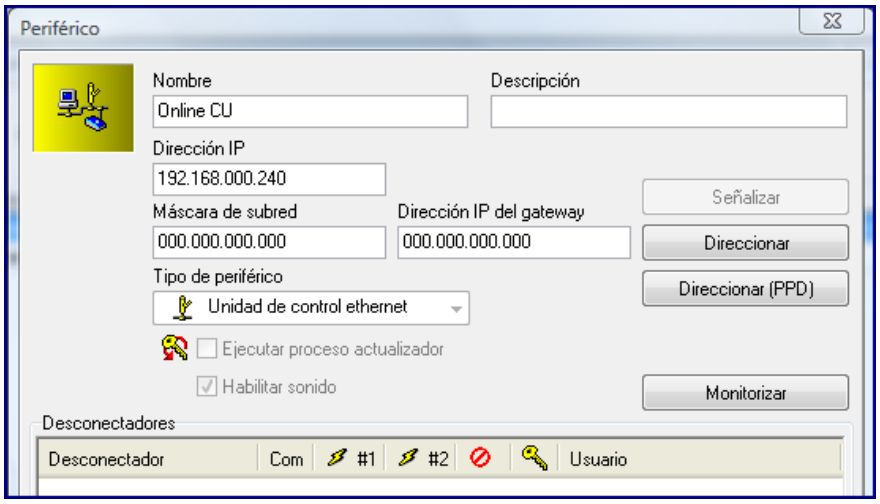
El FW del PPD deberá ser versión 01.07 o superior.

Habitualmente, cuando un PC envía información a la CU, esta contesta usando el mismo puerto de donde la solicitud le ha llegado. En algunas instalaciones, es posible encontrarse con Router que encaminan las respuestas de las CUs por otro puerto que el de la solicitud. Para poder trabajar con este tipo de Routers, se le puede indicar la máscara de subred y la puerta de enlace a la CU. Para hacerlo habrá que seguir los siguientes pasos;

El botón "Asignar máscara de subred e IP del Gateway en las UC por PPD" deberá activarse.



En la ventana de periféricos, debe rellenar los campos "Máscara de subred" y "Dirección IP del Gateway". Una vez esto hecho, es necesario utilizar el PPD para inicializar el periférico como se ha mencionado más arriba.



La CU y su placa Ethernet deben tener las versiones de FW siguientes;

Placa CU5000 versión: **02.01** o superior.

Placa Ethernet versión: **01.40** o superior.

Configuración de editores Ethernet:

Para configurar los editores Ethernet, es necesario editar la lista de periféricos. (HERRAMIENTAS/LISTA DE PERIFÉRICOS). Esta ventana contiene una lista de todos los periféricos declarados en la instalación.

Para cada editor, necesitamos 2 parámetros: un número de identidad y una dirección IP. Para el número de identificación se recomienda empezar por el 2, ya que el 1 está reservado para el editor local (serie). Para averiguar la dirección IP, debemos preguntar al administrador de la red de área local, y asegurarnos que esa dirección es válida y no está siendo utilizada por ningún otro dispositivo. Los conflictos sobre una misma dirección IP pueden conducir a problemas de comunicación.

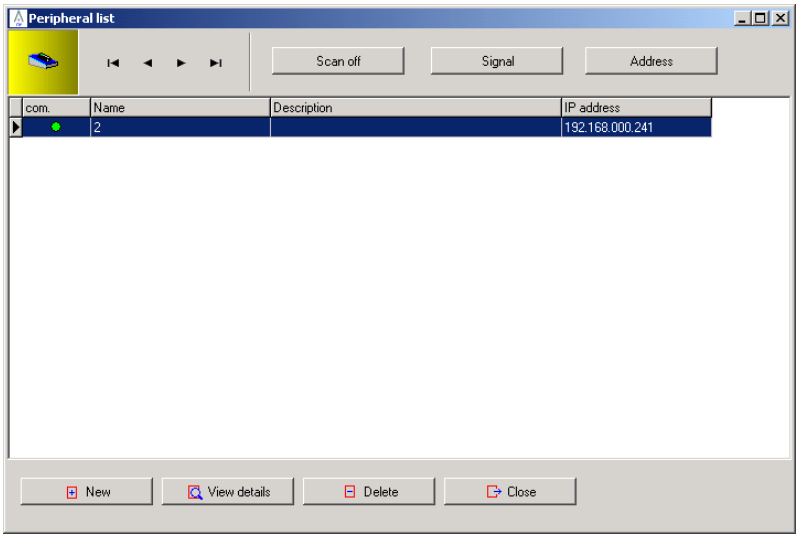
La configuración del editor Ethernet se puede realizar abriendo la ventana LISTA DE PERIFÉRICOS, como se ve en la figura a continuación. Como de costumbre, los botones de la parte inferior de la ventana se pueden utilizar para añadir, quitar o editar editores Ethernet.

En la parte superior de la ventana, se pueden encontrar estos controles:

- **MONITORIZAR:** al pulsar este botón, la aplicación comprobará si el periférico seleccionado de la lista, está conectado al ordenador del PA: un icono verde indicará que el periférico correspondiente está comunicado, mientras que un icono rojo indica que no hay comunicación.

- **SEÑAL:** esta función sirve para que un editor en particular parpadee y emita sonidos durante unos segundos. De esta manera podemos identificar la localización del editor así como comprobar la comunicación.

- **DIRECCIONAR:** esta función se utiliza para dar una nueva dirección IP a un periférico. Primero, hay que presionar el pequeño botón que hay en la parte de atrás del editor (puede hacerlo con un bolígrafo), hasta que el LED verde empiece a parpadear. En ese momento, hay que seleccionar un periférico de la lista y pulsar el botón DIRECCIONAR. Si no aparece ningún mensaje de error, se supone que el editor ha cogido la nueva dirección IP. Utilice SEÑALIZAR o MONITORIZAR para comprobar la comunicación.



Inhibir maestro de comunicaciones

En ciertas instalaciones el administrador puede preferir, porque se adecua mejor a la configuración de su instalación, centralizar todos los softwares en un mismo servidor y ejecutarlos desde estaciones de trabajo de forma remota por medio de Terminal Server o Citrix.

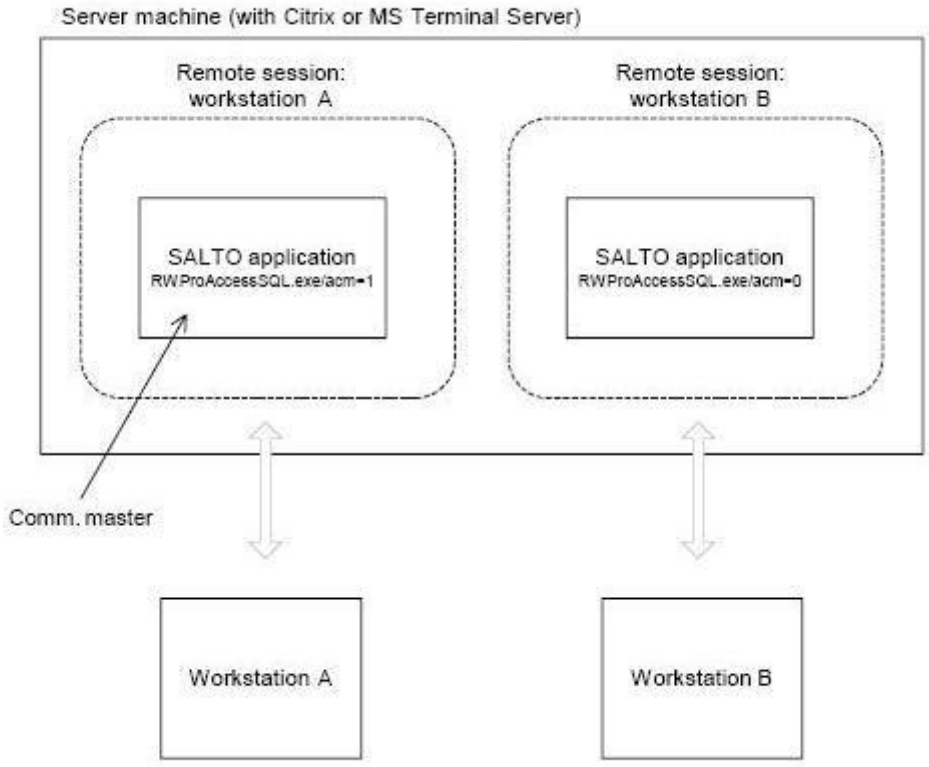
Para evitar confusiones entre los parámetros locales entre diferentes centros de trabajo se debe instalar una carpeta Salto diferente por cada centro. Cada una de esas carpetas debe contener los mismos ficheros descritos en el capítulo de instalación, esto es el fichero ejecutable Salto, el fichero de mensajes(TXT) y lo más importante el fichero configuración(cnfg.ini). Vamos a imaginar que disponemos de 2 centros de trabajo A y B desde los cuales remotamente se ejecutará la aplicación Salto. En este caso, el servidor debería tener dos carpetas Salto(Salto A y SaltoB) las cuales contendrán los archivos comentados arriba. De tal forma que cad sesión abierta desde el centro de trabajo A deberá trabajar en la carpeta A del servidor mientras que las sesiones abiertas desde el centro B lo deberán hacer en la carpeta B.

Bajo Citrix o Terminal Server es posible ejecutar diferentes sesiones SALTO en el servidor(Aunque solo hay una sesión Salto por sesión Windows). Esto no es un problema en si mismo salvo que declaramos el servidor como maestro de comunicaciones. En este caso todas las sesiones del servidor tratarán de trabajar en modo maestro a pesar de que solo una lo será de forma satisfactoria(normalmente la primera que se arrancó). Si necesitamos que una sesión sea el maestro de comunicaciones(sin importar cual se inició primero) se debe utilizar el comando 'acm'

(Allow Comm. Master): Si a este comando se le asigna un cero la característica Maestro de comunicaciones será deshabilitada. Por el contrario si el parámetro es establecido a 1(valor por defecto) el modo maestro de comunicaciones será autorizado. Por lo tanto, la sesión salto que queremos que trabaje como maestro de comunicaciones debería tener "/acm=1" en la línea de comando y el resto de sesiones ''/acm=0''.

C:\?\RWProAccessSQL.exe /acm=0 <- Esto deshabilita comm. Modo maestro
C:\?\RWProAccessSQL.exe /acm=1 <- Esto permite comm. Modo maestro.

En resumen hay que tener en cuenta que dos condiciones son requeridas para que una sesión trabaje en modo maestro. Primero debe ser ejecutado en la máquina declarada como maestro de comunicaciones y en segundo lugar el comando 'acm' si existe ha de ser diferente a cero.



Idiomas. Cambio de idioma.

El software para control de accesos RW De Salto viene por defecto en idioma inglés, pero es posible cambiar de idioma pulsando la tecla IDIOMAS del menú principal de recepción , y escogiendo otro idioma de los disponibles en la lista.

Log-out. Cambiar de operador.

Cuando el administrador quiere hacer uso del programa de control de accesos, basta con pulsar la tecla LOG OUT del menú de recepción para que aparezca la ventana de inicio de sesión.

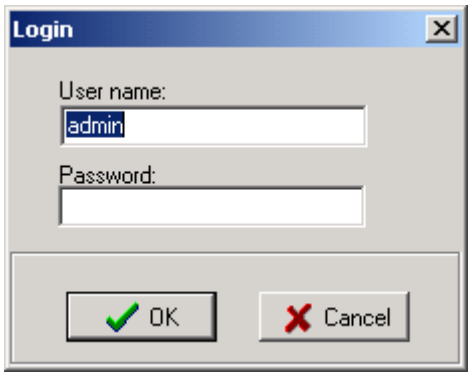


Figura 81

El administrador introducirá una contraseña si así lo especificó en HERRAMIENTAS/ OPERADORES Y PERMISOS.

A continuación se pulsa el botón OK para entrar en el programa, con privilegios de administrador.

Configuración de una base de datos departamental

(Nota: Esta opción solo está disponible en la versión PA departamental o superior)

Introducción

Este capítulo contiene explicaciones básicas sobre la opción "Departamento Operador". El gran logro de esta opción es proporcionar herramientas para controlar diferentes departamentos dentro de una misma instalación y compartir elementos de comunes de control de accesos (puertas, usuarios, etc.) entre departamentos.

Han de tenerse en cuenta ciertos conceptos:

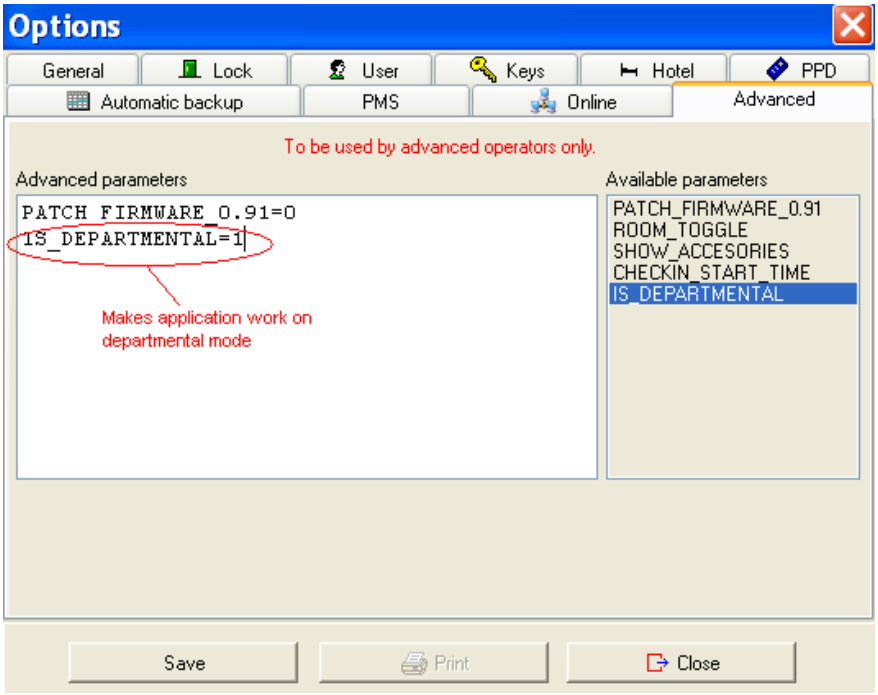
Elemento Interno: Un elemento que pertenece al mismo departamento que el operador.

Elemento externo: Un elemento de otro departamento "compartido" con el operador del departamento.

Activar la opción departamental

La primera cosa que tiene que hacer el administrador después de crear la BD es crear el plan de departamentos. Esto es, decidir cuántos departamentos va a haber en la instalación, que usuarios, puertas, etc. Van a pertenecer a cada departamento... Una vez la planificación éste terminada, los administradores de cada departamento están libres para empezar a trabajar en la configuración de sus departamentos como si fuera una instalación independiente, creando sus elementos (usuarios, puertas, zonas...) y compartiéndolos como suyos.

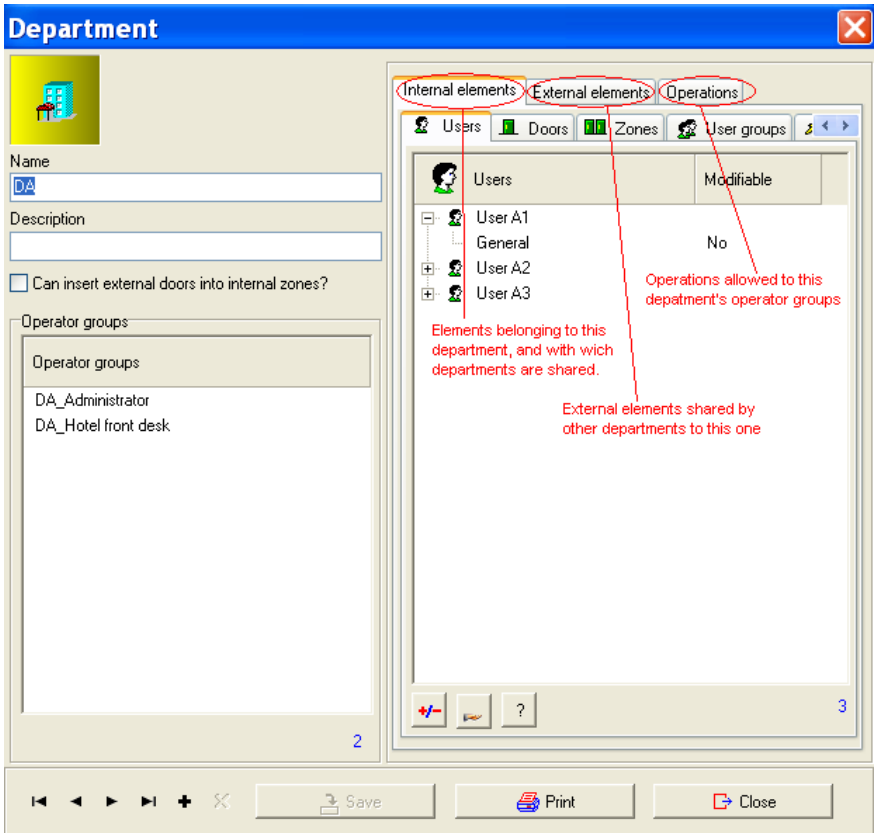
Para hacer trabajar la aplicación como "Departamental" hay que activar esta opción. Para ello, vamos a HERRAMIENTAS/CONFIGURACIÓN/OPCIONES GENERALES y activamos la opción en la pestaña de AVANZADO. (Figura 1)



Como crear departamentos

Después de activar la opción departamental es posible crear nuevos departamentos en HERRAMIENTAS/OPERADORES Y PERMISOS / DEPARTAMENTOS. Desde dónde es posible ver la lista de departamentos existentes, crear nuevos departamentos, ... Los Departamentos sólo pueden ser creados y borrados por el SUPER-ADMIN. Un administrador de departamento puede hacer cambios en la configuración de su departamento y puede cambiar elementos de su departamento a otro. Después de crear un nuevo Departamento, se creará un nuevo Grupo de Operador (2 en el caso de PA) Llamado "Nombre del departamento_admin." Sin contraseña (Ver figura 2). Estos Grupos de Operadores y Operadores no pueden borrarse al no ser que que se borre el departamento por el Super_admin. El administrador de cada departamento puede también, crear nuevos, modificar o borrar Grupos de Operadores y Operadores de su Departamento.

El Super-admin es así mismo, el único con permiso para permitir insertar puertas externas en zonas internas.



Hay 3 conceptos principales en el perfil de un departamento:

- Elementos Internos: Aquí es posible ver elementos internos del departamento y con qué departamentos están siendo compartidos y en que modo (Modificable o asignable).
- Elementos Externos: Aquí es posible ver los elementos externos del departamento, esto es, elementos de otro departamento que operadores de este departamento pueden modificar o asignar dependiendo del modo en que están compartidos (Modificables o Asignable)
- Operaciones: Aquí es posible especificar que operaciones está capacitado a realizar el administrador de este departamento.

Elementos Internos:

Aquí es posible ver elementos internos del departamento y cuáles están siendo compartidos con qué departamentos y en qué modo (Modificable o Asignable) Es posible modificar el dueño de un elemento. Un elemento es añadido a un departamento cada vez que un operador de ese departamento crea uno nuevo. Para mover un

elemento de un departamento a otro hay que ir al perfil del departamento de destino, seleccionar la pestaña de "elementos Internos" y clicar en +/-. Una nueva ventana aparecerá como se indica en la figura 3. En la parte derecha de la pantalla aparecen los elementos que pertenecen al departamento actual y en la parte izquierda los elementos del departamento desde el cual se pueden mover elementos. De esta forma, si queremos hacer pertenecer a un elemento a un departamento, Primero hay que seleccionar el departamento desde el que se quiere mover el departamento y después moverlo con las flechas. Por ejemplo, para hacer que el usuario A del Departamento A pertenezca al Departamento B. Hay que ir al Departamento B, seleccionar los elementos internos y clicar en +/-. Luego en la parte derecha de la ventana seleccionar Dpt. A y mover User A de la lista. Esto causará que el Usuario A pertenezca al Departamento B. El super-admin puede seleccionar elementos de cualquier departamento pero el Administrador de cada departamento sólo puede seleccionar elementos de su departamento.

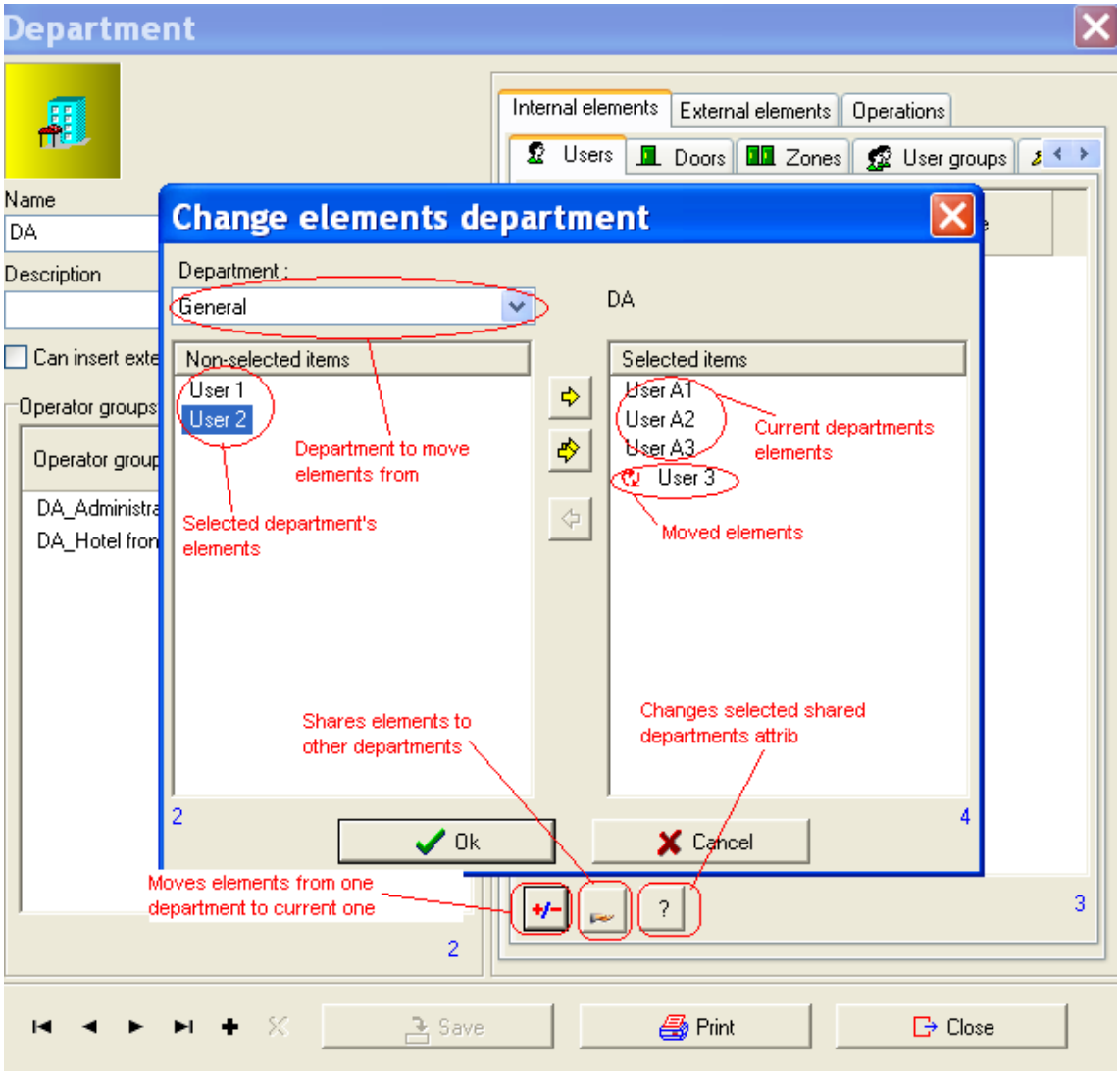


Figure 3: Screenshot of an element department change window.

Cuando movemos elementos de un departamento a otro, es necesario considerar ciertos aspectos: Bien la lista de accesos de los elementos movidos tiene que actualizarse o se tienen que crear nuevas relaciones de compartición para mantener la integridad del departamento. Por ejemplo, consideremos la puerta A en el Departamento A a la que entra un Usuario B del Departamento B. si la puerta A es movida al departamento C, entonces si el usuario A no está compartido con el Departamento C o si la puerta A no está compartida con el Departamento B, el usuario B no tendrá acceso. Por lo tanto hay dos opciones:

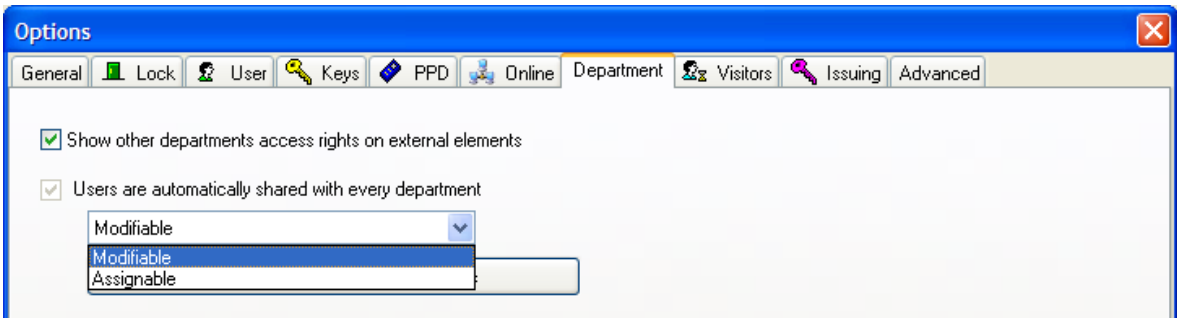
Quitar ese acceso o establecer una relación como asignable. Entre Puerta A y departamento B. De esta forma, cuando hay necesidad de mover elementos de un departamento a otro hay que intentar mover todos los elementos de una misma vea antes de guardar para no crear relaciones innecesarias o para no variar relaciones de acceso necesarias. El software preguntará cada vez

que se elementos entre departamentos si queremos crear nuevas relaciones o quitar accesos)

Compartir Elementos

Desde opciones generales se puede activar la compartición de usuarios de forma automática con el resto de departamentos.

Esta compartición se puede predefinir de dos formas distintas Modificable y Asignable:



- Modificable

Se podrán modificar tantos los parámetros de la ficha del usuario así como los accesos de este.

- Asignable

Se podrán modificar únicamente los accesos del usuario.

Para compartir un elemento interno con otro departamento, seleccionar el elemento y clicar en el icono de la mano. Luego seleccionar los departamentos con los que se quiere compartir. Después el atributo modificable se puede cambiar seleccionando el departamento cuyos atributos se quieren cambiar y clicando el botón"?". Los atributos modificables sólo se pueden cambiar cuando se comparten usuarios o puertas. Cuando se comparten zonas, nivel de accesos o salidas los atributos modificables serán siempre asignados.

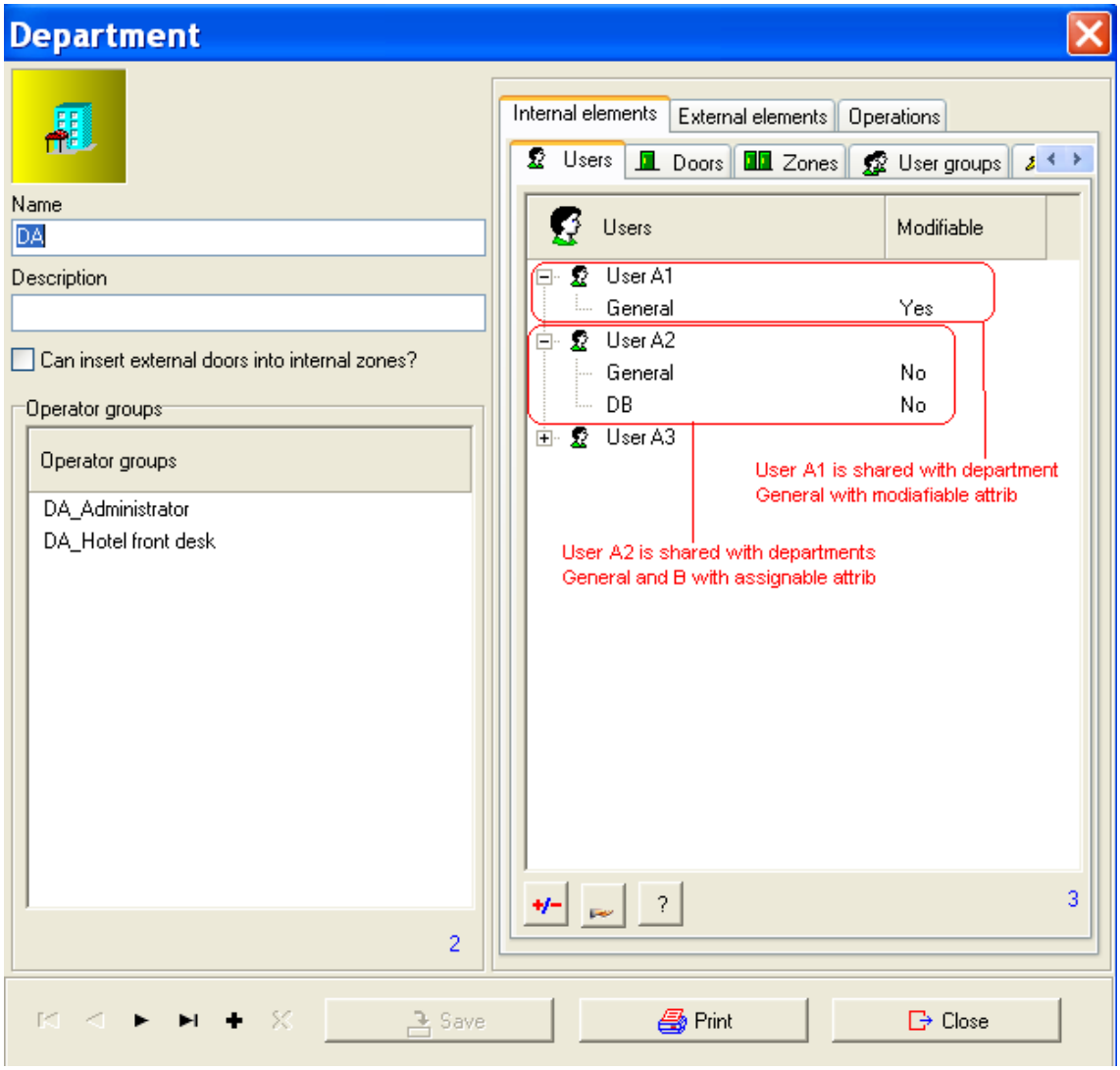


Figure 4: Screenshot of a department shared elements window.

Esta es la opción que el administrador del departamento debe utilizar para compartir o borrar elementos internos con otros departamentos.

Se debe tener especial atención cuando se modifica la compartición de un elemento con otros departamentos ya que esto también implicará la modificación de todos los accesos externos.

Por ejemplo, consideremos Puerta A, DepA. A la que accede el Usuario B. Si la puerta A no está compartida, el usuario A no podrá acceder a ella a no ser que el Usuario B este compartido con el Departamento A.

Elementos externos:

Aquí es posible ver los elementos externos del departamento, esto es, elementos de otros departamentos que los operadores de este departamento pueden modificar o asignar dependiendo del modo en el que están compartidos (Figura 5). Para añadir elementos externos al departamento, clickar en +/- y seleccionar los elementos externos que queremos añadir o quitar. Para modificar los atributos modificables, seleccionar elemento y clicar "?" y seleccionar el valor del atributo. Estas operaciones sólo pueden realizarse por el Super_admin, otros administradores sólo pueden quitar elementos externos pero nunca pueden añadir elementos ni cambiar sus atributos.

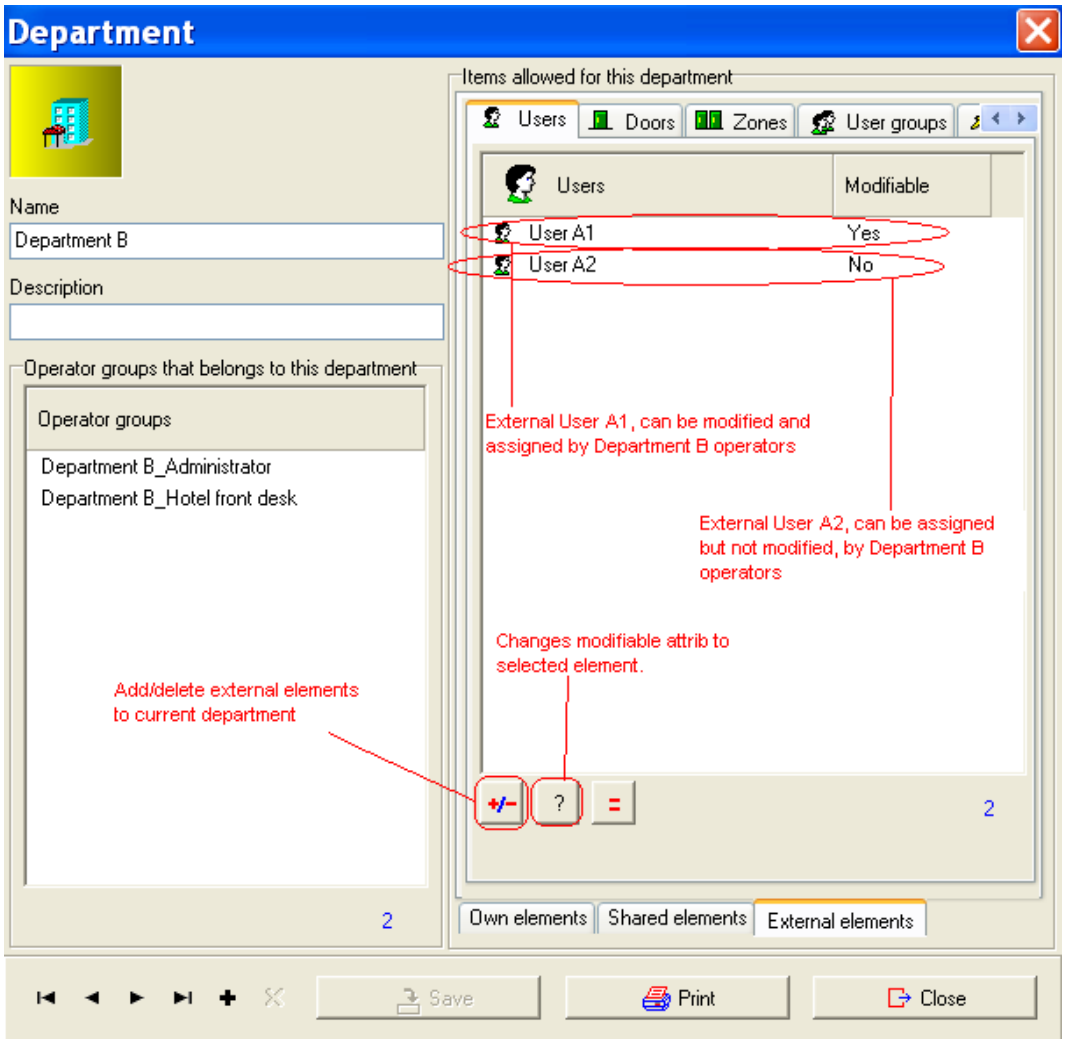


Figure 5: Screenshot of a department external elements window.

Operaciones

Aquí es posible especificar que operaciones se permiten realizar al administrador del departamento y a los grupos de operadores de su departamento. El modo es el mismo que en los grupos de operadores.

Grupos de Operadores

El modo de crear grupos de operadores no ha cambiado pero hay unas nuevas opciones en él (Figura 6). Los permisos se descomponen en un mayor nivel de detalle. Por ejemplo, ahora es posible especificar si un operador puede hacer cambios en puertas, usuarios, si puede añadir o borrar puertas, usuarios. Un Grupo de operadores nunca podrá tener más permisos que su administrador. Esto es, si un administrador no tiene permiso para modificar puertas, los grupos de operadores de ese departamento nunca tendrán esta opción. También esposible definir el nivel de privilegios de cada operador. De esta forma, si el grupo de operadores tienen un nivel bajo de privilegio, sus operadores no podrán hacer cambios en elementos de nivel medio o alto aunque tengan esa opción activada. Para utilizar los niveles de privilegio hay que activarlos en la ventana de configuración de las opciones avanzadas.

Hasta ahora no había ninguna restricción para descargar cualquier puerta al ppd para su inicialización, actualización o apertura de emergencia. Ahora con la opción departamental existe esta restricción: Un operador puede sólo descargar puertas de su departamento. La apertura de emergencia sólo es válida para las puertas de su departamento (PPD con versión de firmware 1.01 o superior)

No obstante, puede darse el caso de no desear esta opción (ej: Grupo de Mantenimiento). Quitando el tic “Controla todas las puertas con el PPD” es posible permitir descargar puertas que pertenezcan a otros departamentos.

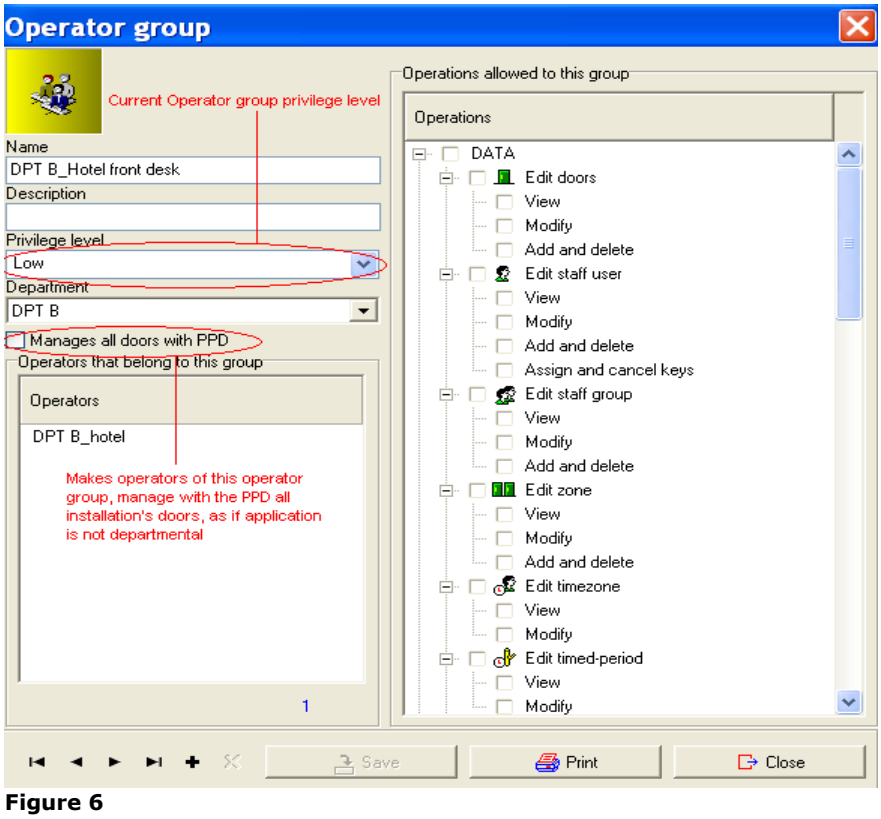
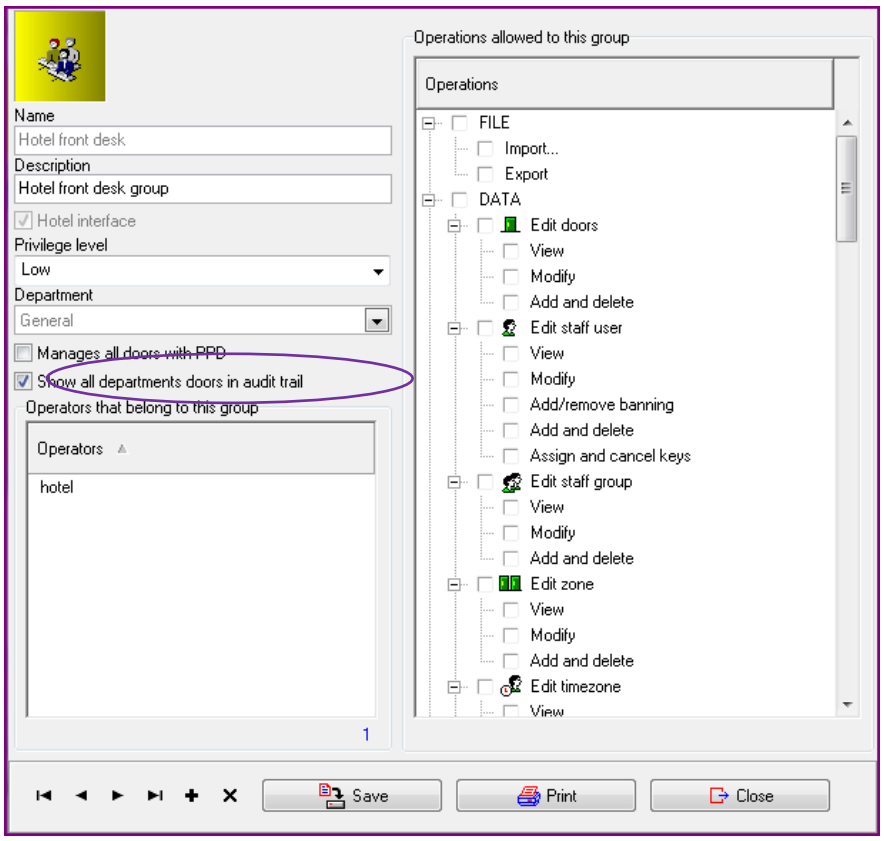


Figure 6

Como se puede ver en la siguiente imagen, se puede permitir la visualización del auditor de cerraduras con puertas que pertenecen a otros departamentos. Para que esto es necesario activar la opción de "Mostrar puertas de todos los departamentos en el auditor de cerraduras".



Cómo trabajar con elementos Externos

Para explicar cómo trabajar con elementos externos, la explicación se basa en Usuarios y Zonas, pero esto puede aplicarse al resto de elementos de la aplicación: Nivel de accesos, puertas, salidas, etc.

Cuando un operador accede a la ventana de un elemento, puede ver dos tipos de elementos: Elementos internos y elementos externos los cuales se ven en distinto color (Figura 7). El operador no puede borrar elementos externos (al no ser que sea el super_admin), puede modificar el perfil y accesos si está compartido con la opción modificable o sólo cambiar accesos si está compartido con el atributo asignable.

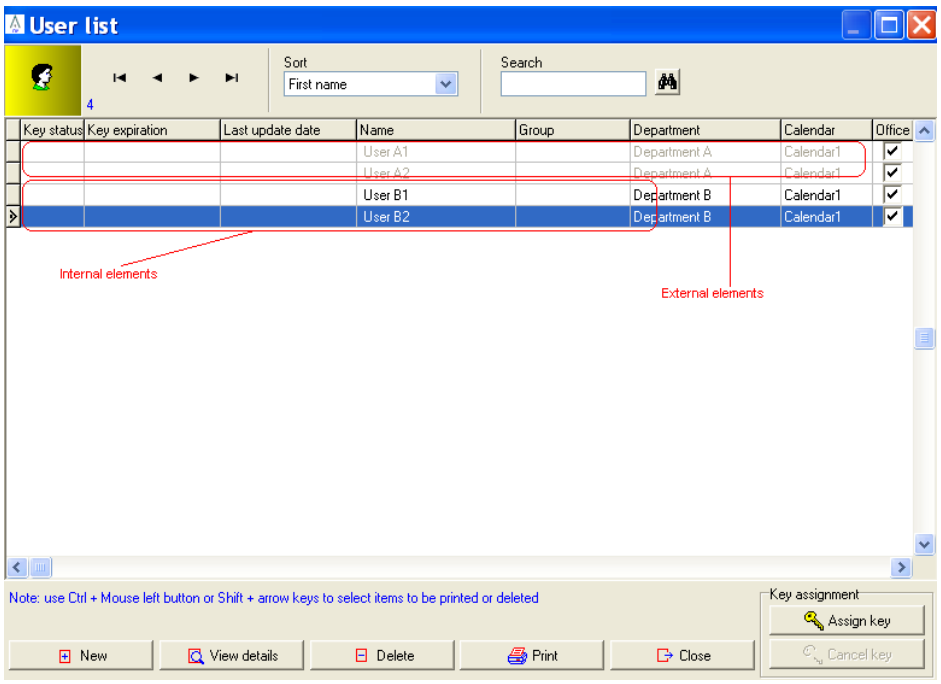


Figure 7

Cuando llega el momento a un operador de editar y modificar el perfil de un elemento que le ha sido asignado, puede encontrarse con alguna restricción debido a diferentes razones como: el elemento es externo, el nivel de privilegio requerido es muy alto, el elemento no ha sido compartido con el atributo modificable, el operador no tiene permiso para realizar modificaciones, etc.

Para ver si un operador puede editar o modificar un perfil se muestra un icono con el siguiente significado:

- Sin candado: El operador tiene el control total sobre ese usuario si es un usuario interno y el control de sus externos (no puede cambiar nivel de accesos de usuarios.

- amarillo: El operador puede sólo cambiar accesos para ese usuario. Esto es, añadir o quitar puertas internas, zonas. Peero no puede hacer ningún cambio en el perfil. Esto ocurre porque está compartido sin atributos modificables.

- rojo: No puede hacer ningún cambio en el usuario. Esto es porque no tiene el nivel de privilegio suficiente o no puede hacer cambios en usuarios

Para modificar accesos de un usuario, hay que tener en cuenta unas consideraciones dependiendo si el usuario es interno o externo:

- Cuando es un usuario externo, el operador sólo puede añadir o quitar accesos internos, nunca externos (Figura 8). También el operador debe tener nivel de privilegio suficiente. Esto es, aunque una zona de otro departamento le haya sido compartida esta no la puede asignar a un usuario externo. Y aunque la zona sea interna deberá tener el nivel de privilegio suficiente. Los elementos que no pueda modificar aparecerán con un candado rojo.

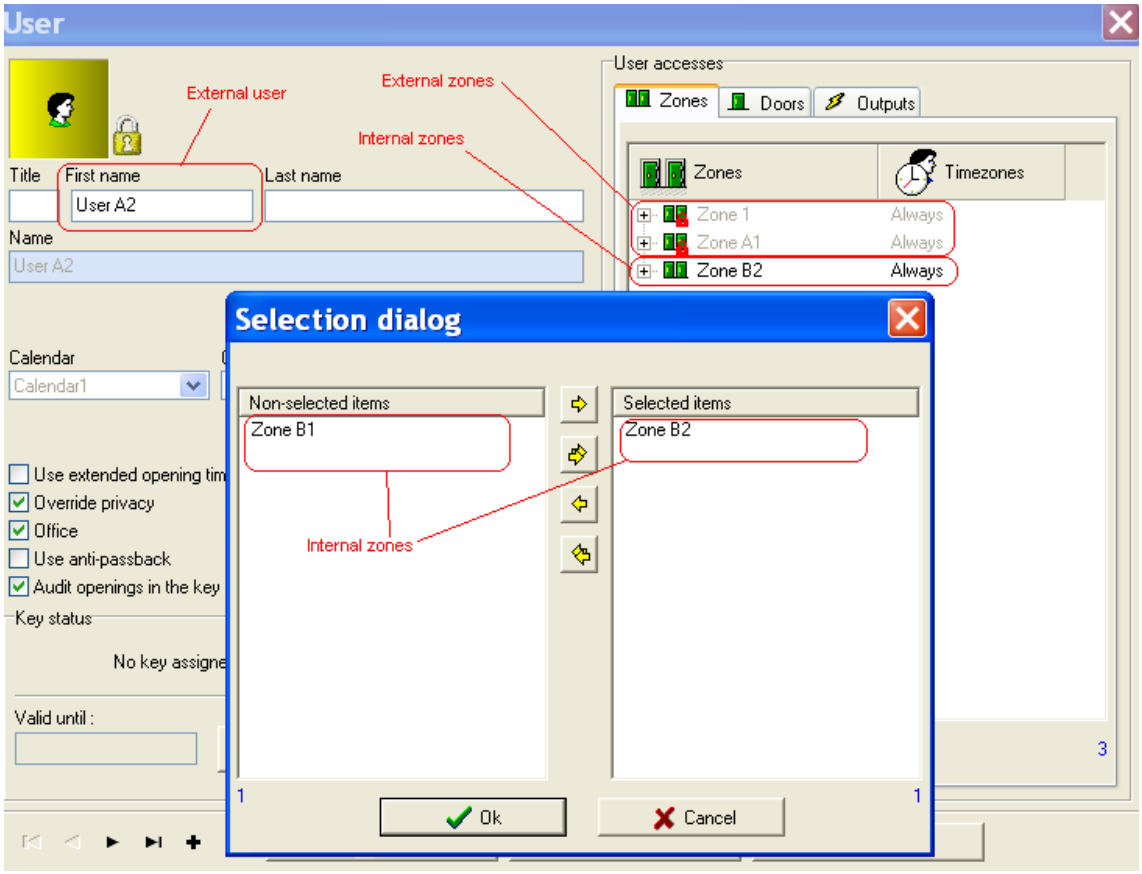


Figure 8: Example of an external user profile. It can be appreciated external elements in a different color and the impossibility to add/remove external zones to an external user.

- cuando se trate de un usuario interno, el operador es capaz de añadir/quitar cualquier acceso con el mismo o menor nivel de privilegio sin importar que sea externo o interno (Figura 9). Tiene control total en usuarios internos con la única excepción que no puede asignar un timezone a un acceso externo si el elemento externo no está compartido. Este caso se presentará con un candado amarillo. Esto es, Dpt A, Usuario A accede a Dpto B con un timezone. Si Dpto a usuario a está compartido Con Dto B la timezone no podrá ser modificada porque asumimos que el dueño de la zona le ha dado acceso al usuario con la timezone que él quería. Pero si Dto B Zone B está compartida con Dpto A entonces la timezone se puede modificar porque es el dueño del usuario el que le ha dado acceso a esa zona.

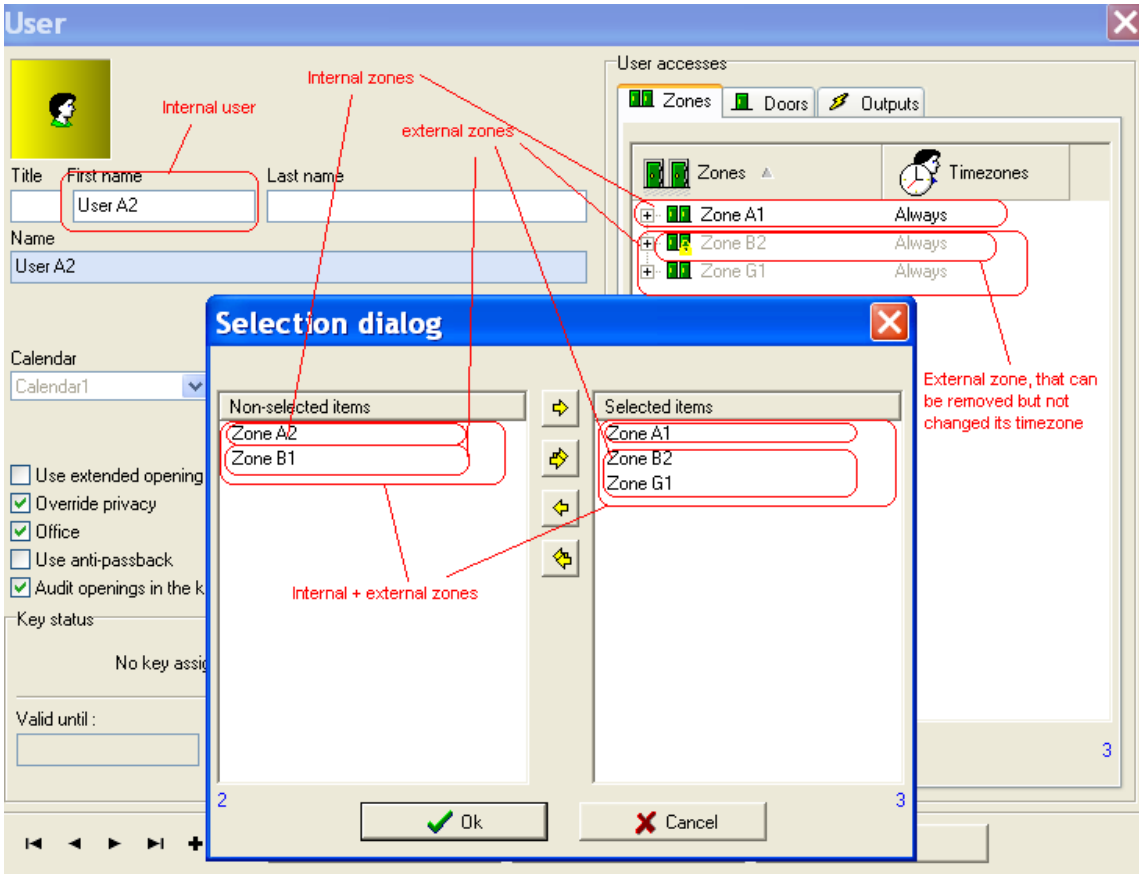
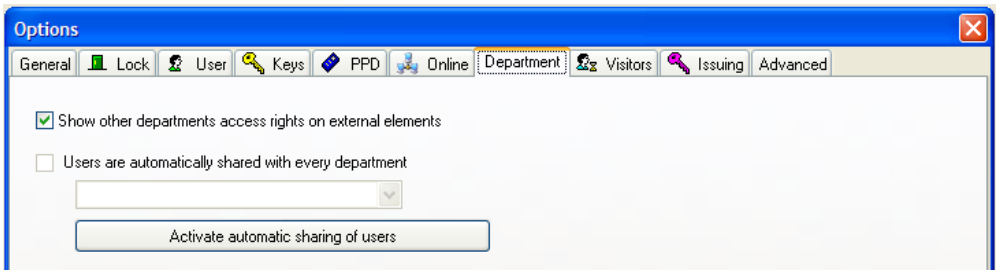


Figure 9: Example of an internal user profile. It can be appreciated external elements in a different color and how can add/remove external + internal zones to an internal user.

Entonces, para añadir una zona interna a un usuario externo hay dos formas de hacerlo; Ir al perfil del usuario externo y darle acceso a la zona interna del departamento o ir al perfil de la zona interna y darle acceso al usuario externo.

En la siguiente figura se muestran los accesos externos de un usuario externo pero estos accesos externos pueden esconderse. Para ello, hay que ir a HERRAMIENTAS/CONFIGURACIÓN/OPCIONES GENERALES y en la ventana del departamento deseleccionar la casilla "Mostrar accesos de otros departamentos en elementos externos".



Conectar el PPD

Programador Portátil

Usted puede necesitar conectar el programador portátil al ordenador para realizar una apertura de emergencia, por ejemplo. Esto puede ser necesario en el caso de que se agoten las pilas del escudo electrónico de una puerta.

Para realizar una apertura de emergencia, siga los pasos explicados a continuación. Pulse la opción de menú PPD del menú principal de recepción. (Asegúrese que el PPD está conectado al puerto serie)

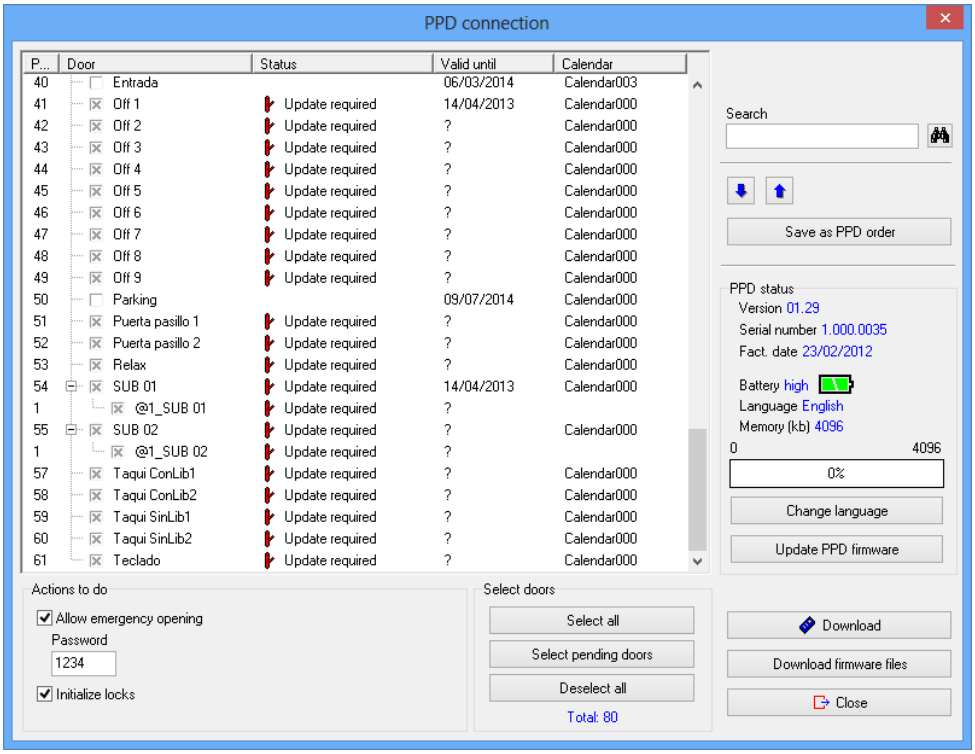
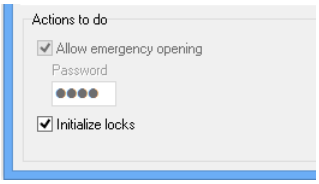


Figura 78

En la ventana de la esquina inferior izquierda, titulada ACCIONES A REALIZAR, seleccione la opción PERMITIR APERTURA DE EMERGENCIA. Seleccione igualmente la puerta que quiera abrir en emergencia en la lista de puertas. En cuanto seleccione esta opción, el campo “Clave” se activará, de esta manera podrá colocar una clave que el PPD pedirá antes de realizar una apertura de emergencia.

Si ya se ha pre configurado una clave en OPCIONES GENERALES, menú PPD, el campo aparecerá en gris y la clave predefinida se solicitará siempre que use el PPD para una apertura de emergencia.



Si el campo se deja en blanco, el PPD no solicitará ninguna clave.

A continuación pulse el botón DESCARGAR para pasar los datos al PPD.

NOTE que esta opción solo está disponible en PPD versión 01.29 y superior.

- La transferencia de información tardará unos segundos. Cuando vea que llega al 100% la barra de progreso, desconecte el PPD del cable serie y diríjase a la puerta que necesita una apertura de emergencia.
- Encienda el PPD, mediante una pulsación de la tecla roja, y seleccione la opción de menú APERTURA DE EMERGENCIA. Utilice las flechas para viajar a lo largo de las opciones de menú.

- Pulse la tecla verde para validar su elección. La pantalla del PPD le dará el siguiente mensaje: CONECTAR CON CERRADURA.

- Conecte el PPD con la cerradura utilizando el cable de comunicación que tiene una tarjeta especial en su extremo. Inserte esta tarjeta en la ranura de manera que los contactos eléctricos queden mirando hacia el lado del chip.

- Escuchará el ruido del motor de la cerradura, y a los pocos segundos verá que la puerta puede ser abierta y la pantalla del PPD le dará el mensaje: PUERTA ABIERTA, NÚMERO DE HABITACIÓN.

Recomendamos cambiar las pilas de la cerradura que acaba de ser abierta, inmediatamente. Los escudos de Salto llevan 3 pilas alcalinas modelo LR03 AAA, 1,5 V.

Después del cambio de pilas, es necesario realizar una actualización del escudo electrónico con el PPD ya que al agotarse las pilas, se para el reloj interno de la cerradura y se pierden los horarios y los calendarios. Para saber cómo se realiza una actualización con el PPD, consulte el manual de usuario del PPD Smart que encontrará en el mismo CD-ROM donde viene el software RW.

Auditor de Cerraduras.

Recoger las aperturas en una puerta.

Es posible averiguar quién ha abierto las puertas del hotel y en qué momento, auditando las puertas de nuestra instalación. Para auditar una puerta, siga los pasos explicados a continuación:

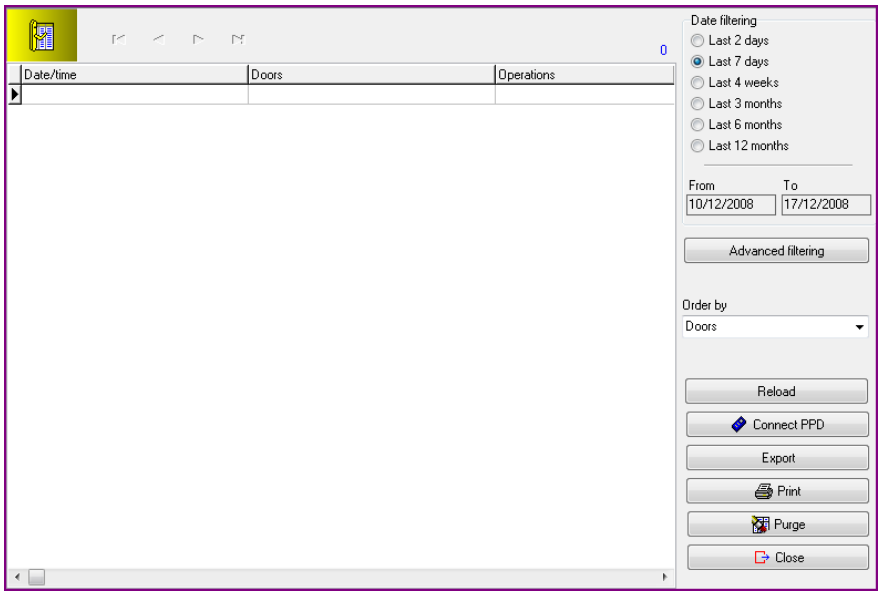
- Tome el PPD y diríjase a la puerta que quiera auditar. Encienda el PPD mediante una pulsación de la tecla roja y busque la opción de menú RECOGER APERTURAS.

- Pulse la tecla verde para validar su elección, y verá que el PPD le da el mensaje CONECTAR CON CERRADURA.

- Conecte el PPD a la cerradura utilizando el cable de comunicación que termina en una tarjeta especial y verá que se produce una transferencia de datos.
- Vuelva a conectar el PPD con el puerto serie del ordenador.

- Si el PPD tiene en su pantalla el mensaje "CONECTAR CON CERRADURA", pulse una vez la tecla roja para subir un nivel en su escala de menús. Si no lo hace así, no podrá comunicarse ahora con el ordenador.

- Pulse la opción AUDITOR DE CERRADURAS del menú de recepción. Se abrirá una ventana como la siguiente:



Ahora pulse el botón CONECTAR PPD de la ventana activa del software. La información que recogió con el PPD aparecerá en la ventana. El botón titulado ORDENAR POR le puede servir para visualizar la información según el criterio que le resulte más cómodo, por fecha, por persona, por puertas, etc…

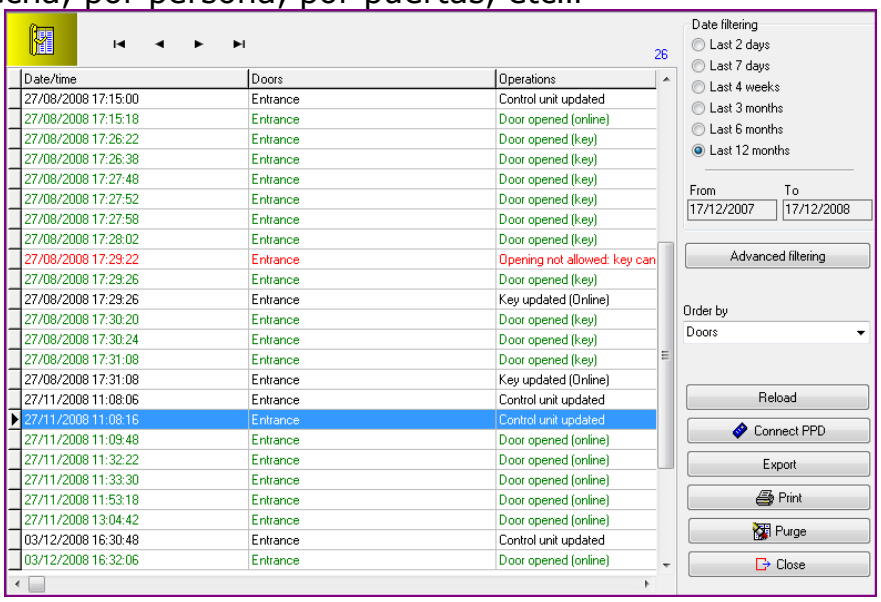
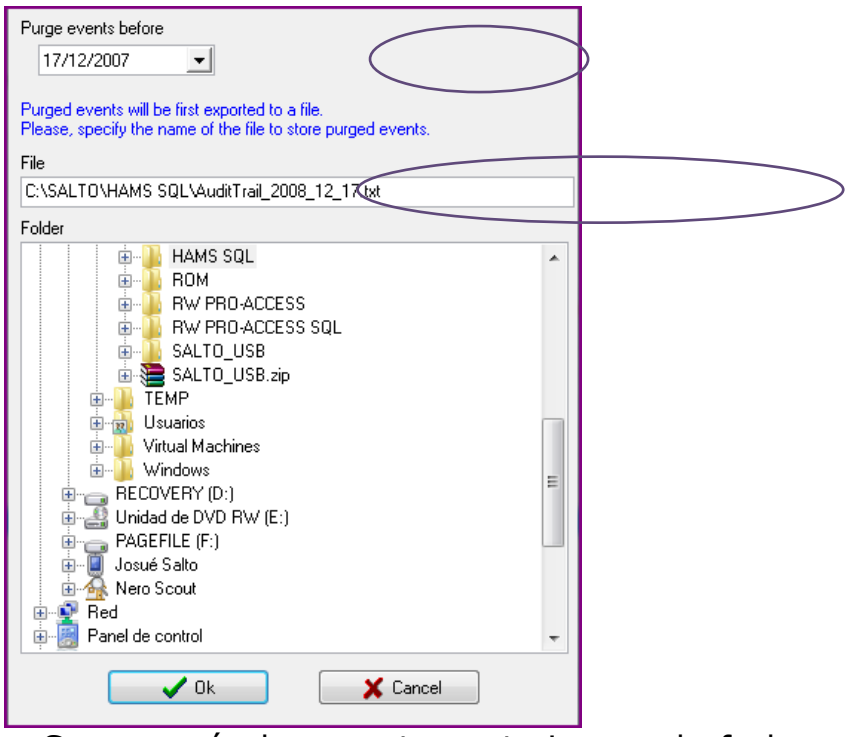


Figura 79

En color rojo aparecen los intentos fallidos de apertura, por parte de clientes que no corresponden a esa habitación, o por parte de miembros de la plantilla del hotel que tampoco tienen acceso a esta habitación.

PURGADO: es recomendable hacer un purgado del auditor de cerraduras por lo menos una vez al mes. El tener el auditor de cerraduras con un mínimo de registros, aligera la comunicación con las unidades online, la carga y descarga del PPD y hace más rápida la búsqueda de registros por el auditor.

Para hacer un purgado de los eventos, presione en el botón "Purgar" y aparecerá una ventana como la que se muestra en la imagen siguiente.



- Se purgarán los eventos anteriores a la fecha seleccionada en el campo "Purgar eventos anteriores a:"
- En los campos "Fichero" y "Carpeta", puede seleccionar donde quiere guardar un copia en formato TXT del auditor de cerraduras que va a purgar.

Llaves de Repuesto y Programadoras

Cada departamento será capaz de realizar llaves programadoras y de repuesto para las habitaciones de su propio departamento. El super_admin. Puede hacer llaves para cualquier departamento seleccionando primero el departamento para el que quiere hacer las llaves

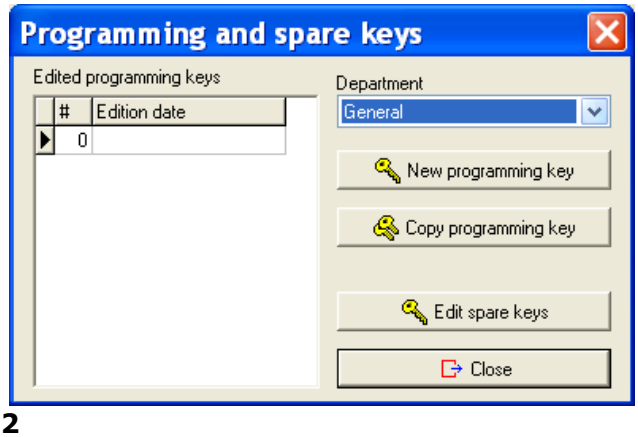


Figure 12

Sincronización automática y Stadging Table

(Standging table solo para servicio)

Nota: Esta herramienta está disponible en los software HAMS/ PA Connected o superior

Por medio de esta herramienta se va a permitir sincronizar datos de usuario entre dos sistemas diferentes, Salto y otro externo (maestro) por medio de ficheros de texto. El sistema maestro es responsable en realizar los ficheros de datos y Salto es responsable de procesarlos y volcarlos a su base de datos.

Básicamente esta aplicación funciona de la siguiente manera (ver el documento de especificaciones para más detalles): el sistema maestro produce un fichero de texto que contenga una lista de usuarios. Para cada usuario de la lista el maestro debe especificar las operaciones que se han de realizar en la base de datos salto. Por el momento las acciones que se pueden realizar son las siguientes:

1) Añadir un nuevo usuario a la base de datos Salto.
2) Actualizar parámetros de un usuario existente.
3) Actualizar parámetros de un usuario existente o crear nuevo si no existe.
4) Eliminar registro.
5) Cancelar usuario

Por lo tanto es importante que quede clara la diferencia entre la sincronización y la importación, con la cual únicamente solo se podían añadir nuevos elementos a la base de datos pero no modificarlos ni eliminarlos.

Hay que tener en cuenta que actualmente la sincronización SOLO trabaja con usuarios, no se puede sincronizar otra clase de elementos de la base de datos (puertas, zonas, etc). En un futuro las herramientas de sincronización podrían ser extendidas al resto de elementos. De forma similar otros tipos de formato de ficheros de texto podrán ser integrados en el proceso.

Es importante tener en cuenta que el proceso de sincronización solo se puede llevar a cabo a través de la aplicación Salto que se ha definido como maestro de comunicaciones.

El software facilita un wizard para guiar al usuario a través de la configuración de la sincronización. Básicamente a través del

wizard al usuario se le consulta sobre la localización de los ficheros de la sincronización, significado de cada columna del fichero y el tipo de plan de calendario (Ver figuras de 9 a 13).

Los procesos de sincronización se pueden programar de forma muy flexible. Por ejemplo como se muestra e la figura 13 es posible ejecutar la sincronización de forma regular (cada 10 minutos todos los días). Gracias a esta programación flexible el sistema maestro puede sincronizar sus datos de usuarios de forma automática sin ninguna intervención manual en el software Salto.

Para comprender el modelo de datos de usuarios en el cual está basado la herramienta de sincronización ver el documento de especificaciones anexado. No todos los datos de los usuarios son sincronizables, por ejemplo en esta primera versión no es posible sincronizar datos referentes a la autorización de accesos (puertas/zonas y horarios)

En cuanto a opciones en el interface gráfico se puede crear sincronizaciones en dos formas diferentes como se ve en las figuras de abajo. O seleccionando Fichero\Importar/Exportar\Sincronización en el menú o en Herramientas\Tareas programadas. En cualquiera de las opciones se acaba por añadir un nuevo trabajo de sincronización a la lista de tareas programadas como se ve en la figura 8. Se pueden modificar los parámetros de una sincronización sin más que pulsando en “Ver detalles” en la ventana de lista de trabajos. Haciendo esto el mismo wizard se muestra otra vez para realizar los cambios deseados.

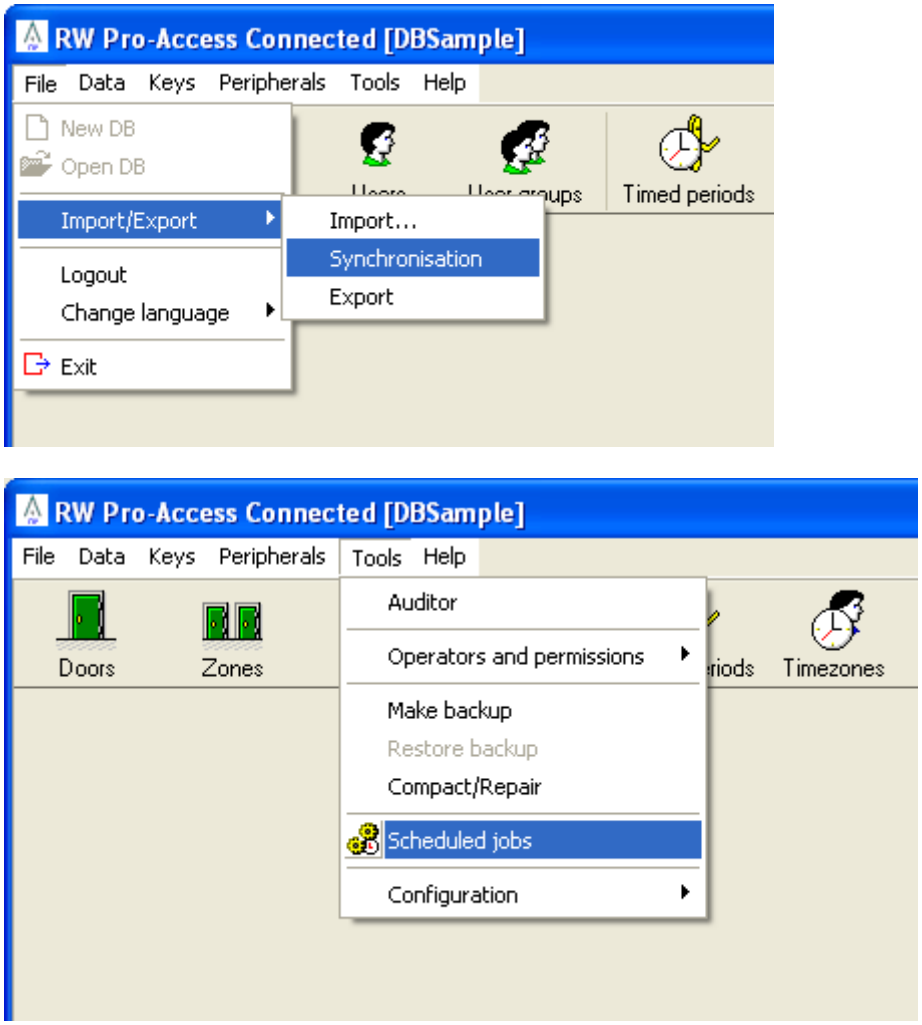


Figura 7: dos opciones diferentes para ejecutar una sincronización.

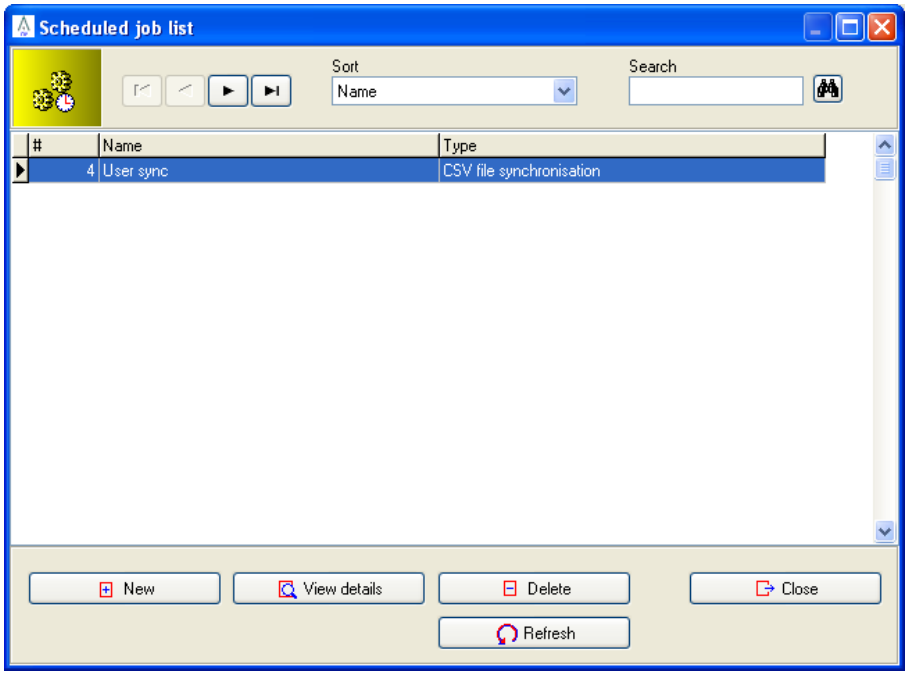


Figura 8: Lista de tareas programadas.

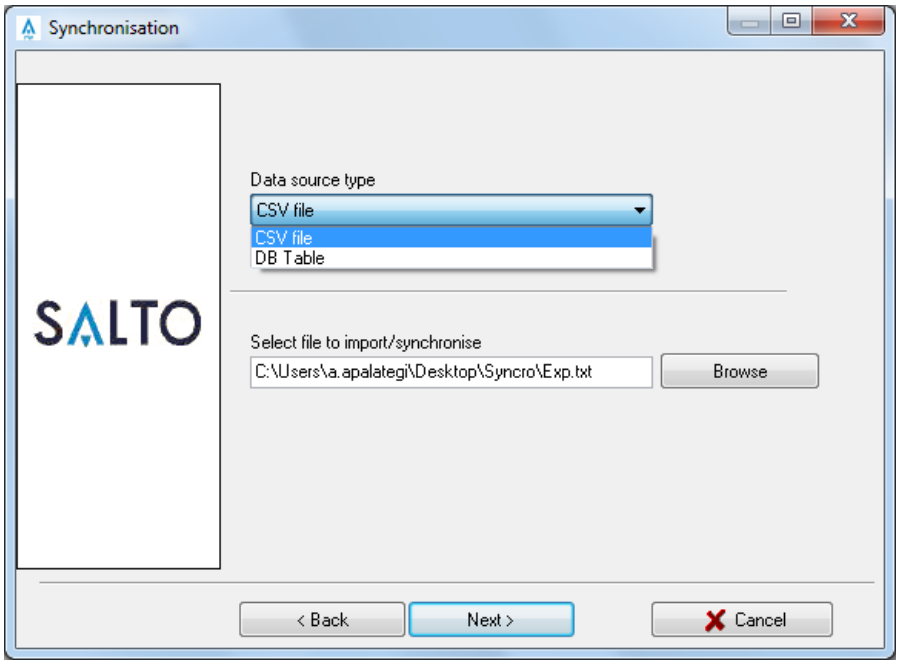


Figura 9: wizard de sincronización de datos. Especificación del tipo y localización de datos.

El tipo de fuente de datos puede seleccionarse en el momento de hacer una sincronización de datos, dependiendo del fichero de origen que vaya a usarse. El fichero puede ser de tipo CSV (ficheros

tipo *.csv, *.txt) o del tipo tabla de base de datos (tablas de SQL Server, Oracle u ODBC).

Consultar por favor los siguientes documentos para obtener más detalles de ambos tipos de ficheros de sincronización:

- Ficheros CSV: El documento **SALTO_Data_Sync_1_9**.
- Tablas de Base de Datos: El documento **SALTO_User_Sync_Staging_Table_0_9**.

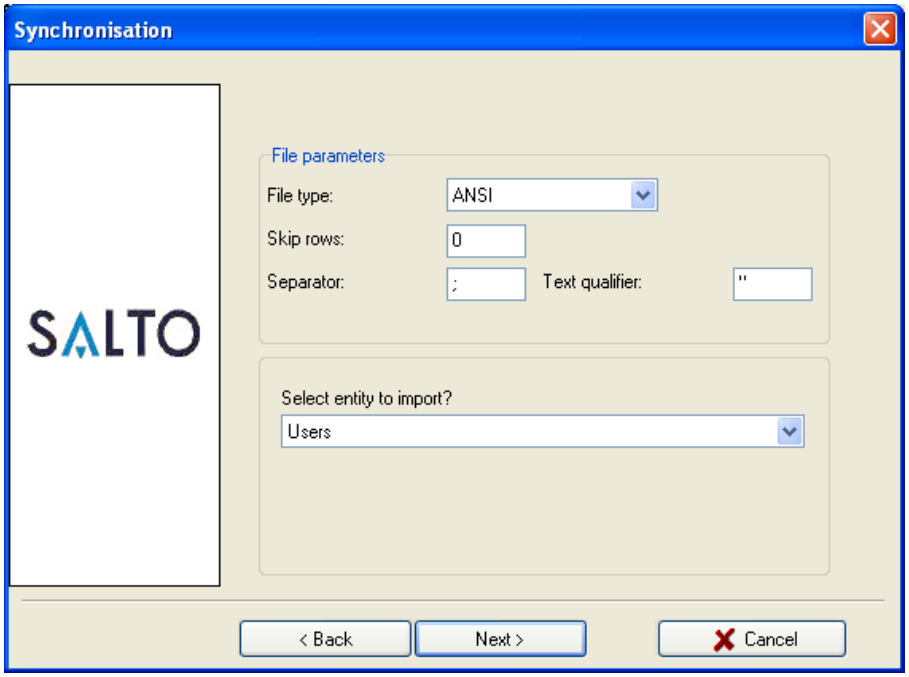


Figura 10: wizard de sincronización de datos. Especificación de los parámetros CSV y tipo de elementos.

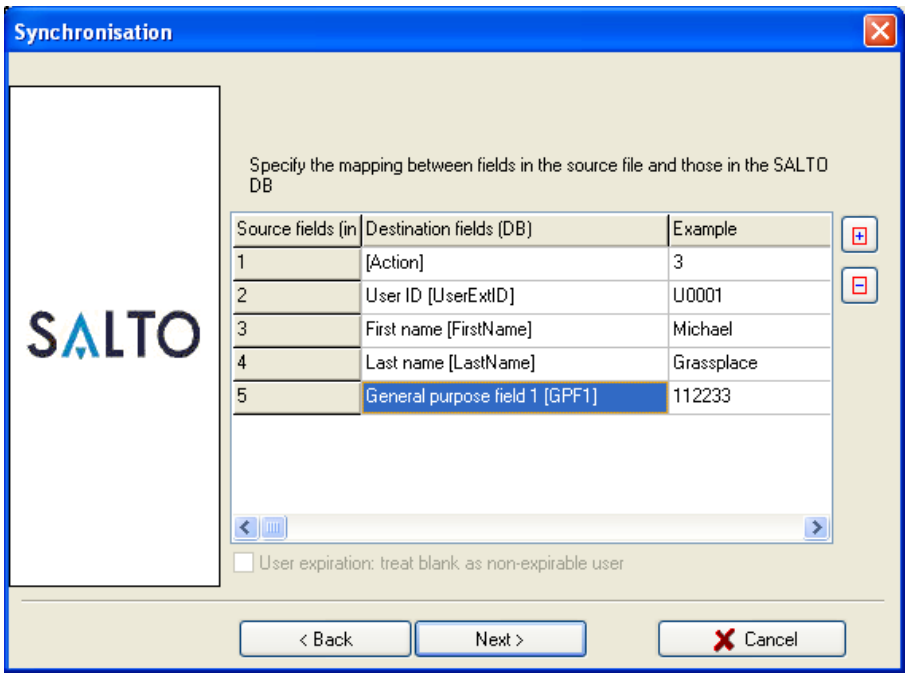


Figura 11: wizard de sincronización de datos. Significado de las columnas del fichero CSV.

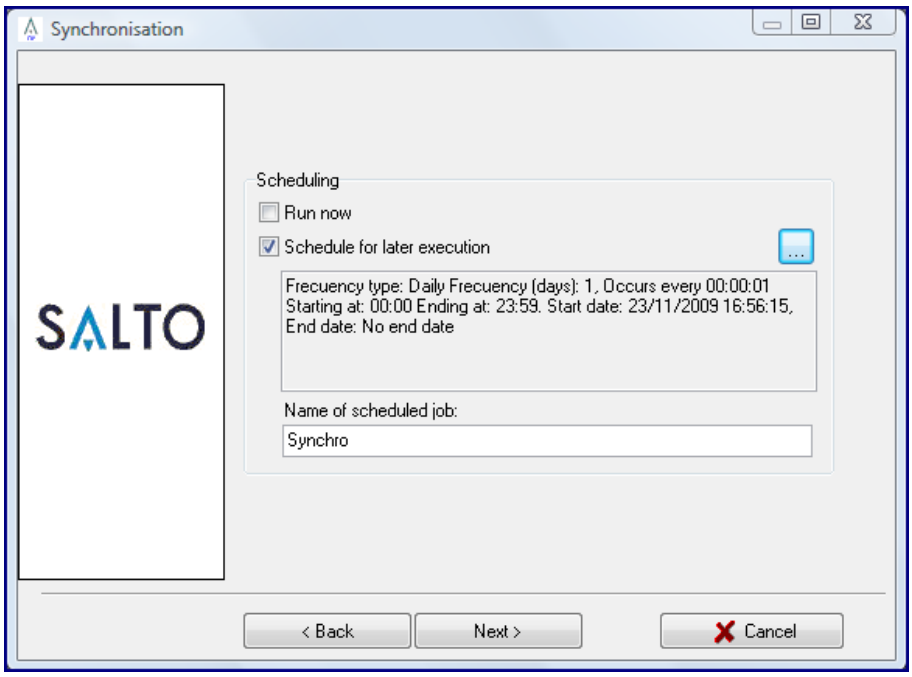


Figura 12: wizard de sincronización de datos. Programación de la sincronización y nombre de la sincronización. Es posible programar una sincronización cada 1 segundo.

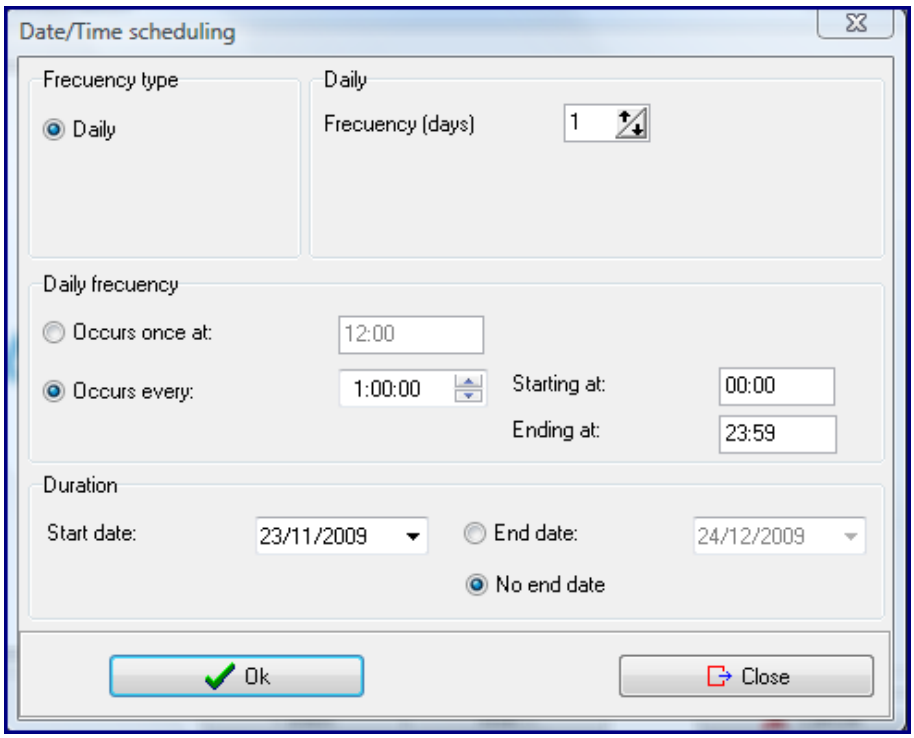


Figure 13: asistente de sincronización de datos. Programación del plan.

Streams de eventos (solo disponible en Servicio SALTO!)

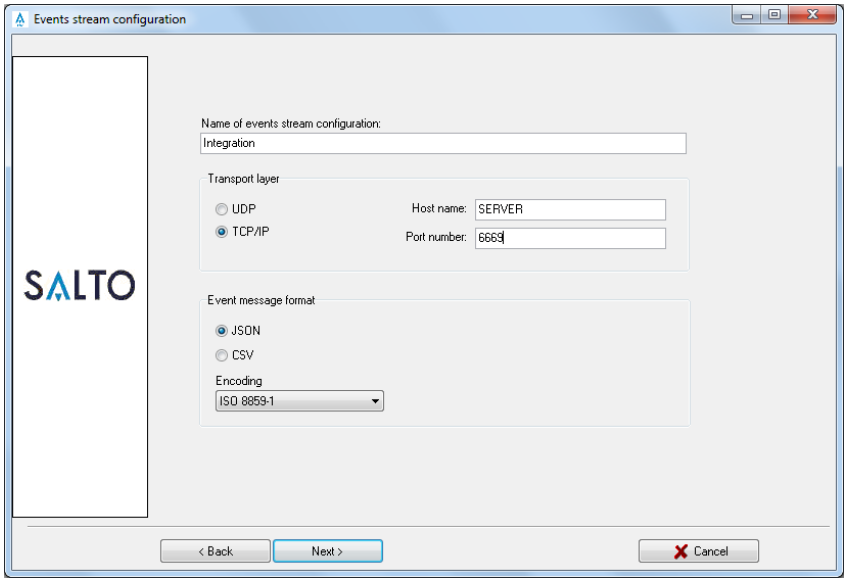
Esta función permite a aplicaciones de terceros la recepción en tiempo real de las incidencias enviadas por el software de SALTO.

A continuación se detallan los pasos a seguir para establecer un proceso de streaming de eventos.

Seleccionar la opción de Streams de eventos situada en HERRAMIENTAS/STREAMS DE EVENTOS.

El botón "NUEVO" abrirá el asistente de configuración.

Seleccionar un nombre para el stream de eventos.
Se debe abrir un puerto UDP o TCP para establecer la comunicación con el software cliente.
Especificar el nombre del HOST y el número de puerto.



Los eventos se pueden representar en los siguientes formatos: JSON o CSV.

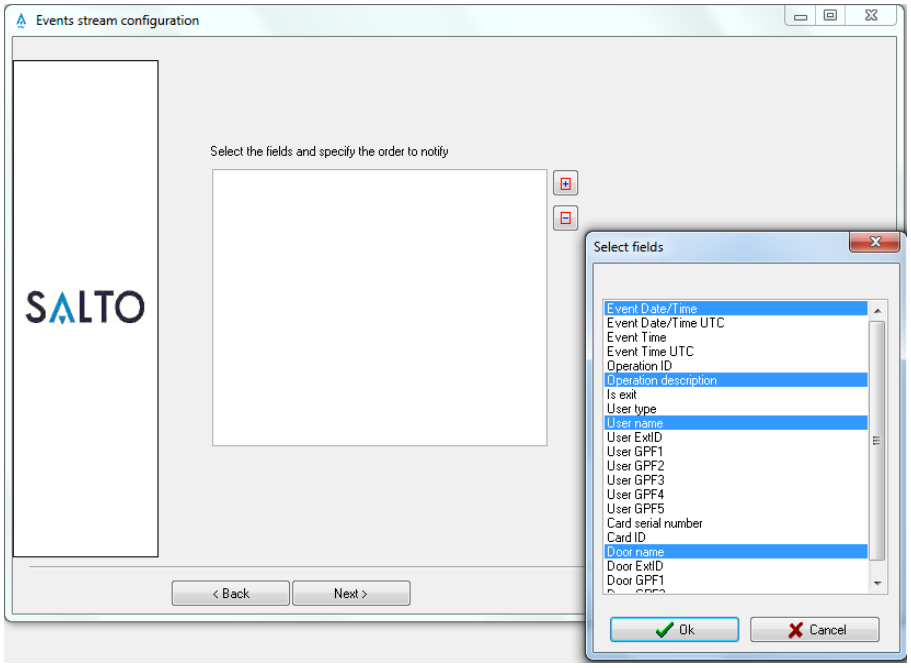
JSON es un formato ligero para el intercambio de datos. El ejemplo siguiente debería servir para tener una idea de cómo se representarán los datos enviados por Salto:

```
[
{
"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 es un formato de texto con valores separados por comas. Ejemplo:

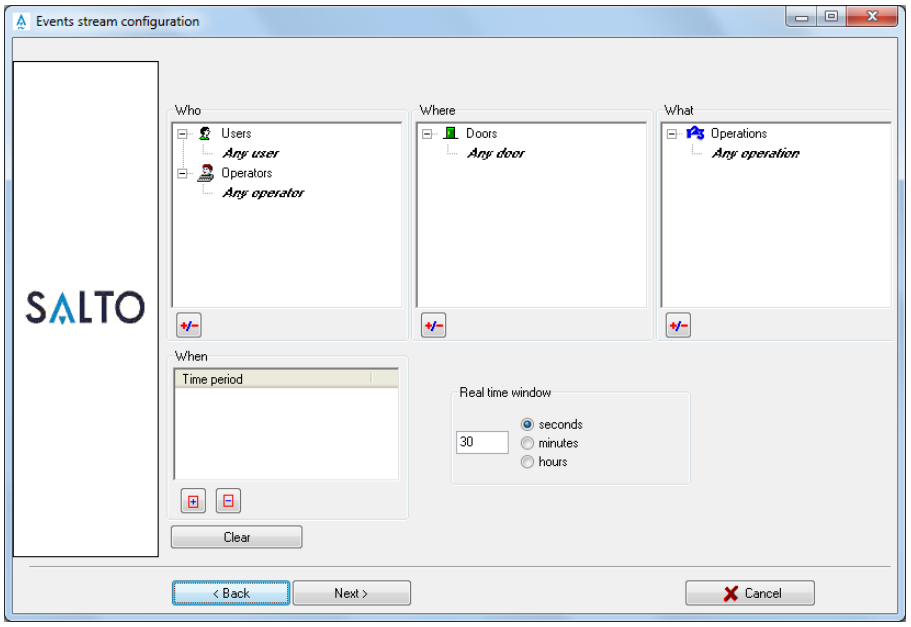
EVENT_START "11223344556677889900"; 2012-04-14T13:03:20; 13:03:20; 2012-04-14T13:03:20z; 17; "Door opened: key"; false; 0; "John Smith"; "Marketing department"; "Gym"; "Leisure area" EVENT_END

Pulsar en "SIGUIENTE"



Seleccionar la información que se va a enviar desde la lista de campos.

Pulsar en "SIGUIENTE"



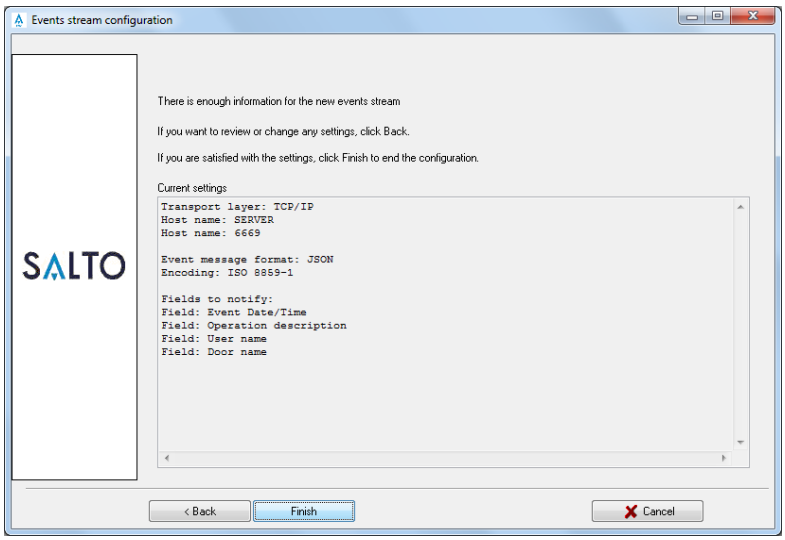
Esta ventana permite filtrar los siguientes parámetros:

- Quién
- Dónde

- Qué
- Cuándo

La "Ventana de tiempo real" permite limitar los eventos en función del tiempo. Un valor de 1 minuto enviará los eventos incluidos en este periodo de tiempo (eventos recogidos desde una tarjeta por ejemplo).

Pulse en "SIGUIENTE"

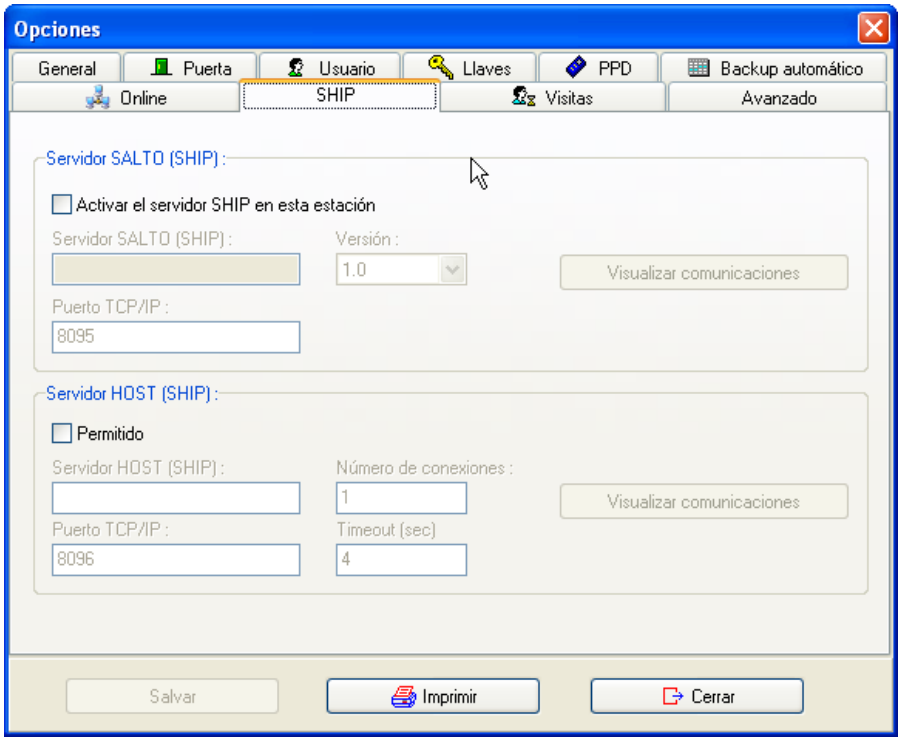


Pulse en "FINALIZAR"

Nota: Diríjase al manual técnico "SaltoEventStream_x_x" para obtener una descripción completa del modelo y listado de los eventos enviados.

SALTO Host Interface Protoco - SHIP

Para activar SHIP debemos ir al menú desplegable HERRAMIENTAS/CONFIGURACIÓN/OPCIONES GENERALES y pulsar la pestaña SHIP. Aparecerá la siguiente ventana (Fig. 1)



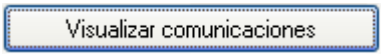
(Fig. 1)

Activar comunicación SALTO (Servidor) – Host (Cliente)

Cuando Salto actúa como servidor primeramente debemos activar la casilla:

Una vez activada, se nos mostrará el nombre del equipo que va actuar como servidor "SERVIDOR SALTO (SHIP)".

Finalmente debemos seleccionar el puerto TCP/IP por el que se va a realizar la comunicación.

La opción: 

nos permite visualizar la información intercambiada entre el servidor SALTO y todos los clientes conectados.

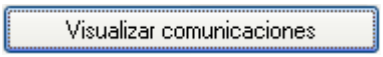
Activar la comunicación SALTO (Cliente) – Host (Servidor)

Cuando el HOST es el servidor debemos habilitar la casilla:

Una vez habilitada debemos rellenar la casilla "SERVIDOR HOST (SHIP)" con el nombre o dirección IP del equipo que va a realizar esa función.

Seguidamente rellenaremos el número de conexiones que se van a establecer así como el puerto TCP/IP por el que se van a realizar estas comunicaciones

El Timeout es el tiempo que espera un cliente SALTO a que el servidor HOST procese una petición y devuelve le resultado.

La opción: 

nos permite visualizar la información intercambiada entre el servidor HOST y todos los clientes de SALTO conectados.

Accesos por MATRIZ

Opción avanzada LOCATION_FUNCTION_MATRIX

Introducción.
Esta sección repasa la opción Matriz del Software de Salto. Se recomienda buscar la ayuda de personal certificado de Salto antes de activar esta opción.

Función. *(Trasfondo)*
La Ubicación y Función de la Matriz se usa en instalaciones muy amplias de Salto donde los límites por defecto de la aplicación no son suficientes a nivel de plan de acceso o que se desee atribuir accesos basándose en ubicaciones y funciones de puertas.

Para hacerse una idea de lo que son las ubicaciones y funciones, a continuación se muestra un pequeño ejemplo;

Tenemos 3 centros comerciales, así que aquí tenemos **ubicaciones**;

- *Centro 1*
- *Centro 2*
- *Centro 3*

Ahora, en cada centro comercial tenemos deferentes comercios. Estos comercios se pueden llamar **funciones**.

- Comercio 1 (presente centros comerciales 1 + 2)
- Comercio 2 (presente en centros comerciales 1 + 3)
- Comercio 3 (presente en centro comercial 1)
- Comercio 4 (presente en centros comerciales 2 + 3)

Las puertas del Comercio 1 en el centro comercial 1 tendrán la ubicación "Centro 1" y la función "Comercio 1". Las puertas del comercio 1 en el centro comercial 2, ubicación "Centro 2" y la función "Comercio 1"

Ahora se le pueden asignar sus derechos a los usuarios, para abrir todas las puertas con la función "Comercio 1" en la ubicación "Centro 1" pero no en "Centro 2"

Es muy importante tener diferentes ubicaciones, esto permitirá usar una herramienta muy potente para un crear un buen plan de acceso, aunque también es muy importante definir la manera como se va a trabajar con esta herramienta. Por eso, Salto recomienda ponerse en contacto con su colaborador de Salto para aclarar el funcionamiento de esta función antes de ponerlo en marcha por cuenta propia.

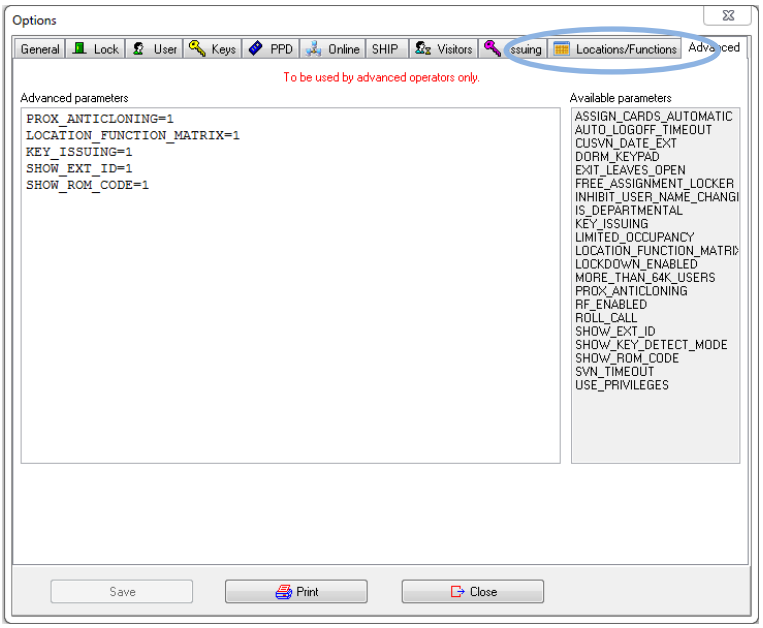
Inicio:

Paso 1. ACTIVANDO "LOCATION_FUNCTION_MATRIX"
Paso 2. CREANDO AGRUPACIONES PARA UBICACIONES Y FUNCIONES
Paso 3. CREANDO UBICACIONES Y FUNCIONES
Paso 4. ASIGNANDO PUERTAS A UBICACIONES Y FUNCIONES
Paso 5. ASIGNANDO ACCESOS Y HORARIOS A USUARIOS

Paso 1. Activando "Location_Function_Matrix"

Para activar esta función, es necesario activar LOCATION_FUNCTION_MATRIX=1" en Herramientas/ Configuración/ Opciones Generales/ y la pestaña Avanzado.

Al salvar el cambio, aparecerá una nueva pestaña llamada Ubicaciones/ Funciones donde se puede configurar la agrupación de la matriz.

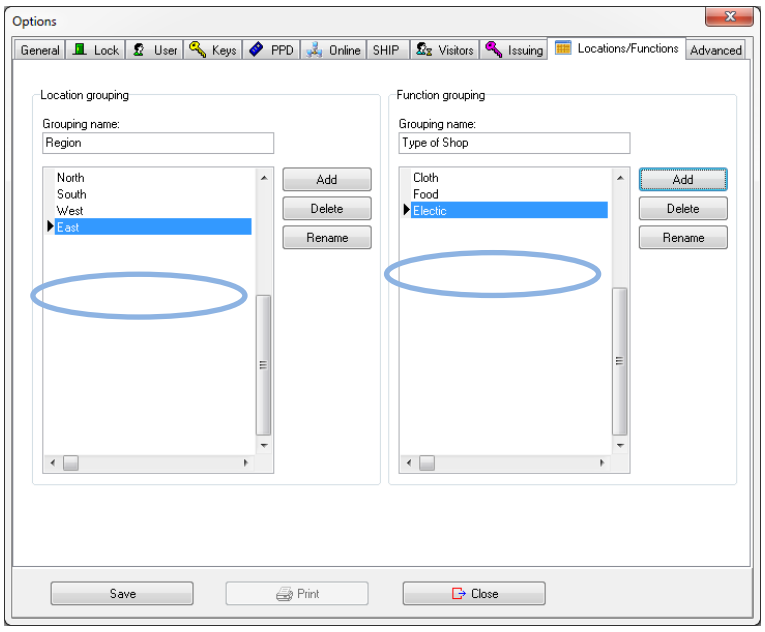


Paso 2. Creando agrupaciones para Ubicaciones y Funciones

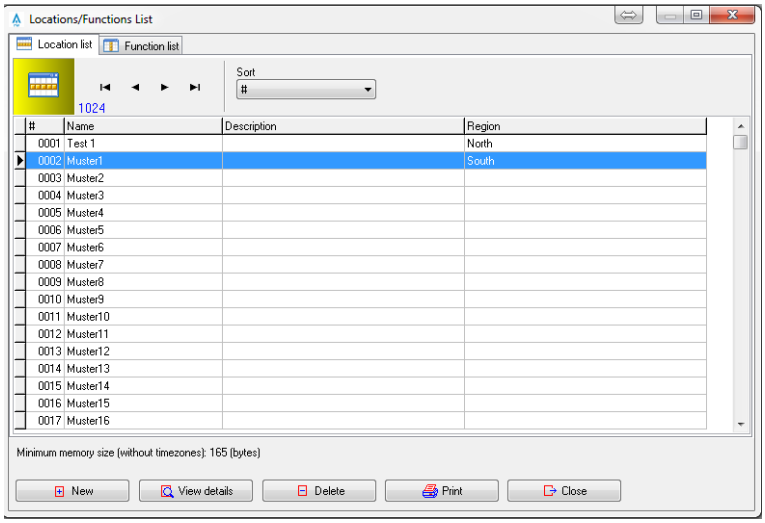
En esta parte, se pueden crear agrupaciones para las ubicaciones y para las funciones.

Importante: Si se va a usar esta opción, es necesario poner un nombre en el campo libre.

Este será el nombre de las agrupaciones, según nuestro ejemplo; "Region" y "Type of Shop".



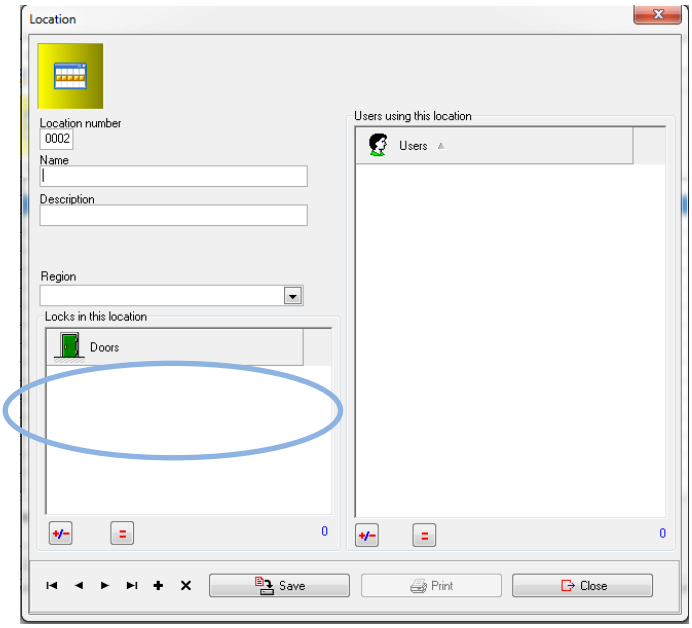
Paso 3. Creando Ubicaciones y Funciones.



Para crear las ubicaciones y funciones es necesario ir a Datos/ "Lista de Ubicaciones/ Funciones"

Aparecerá una ventana donde crear las ubicaciones y funciones necesarias, seleccionando la pestaña deseada y pulsando en "Nuevo".

Hay limitaciones a nivel de cantidades en el software;
Para Ubicaciones, max. 1024
Para Funciones, max. 256.



Para crear una nueva ubicación es imprescindible nombrarla.

Se recomienda que los nombres usados estén relacionados con la instalación y añadir una descripción.

Si se ha activado, es posible asignarla a una agrupación, en este caso, siguiendo con el ejemplo, sería "Region" como visto en el Paso 2.

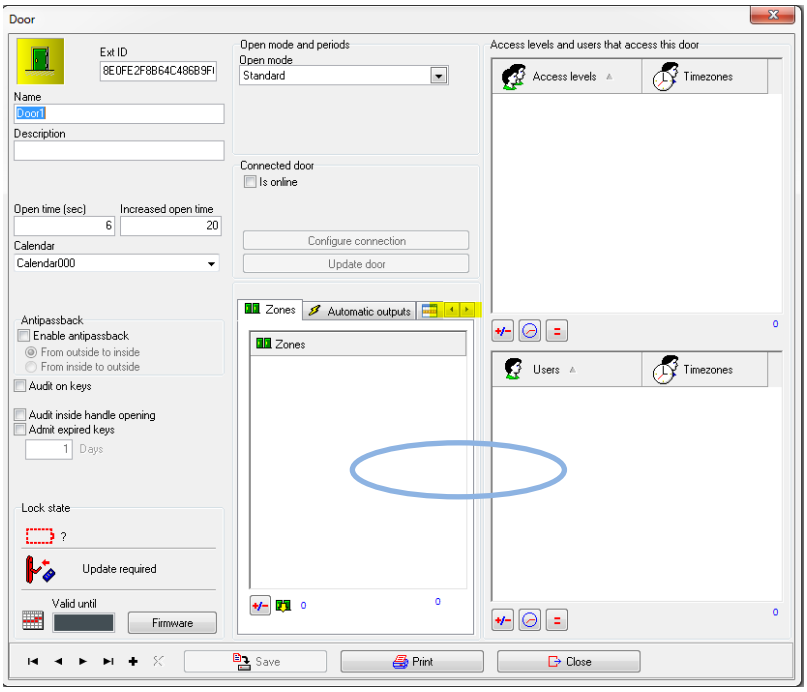
Tras salvar esta información, se puede

seguir creando el resto de ubicaciones y funciones de la misma manera.

Una vez estén creadas las ubicaciones y funciones, se puede comenzar a añadir puertas a la matriz respectivamente según su ubicación y la función que tendrán.

Importante:
Se pueden "añadir" puertas desde ubicaciones y funciones.
Para que los accesos por matriz funciones, el usuario debe ser asignado tanto a ubicaciones como a funciones, aunque aún no hay horarios envueltos.

Paso 4. Asignando puertas a Ubicaciones y Funciones:



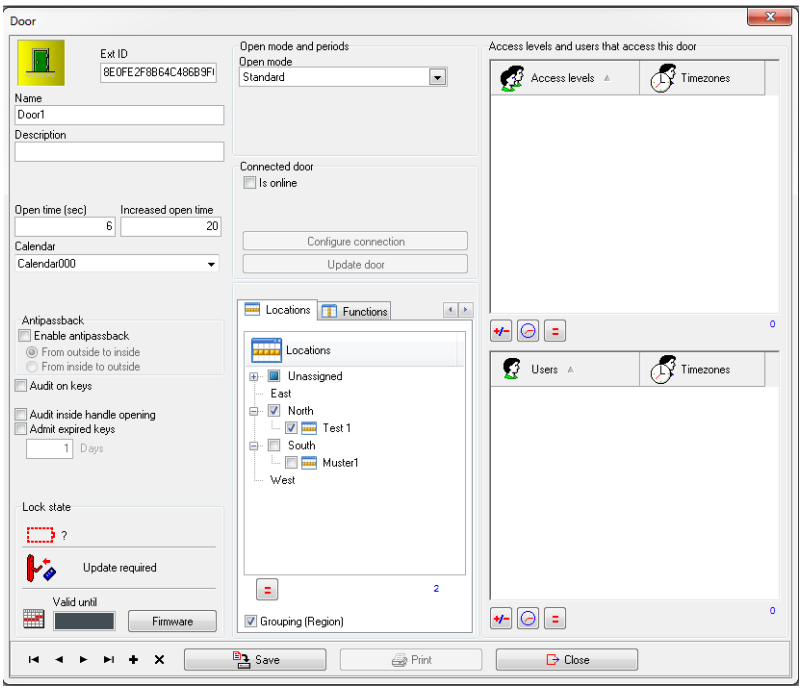
También es posible asignar la ubicación y función de una puerta desde el menú Puertas al entrar en la ficha de la puerta deseada.

En la columna central de la ventana, aparecen dos pestañas con las ubicaciones y funciones.

Para asignar una puerta a una ubicación y una función, hay que seleccionarlas en el menú.

Para una vista más rápida de la matriz, se puede activar la casilla "Agrupar". De esta manera se encontrará más rápidamente una puerta y además permite seleccionar todo un grupo con un tic.

Esta opción está disponible para todas las puertas.



Importante:

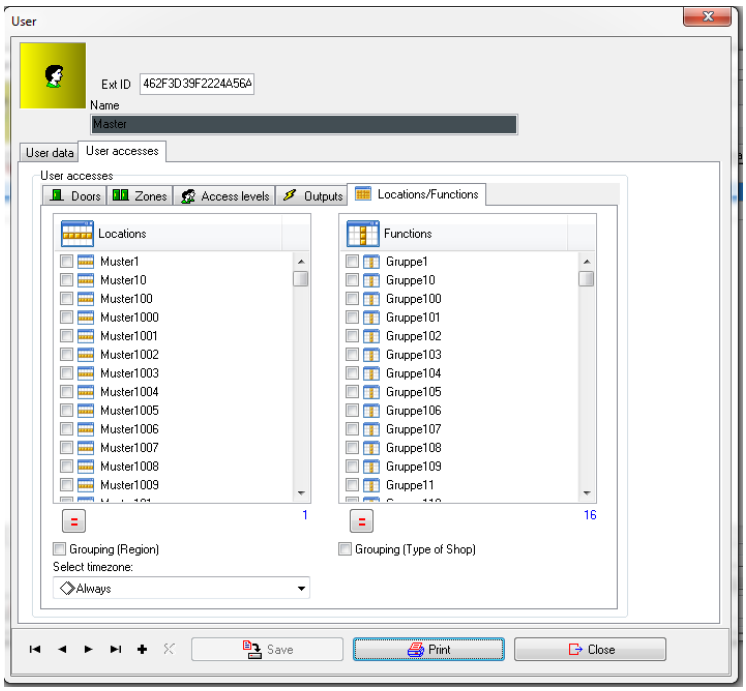
Todas las puertas deberán ser actualizadas tras la configuración de la matriz para que sepan a qué parte de la matriz pertenecen.

Paso 5. Asignando Accesos y horarios a usuarios.

El último paso para la configuración correcta de la matriz, es asignar las ubicaciones y funciones a los usuarios, para que estos tengan acceso a las puertas deseadas y en el horario seleccionado.

Ir a la lista de usuarios, pestaña "Accesos del usuario".

Ahora, seleccionar todas las ubicaciones y funciones necesarias.



CUIDADO, todas las personas que se asignen a ubicaciones y funciones, podrán abrir todas las puertas con la misma combinación de ubicaciones y funciones a las que están asignadas.

For a better view activate the "Grouping" on both lists.

Finalmente, es necesario configurar y seleccionar la zona horaria correcta.

Importante:

Solo se puede asignar **una** zona horaria para todos los accesos.

Para más información, se puede contactar con el colaborador certificado de Salto.

SALTO Wireless

Configuración del sistema

El sistema puede completarse con la incorporación de cerraduras Wireless Salto. Esta sección describe los pasos para configurar una instalación Wireless completa.

En esta sección se verán dos modos de trabajar;

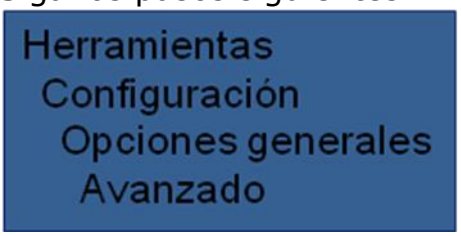
- En MODO RF 1
- En MODO RF 2 (solo para versiones con servicio)

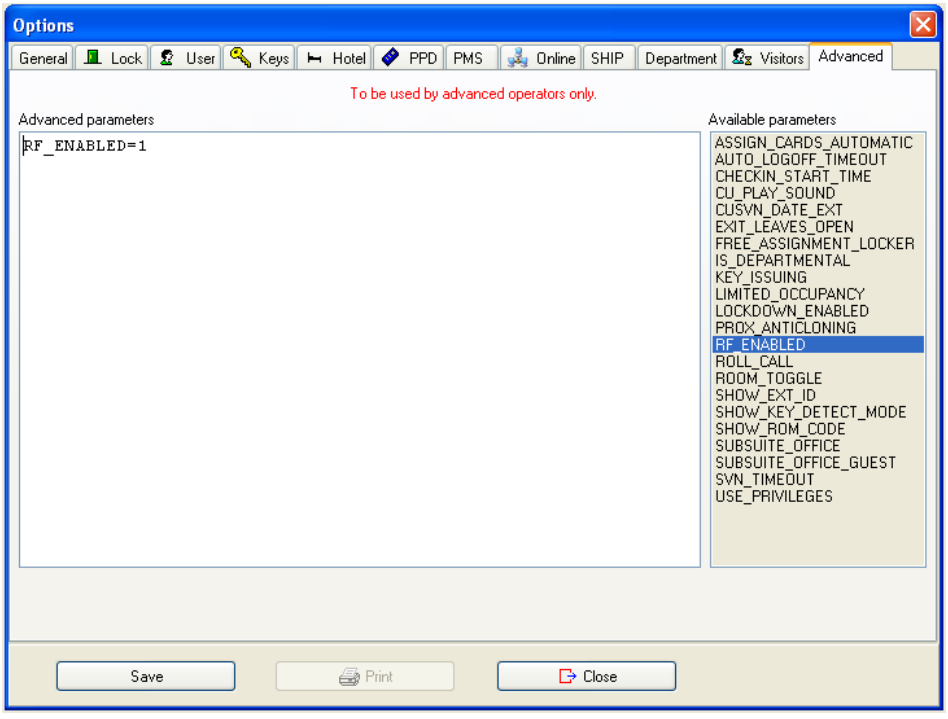
La diferencia principal entre los dos modos son los gateways y la configuración. La primera parte de esta sección tratará sobre la parte común entre los dos modos.

RF_ENABLED=1

Para comenzar con la configuración del sistema, el módulo de radio frecuencia (RF) tiene que ser activado.

Siga los pasos siguientes:

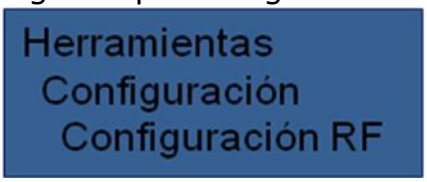




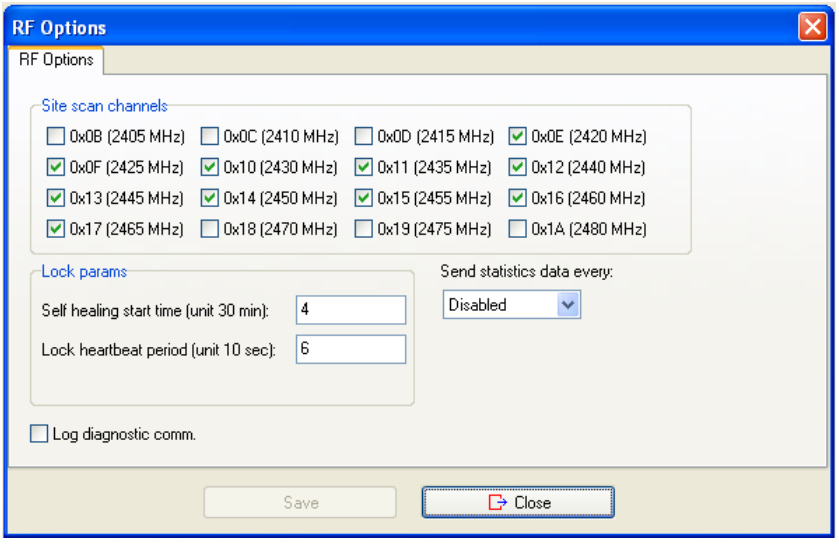
Configuración RF

Bajo la opción CONFIGURACIÓN RF se definen las opciones generales del sistema.

Siga los pasos siguientes:



Escaneo de canales



El sistema Wireless SALTO utiliza el protocolo IEEE 802.15.4 para transmitir la señal con una frecuencia de 2,4GHz. Esta ventana recoge los 16 canales de emisión mostrando su nombre (en hexadecimal) y su correspondiente frecuencia.

De manera a mejorar la calidad de las transmisiones, se recomienda realizar un filtrado de los canales a utilizar. Consulte con su distribuidor SALTO para más detalles sobre este proceso.

Parámetros de cerradura

. Self healing start time

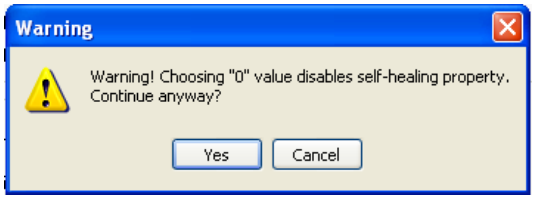
Este parámetro (en unidades de 30min) define el tiempo de espera del sistema antes de arrancar el proceso de self healing.

Por Self healing se define al proceso de búsqueda de un nuevo dispositivo padre cuando la comunicación con el actual (bien sea Gateway o Repetidor) se pierde.

. Lock heartbeat period

Este parámetro define (en unidades de 10s) la frecuencia de heartbeat de la cerradura. Consiste en una breve señal emitida por el escudo de manera a ser visto por su dispositivo padre (Gateway o Repetidor).

Nota: Si no existe redundancia en cuanto a dispositivos padre, se recomienda utilizar el valor "0" para desactivar dicho proceso.

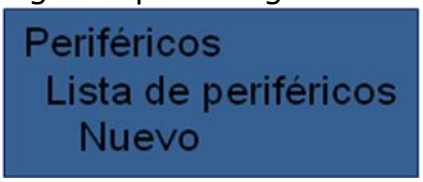


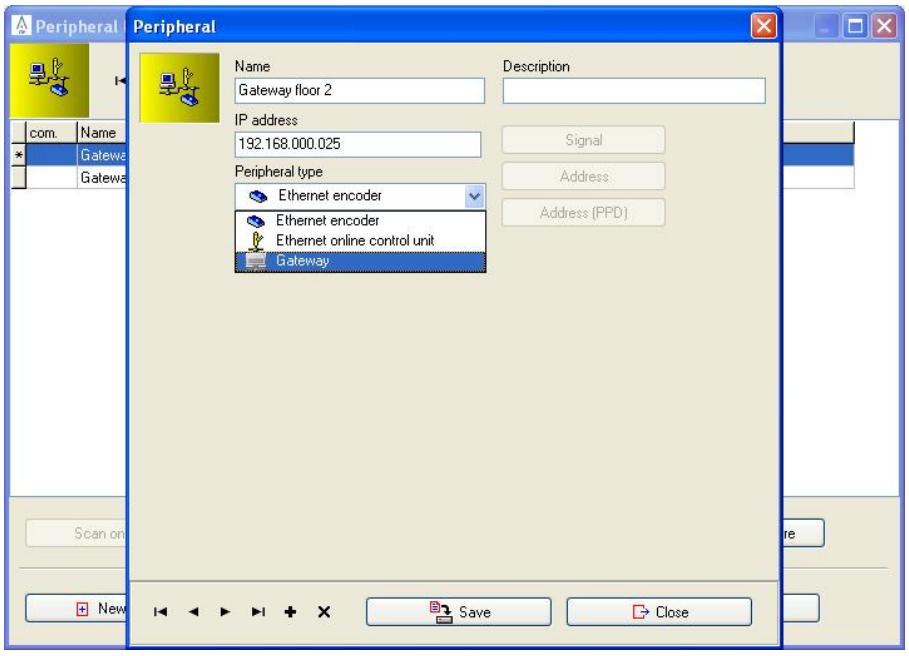
TRABAJANDO EN MODO 1

Gateways RF1

Los Gateways se declaran junto a su dirección IP estática.

Siga los pasos siguientes:





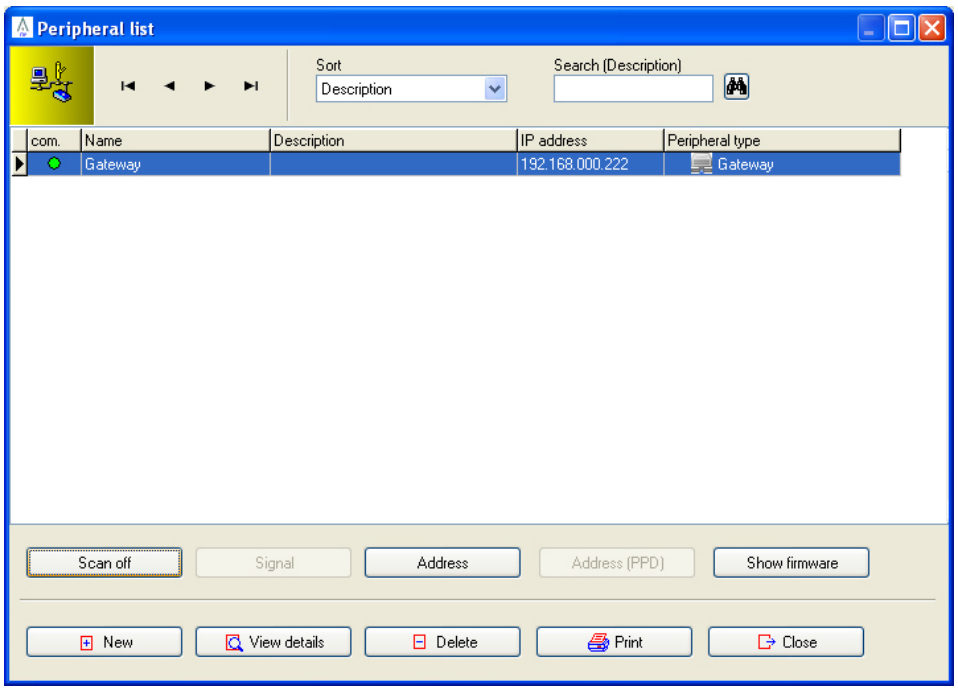
Una vez declarado el Gateway tiene que ser direccionado para establecer la comunicación.

Siga los pasos siguientes:

Periféricos
Lista de periféricos
Direccionar

Para ello, se debe poner el Gateway en modo direccionamiento manteniendo pulsado el botón CLR. A continuación se utiliza la opción Direccionar desde el software.

Pulsando sobre "Monitorizar" el led "com." mostrará el estado del Gateway.



Repetidores RF1

Los repetidores se gestionan desde una ventana distinta.

Siga los pasos siguientes:

Periféricos
Repetidores
Nuevo

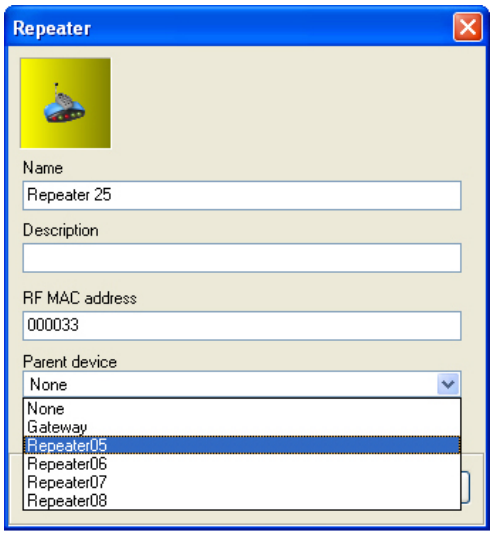
2 parámetros definen a este dispositivo:

- Dirección MAC RF

Este parámetro se compone de 3 pares de números hexadecimales y se encuentra sobre la antena del dispositivo.

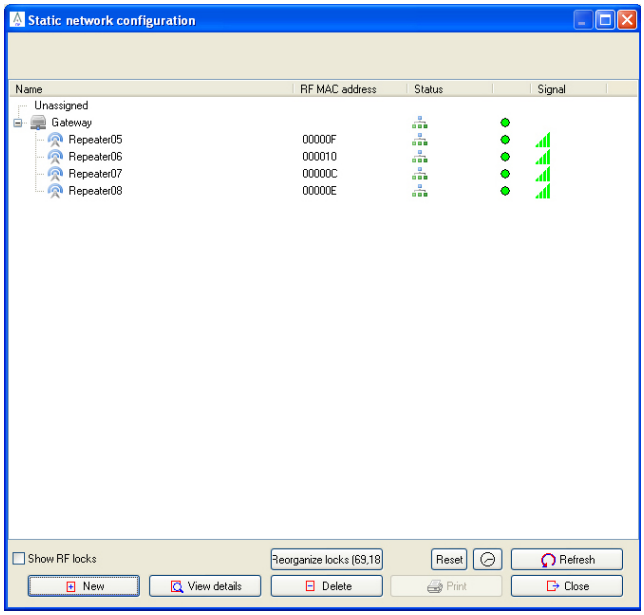
- Dispositivo padre

El Repetidor tiene que ser asociado a otro Gateway o Repetidor (su dispositivo padre).



Nota: el Gateway no necesita ninguna dirección MAC.

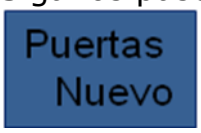
Una vez finalizados estos procesos, los Repetidores se asociarán automáticamente a su dispositivo padre estableciéndose así la comunicación.

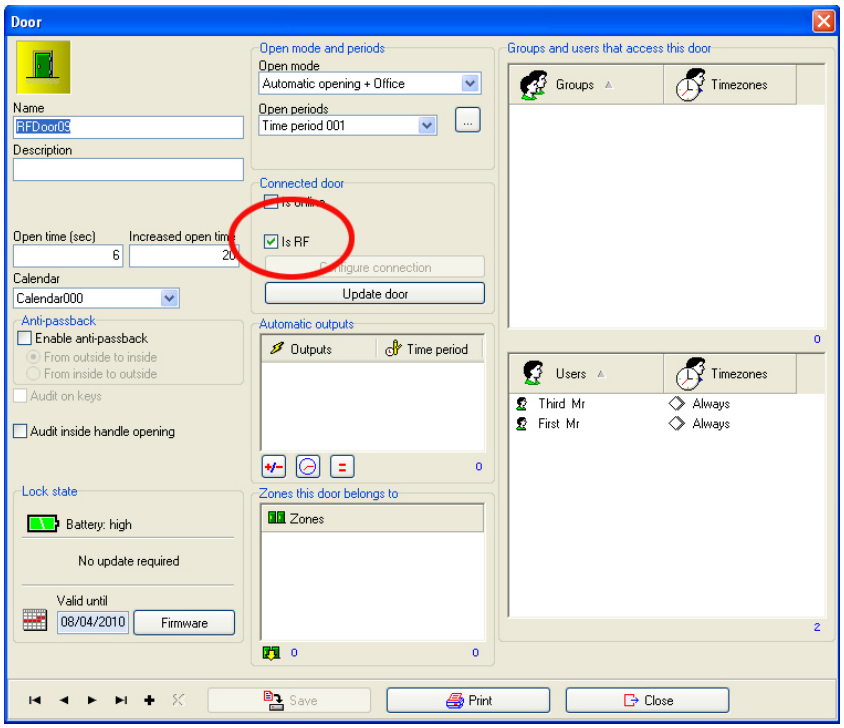


Cerraduras Wireless

Las cerraduras Wireless se crean desde el menú de PUERTAS.

Siga los pasos siguientes:

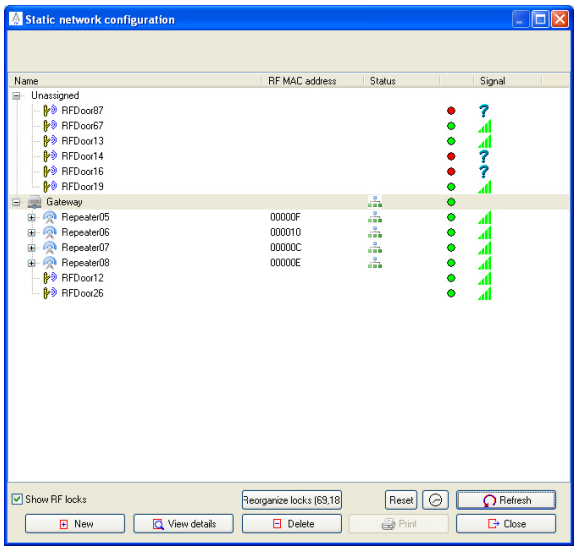




La opción RF debe marcarse para convertir la cerradura en Wireless.

Una vez se crean las diferentes puertas, estas deben ser inicializadas mediante el PPD.

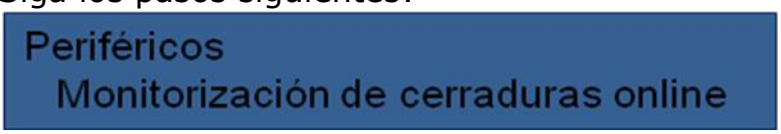
Los escudos comenzarán con el proceso de asociación con los dispositivos padre (Gateways / Repetidores).



Monitorización de cerraduras online

El sistema online wireless se monitoriza desde esta ventana.

Siga los pasos siguientes:

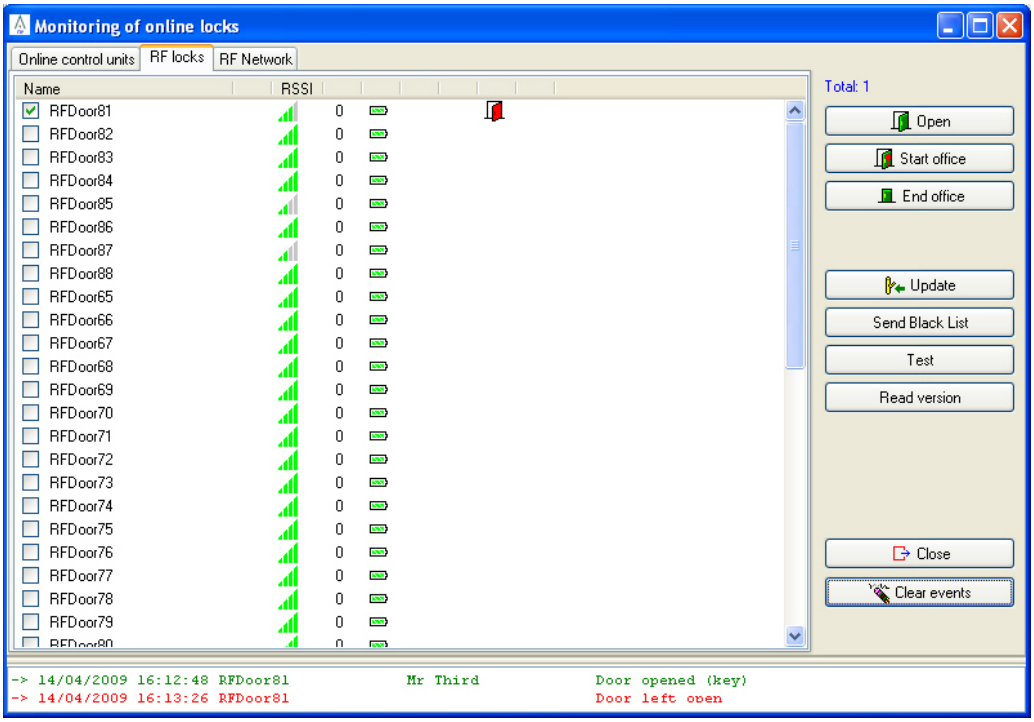


Dos nuevas pestañas muestran el estado de las cerraduras wireless.

Cerraduras RF

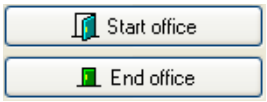
Esta ventana permite la monitorización de las cerraduras wireless. Junto al nombre de la puerta, se muestran datos como el

estado de pilas, y señales de puerta dejada abierta así como intrusión.



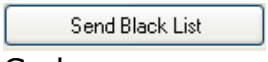
Mientras que la parte de abajo muestra los eventos en tiempo real, en la parte derecha se muestran las siguientes opciones:

Permite la apertura remota temporizada de las cerraduras wireless seleccionadas (el tiempo de apertura dependerá del tiempo ampliado).



Las cerraduras seleccionadas se pueden abrir remotamente (y quedarse abiertas). Previamente, el modo paso tiene que estar definido en la ficha de dichas puertas.

Una actualización online enviará las últimas modificaciones realizadas.



Cada vez que un usuario es cancelado, la lista negra se envía periódicamente a los elementos online (CU + cerraduras wireless).

Esta opción permite forzar manualmente el envío de dicha lista negra.

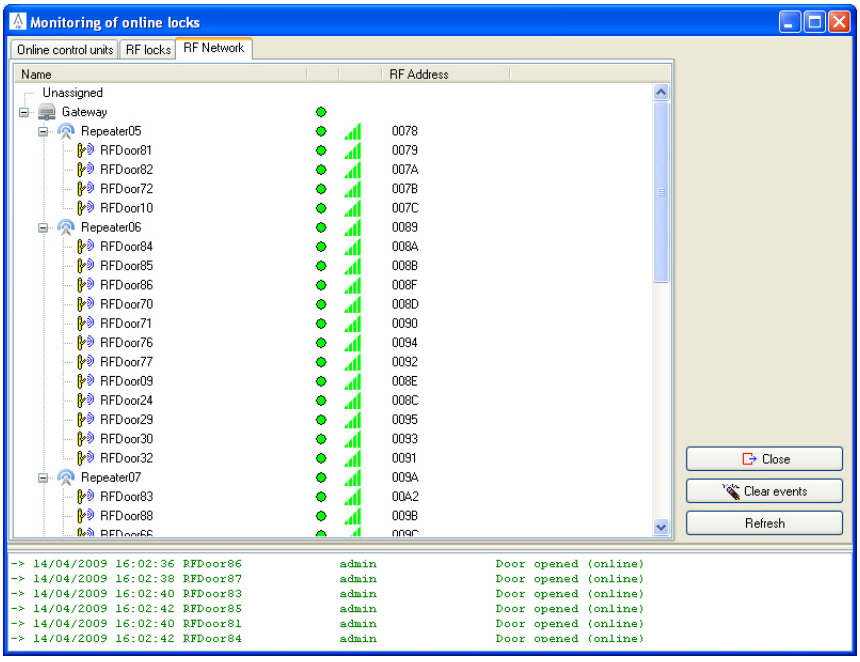
Esta opción envía una señal de test a las cerraduras, contestando estas con un "bip" confirmando así la comunicación.

Se mostrará la versión de firmware de la cerradura:

- Antena RF
- Control
- Lector

Red RF

Las distintas cerraduras wireless se asociarán automáticamente al mejor dispositivo padre (Gateway / Repetidor) en términos de disponibilidad y cobertura.

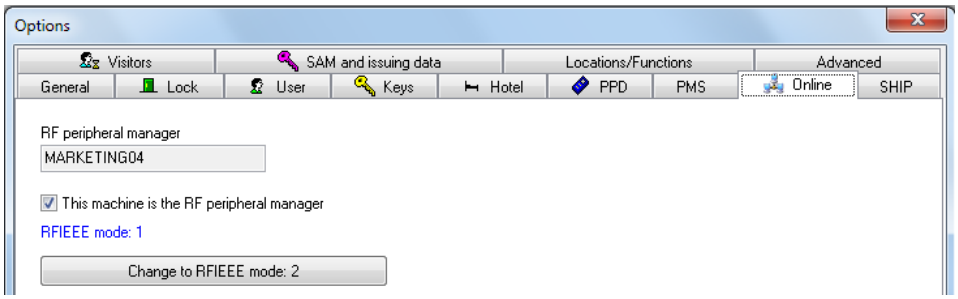


TRABAJANDO EN MODO 2

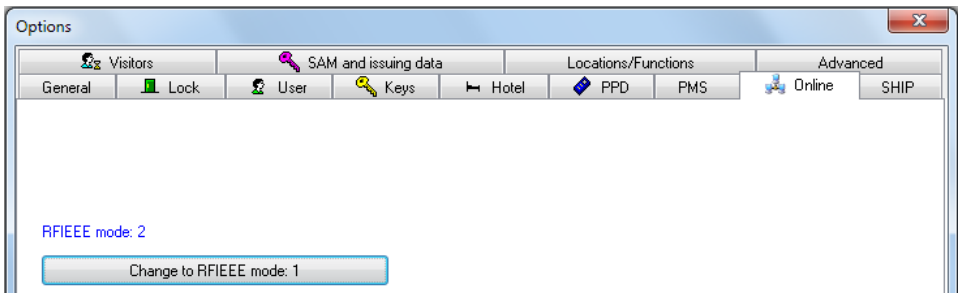
Para trabajar en MODO2, es necesario ir a Opciones Generales, pestaña "Online" y asegurarse de que el texto escrito en azul es "**Modo de**

RFIEEE: 2". En el caso contrario, pulsar el botón "**Cambiar a modo de RFEEE: 2**"

MODO 1;



MODO 2;



En MODO 2, TODAS las comunicaciones se gestionan desde el servicio, incluyendo la RF. En un programa sin servicio o en un programa con servicio pero en MODO 1, las comunicaciones RF se gestionan desde el PA/HAMS sin pasar por el servicio.

Una vez el MODO 2 activado, se puede empezar a crear Gateways y nodos;

Es IMPORTANTE recordar que para trabajar en MODO 2 solo es posible usar Gateways 2, escudos con módulos de control con versión de firmware 01.18 para AElement y 0124 para XS4 o superior.

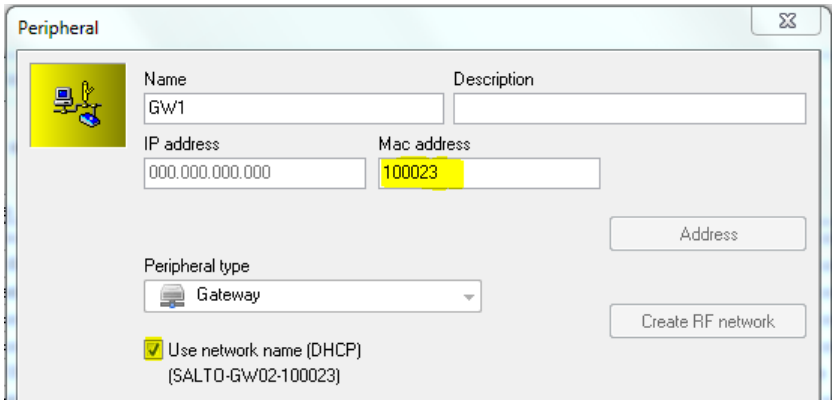
Gateways RF2

Los Gateways se encargan de crear el enlace en la red. Ir a Periféricos/ Lista de periféricos y comenzar a crear los Gateways necesarios.

Hay dos modos de configurar los Gateways;

1/ Usando DHCP

2/ Usando una IP estática



1/ **Usando DHCP**, hay que tener presente que se necesita un servidor DHCP que asignará automáticamente una IP al Gateway. Seleccionar la opción "**Usar nombre de red (DHCP)**". No será necesario rellenar el campo "Dirección IP", solo es necesario rellenar la dirección MAC en el campo "**Dirección MAC**". La dirección MAC del Gateway se encuentra en la propia placa (no confundir con la dirección MAC de la antena/nodo)

Para direccionar el Gateway2, es necesario conectarlo a la red (NO UTILIZAR CABLES CRUZADOS). Presionar el botón CLR por unos 5 segundos hasta que la luz se vuelva **naranja**.

Una vez esté con la luz naranja y conectado a la red, ir al explorador de internet y marcar la dirección **192.168.0.234.** Una vez dentro, seleccionar **DHCP** y presionar "Send"

2/ **Usando IP estática**, la opción "**Usar nombre de red (DHCP)"** debe estar deseleccionada y se deben rellenar los dos campos, "**Dirección IP**" y "**Dirección MAC**" y salvar los cambios.

Para direccionar el Gateway2, es necesario conectarlo a la red (NO UTILIZAR CABLES CRUZADOS). Presionar el botón CLR por unos 5 segundos hasta que la luz se vuelva **naranja**.

Una vez esté con la luz naranja y conectado a la red, ir al explorador de internet y marcar la dirección **192.168.0.234**, seleccionar **STATIC** y presionar "Send"

En ambos casos, DHCP o ESTATICA, la comunicación entre el Gateway y el servicio SALTO se hará automáticamente sin necesidad de ninguna otra operación manual.

NOTA: El Gateway 2 es compatible con los routers PoE. Para más información, ver la documentación del Gateway.

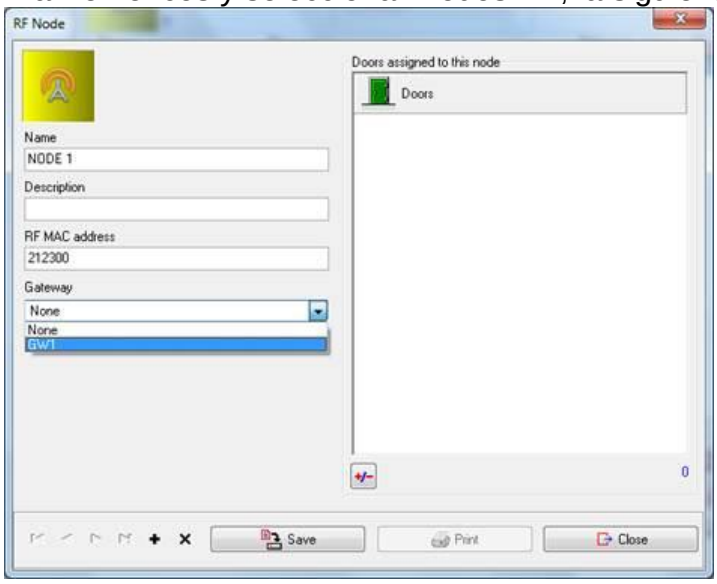
Nodos RF2

Una vez el Gateway está creado, se debe crear el **NODO.** Los NODOS existen de dos formas distintas;

1/ Solo una antena RF que se conecta al Gateway (llamado mini nodo)

2/ De manera independiente con la misma forma que los lectores murales modulares con otro acabado y conectados con conexión RS485.

Ir a Periféricos y seleccionar Nodos RF, la siguiente ventana aparecerá;



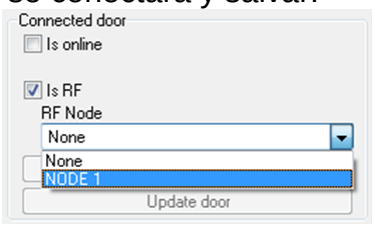
Ponerle un nombre al Nuevo NODO y una descripción si es necesario. En “**Dirección MAC RF**” escribir la dirección MAC de la ANTENA (no confundir con la dirección MAC de la placa Gateway).

En “Gateway”, seleccionar el Gateway del cual el NODO colgará y al cual se conectará. Está conexión es ESTATICA, el NODO estará siempre conectado al Gateway seleccionado en esta ventana y nunca se cambiará a otro Gateway por sí solo.

Una vez el Gateway esté comunicando con el servicio de Salto, el NODO empezará a comunicar por sí solo con su Gateway. Presionar “Salvar” para guardar los cambios.

Crear enlace con PUERTAS

Crear la puerta como se muestra anteriormente en este manual y activar la casilla “Es RF”. A continuación, seleccionar el NODO al que la puerta se conectará y salvar.



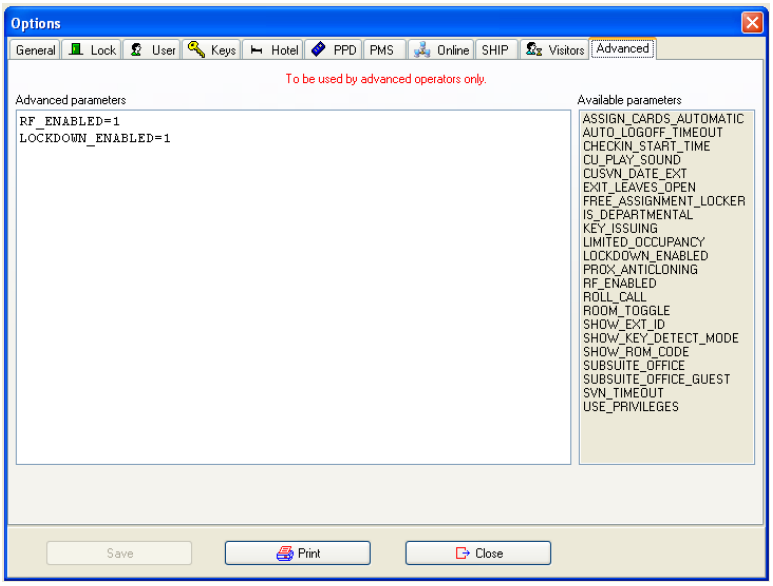
Después**,** descargar la información al PPD e inicializar las puertas. **NO CARGAR EL PPD ANTES**, al cargar el PPD, el sistema informa sobre el NODO al que cada puerta se debe conectar. Si se carga el PPD antes, las puertas no comunicarán con los NODOS.

IMPORTANTE: La versión de FW del PPD debe ser 01.24 o superior. El módulo control AElement debe ser 01.19 o superior y el XS4 01.24 o superior.

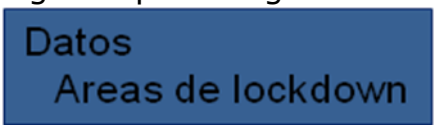
Lockdown

Esta opción permite la gestión de un área de seguridad compuesta por CUs y cerraduras wireless de manera a poder cerrar fácilmente todos los accesos frente a una situación de emergencia.

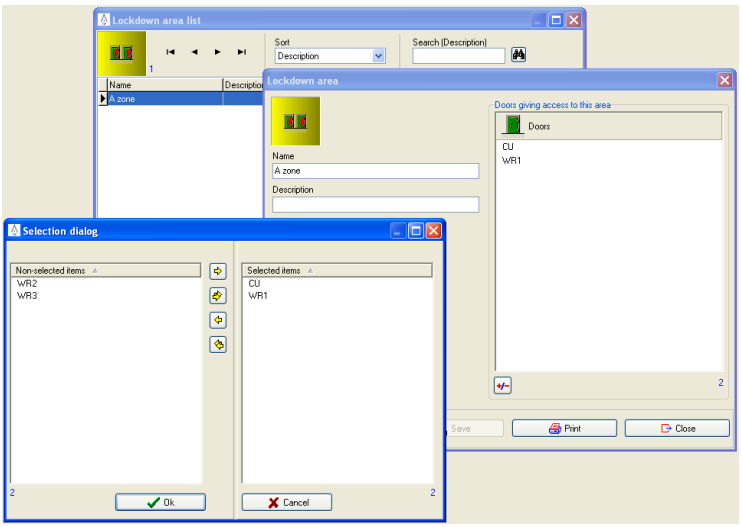
Se tiene que activar previamente esta opción en la pestaña "Avanzado" de "Opciones Generales": LOCKDOWN_ENABLED=1



Siga los pasos siguientes:

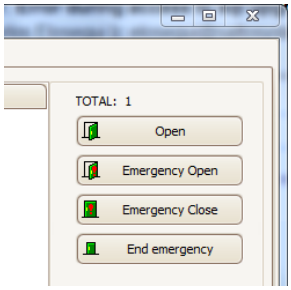


El área de lockdown agrupará un conjunto de lectores online y cerraduras wireless.



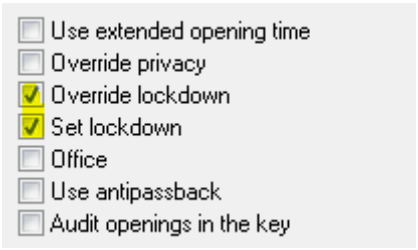
Siga los pasos siguientes:

Una vez definidas las áreas, se puede utilizar el botón "Cerrar en emergencia" para cerrar remotamente todas (o las seleccionadas) las puertas del área o si es necesario "Abrir en emergencia".



El acceso a estos puntos será denegado (incluso a usuarios autorizados) hasta que se utilice el botón de "Fin de emergencia".

Únicamente los usuarios con la opción "Vencer lockdown" podrán acceder.



LOCKDOWN en AMOK

Esta opción solo se podrá utilizar con escudos **AMOK**.

El escudo AMOK admite el Lockdown o cierre de emergencia, siendo puertas offline. Se puede activar presentando una llave valida en el lector de la parte interior del escudo AMOK.

En situación de emergencia, donde sería más seguro permanecer encerrado dentro de un aula o un despacho, el escudo AMOK le permite activar el modo lockdown al instante solo con presentar la llave. El usuario deberá tener activada previamente la opción **SET LOCKDOWN**. Una vez esté activado el lockdown, nadie podrá abrir la puerta desde el exterior. SOLO usuarios que tengan activada la opción "Vencer Lockdown" podrán abrir la puerta.

"Vencer Lockdown" permite abrir la puerta aunque esté cerrada por lockdown.

"Activar Lockdown" permite activar o desactivar el modo lockdown.

LOCKDOWN_ENABLED=1 debe estar activada en el programa de Salto en Herramientas/ Configuración/ Opciones Generales/ pestaña Avanzado.