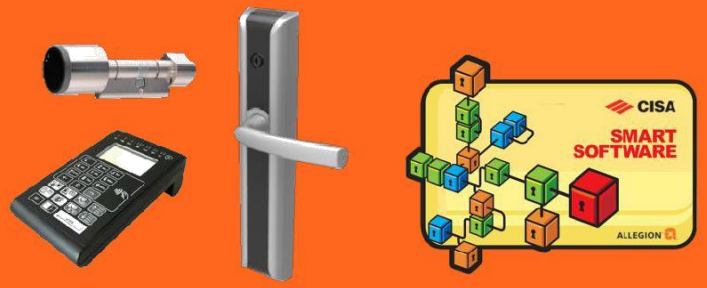
ALLEGION™

PIONEERING SAFETY™

SOLUCIÓN eSIGNO

MANUAL DE USUARIO



CISA

HISTORIAL DE VERSIONES DEL DOCUMENTO

FECHA	*VERSIÓN*	*ESCRITO POR*	*REVISADO POR*	*NOTAS VARIACIONES*
30/05/14	201	Guido Costa	Gianni Fantini	Borrador
20/06/14	202	Guido Costa	Gianni Fantini	Agregado Dashboard
23/07/14	203	Guido Costa	Gianni Fantini	Actualización funciones SSW4
04/08/14	204	Guido Costa	Gianni Fantini	Índice revisión
04/09/14	205	Guido Costa	Gianni Fantini	Procedimiento codificación parámetros
09/09/14	206	Guido Costa	Gianni Fantini	Actualización codificación parámetros
17/09/14	207	Guido Costa	Gianni Fantini	Agregado detalles sincronización
25/09/14	208	Guido Costa	Gianni Fantini	Wall Reader Glass, modo visualización eventos cerradura
28/10/14	209	Guido Costa	Gianni Fantini	Windows Services, actualización registro historial
20/11/14	210	Guido Costa	Gianni Fantini	Corrección suspender/restablecer tarjeta, habitaciones/categorías en tarjetas de cliente
12/11/14	211	Guido Costa	Gianni Fantini	Correcciones modo Fallo
08/04/15	212	Guido Costa	Gianni Fantini	Detalles Active Directory
17/04/15	213	Guido Costa	Gianni Fantini	Notas eliminar datos
18/06/15	214	Marco Zavatta	Guido Costa Gianni Fantini	Extensión Dashboard y Admin Console Detalles agregado tarjeta de cancelación
23/10/15	215	Guido Costa	Marco Zavatta	Detalles validación y recodificación
18/11/15	216	Guido Costa	Marco Zavatta	Actualización señales cerradura
01/03/16	217	Guido Costa	Marco Zavatta	Actualización parámetros para dispositivos offline
15/04/16	218	Guido Costa	Marco Zavatta	Gestión llave ULC
03/05/16	219	Guido Costa	Marco Zavatta	Detalles llave ULC
31/05/16	220	Guido Costa	Marco Zavatta	Mantenimiento eGo
17/06/16	221	Guido Costa	Marco Zavatta	Parámetros adicionales
04/08/16	222	Guido Costa	Marco Zavatta	Notas adicionales desde el campo
01/02/18	223	Guido Costa	F. Ricci Iamino	Actualización para lanzamiento del sistema 2.5
25/01/19	224	Guido Costa	F. Ricci Iamino	Actualización para lanzamiento del sistema 2.5.1
06/09/19	225	Guido Costa	F. Ricci Iamino	Actualización para lanzamiento del sistema 3.0

Abstract

El presente manual de usuario contiene una descripción completa de las características del sistema eSIGNO. Además, también se describen las funciones del software de gestión CISA (Smart Software). Nota importante: El sistema eSIGNO puede ser actualizado en cualquier momento con nuevas versiones de software. A causa del constante desarrollo del producto, algunas características podrían ser modificadas en cualquier momento, sin preaviso.



ÍNDICE

Índice ... 3
Introducción ... 4
Uso de la cerradura eSIGNO ... 7
Uso de la cerradura eGO ... 8
Uso de la cerradura eFLEXO ... 9
Uso de E-Cylinder ... 10
Uso del lector de pared (Wall Reader) ... 11
Dispositivos eSIGNO: indicaciones luminosas ... 12
Uso del Energy Saver ... 13
eSIGNO Mobile ... 14
Tipos de tarjetas ... 16
Zonas de acceso ... 18
Tipos de cerradura ... 18
Funciones de la cerradura ... 19
Funciones especiales ... 20
Funciones wirelesss ... 21
Zonas ... 22
Categorías ... 24
Instalación Smart Software ... 25
Sincronización codificador Backup Server ... 28
Apertura Smart Software ... 29
Smart Software: Usuarios ... 33
Smart Software: Tarjetas ... 34
Smart Software: Zonas de acceso ... 43
Smart Software: Categorías ... 49
Smart Software: Historiales ... 52
Smart Software: Preferencias ... 54
Smart Software: Días festivos ... 57
Smart Software: Parámetros de codificación ... 58
Smart Software: Lista Client ... 59
Dashboard ... 60
Widget: Recepción ... 65
Widget: Técnico ... 66
Widgets: Seguridad ... 67
Widget: Información adicional ... 68
Widget: Administración del sistema ... 69
Dashboard vs. Smart Software ... 70
Widgets: Resumen ... 71
Check-in\Check-out ... 72
Configuración ... 73
HHI Instrumentos de servicio ... 75
HHI: Cerradura eSIGNO y lector de pared ... 76
Botones especiales ... 77
HHI: E-Cylinder ... 78
Menú principal HHI ... 79
Visualizar datos ... 79
Inicializar cerradura ... 80
Reset cerradura ... 81
Descargar programa cerradura ... 81
Leer lista negra ... 81
Menú Tarjetas de servicio ... 82
Escenario Fallo ... 84
Login al codificador ... 86
Creación tarjetas de cliente ... 87
Gestión tarjetas de cliente ... 87
eKEY ... 88
Reserva y check-in ... 90
Gestión credenciales Mobile ... 92
Gestión llave ULC ... 95
Controlador online ... 99
Mantenimiento ... 100
Cerradura eSIGNO ... 100
Cerradura eGO ... 102
Cerradura eFLEXO ... 103
E-Cylinder eSIGNO ... 104
eSIGNO Wall Reader Glass ... 106
eSIGNO Energy Saver ... 108
Apéndice ... 109
Eventos de historial ... 109
Capacidad tarjeta de historial ... 112
Configuraciones de sistema ... 112

INTRODUCCIÓN

La solución Hospitality descrita en este manual presenta una arquitectura basada en ordenador con una base de datos central para todas las actividades de gestión; para codificar las tarjetas y para la opción fail-over, se utilizan dispositivos integrados (codificadores).

El sistema de control de accesos se configura durante la instalación con un instrumento específico (el configurador CISA); este describe la instalación con todas las puertas y componentes que constituyen la base del sistema.

Las principales actividades de gestión se realizan con un sistema de PC multi-client (Smart Software, abreviado con SSW), basado en una base de datos SQL como fuente principal de los datos, que se encuentra en un servidor. Esta base de datos memoriza toda la información y la pone a disposición según las necesidades.

Para administrar la instalación, se puede utilizar un sistema compuesto por Smart Software clients conectados con un lector RFID; los usuarios deben identificar sus derechos de acceso con una credencial; a continuación, pueden utilizar el Smart Software client.

La codificación de las tarjetas para los huéspedes o de las otras tarjetas (servicio, operador, etc.) es controlada por una estación de codificación, que generalmente se encuentra a la recepción, cerca de una estación de trabajo PMS (Property Management System).

En las puertas de las habitaciones para huéspedes se instalan cerraduras electrónicas eSIGNO, dispositivos alimentados a batería con diseño italiano por fuera, un cerradero interno y cerraduras de embutir. La cerradura electrónica puede leer tarjetas Mifare (13.56 MHz) y RFID (Ultralight C y Classic), y evalúa los derechos de acceso a partir de los datos de la tarjeta. Controla el estado de la cerradura de embutir y la función Privacy. La información se puede enviar al Smart Software, el sistema centralizado de gestión de los huéspedes, mediante una red privada wireless ultrabaja (PAN, ZigBee), o mediante los instrumentos de servicio o las tarjetas.

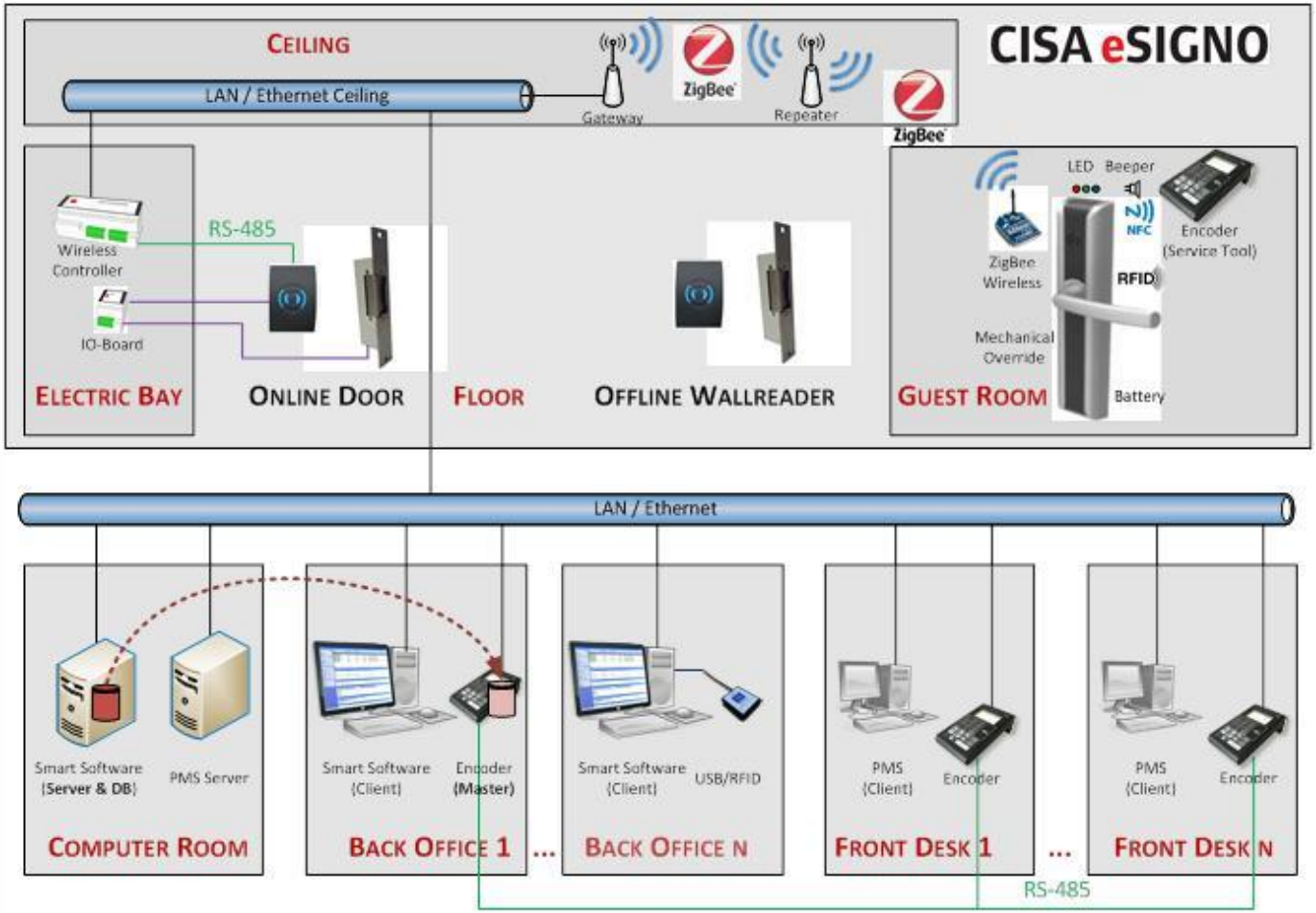
Quienes deben entrar en las habitaciones pueden ser vistos como clientes o como miembros del personal de servicio (limpieza o gestores).

Para abrir la puerta se deben presentar las credenciales al lector de la cerradura electrónica (que se encuentra en la parte superior de la placa externa): en base a los derechos codificados en la tarjeta, el firmware incorporado en la cerradura electrónica muestra los permisos con una señal luminosa roja (permiso negado) o verde; en este último caso, activa el acoplamiento para conectar la manilla externa con la cerradura interna y el usuario puede abrir la puerta.

Además, una aplicación servidor ofrece otras funciones; entre otras, una nueva interfaz de usuario, proporcionando un dashboard con varios datos para un hotel o para diferentes estructuras (por ejemplo, campus).

INTRODUCCIÓN

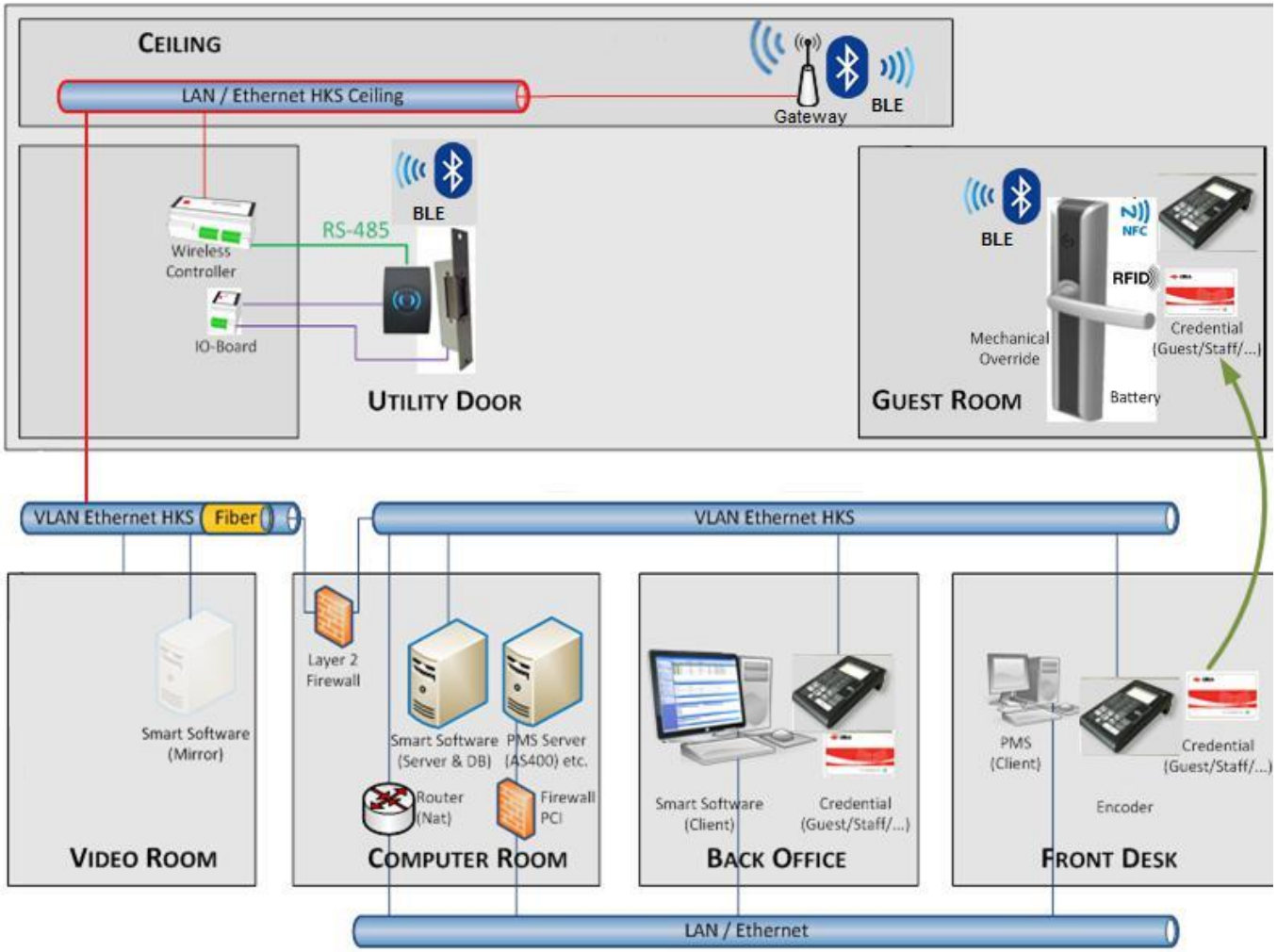
La infraestructura wireless ha sido proyectada con funciones avanzadas, como la red Mesh; la primera generación del sistema eSERVER utiliza la tecnología ZigBee para la comunicación wireless, constituida por diferentes componentes, que permite una monitorización más precisa del estado y del uso de las puertas, además de facilitar las actividades de la recepción y de la oficina interna.



La infraestructura de red wireless PAN está compuesta por controladores, gateways (es decir, antenas) y, potencialmente, repetidores. Está conectada a una infraestructura Ethernet y permite la transmisión de datos desde un servidor central a las cerraduras electrónicas (principalmente por motivos de servicio) en ambas direcciones. Por ejemplo, todas las actividades de una puerta (tarjetas, estado de la puerta, privacy) pueden ser memorizadas y transferidas a la base de datos principal para un control posterior. Además, se puede transferir la lista de las tarjetas canceladas de la base de datos principal a la cerradura electrónica, para garantizar que estas tarjetas ya no sean válidas.

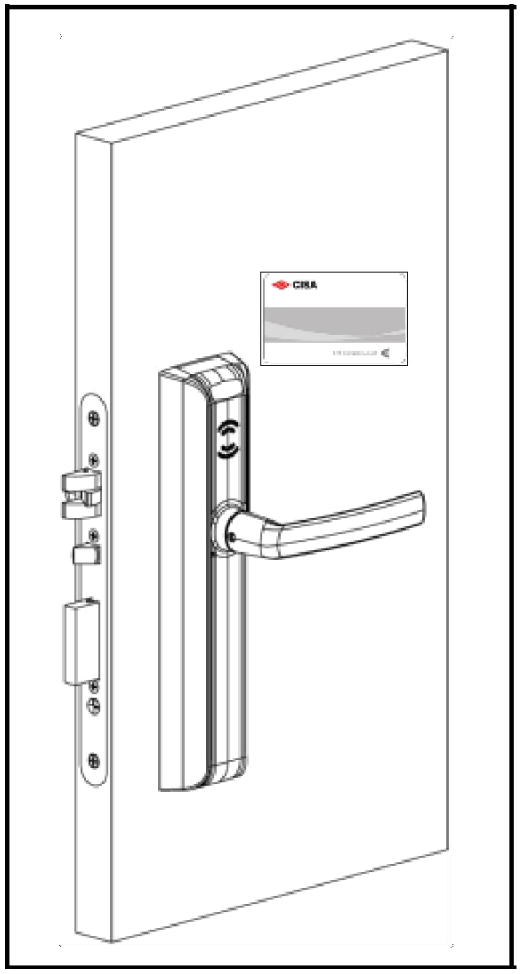
INTRODUCCIÓN

La segunda generación del sistema eSERVER utiliza la tecnología Bluetooth 5.0 para la comunicación wireless, constituida por diferentes componentes, que permiten una monitorización más precisa del estado y del uso de la puerta, además de facilitar las actividades de la recepción y de la oficina interna.



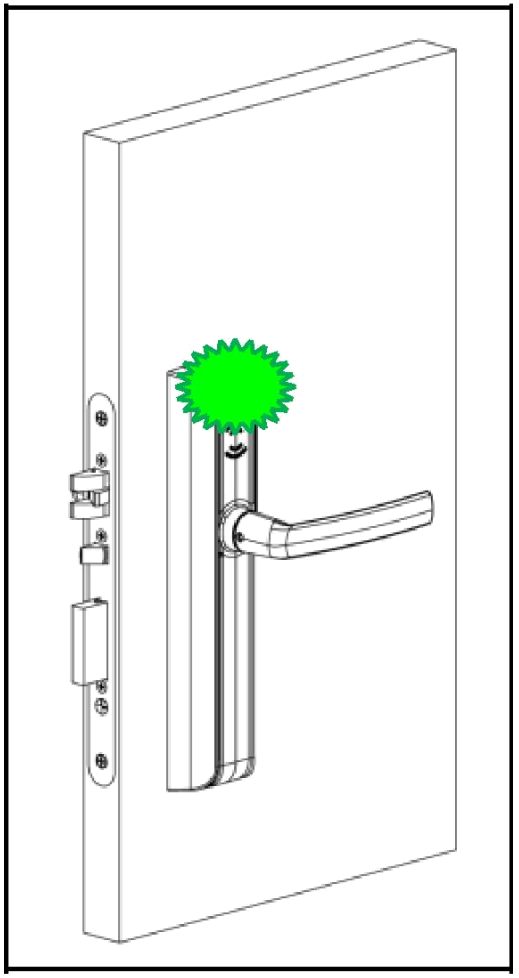
Con esta arquitectura de sistema, es posible tener tanto funciones wireless como credenciales Mobile en la misma cerradura.

USO DE LA CERRADURA ESIGNO



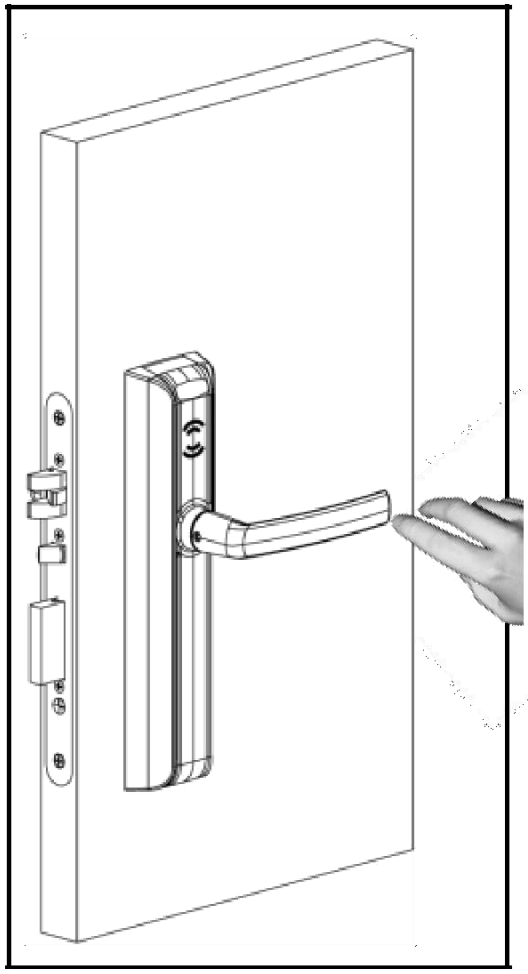
1

Mantenga la tarjeta cerca del lector durante 1 segundo para permitir una correcta comunicación.



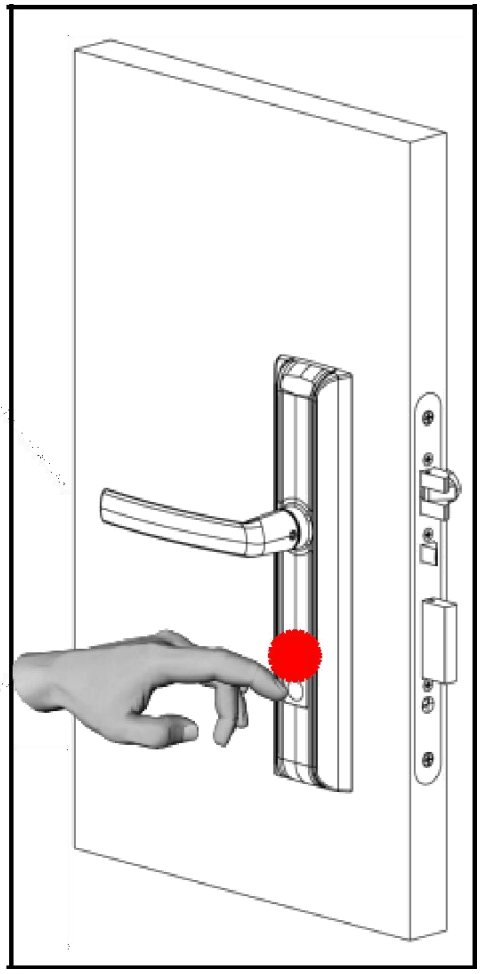
2

Espere hasta que la cerradura emita destellos verdes: indica que la lectura de la tarjeta se ha producido en forma correcta.



3

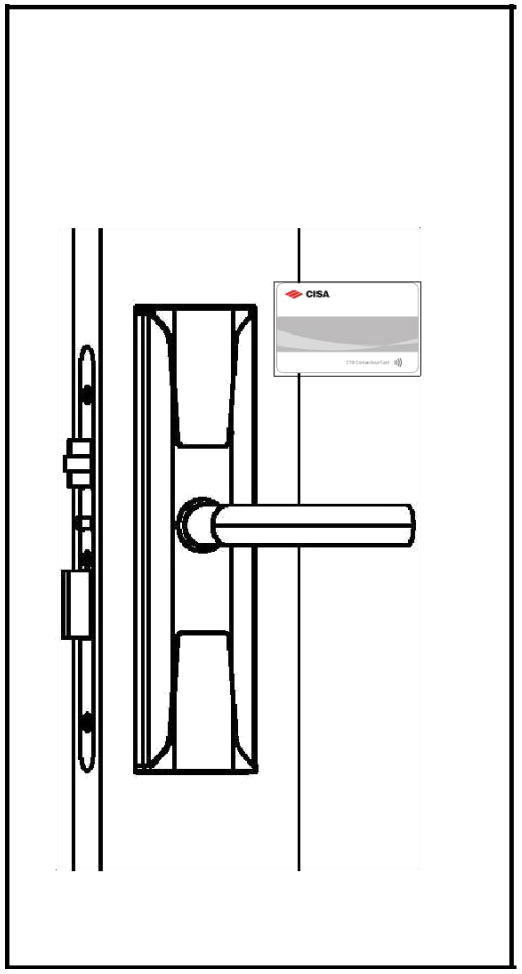
Gire la manilla externa, al para abrir la cerradura, antes de la caducidad del retraso de apertura (por defecto, 5 segundos).



4

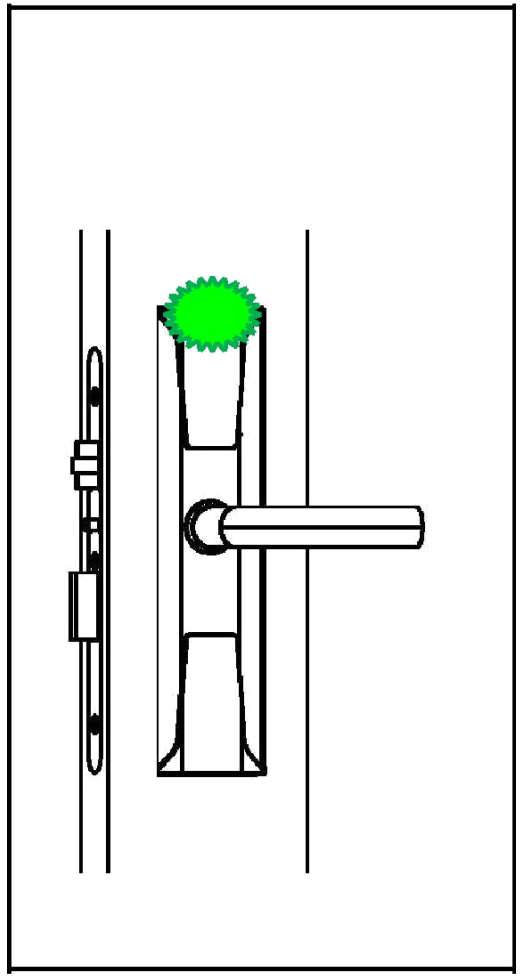
Después de entrar en la habitación, si se desea habilitar la función Privacy, pulse el botón DO NOT DISTURB, que se enciende de color rojo (o gire el pomo en la versión mecánica manual)

USO DE LA CERRADURA EGO



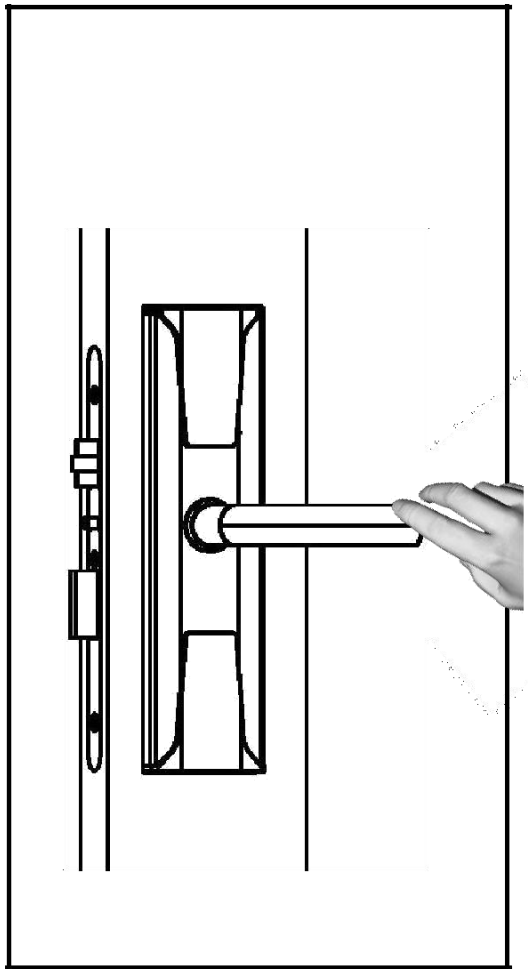
1

Mantenga la tarjeta cerca del lector para 1 segundo para permitir una correcta comunicación.



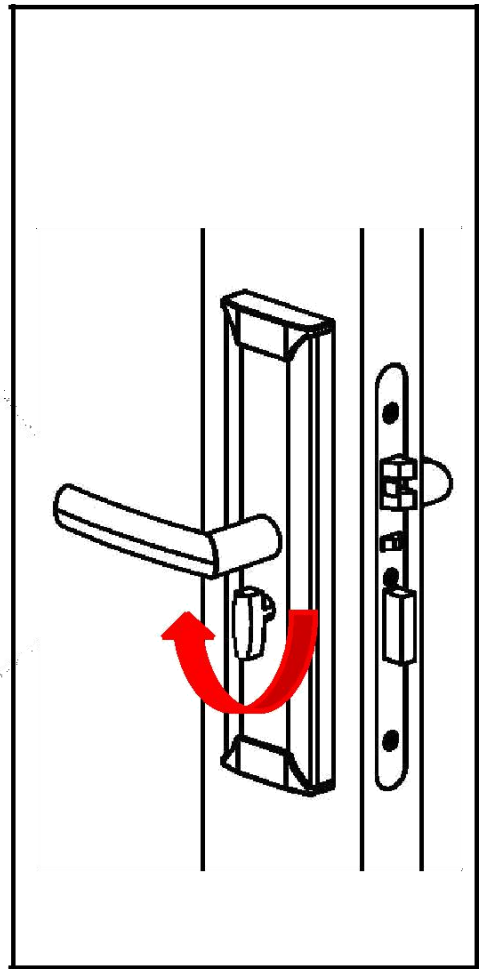
2

Espere hasta que la cerradura emita destellos verdes: indica que la lectura de la tarjeta se ha producido en forma correcta.



3

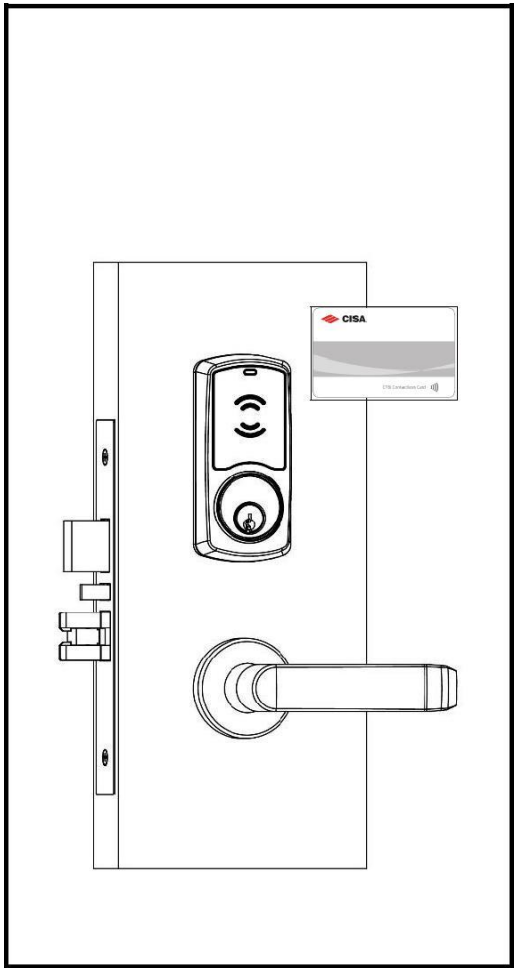
Gire la manilla externa, al para abrir la cerradura, antes de la caducidad del retraso de apertura (por defecto, 5 segundos).



4

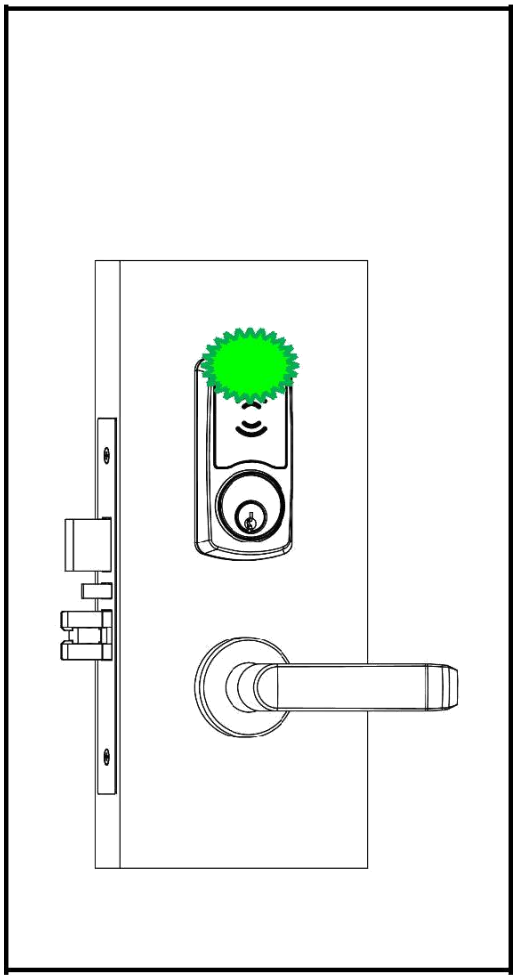
Después de entrar en la habitación, si se desea habilitar la función Privacy, gire el pomo.

USO DE LA CERRADURA EFLEXO



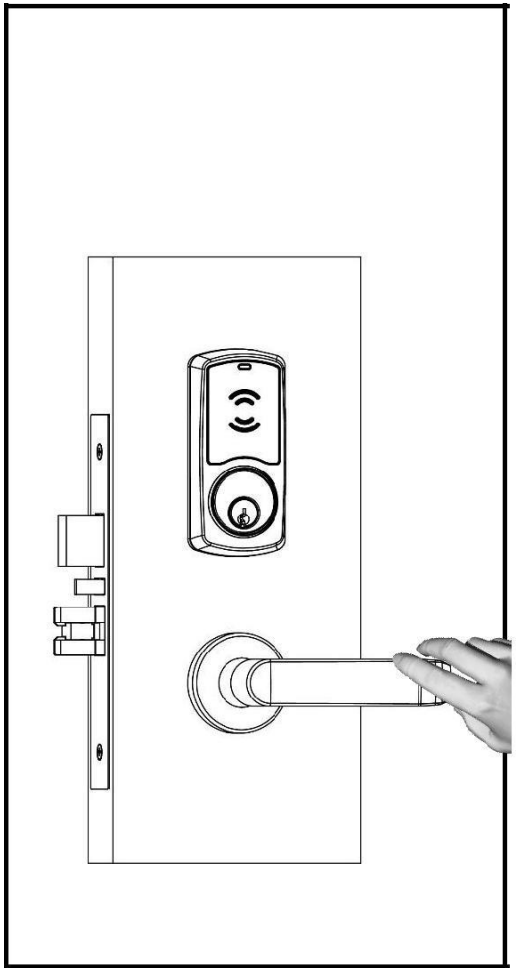
1

Mantenga la tarjeta cerca del lector para 1 segundo para permitir una correcta comunicación.



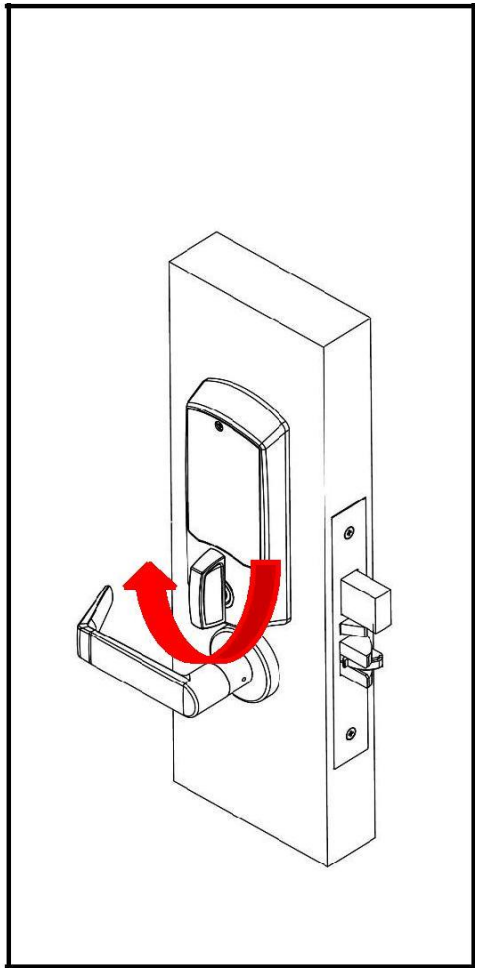
2

Espere hasta que la cerradura emita destellos verdes: indica que la lectura de la tarjeta se ha producido en forma correcta.



3

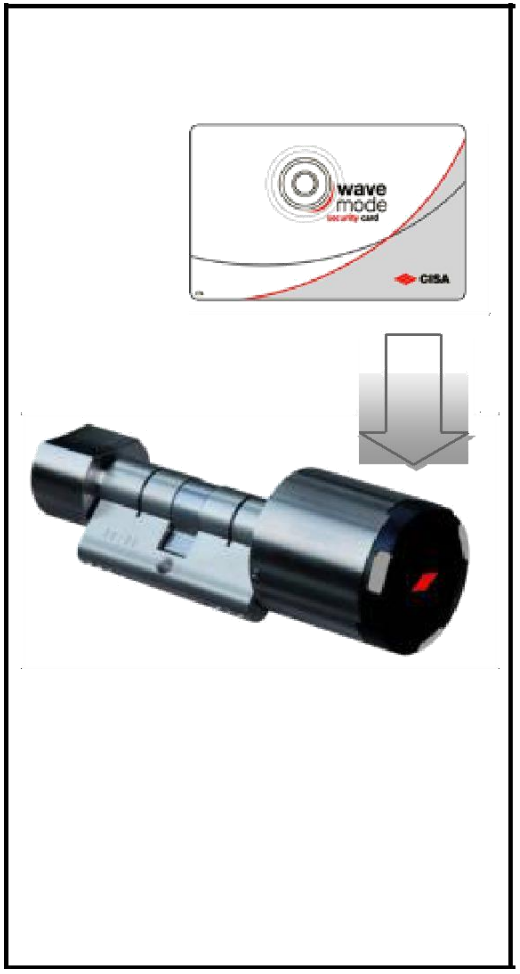
Gire la manilla externa, al para abrir la cerradura, antes de la caducidad del retraso de apertura (por defecto, 5 segundos).



4

Después de entrar en la habitación, si se desea habilitar la función Privacy, gire el pomo.

USO DE E-CYLINDER



1

Mantenga la tarjeta cerca del cilindro electrónico durante 1 segundo, para permitir una correcta comunicación.



2

Espere hasta que el cilindro emita 5 destellos verdes: indica que la lectura de la tarjeta se ha producido en forma correcta.



3

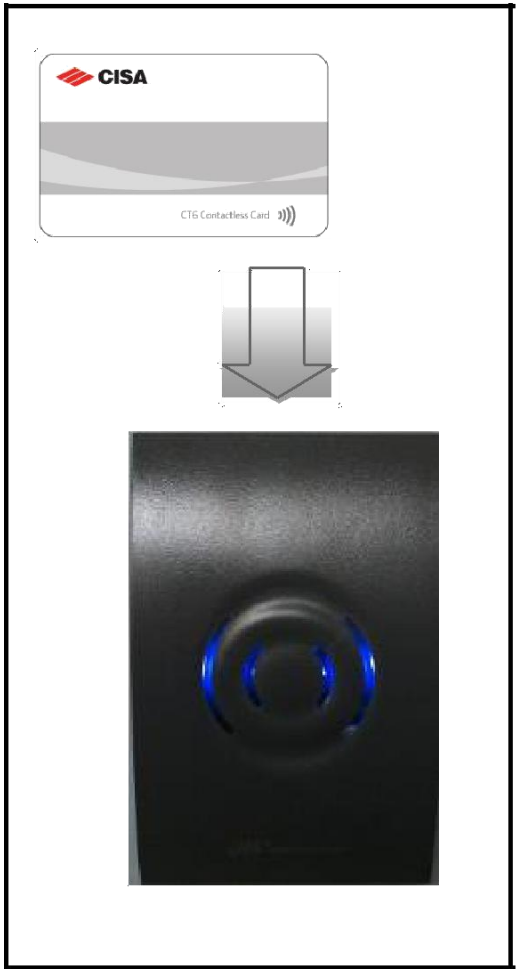
Gire el pomo para abrir la cerradura, antes de terminar el retraso de apertura (por defecto, 5 segundos).



4

Después de entrar en la habitación, para cierre la puerta con llave, gire el pomo interno.

USO DEL LECTOR DE PARED (WALL READER)



PRESENTACIÓN DE LA TARJETA

Mantenga la tarjeta cerca del lector de pared durante 1 segundo, para permitir una correcta comunicación.



TARJETA VÁLIDA

Espere hasta que el lector de pared emita 5 destellos verdes, señal que la lectura de la tarjeta se ha realizado en forma correcta. El relé se activa.



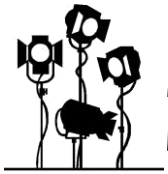
TARJETA INVÁLIDA

Si la tarjeta presentada no es válida, el lector de pared emite tres destellos rojos.

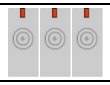
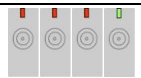


MANTENIMIENTO

Cuando el ratón eSIGNO es presentado al lector de pared, este emite una luz azul y violeta.



DISPOSITIVOS ESIGNO: INDICACIONES LUMINOSAS

5 VERDES		Apertura habilitada (con configuraciones por defecto). En general, un destello verde por cada segundo de apertura
3 ROJOS		Tarjeta inválida (caducada, invalidada por una nueva, etc.)
3 ROJOS + 1 VERDE		Tarjeta temporalmente inválida (función Privacy activa, tarjeta fuera de los horarios permitidos)
1 ROJO		Error de lectura. Si se repite cada 3 segundos: Función Privacy activa (también en el logotipo CISA, cerca del botón PRIVACY interno)
1 VERDE		Cerradura en función Oficina o en estado de peligro (si se presenta una tarjeta válida)
10 VERDES	10x  RÁPIDOS	Cerradura no inicializada
3 ROJO y VERDE	 LENTOS	Batería descargada (solo con tarjetas de servicio). La cerradura abre igualmente con las tarjetas válidas.
6 ROJO & VERDE	6x  LENTOS	Batería muy descargada. Un tono simultáneo al primer destello. La cerradura se abre igualmente con tarjetas válidas.
12 ROJO & VERDE	12x  LENTOS	Batería agotada. Un tono simultáneo al primer destello. La cerradura no se abre.
4 ROJO & VERDE		Operación de tarjetas en secuencia realizada correctamente (oficina on/off, tidy up)
4 ROSSO & VERDE	4x  RAPIDOS	Cierre retardado (solo con tarjetas de servicio y DPR habilitado). Con FW < 2.05: 10 rojo y verde
8 ROJO & VERDE	8x  RAPIDOS	Control palanca: circuito DPR desconectado, la palanca no se puede mover (la cerradura requiere mantenimiento) o tarjeta presentada 3 veces sin abrir la cerradura (solo con tarjetas de servicio). Con FW < 2.05: 20 rojo y verde
1 AZUL		Comunicación con HHI mediante ratón en curso (solo dispositivos eSIGNO/eGO)
1 ROJ & VERDE		Operación en curso (solo recodificación o descarga historial con 30+ registros, solo dispositivos eSIGNO/eGO)
3 VERDES + 1 ROJO + 2 VERDES		Inicialización OK. Dos tonos simultáneos al primer destello.
2 VERDES		Operación realizada correctamente (bloqueo, sincronización, reset, etc.)
6 ROJOS	6x  RAPIDOS	Dispositivo no sincronizado (solo dispositivos eSIGNO/eGO). Acompañado por seis tonos.

Notas:

- En algunas condiciones de iluminación o con ciertas placas de plástico, las indicaciones luminosas con led rojo y verde juntos pueden parecer amarillas o anaranjadas.
- Si no se especifica lo contrario, una señal luminosa corresponde a un destello de un segundo.
- Las señales de batería descargada, cierre retardado y control palanca son mostradas por la cerradura antes de la secuencia normal de apertura.

USO DEL ENERGY SAVER



1

Si no hay ninguna tarjeta introducida en el energy saver, todos los dispositivos dentro de la habitación están apagados.



2A

Introduciendo una tarjeta de cliente en el energy saver, todos los dispositivos dentro de la habitación pueden estar encendidos.



2B

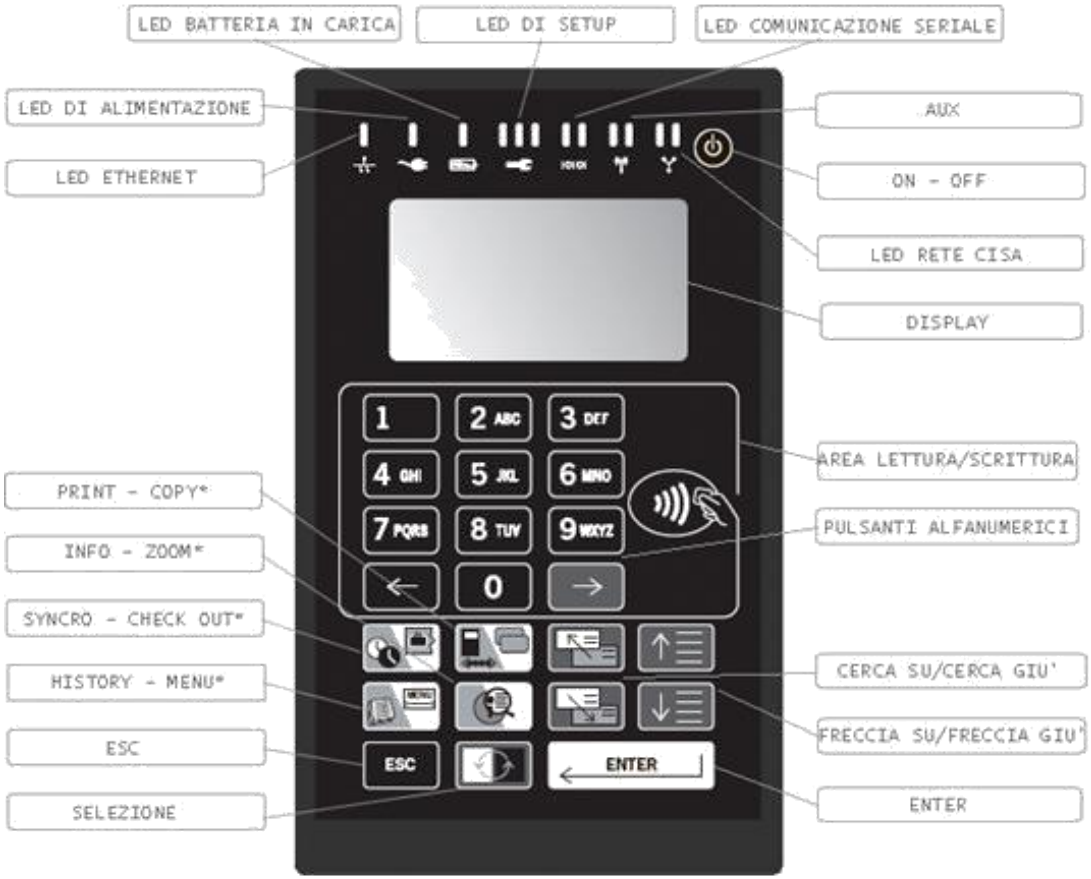
Introduciendo una tarjeta de servicio en el energy saver, solo los dispositivos básicos (por ejemplo, iluminación) pueden estar encendidos.

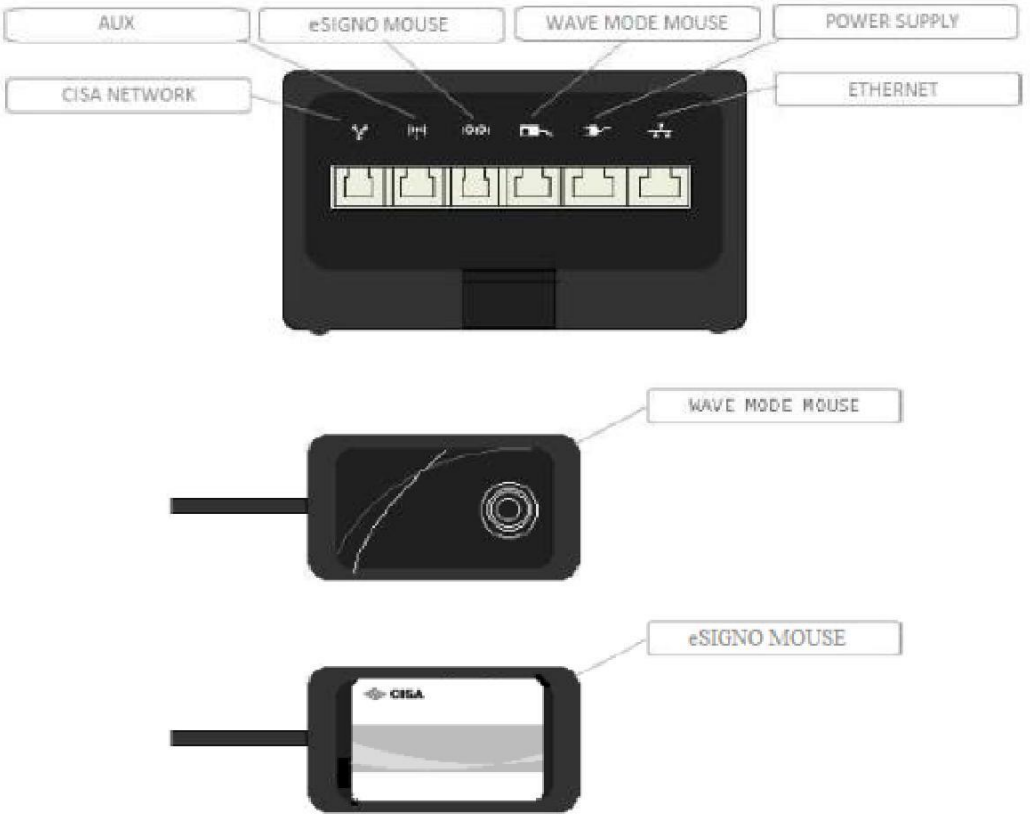


3

Cuando se extrae la tarjeta, comienza el tiempo de cortesía de 50 segundos; después de este intervalo, todos los dispositivos se apagan.

eSIGNO MOBILE





* Botón de doble función: la función varía en función del modo de funcionamiento.

Para configurar el contraste del display, pulse  o , una vez que se ha registrado.

ATENCIÓN

RIESGO DE EXPLOSIÓN SI LA BATERÍA ES SUSTITUIDA CON OTRA DE TIPO ERRÓNEO.

ELIMINE LAS BATERÍAS USADAS SEGÚN LAS INSTRUCCIONES. NO SUSTITUYA EL PAQUETE DE BATERÍAS. EL PAQUETE DE BATERÍAS DEBE SER SUSTITUIDO SOLO POR PERSONAL AUTORIZADO

TEMPERATURA DE FUNCIONAMIENTO: 0 - 50 °C PRODUCTO CONFORME A LA DIRECTIVA RED 2014/53 UE

TECLADO

eSIGNO Mobile está dotado de un teclado de última generación, caracterizado por una serie de botones multifunción, cada uno de los cuales actúa en forma diferente según la posición del cursor y el modo de funcionamiento (Codificador o HHI).



DISPOSITIVO eSIGNO MOBILE



BOTONES ALFANUMÉRICOS

Los botones de 1 a 9 se pueden utilizar para introducir letras y cifras, respectivamente, en los campos de texto o en los campos numéricos:

- a la primera presión de un botón, se visualiza una cifra;
- a las presiones sucesivas del mismo botón, se visualizan las letras impresas en el mismo;
- al final de cada secuencia, una ulterior presión del botón hace recomenzar la secuencia.

Para escribir una palabra compuesta por más de un carácter:

- seleccione el primer carácter, pulsando el botón correspondiente;
- si el segundo carácter está contenido en el mismo botón, pulse → o espere 1 segundo para permitir al cursor moverse automáticamente a la posición siguiente; por el contrario, si el segundo carácter está contenido en otro botón, pulse simplemente el botón para introducir el carácter en la posición siguiente;
- para cancelar el último carácter visualizado, pulse ←;
- para dejar un espacio en blanco o para pasar a la posición siguiente, pulse →.

BOTONES MULTIFUNCIÓN

La función de estos botones depende del modo de funcionamiento de eSIGNO Mobile, Codificador (fondo blanco) o HHI (fondo gris).



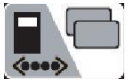
Pantalla detallada: para visualizar todos los detalles de la tarjeta.
Información: para recoger datos de las cerraduras.



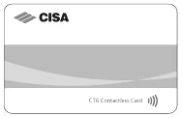
Check-out: para realizar el check-out de una tarjeta de cliente (se inactivará la tarjeta, pero no será cancelada del archivo).
Sincronización: para sincronizar las cerraduras con el HHI.



Menú: para acceder al menú del codificador.
Lectura historial: para leer las operaciones realizadas en una cerradura.



Copiar tarjeta de cliente: para copiar rápidamente una tarjeta de cliente.
Guardar: para guardar información en la memoria, usando un ordenador.



TIPOS DE TARJETAS



SUGERENCIA

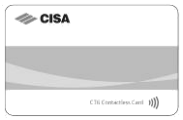
Una tarjeta de cliente puede incluir un número máximo de habitaciones y una categoría en base al soporte físico utilizado:

- CT3: hasta 4 habitaciones + una categoría que incluye una combinación cualquiera de los primeros 16 servicios
- CT4, CT5 and CT6: hasta 4 habitaciones + una categoría que incluye una combinación cualquiera de los primeros 2032 servicios
- Ultralight C: hasta 9 habitaciones + una categoría que incluye una combinación cualquiera de los primeros 40 servicios

Si un operador intenta codificar una combinación imposible, el Smart Software restituye el mensaje de error "Formato de tarjeta no compatible".

Para garantizar la máxima seguridad del sistema y optimizar la gestión de la lista de cancelación en las cerraduras, se recomienda crear tarjetas de servicio a corto plazo que se renovarán en caso de necesidad (en lugar de crear tarjetas de servicio válidas hasta 2051).

TIPO DE TARJETA	CARACTERÍSTICAS
CLIENTE	Utilizada por un cliente para acceder a una cerradura normal de una habitación. Una tarjeta de cliente contiene los datos esenciales, como el número de habitación, el nombre del cliente y la duración de la estadía; según las necesidades, se pueden añadir otras características: • Apertura hasta 4 o hasta 9 puertas con la misma tarjeta de cliente (el máximo efectivo depende de la configuración de la instalación y del soporte físico); • Reglamentar el uso de las puertas de servicio del hotel. • Habilitar la función Oficina y/o la función Superar Privacy. • Configurar el tiempo de validez de la tarjeta. Cuando se presenta una nueva tarjeta de cliente a la cerradura correspondiente, invalida todas las tarjetas de cliente anteriores utilizadas para la misma cerradura. Sin embargo, es posible crear varias copias de una misma tarjeta: todas tienen la misma validez; cuando una tarjeta abre una puerta, las otras copias siguen abriéndola. Las tarjetas de cliente también se pueden utilizar para la función Camas.
SERVICIO	Utilizada por el personal del hotel. Para crear una tarjeta de Servicio, es necesario definir las zonas y las puertas que les pertenecen durante la creación de la instalación. La validez tiene una precisión de 15 minutos: • la codificación redondea a los 15 minutos más cercanos • el fin de la validez incluye los 15 minutos siguientes Si el inicio y el fin del tiempo de validez coinciden, la validez es nula. Para tener una tarjeta con 24 horas de validez, es necesario considerar el intervalo temporal de 15 minutos (00:00 a 23:45). Tipos de tarjetas de servicio: • el tipo (las posibilidades son 1, 2, 3, 4) es asignado automáticamente por el sistema y depende de la zona asignada a la tarjeta. • El tipo es importante para las tarjetas de bloqueo, con el fin de determinar cuál se debe bloquear. • Las tarjetas de servicio tipo 3 pueden tener la función Tidy Up. Las tarjetas de operador son tarjetas de servicio tipo 4.



TIPOS DE TARJETAS

Nota: Para los siguientes tipos de tarjeta, una nueva tarjeta con inicio de validez posterior invalidará la tarjeta anterior cuando se presenta a la cerradura:

- Cliente
- Emergencia
- Peligro/Fin peligro
- Bloqueo/Desbloqueo

TIPO DE TARJETA	CARACTERÍSTICAS
USUARIO	Utilizada para abrir puertas de servicio controladas por servicios. Para crear una tarjeta de usuario, se debe definir la categoría y las puertas de servicio que deben pertenecer a la categoría. Las configuraciones de validez de las tarjetas de usuario son las mismas que las de las tarjetas de servicio.
OPERADOR	Una tarjeta de operador permite al operador trabajar en cualquier estación de codificación; por este motivo está asociada a: • una contraseña, que se debe introducir en SSW/Dashboard para conectarse; • un nivel jerárquico, para habilitar funciones particulares • un nombre de usuario de Active Directory (que debe ser unívoco), para permitir una forma de login alternativa en SSW/Dashboard • un set de iniciales PMS (que debe ser unívoco), para tener un rastro de las tarjetas creadas por el operador mediante el dashboard. Si la tarjeta puede abrir cualquier puerta, tiene las mismas características que una tarjeta de servicio tipo 4. Cuando una tarjeta de operador se cancela, ya no podrá abrir las puertas y acceder a las estaciones de codificación.
EMERGENCIA	Una tarjeta de emergencia abre la puerta para la cual ha sido programada, retirando también la palanca, si el huésped ha activado el modo Privacy. Estas tarjetas se pueden crear solo para una habitación. Una tarjeta para cada habitación de huéspedes se debería conservar en la caja fuerte de la recepción y se debería utilizar solo si el sistema de codificación falla, entregándola al cliente y retirándola en el momento del check-out.
PELIGRO/ FIN PELIGRO	Una tarjeta de peligro abre todas las puertas (superando también el estado Privacy) y deja la cerradura abierta hasta que se presenta la tarjeta de fin peligro. Esto permite a los huéspedes y al personal de servicio, salir rápidamente en caso de eventos de peligro e impide el cierre de las puertas. Se pueden crear tarjetas de peligro (o fin peligro) solo para la zona máster; esto significa que estas tarjetas son válidas para todas las habitaciones.
BLOQUEO/ DESBLOQ UEO	Este tipo de tarjeta permite bloquear (o desbloquear) otros tipos de tarjetas, como las tarjetas de cliente o las tarjetas de servicio (tipo de 1 a 4). Estas tarjetas se pueden crear solo para una zona específica; si se bloquean todos los tipos de tarjetas, la cerradura puede ser abierta solo por la tarjeta de emergencia.
MONOUSO	Estas tarjetas se crean en casos especiales (mantenimiento dentro de la habitación) y abre la puerta solo una vez.

ZONAS DE ACCESO

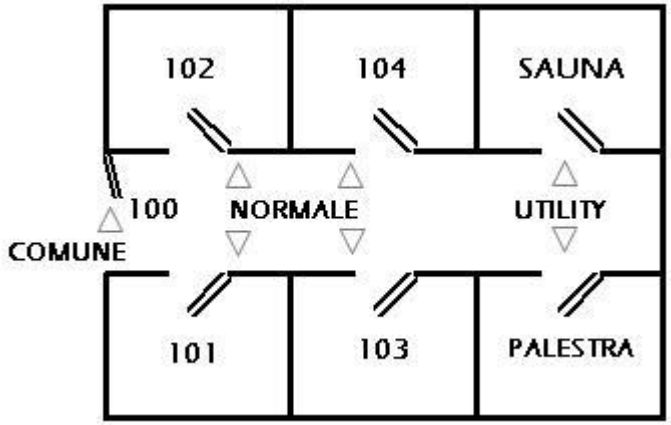


TIPOS DE CERRADURA



SUGERENCIA

Ejemplos de casos de uso de los tres tipos diferentes de cerradura se pueden ver en la figura.



NORMAL

Cerradura para una habitación normal para huéspedes, con las siguientes características:

- con tarjetas de cliente:

solo una tarjeta de cliente por vez (o copias de la misma) puede tener acceso, con la condición de que coincidan los siguientes parámetros: código de instalación, número de habitación, fecha y horario de validez, tarjeta no invalidada por otra con fecha de inicio de validez posterior, tarjeta no bloqueada ni anulada;

- con tarjetas de servicio:

cada tarjeta de servicio está habilitada, si la cerradura se encuentra en el intervalo en el cual la tarjeta tiene derechos de acceso, con la condición de que coincidan los siguientes parámetros: código de instalación, puerta perteneciente a la zona de la tarjeta, fecha y horario (entendido como horario de trabajo) de validez, cliente no en estado de Privacy, tarjeta no bloqueada, tarjeta no anulada (se pueden anular hasta 20 tarjetas de servicio).

COMÚN

Este tipo de cerradura se puede instalar en puertas que dan acceso a diferentes habitaciones en las cuales, a su vez, hay cerraduras normales instaladas (por ejemplo, puertas de corredores). Durante la inicialización del sistema, a cada puerta común se asigna un intervalo de puertas normales. Las características de este tipo de puertas son:

- con tarjetas de cliente:

todas las tarjetas de cliente que han sido codificadas para una puerta que se encuentra en el intervalo configurado durante la configuración de la estructura topológica tienen acceso. Los parámetros y las características son las mismas que las de una puerta normal, salvo por el hecho de que una tarjeta de cliente posterior no invalida las anteriores; además, es posible anular hasta 20 tarjetas de cliente y 20 tarjetas de servicio;

- con tarjetas de servicio:

cada tarjeta de servicio tiene acceso, si la cerradura pertenece a su zona. Los parámetros de control son los mismos mencionados en el párrafo de las cerraduras normales.

SERVICIOS

Estas puertas dan acceso a áreas especiales o de pago dentro de la instalación. Es posible asignar una cerradura de servicio a cada servicio extra ofrecido por el hotel (por ejemplo, sauna, garaje, gimnasio), hasta un máximo de 1024 en instalaciones eSIGNO y de 2032 en instalaciones eSIGNO Extended. Las puertas de servicio se pueden agrupar en categorías, que se describen en el próximo capítulo.

En consecuencia, cada tarjeta se caracteriza por el nombre de la cerradura normal que puede abrir y por la categoría a la cual puede tener acceso.

HÍBRIDAS

Estas cerraduras incluyen las diferentes funciones de las cerraduras normales y de servicio.



FUNCIONES DE LA CERRADURA

FUNCIÓN OFICINA

Consideraremos que esta función ha sido programada en la cerradura y, simultáneamente, habilitada en una tarjeta válida cualquiera; presentando la tarjeta a la cerradura, esta última se abre y permanece en estado de apertura.

Durante la configuración de la instalación, es posible elegir uno de los siguientes modos de funcionamiento de la función Oficina:

- Modo Normal: para activar la función Oficina en una cerradura, es necesario presentar dos veces la tarjeta en secuencia. Para desactivar la función, presente la tarjeta otras dos veces;
- Modo Paso individual (Toggle): presente la tarjeta a la cerradura una sola vez para habilitar (o inhabilitar) la función Oficina.

SUPERACIÓN PRIVACY

La función Privacy es un instrumento útil para el cliente que, una vez dentro de su habitación, desea impedir la apertura de la puerta con cualquier otra tarjeta válida: se puede activar simplemente pulsando el botón DO NOT DISTURB en el lado interno de la cerradura. Sin embargo, con la función Superación Privacy es posible decidir si una tarjeta puede ignorar la función Privacy o no.

- Las tarjetas de cliente tienen la función Superación Privacy activa por defecto.
- Las tarjetas de servicio tienen la función Superación Privacy inactiva por defecto; sin embargo, es posible crear tarjetas de servicio con esta función habilitada.

FUNCIÓN PREPARACIÓN HABITACIÓN

Si esta función ha sido programada en la cerradura durante la instalación, una tarjeta de servicio tipo 3 puede invalidar todas las tarjetas de cliente activas y válidas para esa cerradura. Los pasos que se deben realizar para utilizar la función Preparación habitación se describen a continuación:

- presente la tarjeta de servicio tipo 3 a la cerradura, que se abre;
- presente nuevamente la tarjeta de servicio tipo 3 a la cerradura, que emite 1 destello rojo y 1 verde;
- presente nuevamente la tarjeta de servicio tipo 3 a la cerradura, que emite 4 destellos rojos y 4 verdes;
- las tarjetas de cliente activas han sido incluidas en la lista negra de la cerradura y, en consecuencia, invalidadas.

Esta función es útil en el caso de que el personal del hotel ya haya preparado la habitación a las 10.00 horas, dado que el cliente ya ha realizado el check-out, pero posee una tarjeta válida hasta las 12.00 horas (hora de check-out por defecto).



FUNCIONES ESPECIALES

FUNCIÓN HISTORIAL

Si esta función está habilitada, cada operación realizada por una tarjeta es registrada en la memoria de la misma; una vez que esta ha sido grabada, es posible descargar la lista de operaciones utilizando el eSIGNO Mobile en modo Codificador.

Durante la instalación del sistema es posible optar entre dos modos diferentes de registro del historial:

- No regrabable: la tarjeta puede registrar hasta 30 operaciones. Si la memoria de la tarjeta está llena y la misma se presenta a una cerradura, esta última emitirá 3 destellos rojos: en tal caso, es necesario descargar el historial de la tarjeta, utilizando eSIGNO Mobile en modo codificador, mediante el menú Carga Historial Tarjeta.

  Si ha sido configurado este modo de funcionamiento, cada vez que una tarjeta se presenta a una puerta especial online (por ejemplo, la entrada principal del hotel), se realiza la carga del historial de la tarjeta, para no perder datos de las operaciones.
- Regrabable: la trigésimo primera operación se registrará, pero sobrescribirá el primer registro. Lo mismo ocurrirá para los registros siguientes.

FUNCIÓN DE VALIDACIÓN

Esta función está activa solo si ha sido habilitada durante la configuración de la instalación.

La validación es una función especial que permite un ulterior control de la validez de las tarjetas emitidas. En el momento de emitir tarjetas de cliente, de servicio o de operador, es posible configurar un intervalo de validación: en este período, el propietario de la tarjeta debe presentarla a una puerta especial (inicializada como validador) para restablecer la validez de la tarjeta. Si el intervalo de validación ha caducado y la tarjeta no ha sido presentada en una puerta especial, los derechos de acceso de la tarjeta ya no son válidos: para restablecerlos, la tarjeta se debe presentar al validador.

FUNCIÓN DE RECODIFICACIÓN

Esta función permite cambiar algunos parámetros de tarjetas de usuario o de servicio (por ejemplo, validez o derechos de acceso) sin usar el codificador, sino a través de un lector conectado a una puerta especial online.

- Utilizando el codificador, un operador envía un mando de recodificación a la puerta especial (por ejemplo, la entrada principal del hotel), configurada como validador, con la función Recodificación habilitada.
- Cuando la tarjeta de servicio (o usuario) es leída por el lector conectado a la puerta especial, los parámetros de la tarjeta varían según las instrucciones contenidas en el mando de recodificación.

Para usar la función Recodificación, es necesario habilitar la función Validación durante la fase de inicialización de la puerta especial.



ZONAS DE ACCESO



FUNCIONES WIRELESS

GESTIÓN REMOTA DEL SISTEMA

FUNCIÓN	eSIGNO WIRELESS
Recopilación de datos de historial	Los datos de acceso son puestos a disposición en el ordenador central; ningún límite impuesto al archivo de los datos en las cerraduras offline. (tiempo de latencia: 1 min)
Cancelación de tarjetas de personal	Cada tarjeta de personal puede ser cancelada (inhabilitando la apertura de la cerradura) mediante conexión wireless directamente desde la recepción
Monitorización del personal	Es posible crear automáticamente un informe para mostrar todos los accesos de un empleado a cada habitación, grupo de habitaciones o todas las habitaciones.
Apertura remota de la puerta	Posibilidad de abrir la puerta mediante un mando remoto (tiempo de latencia: 1 min) (solo cerraduras ZigBee)

DIAGNÓSTICO Y MANTENIMIENTO REMOTO

FUNCIÓN	eSIGNO WIRELESS
Estado de la puerta	Si la puerta se deja abierta por un período determinado, es posible emitir una señal especial de alerta directamente a la oficina de seguridad (tiempo de latencia: 1 min)
Estado de las baterías	El estado de las baterías se envía automáticamente al ordenador cada vez que se produce un evento en la cerradura.
Mantenimiento temporal cuidadoso	Sincronización automática de la cerradura desde el ordenador central (una vez por día).
Configuraciones y diagnóstico cerradura	Posibilidad de realizar operaciones a distancia: lectura información hardware, modificación de los parámetros como tiempo de apertura, autoprogramación (tiempo de latencia: 1 min)
Calidad de campo inalámbrico	La calidad del campo inalámbrico para cada cerradura se pone a disposición en el ordenador central cada vez que se produce un evento en la cerradura (solo cerraduras ZigBee)
Instrumento inalámbrico Analyzer	Instrumento (eSIGNO Mobile + antena Analyzer) para realizar análisis de campo inalámbrico para la instalación y el mantenimiento de la instalación (solo cerraduras ZigBee)



ZONAS DE ACCESO

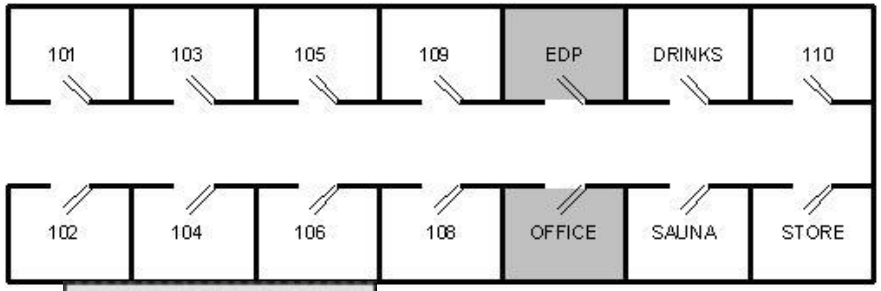


ZONAS (1)

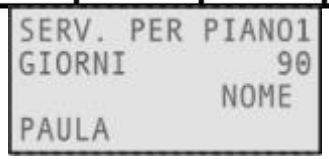
ZONAS ESTÁTICAS

Grupos de cerraduras definidos durante la configuración del sistema.

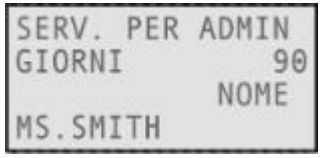
Ejemplo 1



PISO1 101 - 110
PISO2 201 - 209
PISO3 301 - 309
MÁSTER Todas las habitaciones
ADMIN OFFICE + EDP
GUESTS Habitaciones clientes



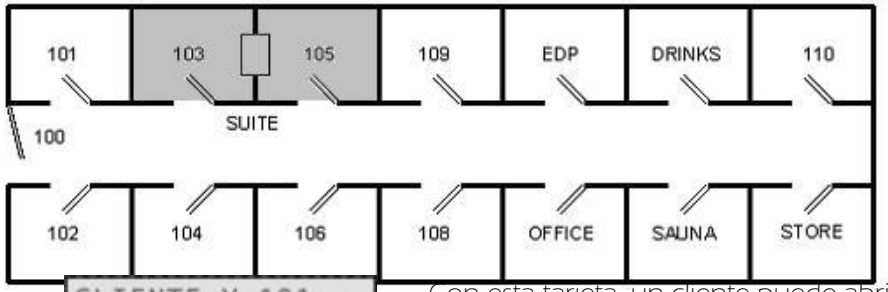
A cada tarjeta se puede asignar una zona: con esta tarjeta, un miembro del personal puede abrir todas las cerraduras en la zona denominada PISO1 (PIANO1) (habitaciones de 101 a 110).



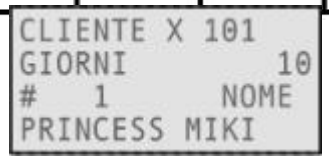
Con esta tarjeta, un miembro del personal puede abrir todas las cerraduras en la zona ADMIN, es decir, OFFICE y EDP. Hay 2 funciones adicionales:

- Superación Privacy: apertura incluso con la función Privacy activa;
- Función Oficina: habilitada cuando la tarjeta se presenta 2 veces.

Ejemplo 2



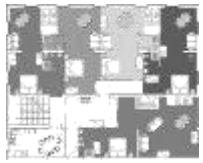
PISO1 101 - 110
MÁSTER Todas las habitaciones
ADMIN OFFICE + EDP
GUESTS Habitaciones clientes
SUITE 103 + 105
MINBAR Habitaciones clientes + DRINKS



Con esta tarjeta, un cliente puede abrir las cerraduras incluidas en la zona SUITE (habitaciones 103 y 105); en alternativa, se pueden emitir tarjetas para cada una de las habitaciones. Nótese que una tarjeta emitida posteriormente invalida siempre las anteriores



ZONAS DE ACCESO

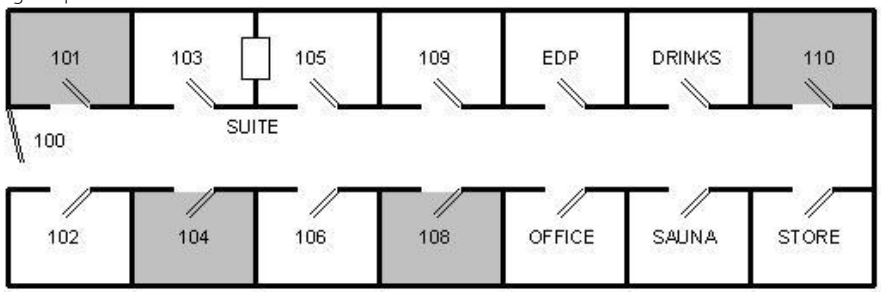


ZONAS (2)

ZONAS DINÁMICAS (PARA CLIENTES)

Grupos de cerraduras definidos, solo para los clientes y en función de las necesidades, en el momento del check-in.

Ejemplo



PISO1 101 - 110
PISO2 201 - 209
PISO3 301 - 309
MÁSTER Todas las habitaciones
ADMIN OFFICE + EDP
GUESTS Habitaciones clientes

```
NOME
MR.ANDERSON
PER     (1)
          101
E PER   (2)
          104
E PER   (3)
          108
E PER   (4)
          110
...

TIPO DI CARTA
  CLIENTE
```

◁ Se pueden seleccionar hasta 4 puertas completamente independientes.

◁ Todos los otros datos de la tarjeta.

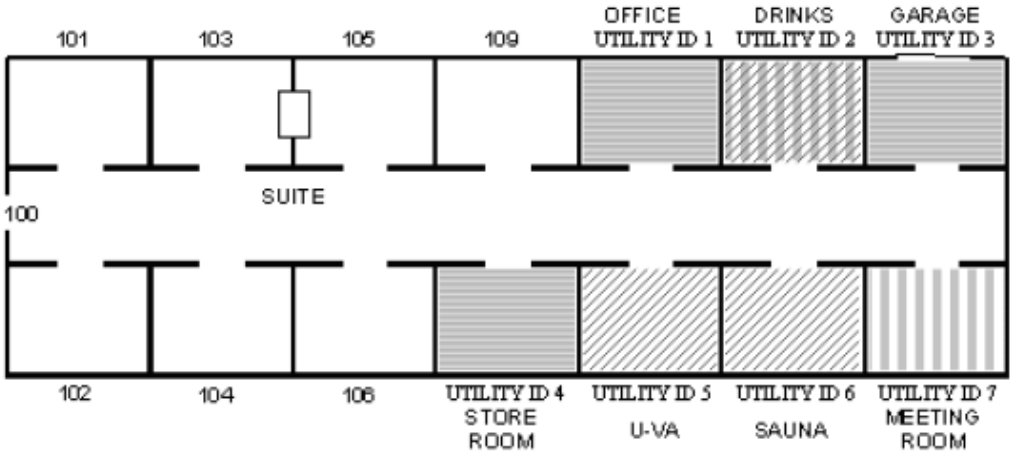


ZONAS DE ACCESO

CATEGORÍAS

Las categorías son grupos de puertas de servicio: es posible crear diferentes categorías, en función de las necesidades de gestión del hotel.
Después de definir un conjunto de categorías, es posible utilizarlas varias veces para tarjetas diferentes; de esta forma, el recepcionista no debe redefinir el mapa de las puertas de servicio cada vez que debe emitir una tarjeta.

Ejemplo



1 keyplan
3 usuarios de tarjeta:
- Membro del personal
- Turista
- Hombre

MAPA DE LOS IDENTIFICADORES DE LOS SERVICIOS

1	2	3	4	5	6	7
OFFICE	DRINKS	GARAGE	STORE	UVA	SAUNA	MEETING

```
MAPPA UTILITY
1     ---     16
SERRATURE UTIL.
X-XX-----------
```

Categoría HOTEL
Utilizada por los miembros del personal del hotel; incluye Office, Garage y Store.

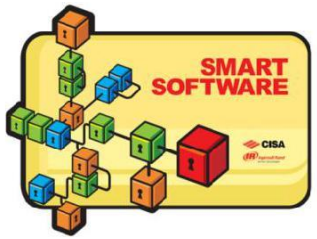
```
MAPPA UTILITY
1     ---     16
SERRATURE UTIL.
-X--XX---------
```

Categoría TURISTA
Se puede utilizar para todos los clientes que deben tener acceso a los servicios extra del hotel (en este caso, Drinks, UVA y Sauna).

```
MAPPA UTILITY
1     ---     16
SERRATURE UTIL.
-X----X--------
```

Categoría NEGOCIOS
Da acceso a todos los servicios vinculados al desarrollo de un negocio específico (en este caso, Drinks y Meeting Room).

INSTALACIÓN SMART SOFTWARE





REQUISITOS DEL SISTEMA

Procesador: Mínimo 2 GHz Quad-core o 3 GHz Dual-core

Disco duro: al menos 20 % de espacio disponible en el disco, mínimo 200 MB, recomendado 1 GB RAM: Mínimo 4 GB. Recomendado 8 GB

Pantalla con resolución mínima de 1024 x 768 recomendada

Sistema operativo: a elección entre las siguientes versiones 32 bit o 64 bit (incluido .NET Framework 4):

- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows 10
- Windows Server 2016

SQL Server Express 2008 R2 SP2 o 2014

Navegadores compatibles para dashboard y Admin App:

- Internet Explorer 11
- Mozilla Firefox 46 o posterior
- Google Chrome 50 o posterior
- Microsoft Edge 41 o posterior

Notas:

- Se recomienda desactivar el modo stand-by/suspensión en el ordenador en cuestión;
- las prestaciones del software dependen fuertemente de la estructura de la instalación;
- es necesario que el eventual firewall permita la comunicación entre el ordenador y los dispositivos online en los puertos de 10000 a 10240 (protocolo UDP).

PROCEDIMIENTO DE INSTALACIÓN

1. Ejecute el archivo setup.exe como administrador, haciendo clic con el botón derecho en el archivo y seleccionando el ítem correspondiente.
2. Seleccione el idioma deseado y comience la instalación siguiendo las instrucciones.
3. Si es necesario, se instalarán los siguientes componentes:
   - Windows Installer 4.5
   - Microsoft Visual C++ Runtime Libraries 2005
   - SAP Crystal Reports
4. Complete la instalación siguiendo las instrucciones.
5. Al final de la instalación de Smart Software, reinicie el ordenador.

INSTALACIÓN SMART SOFTWARE

Nota: Esta operación debe ser realizada solo por una persona del Centro de Asistencia Técnica CISA.

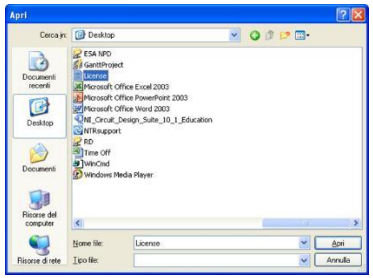
LICENCIA

En la primera activación del software, es necesario cargar un archivo de licencia válido. Esta licencia es un archivo .xml suministrado por un Centro de Asistencia Técnica CISA; una vez recibida, esta debe ser copiada en el ordenador en el que está instalado el Smart Software.

1. Pulse

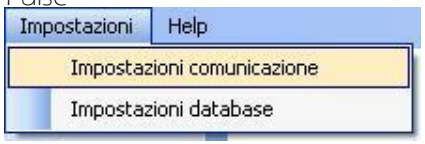


2. Localice el archivo .xml de licencia en el ordenador y pulse ABRIR (APRI).



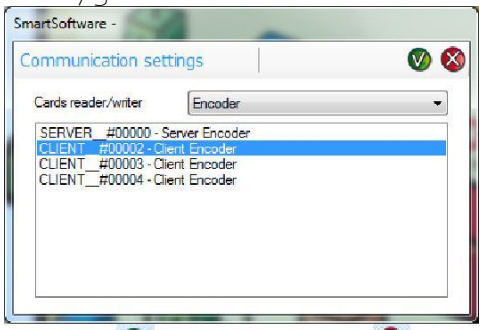
CONFIGURACIONES DE COMUNICACIÓN

1) Pulse



2) Elija el tipo de lector/grabador:

Codificador: un sistema de codificación CISA (M305).
Lector/grabador Smart Card: un lector externo NFC.



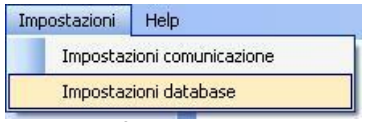
3) Pulse  para aceptar o  para cancelar.

INSTALACIÓN SMART SOFTWARE

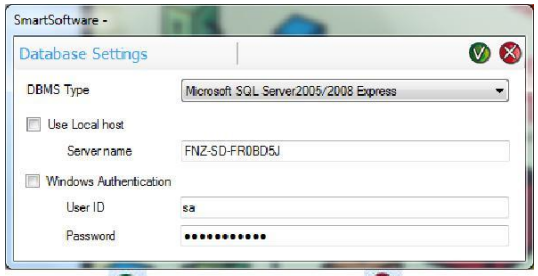
Nota: Esta operación debe ser realizada solo por una persona del Centro de Asistencia Técnica CISA.

CONFIGURACIONES DE LA BASE DE DATOS

1) Pulse



2) Si se utiliza Microsoft SQL Server 2008, deje las configuraciones por defecto. Si se utiliza un servidor SQL diferente, configure los parámetros de conexión basándose en su configuración.
3) En el ordenador servidor, deje seleccionados los cuadros Usar ordenador local (Use Local host) y Autenticación de Windows (Windows Authentication). En un ordenador client, deselecciónelos y configure el nombre del ordenador servidor y los detalles de la cuenta utilizados para la autenticación de Microsoft SQL.

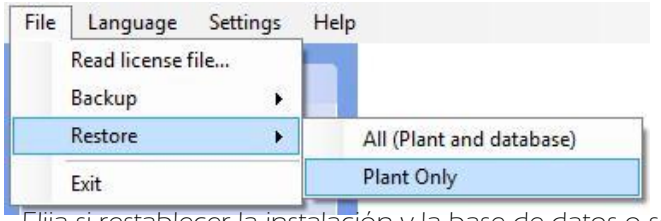


4) Pulse para aceptar o para cancelar.
5) Reinicie el Smart Software.

RESTABLECIMIENTO

Para restablecer la instalación deseada en el Smart Software:

1) Pulse:



2) Elija si restablecer la instalación y la base de datos o solo la instalación:
El archivo de la instalación contiene datos estadísticos como las cerraduras, las zonas de acceso y las categorías.
La base de datos contiene datos guardados durante el uso del Smart Software (por ejemplo, usuarios).
3) El archivo de backup a restablecer es proporcionado por el Centro de Asistencia Técnica CISA (Technical Assistance Centre) y se encuentra en el disco duro del ordenador (hard drive). Identifique el archivo de backup plant_name.zip y pulse Abrir.
4) Cuando aparece el mensaje de terminación, pulse OK. El software se cierra automáticamente.
5) Pulse el ícono presente en el escritorio para reiniciar el Smart Software.

INSTALACIÓN SMART SOFTWARE

Nota: Esta operación debe ser realizada solo por una persona del Centro de Asistencia Técnica CISA.

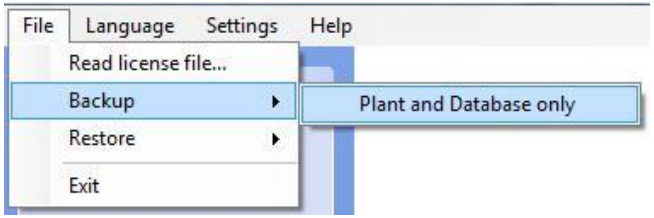
SINCRONIZACIÓN CODIFICADOR BACKUP SERVER

Nota: Esta operación debe ser realizada solo por una persona del Centro de Asistencia Técnica CISA.

BACKUP

Para crear un archivo de backup de la instalación, controlado con el Smart Software:

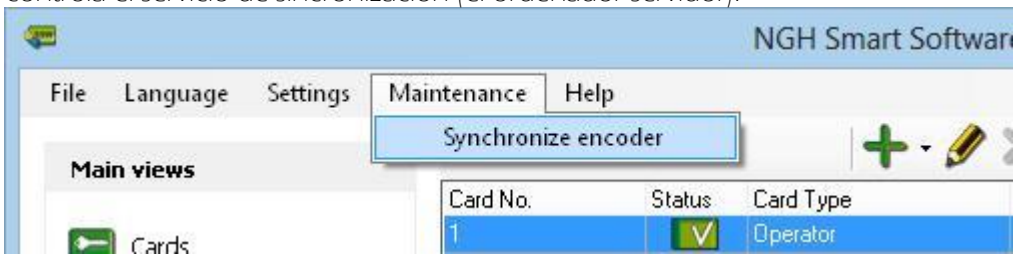
1) Pulse:



2) Elija la carpeta en la cual guardar el archivo de backup y pulse OK.

Cuando se instala por primera vez un codificador Backup Server o cuando se verifica un caso de desalineación de los datos (por ejemplo, después de una falla del codificador Backup Server), el usuario del Smart Software debe realizar una sincronización completa de los datos.

El menú de Sincronización (Stynchronize encoder) está activo solo en la estación de trabajo Smart Software que controla el servicio de sincronización (el ordenador servidor).



El servicio se detiene automáticamente antes de realizar la sincronización y se reinicia una vez completado el proceso.

La sincronización completa del codificador Backup Server incluye:

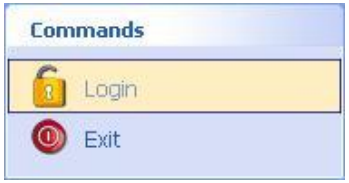
- Inicialización de los datos
- Configuración de los datos (keyplan)
- Tarjetas
- Categorías

El servicio de sincronización del codificador mantiene el codificador actualizado, sincronizando cada cambio en las categorías y en las tarjetas.

El servicio de sincronización del codificador Backup Server recibe cada evento de codificación después de una falla para realinear la base de datos del ordenador servidor con tarjetas emitidas en modo Fallo.

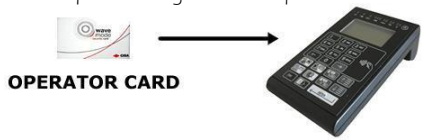
LOGIN

1) Pulse:



2) El codificador muestra el mensaje "Leer tarjeta" (Leggi Carta) y emite un tono.

3) Coloque la tarjeta de operador en el codificador:



4) Introduzca la contraseña:



5) En alternativa, si ha sido configurada la opción Habilitar login con usuario Active Directory en la vista Preferencias (Preferenze), el operador puede acceder introduciendo el nombre de usuario correspondiente y la contraseña Active Directory.

6) Pulse 

7) La barra superior del Smart Software muestra el nombre del operador actualmente registrado.

LOGOUT

Para realizar el logout del Smart Software, en cualquier página, pulse 

Una vez que el usuario ha realizado el logout, para acceder al Smart Software será necesario realizar nuevamente el procedimiento de login.

SALIDA

Para salir del Smart Software, en cualquier página, pulse 

Si el usuario ha realizado el login, aparece un mensaje de aviso:



Para proceder, pulse OK. De esta forma, el Smart Software se reduce a un ícono.



Para cerrar completamente el Smart Software, pulse el ícono con el botón derecho y luego Salir (Exit).



IDIOMA

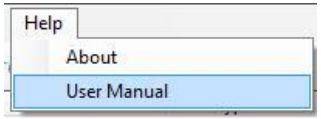
Para cambiar el idioma del software, pulse



Están disponibles los siguientes idiomas: Inglés Italiano Francés Alemán

MANUAL DE USUARIO

Para abrir el manual de usuario, pulse:



PANEL LATERAL MENÚ

El panel lateral sirve como instrumento de exploración durante el uso del Smart Software.

Está dividido en 4 secciones; dentro de cada una, hay un conjunto de funciones agrupadas lógicamente.



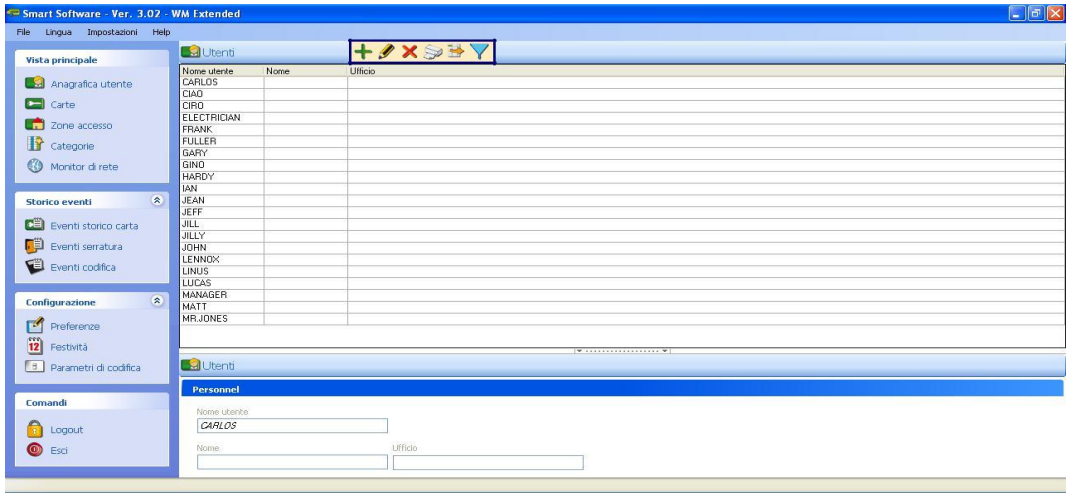
Anagrafica utente	Para crear y controlar a los usuarios. 1
Carte	Creación y gestión de tarjetas.
Zone accesso	Para visualizar cerraduras, zonas y camas.
Categorie	Para crear y controlar las categorías (grupos de cerraduras de servicios). 2
Monitor di rete	Visualización de los dispositivos actualmente conectados a la red.
Storico eventi	Para cargar el historial de la tarjeta desde la unidad de control de accesos especial.
Eventi storico carta	Visualiza el historial de la cerradura cargado en el codificador.
Eventi serratura	Visualiza el historial de eventos de codificación.
Eventi codifica	
Configurazione	
Preferenze	Para configurar parámetros generales.
Festività	Para gestionar el control de accesos durante los días festivos.
Parametri di codifica	Define los parámetros por defecto para la codificación de tarjetas.
Comandi	
Logout	Para desconectar al operador de la sesión de trabajo.
Esci	Para cerrar la aplicación.

[1] Solo si la descripción de los usuarios está habilitada en la sección Preferencias (Preferenze).

[2] Solo si ha sido definida al menos una categoría durante la configuración de la instalación.

ÍCONOS COMUNES

Los siguientes íconos son comunes a diferentes secciones del Smart Software. Además, cada página presenta otros íconos dedicados a esa función específica. Desplazando el ratón sobre cada ícono, se visualiza el nombre/función del mismo.



 Añadir: se utiliza para añadir un nuevo ítem a la lista (por ejemplo, un nuevo usuario). Una vez pulsado el ícono, aparecen en la pantalla los campos blancos para rellenar con los datos.

 Modificar: se utiliza para modificar las propiedades del ítem seleccionado. Una vez pulsado el ícono, las modificaciones se pueden realizar en el panel inferior; a continuación, confirme o anule con 

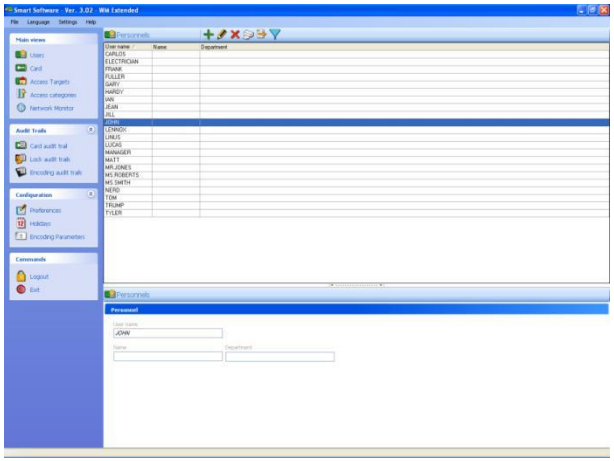
 Eliminar: se utiliza para eliminar un ítem de la lista. Pulse primero el ítem que desea cancelar y, a continuación, el ícono Eliminar; aparece una ventana de confirmación.

 Filtrar: se utiliza para la búsqueda de datos, basada en la congruencia con lo los criterios introducidos. Una vez pulsado el ícono, en la parte superior de la página aparece una línea vacía, en la que el usuario debe introducir los criterios de búsqueda. Todos los parámetros introducidos para la operación de filtración son elaborados en AND lógico. Los resultados se pueden ordenar a gusto, pulsando la columna deseada.

 Limpiar: cancela la visualización actual.

 Imprimir: imprime la página visualizada. Una vez pulsado el ícono, se abre una ventana de vista previa de impresión, en la que el usuario puede elegir si memorizar el documento en una tarjeta o exportar los datos en uno de los formatos disponibles (Adobe .pdf, Microsoft Excel .xls, Microsoft Word .doc, Crystal Reports .rpt, Rich Text Format .rtf)

SMART SOFTWARE: USUARIOS



Para habilitar la gestión de usuarios:

1) Pulse 

2) Pulse 

3) Configure el número y la descripción de los campos de usuario (Campi utente):



4) Pulse  para aceptar las modificaciones.

FUNCIONES
En la página Datos del Usuario (Anagrafica Utente), es posible:

 Añadir un nuevo usuario, introduciendo un nombre y un valor para cada campo;



 Modificar un usuario preexistente, introduciendo nuevos valores para los campos deseados;

 Eliminar un usuario preexistente;

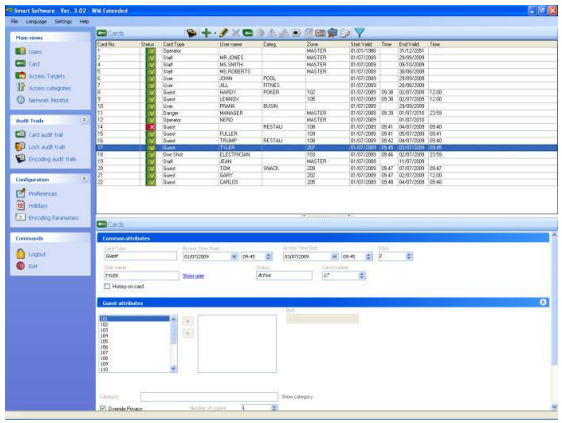
 Buscar en la lista de usuarios, utilizando uno o más criterios;

 Importar una lista de usuarios desde un archivo .csv;

 Imprimir o exportar la lista de usuarios.  Mostrar/esconder usuarios creados por PMS.

Nota: Cada vez que se emite una tarjeta, el nombre de usuario correspondiente se añade a la lista de usuarios.

SMART SOFTWARE: TARJETAS





TIP

Para crear una tarjeta de operador con atributos para el acceso con Active Directory:

1) En la vista Preferencias (Preferenze) debe estar seleccionado el cuadro "Habilitar login con usuario Active Directory" (Abilita login con utente Active Directory)
2) Pulse "Agregar tarjeta" (Aggiungi carta) y seleccione "Operador" (Operatore)
3) Configure los parámetros deseados (validez, nombre de usuario, contraseña, perfil jerárquico, zona)
4) En el campo "Usuario Active directory" (Utente Active directory), introduzca solo el nombre de usuario Active Directory (por ejemplo, gcosta)
5) Confirme y codifique la tarjeta.

Este operador podrá realizar el login:

- Presentando la tarjeta de operador al codificador e introduciendo la contraseña.
- Introduciendo el correspondiente nombre de usuario Active Directory y la contraseña.

Cuando se accede a esta vista, se muestran todas las tarjetas emitidas, ordenadas por número de tarjeta. En particular, en primer lugar se enumeran:

- las tarjetas importadas de la instalación anterior de SSW3
- las tarjetas emitidas en modo Fallo

Luego se enumeran todas las tarjetas emitidas durante las operaciones normales.

CREACIÓN DE TARJETAS

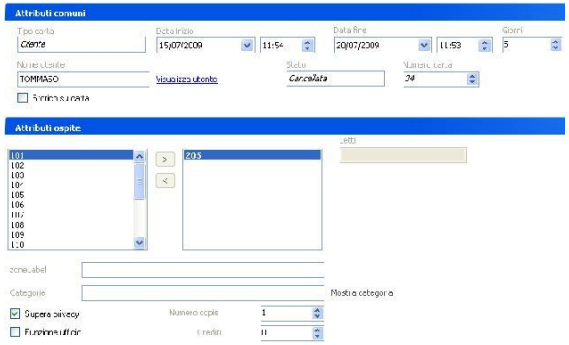
Esta operación permite crear nuevas tarjetas.

1) En cualquier página, pulse 

2) Pulse la flecha del botón 
3) Seleccione qué tipo de tarjeta crear. Nota: las opciones presentes en la lista dependen del nivel jerárquico del operador que ha realizado el login.

   A continuación, simplemente pulsando , el programa crea una tarjeta del mismo tipo que la anterior.

4) Introduzca los parámetros deseados, en función del tipo de tarjeta:



5) Pulse  para aceptar las modificaciones.

6) El codificador emite un sonido agudo.

7) Apoye una tarjeta en el teclado. 

SMART SOFTWARE: TARJETAS

Nota: Si para crear una nueva tarjeta se utiliza una tarjeta física que contiene credenciales válidas (presentándola nuevamente al codificador), la credencial anterior se marca como cancelada, dado que ya no existe.

Ejemplo:

1. Una credencial de servicio se crea usando un soporte físico; esta tarjeta de servicio se marca como válida en el SSW.
2. Se crea una nueva credencial de usuario usando la misma tarjeta física. Esta última tarjeta de usuario se marca como válida en el SSW, mientras que la tarjeta de servicio se marca como cancelada (dado que físicamente ya no existe).

MODIFICACIÓN TARJETAS

Esta operación permite modificar los parámetros de una tarjeta preexistente, para codificar una nueva. La tarjeta original permanece activa.

Tipos de tarjetas: todos (solo tarjetas válidas)

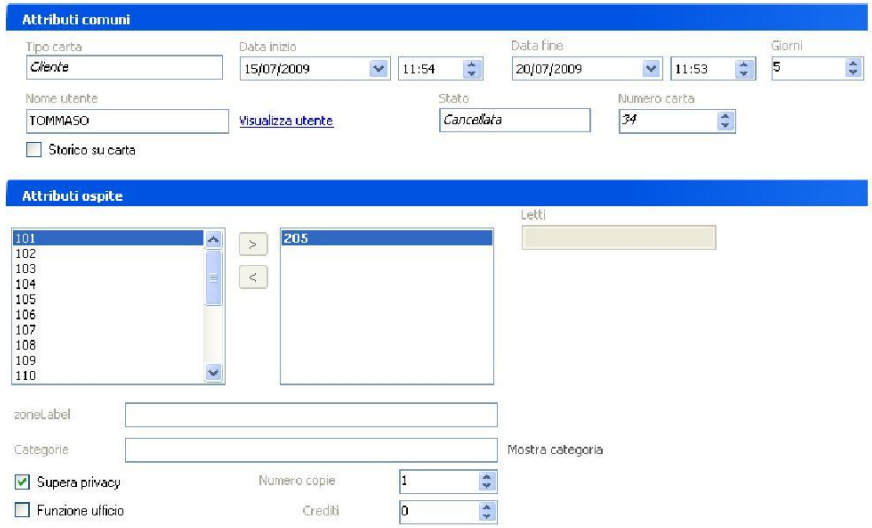
1) En cualquier página, pulse 

2) Seleccione la tarjeta que se debe modificar en la lista de tarjetas disponibles.

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
39		Cliente	SANDRA		109	21/07/2009	10.40	25/07/2009	10.40
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

3) Pulse 

4) Realice las modificaciones deseadas:



5) Pulse  para aceptar las modificaciones o  para cancelar.

6) El codificador emite un sonido agudo.
7) Apoye una tarjeta en el teclado.



SMART SOFTWARE: TARJETAS

Nota: Si la función SmartMedia ha sido habilitada en la instalación, solo es posible crear copias de tarjetas de cliente ULC encriptadas con la llave actual.

COPIA TARJETAS

Esta operación se debe realizar para crear copias idénticas de una tarjeta de cliente. La nueva tarjeta no inhabilita el acceso con la tarjeta original.

Tipos de tarjetas: solo tarjetas de cliente válidas.

Caso de uso: para proporcionar a cada miembro de un grupo una credencial de acceso a su habitación o apartamento.

1) En cualquier página, pulse 

2) Seleccione la tarjeta que se debe copiar en la lista de tarjetas disponibles.

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
39		Cliente	SANDRA		109	21/07/2009	10.40	25/07/2009	10.40
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

3) Pulse 

4) Elija si la copia debe superar la función Privacy:



5) Pulse  para aceptar las modificaciones o  para cancelar.

6) El codificador emite un sonido agudo.

7) Apoye una tarjeta en el teclado.



Nota: después de seleccionar una tarjeta para realizar:

- Si se pulsa se restablece la última recodificación, agregando una nueva y volviendo al conjunto original de datos
- Si se pulsa se cancelan la tarjeta para realizar, la original y todas las eventuales intermedias para realizar

Nota: Un lector de pared configurado como validador

- No emite destellos adicionales, si la tarjeta presentada solo debe ser validada;
- Emite un destello largo rojo y verde, si la tarjeta presentada debe ser recodificada. Mientras este destello está activo, mantenga la tarjeta frente al lector de pared.

RECODIFICACIÓN TARJETAS

Esta operación permite cambiar los parámetros y/o derechos de acceso de una tarjeta, presentándola a una unidad de control de accesos especial, configurada como validador. La función está disponible solo con la utilización de tarjetas CT4 o Mifare Classic.
Tipos de tarjetas: Servicio, usuario u operador.

Caso de uso: el director del sistema desea extender la validez de la tarjeta de un miembro del personal de servicio. El director no debe solicitar necesariamente la tarjeta al empleado, sino que puede cambiar la validez mediante el Smart Software. Cuando el empleado presenta la tarjeta a una unidad de control de accesos especial (situada, por ejemplo, en la entrada del hotel), la validez de la tarjeta se modifica.

1) En cualquier página, pulse Carte
2) Seleccione la tarjeta que se debe recodificar en la lista de tarjetas disponibles.

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
4		Servizio	MS.SMITH		MASTER	01/07/2009		09/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

3) Pulse (botón TO DO)
4) Modifique los campos deseados:



5) Pulse para aceptar las modificaciones o para cancelar.
6) A continuación aparece una línea que contiene los datos de la tarjeta, tal como se recodificará; el correspondiente ícono de estado representa un engranaje:

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
4		Servizio	MS.SMITH		MASTER	01/07/2009		09/10/2009	
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	

7) Cuando la tarjeta se presenta al validador, los parámetros se modifican.
En el Smart Software, el ícono de estado de la tarjeta original se vuelve rojo, mientras que el de la tarjeta recodificada se vuelve verde:

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
4		Servizio	MS.SMITH		MASTER	01/07/2009		09/10/2009	
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	

SUSPENSIÓN TARJETAS (CERRADURAS OFFLINE)

Esta operación, reversible mediante el mando de restablecimiento, permite suspender temporalmente la validación de una tarjeta en la que esta función está habilitada. La validación permite un ulterior control de la validez de las tarjetas en fase de emisión, configurando un intervalo de validación: en este período, el propietario de la tarjeta debe presentarla a una puerta especial para restablecer la validez de la misma. Si el intervalo de validación ha caducado y la tarjeta no ha sido presentada en una puerta especial, los derechos de acceso de la tarjeta ya no son válidos: para restablecerlos, la tarjeta se debe presentar al validador.

Tipos de tarjetas: todas las tarjetas válidas

Caso de uso: un estudiante residente en un campus, que accede a su habitación con una tarjeta de usuario, aún no ha pagado el canon mensual. El director del campus puede suspender la validación de la tarjeta de usuario (suspendiendo también su validez); cuando el estudiante paga el canon, su tarjeta puede ser restablecida.

1) En cualquier página, pulse 

2) Seleccione la tarjeta que se debe suspender (con función de validación habilitada).

30		Cliente	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Servizio	JEFF		MASTER	08/07/2009		01/10/2009	
32		User	CIAO	BUSIN		13/07/2009		11/10/2009	
33		User	JILLY	FITNES		01/07/2009		20/08/2009	

3) Pulse  y confirme.
4) El ícono de estado de la tarjeta suspendida se vuelve anaranjado:

30		Cliente	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Servizio	JEFF		MASTER	08/07/2009		01/10/2009	
32		User	CIAO	BUSIN		13/07/2009		11/10/2009	
33		User	JILLY	FITNES		01/07/2009		20/08/2009	

RESTABLECIMIENTO TARJETAS (CERRADURAS OFFLINE)

Esta operación permite invertir un mando de suspensión, en una tarjeta en la que está habilitada la función de validación.

1) En cualquier página, pulse 

2) Seleccione la tarjeta suspendida que se debe restablecer en la lista de tarjetas disponibles.

30		Cliente	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Servizio	JEFF		MASTER	08/07/2009		01/10/2009	
32		User	CIAO	BUSIN		13/07/2009		11/10/2009	
33		User	JILLY	FITNES		01/07/2009		20/08/2009	

3) Pulse  y confirme.
4) El ícono de estado de la tarjeta restablecida se vuelve verde:

30		Cliente	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Servizio	JEFF		MASTER	08/07/2009		01/10/2009	
32		User	CIAO	BUSIN		13/07/2009		11/10/2009	
33		User	JILLY	FITNES		01/07/2009		20/08/2009	

SUSPENDER (CERRADURAS WIRELESS)

Esta operación permite suspender temporalmente la validez de una tarjeta.
Tipos de tarjetas: todas las tarjetas válidas

Caso de uso: un estudiante residente en un campus accede a su habitación con una tarjeta de usuario, pero aún no ha pagado el alquiler mensual. El director del campus puede suspender esta tarjeta de usuario (es decir, suspender su validez); en el momento en que el estudiante paga el alquiler, su tarjeta puede ser restablecida.

1) En cualquier página, pulse 

.
2) Seleccione la tarjeta válida para suspender.

24		Guest	IAN		201	01/07/2009	14.41	02/07/2009	12.00
26		Staff	LINUS		MASTER	01/07/2009		29/09/2009	
27		Staff	LINUS		MASTER	01/07/2009		03/10/2009	
30		Guest	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Staff	JEFF		MASTER	08/07/2009		01/10/2009	

3) Pulse  y confirme.
4) El ícono de estado de la tarjeta suspendida se vuelve anaranjado:

24		Guest	IAN		201	01/07/2009	14.41	02/07/2009	12.00
26		Staff	LINUS		MASTER	01/07/2009		29/09/2009	
27		Staff	LINUS		MASTER	01/07/2009		03/10/2009	
30		Guest	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Staff	JEFF		MASTER	08/07/2009		01/10/2009	

5) En la vista Eventos codificación (Eventi codifica) se registra el evento Tarjeta suspendida (Carta sospesa); cuando la cerradura recibe el mando, en la vista Eventos cerradura (Eventi serratura) se muestra la línea Nuevo elemento lista de cancelación (Nuovo elemento lista di cancellazione).

RESTABLECIMIENTO (CERRADURAS WIRELESS)

Esta operación permite invertir el mando Suspender en una tarjeta.

1) En cualquier página, pulse 

.
2) Seleccione la tarjeta a restablecer.

24		Guest	IAN		201	01/07/2009	14.41	02/07/2009	12.00
26		Staff	LINUS		MASTER	01/07/2009		29/09/2009	
27		Staff	LINUS		MASTER	01/07/2009		03/10/2009	
30		Guest	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Staff	JEFF		MASTER	08/07/2009		01/10/2009	

3) Pulse  y confirme.
4) El ícono de estado de la tarjeta restablecida se vuelve verde:

24		Guest	IAN		201	01/07/2009	14.41	02/07/2009	12.00
26		Staff	LINUS		MASTER	01/07/2009		29/09/2009	
27		Staff	LINUS		MASTER	01/07/2009		03/10/2009	
30		Guest	MATT		110	07/07/2009	16.44	08/07/2009	12.00
31		Staff	JEFF		MASTER	08/07/2009		01/10/2009	

5) En la vista Eventos codificación (Eventi codifica) se registra un evento Tarjeta restablecida (Carta ripristinata); cuando la cerradura recibe el mando, en la vista Eventos cerradura (Eventi serratura) se muestra la línea Cancelado elemento lista de cancelación (Rimosso elemento lista di cancellazione).

CHECK OUT

Esta operación permite la cancelación de una tarjeta de cliente, incluso si la tarjeta no está físicamente disponible.

Tipos de tarjetas: Cliente.
Caso de uso: cuando un cliente realiza el check-out del hotel.

Después de esta operación, la tarjeta excluida mediante el check-out se inhabilita para acceder a las unidades especiales de control online.

Nota: El check-out provoca la invalidación automática de la tarjeta en las cerraduras normales online wireless; la tarjeta puede ser válida hasta las 23:59 de la fecha de check-out, según la configuración de la instalación.

1) En cualquier página, pulse

2) Seleccione la tarjeta para la cual realizar el check-out en la lista de tarjetas disponibles.

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
39		Cliente	SANDRA		109	21/07/2009	10.40	25/07/2009	10.40
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

3) Pulse 

4) El ícono de estado de la tarjeta para la que se ha realizado el check-out se vuelve rojo:

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
39		Cliente	SANDRA		109	21/07/2009	10.40	25/07/2009	10.40
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

Nota: Cuando una tarjeta de cliente válida se reutiliza para codificar una nueva credencial, la credencial anterior se marca como excluida mediante check-out; en este caso no se envía ningún evento en forma wireless hasta que la tarjeta se elimina físicamente. Este comportamiento es válido solo para las tarjetas de cliente con 1 sola copia.

CANCELACIÓN DE TARJETAS

Esta operación permite cancelar una tarjeta, incluso si la misma no está físicamente disponible. Se crea una tarjeta de cancelación: presentándola a las cerraduras offline, la tarjeta cancelada se incluirá en su lista negra. Las cerraduras online (especiales e wireless), por el contrario, se actualizan automáticamente.

Tipos de tarjetas: cliente, servicio, usuario, operador, emergencia.

Caso de uso: cuando un miembro del personal de servicio es despedido, su tarjeta no debe abrir las cerraduras a las que tenía acceso.

Cuando la tarjeta de cancelación se presenta a las cerraduras offline, se inhabilita el acceso a las cerraduras para la tarjeta cancelada. Para las cerraduras especiales e wireless, es suficiente esperar 10 minutos (tiempo de latencia): la inhabilitación de la tarjeta cancelada es automática.

1) En cualquier página, pulse 

2) Seleccione la tarjeta que se debe cancelar en la lista de tarjetas disponibles.

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
39		Cliente	SANDRA		109	21/07/2009	10.40	25/07/2009	10.40
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

3) Pulse 
4) El ícono de estado de la tarjeta cancelada se vuelve rojo:

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
39		Cliente	SANDRA		109	21/07/2009	10.40	25/07/2009	10.40
29		Servizio	MS.SMITH		MASTER	01/07/2009		19/10/2009	
5		Servizio	MS.ROBERTS		MASTER	01/07/2009		30/08/2009	
6		User	JOHN	POOL		01/07/2009		29/09/2009	
7		User	JILL	FITNES		01/07/2009		20/08/2009	

5) El codificador emite un sonido agudo; apoye una tarjeta en el teclado.
6) La tarjeta de cancelación debe ser leída por todas las cerraduras offline, para incluir la tarjeta cancelada en su lista negra. Por el contrario, no es necesario presentarla a las cerraduras online (especiales e wireless), que se actualizan automáticamente.

Nota: Cuando una tarjeta de servicio/usuario/operador válida se reutiliza para codificar una nueva credencial, la credencial anterior se marca como cancelada; en este caso no se envía ningún evento en forma wireless a la cerradura, hasta que la tarjeta es eliminada.
Nota: Las tarjetas de peligro y de bloqueo no se pueden cancelar.

CONFIGURACIÓN DE LA CONTRASEÑA

Esta operación permite cambiar la contraseña, el usuario Active Directory y las iniciales PMS de una tarjeta de operador; para poder utilizar esta función, el login al Smart Software se debe realizar con una tarjeta de operador de nivel jerárquico suficiente.

Tipos de tarjetas: Operador.

1) En cualquier página, pulse 

2) Seleccione la tarjeta de operador que se debe controlar en la lista de tarjetas disponibles.

No. carta	Stato	Tipo carta	Nome utente	Categ.	Zona	Inizio valid.	Ora	Fine valid.	Ora
1		Operatore			MASTER	01/01/1988		31/12/2051	
2		Servizio	MR.JONES		MASTER	01/07/2009		29/09/2009	
4		Servizio	MS.SMITH		MASTER	01/07/2009		09/10/2009	

3) Pulse 
4) Introduzca la contraseña, el usuario Active Directory y las iniciales PMS deseados; estos dos últimos parámetros deben ser unívocos.
5) Pulse  para aceptar las modificaciones o  para cancelar.

IMPRIMIR

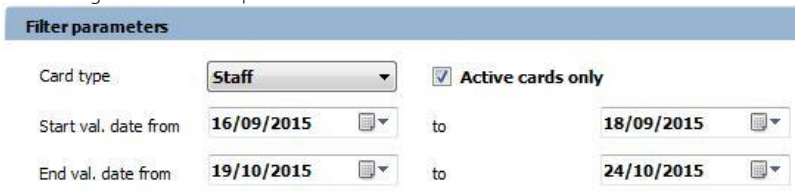
Esta operación permite imprimir la lista de tarjetas o exportarla en diferentes formatos.

1) Pulse 
2) Se abre una nueva ventana que contiene una lista detallada de las tarjetas. Pulse  para imprimir la lista
3) Pulse  para exportar la lista; seleccione la ruta de acceso, el nombre del archivo y el formato entre Adobe (.pdf), Microsoft Excel (.xls), Microsoft Word (.doc), Crystal Reports (.rpt), Rich Text Format (.rtf)

FILTRO AVANZADO

Además del filtro base, está disponible un filtro avanzado. Pulsando , es posible filtrar la lista de tarjetas, seleccionando:

- El tipo de tarjeta (para visualizar solo las tarjetas activas);
- Un conjunto correspondiente a la fecha de inicio validez y/o
- Un conjunto correspondiente a la fecha de fin validez.



CERRADURAS

Esta página muestra la lista de cerraduras incluidas en la instalación restablecida en el Smart Software.
Para acceder:

1) En cualquier página, pulse 

2) Pulse 

3) Se visualiza la lista de cerraduras incluidas en el sistema

Name	Description	Hidden	Battery level	Door Status	Privacy Status	Antenna Signal	Last reading	Office Function
101	Wireless						12/07/2010 6.14	
201	Wireless						12/07/2010 9.02	
301	Wireless						12/07/2010 9.31	
302	Wireless						05/07/2010 10.42	
303	Stand-Alone							
SAUNA	Wireless						08/07/2010 19.08	
UTIL#1	Wireless						12/07/2010 5.06	

Esta página muestra, para cada cerradura, los siguientes datos:

- nombre y descripción;
- tipo de puerta;
- indicador de visibilidad: si el cuadro está seleccionado, la puerta está oculta;
- nivel de batería[3];
- indicador de estado de la puerta: el símbolo indica que la puerta está abierta[4, 5];
- indicador de Privacy: el símbolo indica que la función Privacy está activa[4];
- nivel de señal de la antena, con fecha y hora de última lectura[4];
- indicador de función Oficina: el símbolo indica que esta función está activa[4].

IMPRIMIR LISTA DE CERRADURAS

Pulse y, en la ventana separada que se abre, elija si imprimir la lista de cerraduras o exportarla en uno de los formatos disponibles.

SINCRONIZACIÓN HHI

1. Desconéctese del HHI y conéctese a la red Ethernet;
2. Pulse
3. Seleccione el dispositivo HHI a sincronizar y confirme la operación;
4. Cuando la sincronización ha terminado, el HHI se puede desconectar de la red Ethernet.

---

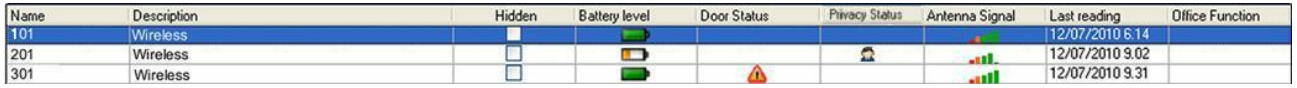
[3] La lectura del nivel de las baterías se realiza a distancia para las cerraduras wireless, y mediante la función History on card para las cerraduras offline.
[4] Datos disponibles solamente para las cerraduras wireless.
[5] La alerta de puerta abierta se activa después de 1 minuto de la apertura de la misma.

MODIFICACIÓN PARÁMETROS DISPOSITIVO Y AUTOPROGRAMACIÓN

Pulsando el botón MODIFICAR (Modifica), es posible controlar los parámetros y las autoprogramaciones, y visualizar la información hardware de los dispositivos (cerraduras y lectores de pared).

1)

1) Seleccione el dispositivo deseado en la lista:





2) Pulse.

3) Modifique los parámetros:

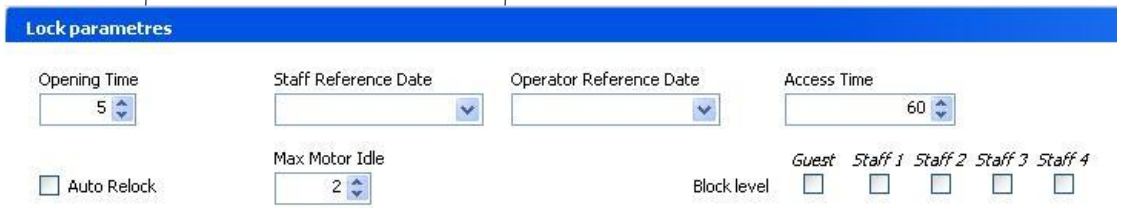
Descripción: se muestra al lado del nombre del dispositivo cuando se crea una nueva tarjeta.

Esconder: si está seleccionado, el dispositivo no es visible cuando se crean nuevas tarjetas.

4) Visualice la información hardware del dispositivo:



5) Controle los parámetros avanzados del dispositivo:



6) Configure en el dispositivo seleccionado hasta 10 autoprogramaciones, eligiendo para cada una el tipo y el período de validez.



Introduzca las autoprogramaciones deseadas, eligiendo el respectivo período de validez, entre:

- Función Oficina (Office On): el dispositivo permanece abierto durante el período seleccionado;
- Bloqueo (Lock Out): los tipos de tarjetas seleccionados son inhabilitados por la apertura del dispositivo.

7) Pulse para confirmar los cambios o para anular.

Esta operación se puede realizar para:

- Cerraduras wireless: la información se transfiere automáticamente desde y hacia la cerradura en forma wireless
- Lector de pared online: la información se transfiere automáticamente desde y hacia el dispositivo vía Ethernet
- Cerraduras y lectores de pared offline: una vez guardada la información deseada, es necesario sincronizar un dispositivo HHI (véase más arriba), Y luego utilizar este HHI para comunicar los parámetros del dispositivo seleccionado (menú Sincronizar Parámetros Cerradura).

APERTURA REMOTA DE UNA CERRADURA

Utilizando esta función, es posible abrir la cerradura a distancia, poniéndola en modo Función Oficina durante 15 minutos. El tiempo que transcurre entre la emisión del mando y su ejecución es de aproximadamente 1 minuto.

1) Pulse
2) Confirme la apertura



3) En la columna Función Oficina (Office On) aparece el símbolo durante los 15 minutos siguientes.

INFORME DE ESTADO DE LAS BATERÍAS

Cada cerradura está caracterizada por el nivel de la batería instalada en ella. Los posibles niveles de carga de la batería visualizados en la pantalla son los siguientes:

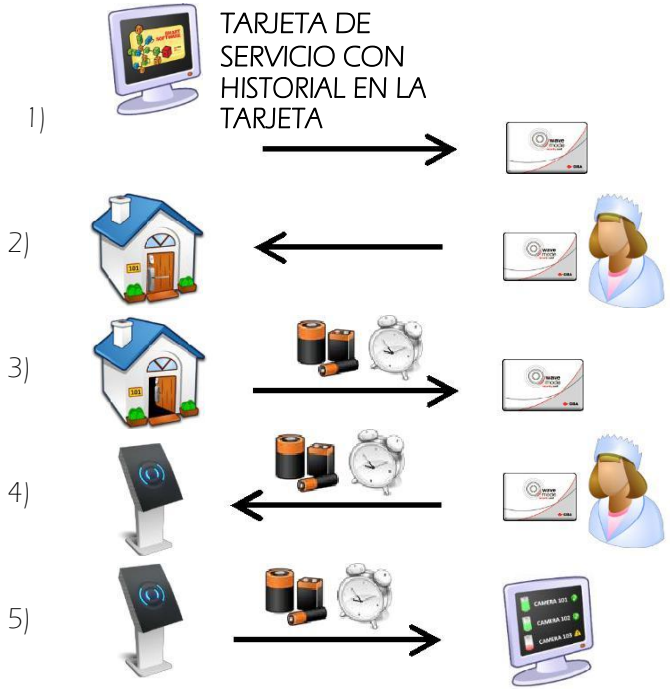
	100%
*	75%
*	50%
	25%
	10% o meno

* Niveles visibles solo en instalaciones con cerraduras eSIGNO o Wave Mode.

La recopilación de esta información se realiza en forma diferente en función del tipo de cerradura.

CERRADURA OFFLINE

El nivel de las baterías es visible mediante el Smart Software, solo si la función History on Card ha sido habilitada durante la configuración de la instalación. El estado de las baterías visualizado en la pantalla no se muestra en tiempo real, sino que corresponde al instante indicado en la columna Última Lectura (Ultima Lettura), es decir, la última vez que la cerradura fue abierta por una tarjeta de servicio, presentada posteriormente a un validador online.



CERRADURA WIRELESS

La lectura del nivel de las baterías está habilitada por defecto. El estado de las baterías se envía automáticamente al Smart Software cada vez que se produce un evento en la cerradura. Por lo tanto, la hora de última lectura visualizada en la pantalla es en tiempo real, salvo un tiempo de latencia de 1 minuto.

ZONAS

Esta página muestra la lista de zonas incluidas en la instalación restablecida en el Smart Software.

Una zona es un grupo de cerraduras, definido durante la configuración de la instalación por un técnico Cisa. Las cerraduras incluidas en una zona no se pueden cambiar mediante el Smart Software. En cada instalación hay una zona que incluye todas las cerraduras, llamada zona máster.

Caso de uso: un miembro del personal debe tener acceso a todas las cerraduras del primer piso de un edificio; es posible crear una zona llamada PISO1 (PIANO1) y proporcionar dicha zona como input para la tarjeta del empleado.

Para acceder:

1) En cualquier página, pulse 

2) Pulse 

MODIFICACIÓN DE PARÁMETROS DE ZONA

1) Seleccione la zona deseada en la lista:

Nome	Descrizione	Nascosto
MASTER		☐
SUITE		☐
PIANO 1		☐
PIANO 2		☐
UTIL		☐

2) Pulse 

3) Descripción: se visualiza al lado del nombre de la zona durante la creación de nuevas tarjetas. Esconder: si está seleccionado, la zona no será visible durante la creación de nuevas tarjetas.



4) Pulse  para aceptar las modificaciones o  para cancelar.

IMPRIMIR LISTA DE ZONAS

Pulse  y, en la ventana separada que se abre, elija si imprimir la lista de zonas o exportarla en uno de los formatos disponibles.

CAMAS

Esta página muestra la lista de camas incluidas en la instalación restablecida en el Smart Software.

La función Camas (Letti) es una configuración especial que permite emitir hasta 7 tarjetas de cliente para la misma habitación, con diferente validez temporal. Cada nueva tarjeta de cliente para una cama invalida la anterior para la misma cama; cada nueva tarjeta de cliente para toda la habitación invalida todas las tarjetas de cliente para cada cama. Esta función está disponible solo si ha sido configurada durante la configuración de la instalación.

Caso de uso: la recepción de un albergue puede emitir tarjetas válidas para una habitación entera o para una sola cama dentro de la habitación.

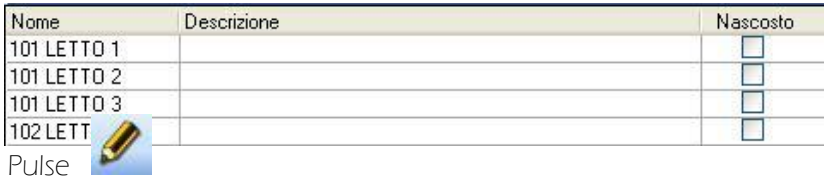
Para acceder:

1) En cualquier página, pulse 

2) Pulse 

MODIFICACIÓN DE PARÁMETROS DE CAMA

1) Seleccione la cama deseada en la lista:



2) Pulse

3) Descripción (Descrizione): se visualiza al lado del nombre de la cama durante la creación de nuevas tarjetas.
Esconder (Nascosto): si está seleccionado, la cama no será visible durante la creación de nuevas tarjetas.

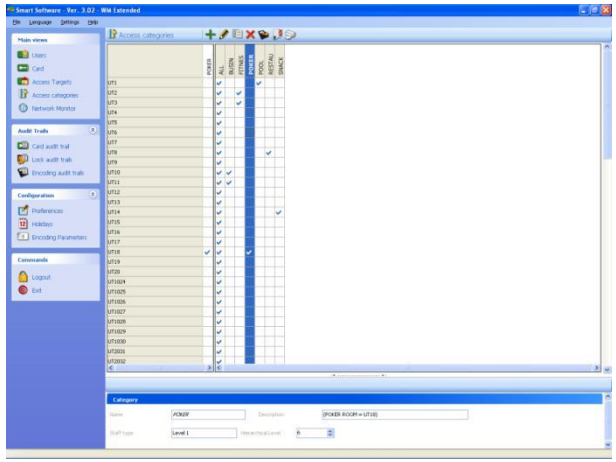


4) Pulse para aceptar las modificaciones o para cancelar.

IMPRIMIR LISTA DE CAMAS

Pulse y, en la ventana separada que se abre, elija si imprimir la lista de camas o exportarla en uno de los formatos disponibles.

SMART SOFTWARE: CATEGORÍAS



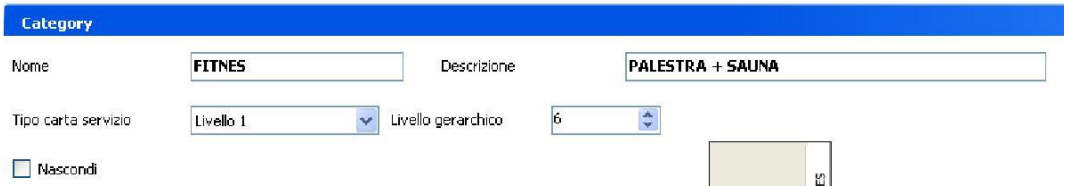
Esta página permite gestionar las categorías incluidas en la instalación restablecida en el Smart Software.

Notas: la columna "Hybrid Lock", cerca de los nombres de las cerraduras indica qué cerradura está configurada como hybrid (las no seleccionadas son simples servicios).

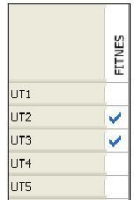
AGREGADO DE CATEGORÍAS

1) En cualquier página, pulse 

2) Pulse 
3) Nombre (Nome): identificativo de la categoría.
   Descripción (Descrizione): se visualiza al lado del nombre durante la creación de nuevas tarjetas. Tipo de tarjeta de servicio creada con acceso a la presente categoría.
   Nivel jerárquico (Livello gerarchico): nivel mínimo de un operador para poder usar esta categoría.
   Esconder (Nascondi): si está seleccionado, la categoría puede ser fácilmente oculta a la vista.



4) Seleccione qué servicios se deben incluir en la categoría:

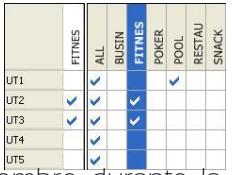


5) Pulse  para aceptar las modificaciones o  para cancelar.

MODIFICACIÓN DE CATEGORÍAS

1) En cualquier página, pulse 

2) Seleccione la categoría que desea modificar:



3) Pulse 
4) Descripción (Descrizione): se visualiza al lado del nombre durante la creación de nuevas tarjetas. Tipo de tarjeta de servicio creada con acceso a la presente categoría.[6]
   Nivel jerárquico (Livello gerarchico): nivel mínimo de un operador para poder usar esta categoría.[6]
   Esconder (Nascondi): si está seleccionado, la categoría puede ser fácilmente oculta a la vista.
5) Seleccione qué servicios se deben incluir en la categoría modificada[6]



6) Pulse  para aceptar las modificaciones o  para cancelar.

[6] Modificación disponible solo si la categoría no ha sido asignada a ninguna tarjeta.

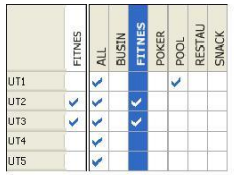
CANCELACIÓN DE CATEGORÍAS

Esta operación permite cancelar las categorías (si es posible). En particular:

- una categoría con tarjetas activas asociadas nunca se puede cancelar;
- una categoría solo con tarjetas no activas asociadas se puede cancelar si el ítem
- Consenti cancellazione di categorie associate a carte non più attive está seleccionado en Preferencias (Preferenze);
- una categoría sin tarjetas asociadas se puede cancelar.

Para cancelar una categoría:

1) En cualquier página, pulse Categorie
2) Seleccione la categoría que desea cancelar:



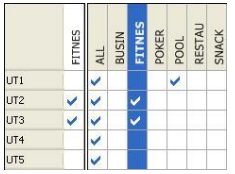
3) Pulse y confirme.
4) Si la categoría no se puede cancelar, aparece el mensaje:



COPIAR CATEGORÍAS

Esta operación permite crear una nueva categoría a partir de una preexistente.

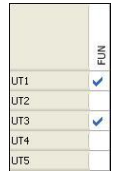
1) En cualquier página, pulse Categorie
2) Seleccione la categoría que desea copiar:



3) Pulse

4) Nombre (Nome): identificativo de la nueva categoría.
   Descripción (Descrizione): se visualiza al lado del nombre durante la creación de nuevas tarjetas. Tipo de tarjeta de servicio creada con acceso a la presente categoría.
   Nivel jerárquico (Livello gerarchico): nivel mínimo de un operador para poder usar esta categoría.
   Esconder (Nascondi): si está seleccionado, la categoría puede ser fácilmente oculta a la vista.

5) Seleccione qué servicios se deben incluir en la nueva categoría:



6) Pulse para aceptar las modificaciones o para cancelar.

MOSTRAR CATEGORÍAS CANCELABLES

Con esta operación es posible visualizar solo las categorías cancelables; una categoría se considera cancelable si no hay tarjetas activas asociadas a ella. Para habilitar esta función:

1) En cualquier página, pulse 

2) Pulse . Para volver a ver todas las categorías, pulse nuevamente 

Una categoría a la que no está asociada ninguna tarjeta (activa o no) es filtrada por el botón  y puede ser efectivamente seleccionada y cancelada (botón  habilitado).
Una categoría a la cual están asociadas solo tarjetas inactivas es filtrada por el botón  y, una vez seleccionada, puede ser efectivamente cancelada (botón  habilitado) solo si el cuadro de control 

en la vista Preferencias (Preferenze) está seleccionado.

OCULTAR/MOSTRAR CATEGORÍAS "OCULTAS"

Con esta operación es posible excluir de la visualización las categorías marcadas como ocultas; una categoría se considera oculta si el cuadro correspondiente ha sido seleccionado en el momento de su creación o modificación.



Para habilitar esta función:

1) En cualquier página, pulse 

2) Pulse . Para volver a ver todas las categorías, pulse nuevamente .

IMPRIMIR LISTA DE CATEGORÍAS

Esta operación permite imprimir la lista de categorías o exportarla en uno de los formatos disponibles:

1) Pulse 
2) En la ventana que se abre, pulse  para imprimir la lista o  para exportarla.

FILTRAR TIPO DE SERVICIO

Con el filtro apropiado, es posible seleccionar si visualizar en la lista de cerraduras:

- Solo las cerraduras Utility (de servicios);
- Solo las cerraduras Hybrid (incluso aquellas en las cuales el cuadro Hybrid Lock cerca del nombre está seleccionado);
- Todos los tipos de cerraduras.

EVENTOS DE LA CERRADURA

Las operaciones realizadas en una cerradura pueden ser numerosas; por ejemplo: inicialización, reset, apertura. Es posible descargar los eventos (guardados en la memoria de la cerradura) de:

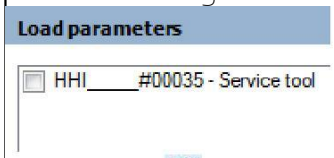
- Cerraduras wireless; estos eventos se visualizan automáticamente en el Smart Software, con un tiempo de latencia de 2-3 minutos;
- Cerraduras offline, con el uso de
  - Un dispositivo (en el cual se descarga el historial), luego visualizado en el Smart Software;
  - Una tarjeta de descarga historial, luego visualizado en el Smart Software;
  - Una tarjeta con el historial en la tarjeta, que debe ser presentada a un controlador online; en este caso, los eventos se transfieren automáticamente al Smart Software

Para visualizar los eventos de una cerradura offline (mediante HHI):

En vista, pulse 

y luego .

1) Aparece una nueva ventana en la parte inferior de la pantalla. Seleccione el dispositivo HHI a descargar:



2) Pulse  para aceptar o  para cancelar.
3) La página visualiza el historial de la cerradura descargado:



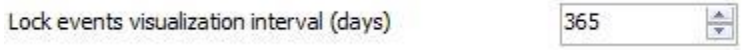
Lock Name	Event Date	Operation	Result	User name	Access Target	Card Number	Valid from	Copy Number
101	06/07/2009 17.18	HHI init	Successful	*** SSWEngine.Ge		1	06/07/2009	
101	06/07/2009 17.18	Staff 4 card	Successful		MASTER	2	06/07/2009	
101	07/07/2009 14.56	Emergency key	Successful					
101	09/07/2009 12.21	Danger card	Successful		MASTER	5	09/07/2009	

Para visualizar los eventos de una cerradura offline (con una tarjeta de descarga historial):

1) Desde cualquier vista, pulse 

.
2) Para crear una tarjeta de descarga historial, pulse  y presente una tarjeta Mifare o CT4 al codificador.
3) Presente la tarjeta de descarga historial al dispositivo offline, que emite 2 destellos verde + rojo y 2 tonos.
4) Vuelva al SSW4; pulse 
5) Presente la tarjeta al codificador.
6) La página visualiza el historial de la cerradura descargado.

Es posible definir los detalles correspondientes a los eventos a visualizar en la pantalla.
Para elegir el intervalo de referencia (en días) de los eventos de la cerradura a visualizar, configure el valor deseado en el campo correspondiente, en la vista Preferencias (Preferenze).



Para seleccionar si visualizar solo los eventos correspondientes al intervalo anterior (eventos actuales) o los eventos correspondientes a toda la vida de la instalación (eventos pasados), pulse  y seleccione la opción deseada.

CARACTERÍSTICAS
Después de descargar el historial de la cerradura, es posible:

 Limpiar la lista de eventos del historial de la cerradura;

 Imprimir o exportar la lista de eventos del historial de la cerradura;

 Buscar en la lista de eventos, usando uno o más criterios;



Filtrar solo los elementos en un cierto intervalo de tiempo

 Visualizar retrasos de recepción de eventos: este instrumento de monitorización habilita la visualización de los retrasos en la recopilación de los eventos. La información enviada por el dispositivo (columna Fecha Evento/DataEvento) pasa primero a través del controlador (columna Retraso CTRL/Ritardo CTRL), luego a través de la aplicación LockBridge (columna Retraso LKBR/Ritardo LKBR) y, por último, es memorizada en la base de datos de sistema.
Si el retraso es superior al valor configurado en la vista Preferencias (Preferenze), se enciende una alarma en la vista Zonas de acceso (Zone accesso).

EVENTOS DE CODIFICACIÓN
Todas las operaciones realizadas por un codificador son memorizadas en el SSW.

FUNCIONES
Una vez que el historial del codificador ha sido cargado, es posible:

 Mostrar detalles tarjeta: visualiza los datos de la tarjeta en la que se ha realizado la operación;

 Mostrar detalles tarjeta op.: visualiza los datos de la tarjeta de operador utilizada para acceder;

 Limpiar la pantalla, cancelando la lista de eventos de historial del codificador;

 Eliminar evento de codificación: se elimina el evento de codificación seleccionado;

 Imprimir o exportar la lista de eventos de historial;

 Buscar en la lista de eventos, usando uno o más criterios;

Filtrar y visualizar solo los elementos pertenecientes a un cierto intervalo temporal.



SMART SOFTWARE: PREFERENCIAS

Esta página permite modificar diferentes configuraciones, para habilitar diferentes funciones del Smart Software.

Para acceder y modificar los datos:

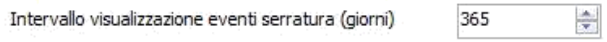
1) En cualquier página, pulse 

2) Pulse 
3) Modifique los campos deseados.
4) Pulse  para aceptar o  para cancelar.

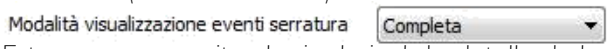
GENERAL



Si esta opción está seleccionada, es posible cancelar categorías solo con tarjetas inactivas asociadas.

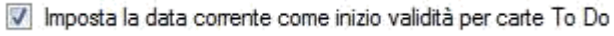


Este campo permite elegir el intervalo de referencia (en días) de los eventos a visualizar en la vista Eventos cerradura (Eventi serratura).

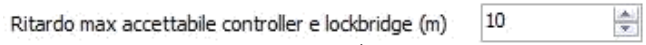


Este campo permite elegir el nivel de detalle de los eventos visualizados en la vista Eventos cerradura (Eventi serratura). A continuación, elija los niveles de detalle y los correspondientes tipos de eventos visualizados.

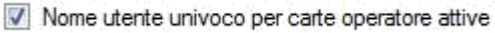
- Mínima: se visualizan solo los eventos correspondientes a las pestañas presentes en la vista Zonas de acceso/Zone accesso (puerta abierta/cerrada, estado privacy, función oficina, advertencia de nivel de baterías).
- Media: se visualizan también los eventos con resultado negativo (por ejemplo, credencial inválida).
- Completa: se visualizan todos los eventos.



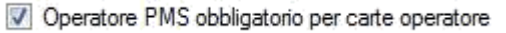
Si está seleccionado este cuadro, la fecha de inicio de validez para las tarjetas To Do se configura automáticamente a la fecha actual.



Si el retraso en la comunicación de los eventos por una cerradura es superior a este parámetro, aparece un mensaje de alarma en la columna "Retraso evento" (Ritardo evento) en la vista Zonas de acceso (Zone accesso).

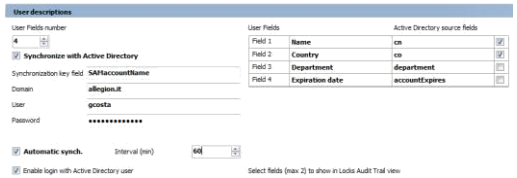


Si está seleccionado este cuadro, es obligatorio configurar un nombre unívoco para tarjetas de operador activas.



Si está seleccionado este cuadro, es obligatorio configurar de las iniciales PMS para tarjetas de operador.

DESCRIPCIÓN USUARIOS



Esta sección permite habilitar la gestión de usuarios, configurando el número de campos de usuario deseados y rellenando la descripción de los mismos en la tabla que se encuentra a la derecha.

Además, es posible seleccionar hasta 2 campos de usuario para mostrar en la vista Eventos cerradura (Eventi serratura) (y, en consecuencia, en el informe correspondiente).

Es posible sincronizar el Smart Software con el servicio de Windows Active Directory en el dominio deseado; para iniciar la sincronización, seleccione el cuadro correspondiente y rellene los campos subyacentes:

- campo clave de sincronización: sAMAccountName (recomendado, por defecto);
- dominio: para introducir en formato LDAP://nombre_dominio.com
- nombre de usuario y contraseña para acceder al servicio de Active Directory en el dominio seleccionado.

A partir de este momento es posible asociar a los diferentes campos de usuario del Smart Software, definidos previamente, los campos de origen de los cuales tomar los datos mediante Active Directory. En el ejemplo indicado en la figura, los datos contenidos en el campo givenName de Active Directory se indicarán en el campo Nombre de cada usuario del Smart Software, y así sucesivamente.

Una vez confirmada la introducción de los parámetros, se realizará la primera sincronización entre Active Directory y Smart Software; el procedimiento puede requerir varios minutos. En este punto, será posible:

- realizar manualmente nuevas sincronizaciones, pulsando el botón  que aparece en la vista Usuarios (Utenti) al activar la sincronización;
- configurar la sincronización automática, con el correspondiente intervalo de repetición, seleccionando el cuadro correspondiente.

Si está seleccionado el cuadro Habilitar login (Abilita login) con usuario Active Directory, durante la creación de la tarjeta de operador se visualiza este campo adicional. Si se introduce el nombre de usuario Active Directory en este campo, el operador correspondiente puede realizar el login:

- presentando la tarjeta de operador al encoder e introduciendo luego la contraseña de la tarjeta;
- introduciendo el nombre de usuario y la contraseña correspondientes a la Active Directory.

CONFIGURACIONES APP PROVIDER

Para configurar solo en los sistemas eKEY; para más información, consulte la sección eKEY de este documento.

CONFIGURACIONES PMS

Esta sección permite la conexión del servicio PMS de Cisa a cualquier software PMS conectado; estos parámetros deben ser configurados dentro de la instancia SSW4 instalada en el servidor de sistema.



Elija el tipo de conexión entre el servidor Cisa y la máquina en la que está instalado el PMS:

- Serial: esta configuración se utiliza para trabajar con el protocolo PMS CISA con una comunicación serial (legacy). En este caso, seleccione el puerto COM para la conexión.

- TCP/IP (CISA): esta configuración se utiliza para trabajar con el protocolo PMS CISA. Seleccione el puerto TCP/IP #1 para la comunicación con el software PMS de terceras partes deseado e introduzca la etiqueta correspondiente, que identifica el origen de la comunicación (por ejemplo, "PMS" o el nombre efectivo del software PMS); el contenido de la etiqueta será incluido en los informes de tarjetas e historial.

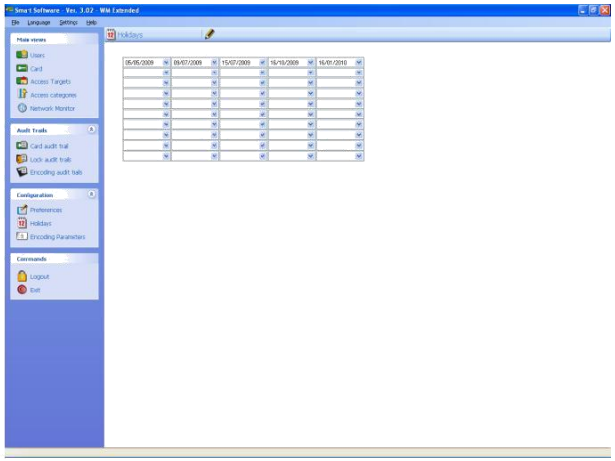
  Seleccione el puerto TCP/IP #2 para la comunicación con el dashboard (este valor debe ser coherente con el configurado en el campo PMSSERVICE_TCP_PORT de la Admin Console) e introduzca la etiqueta correspondiente, que identifica el origen de la comunicación (por ejemplo "DASH"); el contenido de la etiqueta será incluido en los informes de tarjetas e historial.

  El puerto RPC (para el encoder Cisa) se debe dejar al valor preestablecido 3001.

- TCP/IP (FIAS): esta configuración se utiliza para trabajar con el protocolo PMS FIAS. Seleccione la dirección IP y el puerto del software PMS basado en FIAS al conectarse.

  Seleccione el puerto TCP/IP #2 para la comunicación con el dashboard (este valor debe ser coherente con el configurado en el campo PMSSERVICE_TCP_PORT de la Admin Console)
  Configure los valores deseados para el mando "keep alive" (campo "Actualizar conexión cada"/"Aggiorna connessione ogni", enviado cada N minutos para actualizar la comunicación entre Cisa y PMS) y para la llave de autenticación (que puede ser creada casualmente por SSW4).
  El puerto RPC (para el encoder Cisa) se debe dejar al valor preestablecido 3001.

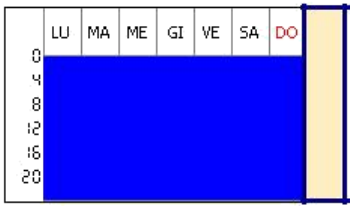
SMART SOFTWARE: DÍAS FESTIVOS



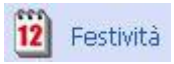
Esta página permite configurar los días del año considerados como festivos; estos se consideran un grupo diferente de días, para los que se pueden configurar turnos especiales durante la creación de nuevas tarjetas de servicio, usuario u operador.

Turni orari

Ora inizio 1	Ora fine 1	Ora inizio 2	Ora fine 2	LU	MA	ME	GI	VE	SA	DO
00:00	23:45	00:00	00:00	☑	☑	☑	☑	☑	☑	☑
00:00	00:00	00:00	00:00	☐	☐	☐	☐	☐	☐	☐
00:00	00:00	00:00	00:00	☐	☐	☐	☐	☐	☐	☐
00:00	00:00	00:00	00:00	☐	☐	☐	☐	☐	☐	☐



Para configurar los días festivos:

1) En cualquier página, pulse 

2) Pulse 

3) Pulse en un cuadro desplegable y seleccione una fecha en el calendario que se abre:



4) Pulse  para aceptar o  para cancelar.

SMART SOFTWARE: PARÁMETROS DE CODIFICACIÓN

Esta página permite cambiar diferentes parámetros utilizados por el sistema de codificación. Para acceder y cambiar los parámetros:

1) Pulse 

2) Pulse 
3) Un aviso solicita configurar el codificador Backup Server en modo Mantenimiento.
4) Apague y reencienda el codificador Backup Server.
5) Pulse OK en el mensaje del SSW: el codificador Backup Server entra automáticamente en modo Mantenimiento.
6) Modifique los parámetros deseados.
7) Pulse  para aceptar o  para cancelar.
8) El codificador Backup Server sale automáticamente del modo Mantenimiento.
9) Repita los siguientes pasos en todos los codificadores client del sistema:
   a) Cierre el SSW conectado al codificador client.
   b) Verifique que el display del codificador muestre READ OP. CARD.
   c) Presente una tarjeta de operador válida al codificador client.
   d) Cuando se solicite, introduzca la contraseña de operador en el teclado del codificador y pulse Enter.
   e) Verifique que el display del codificador visualice UNAUTHORIZED – PRESS ANY KEY.
   f) Pulse Enter y verifique que el codificador visualice READ OP.CARD.

PARÁMETROS PRINCIPALES



Para configurar la validez por defecto de las tarjetas de cliente.



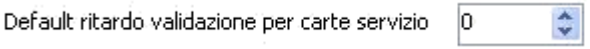
Para configurar el número de copias por defecto de cada tarjeta de cliente.



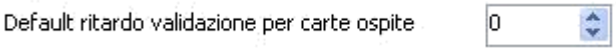
Para configurar la hora de check-out por defecto para las tarjetas de cliente.



Retraso añadido a la hora de check-out enviado por el PMS para obtener la hora efectiva.



Una tarjeta de servicio con validación habilitada debe ser validada antes del vencimiento de este intervalo.



Una tarjeta de cliente con validación habilitada debe ser validada antes del vencimiento de este intervalo.



Para configurar el número de créditos asignados por defecto a cada tarjeta de cliente.

CATEGORÍA POR DEFECTO

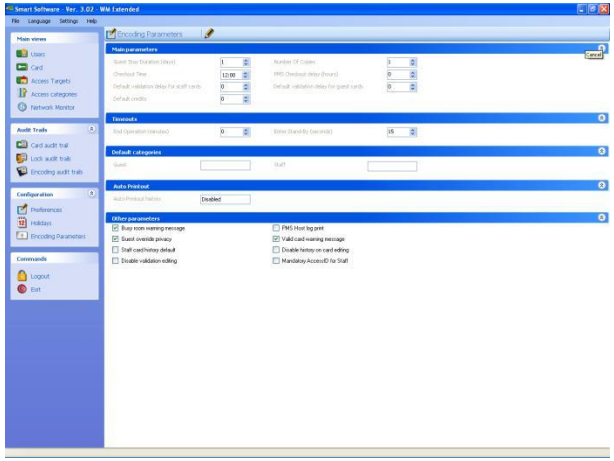


Esta es la categoría por defecto para las tarjetas de cliente.



Esta es la categoría por defecto para las tarjetas de servicio.

SMART SOFTWARE: PARÁMETROS DE CODIFICACIÓN



SMART SOFTWARE: LISTA CLIENT

OTROS PARÁMETROS

☑ Messaggio di avviso di stanza occupata

Durante la creación de una tarjeta de cliente, si la habitación está ocupada, aparece un mensaje de aviso.

☐ PMS Host stampa log

Para habilitar la creación de un archivo de log para la comunicación entre el codificador y el PMS.

☑ Default supera privacy

Para emitir tarjetas de cliente con la función Superar Privacy (Supera Privacy) activa.

☑ Messagio di carta valida

Durante la grabación de una credencial en una tarjeta válida, aparece un mensaje de aviso.

☐ Default storico su carta di servizio

Para emitir tarjetas de servicio con el historial en la tarjeta activo por defecto.

☐ Disabilita modifica parametro storico su carta

Durante la emisión de una nueva tarjeta, el operador no puede modificar el estado del historial en la tarjeta.

☐ Disabilita modifica parametro validazione

Durante la emisión de una nueva tarjeta, el operador no puede modificar el estado de validación.

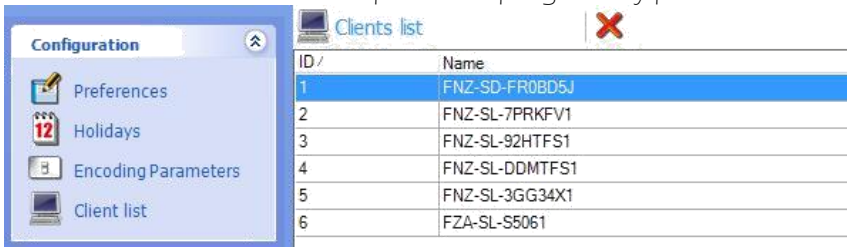
☐ Nome utente (AccessID) obbligatorio per carte servizio

Durante la creación de un nuevo usuario, es obligatorio rellenar todos los campos disponibles.

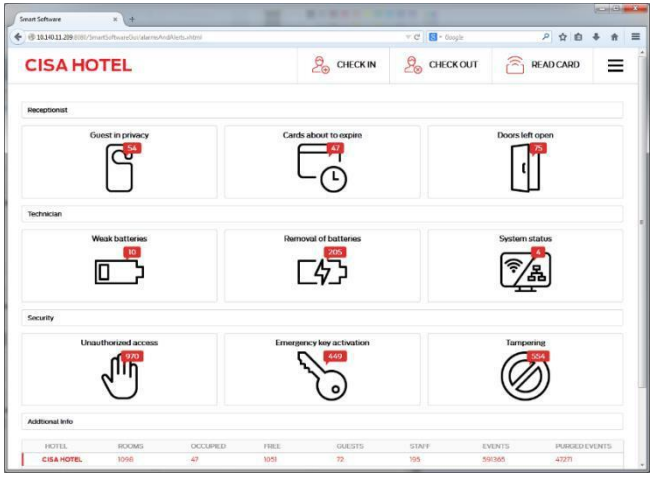
☐ Abilita messaggio di conferma su cancellazione e checkout carta

Cuando una tarjeta se cancela o se realiza el check-out, aparece un mensaje de confirmación.

La pantalla muestra la lista de ordenadores client conectados a la base de datos servidor para el sistema actual. Cada client está caracterizado por un ID progresivo y por el nombre del ordenador.



DASHBOARD



Navegadores compatibles para dashboard y Admin App:

- Internet Explorer 11
- Mozilla Firefox 46 o posterior
- Google Chrome 50 o posterior

El dashboard es un componente web que extiende las funciones del Smart Software. Se puede visualizar desde cualquier ordenador Client dentro del sistema y contiene un cierto número de widgets que muestran diferentes indicaciones provenientes del sistema, para dar al usuario una rápida panorámica del estado del sistema.

Los widgets están agrupados por tipo de indicación:

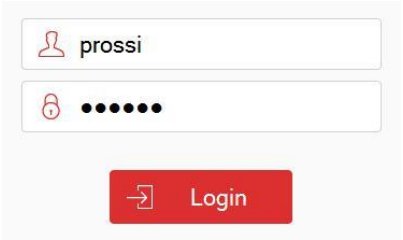
- Recepción
  - Cliente en estado Privacy
  - Tarjetas que expiran
  - Puertas dejadas abiertas
- Técnico
  - Baterías descargadas
  - Extracción baterías
  - Estado del sistema
- Seguridad
  - Acceso no autorizado
  - Uso llave de emergencia
  - Sabotaje
- Información adicional
  - Puertas en modo Peligro
  - Puertas en modo Bloqueo
  - Puertas en función Oficina
- Administración del sistema
  - Llaves ULC cerraduras
  - Llaves ULC codificadores

El dashboard contiene también una síntesis de los datos del hotel actual, así como de diferentes hoteles (campus). Los componentes visualizados dependen del nivel jerárquico del usuario.

CONEXIÓN Y LOGIN

Para acceder al dashboard, abra un explorador cualquiera e introduzca la dirección con el siguiente formato: http://server_PC's_IP_address:8080/SmartSoftwareGui

La página de acceso es la siguiente:



Introduzca:

- Nombre de usuario y contraseña correspondientes a la tarjeta de operador, o
- El nombre Active Directory y la contraseña asociados a una tarjeta de operador

A continuación, pulse el botón *LOGIN*

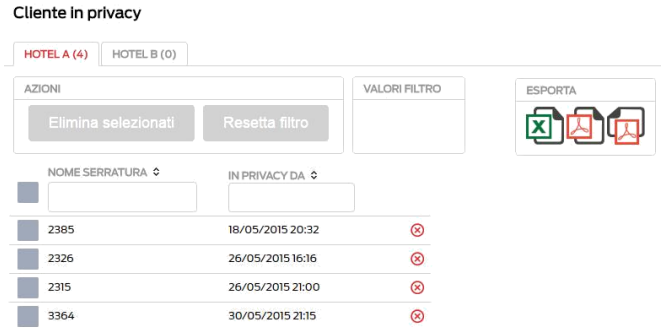
WIDGETS Y DETALLES



Cuando ninguna indicación está activa, el widget correspondiente no está evidenciado (gris).

Cuando una indicación está activa, el widget correspondiente está evidenciado con un dibujo negro y un cartel rojo que contiene el número de anotaciones.

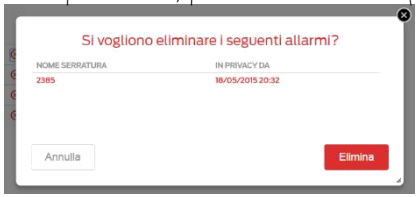
Para ver los detalles de las indicaciones, pulse el widget: se abre una página en la que se muestran todas las indicaciones activas actuales:



Desde esta vista es posible realizar diferentes actividades en los datos visualizados; estas son comunes a todos los widgets.

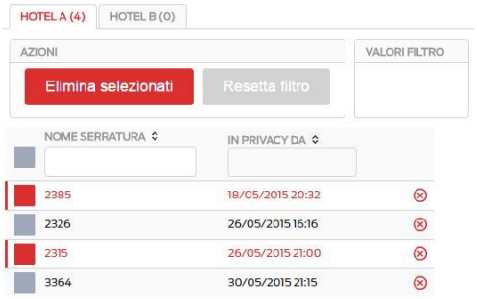
CANCELACIÓN DE REGISTRO

Para cancelar un solo registro, pulse ; aparece un mensaje de aviso que pregunta si desea continuar. Para proceder, pulse CANCELAR (Elimina).



Una vez terminada, esta operación se incluye en el Historial Codificación en forma de registro en formato "Campus Canc. (nombre widget)".

Para cancelar más de un registro, pulse el cuadro rojo al lado de los registros que se deben cancelar y, a continuación, el botón ELIMINAR SELECCIONADOS (Elimina selezionati); aparece un mensaje de aviso que pide confirmación. Para proceder, pulse CANCELAR (Cancella). Para seleccionar todos los registros de la lista, pulse el cuadro al lado de los encabezamientos de columna.



Una vez terminada, esta operación se incluye en el Historial Codificación en forma de registro en formato "Campus Canc. (nombre widget)".

RECONOCIMIENTO REGISTRO

Esta función está disponible para todos los widgets excepto "Llaves ULC cerradura" (Chiavi ULC serratura) y "Llaves ULC encoder" (Chiavi ULC encoder).

Dentro de cada widget es posible seleccionar uno o más registros (pulsando el cuadro al lado de los encabezamientos de columna) y marcarlos como leídos, pulsando el botón MARCAR COMO LEÍDOS (Segna come letti). Los registros marcados como leídos no se cancelan de la lista, sino que solo se marcan como leídos (Ack):



Una vez terminada, esta operación se incluye en el Historial Codificación en forma de registro en formato "Campus Ack (nombre widget)".

A continuación, es posible marcar los registros nuevamente como no leídos, en caso de error, pulsando el botón MARCAR COMO NO LEÍDOS (Segna come non letti); esto elimina la pestaña aplicada previamente y vuelve al Historial Codificación en forma de registro en formato "Campus UnAck (nombre widget)".

El comportamiento de los registros dentro de los widgets no depende de cada operador: cuando una alarma es marcada como leída por un operador, se indica como leída a todos los otros operadores que acceden al widget en un segundo momento. En el contador externo de widgets, los registros marcados como leídos se cuentan igualmente (al contrario que los registros cancelados, que ya no se totalizan en el contador externo).

Caso de uso:

- Operador A realiza el login al dashboard y verifica que el contador externo del widget "Controlar cerradura" (Controlla serratura) muestra 10 alarmas.
- Operador A accede al widget "Controlar cerradura" (Controlla serratura) y controla la lista de alarmas activas (10 registros, como se visualiza en el contador externo).
- Operador A controla físicamente 3 de las cerraduras indicadas como no operativas.
- Operador A vuelve al dashboard y marca los 3 registros que ha controlado como leídos (los 3 registros no se cancelan).
- Operador B, en un segundo momento, realiza el login al dashboard y aún ve 10 alarmas en el contador externo del widget "Controlar Cerradura" (Controlla serratura).
- Operador B accede al widget "Controlar Cerradura" (Controlla serratura) y controla la lista de alarmas activas: 3 se muestran como leídas, 7 como no leídas.
- Operador B comprende que debe controlar las 7 alarmas restantes y que el otro operador ya ha controlado 3.

FILTRACIÓN Y EXPORTACIÓN DE DATOS

Para filtrar la lista de registros, introduzca los datos deseados en el filtro o seleccione los valores deseados en los menús desplegables; solo se visualizarán los registros correspondientes. Es posible aplicar criterios de filtración múltiples al mismo tiempo; estos se muestran en el cuadro "Valores Filtro" (Valori Filtro).



Para resetear el filtro y volver a la lista completa, pulse el botón RESETEAR FILTRO (Resetta filtro).

Para exportar los datos, pulse el ícono correspondiente a uno de los tres formatos posibles:

- Archivo Excel en formato vertical
- Archivo PDF en formato vertical
- Archivo PDF en formato horizontal



Si se exporta una lista de datos filtrados, los criterios de filtración se visualizan dentro del archivo exportado.

Para ordenar los registros según un parámetro, pulse las flechas cerca de los encabezamientos de las columnas; para invertir el orden, pulse nuevamente las flechas.

Si la función Campus está activa (se cargan datos de más de un hotel en un solo dashboard), es posible pasar de los datos referidos a un hotel a los referidos al otro, pulsando la tabla correspondiente debajo del nombre del widget.



El widget "Acceso no autorizado" (Accesso non autorizzato) tiene un instrumento de filtración adicional que permite visualizar solo el último evento que ha provocado la activación de la alarma (Últimos/Ultimi) o todos los eventos que han contribuido a la activación de la alarma (Todos/Tutti).



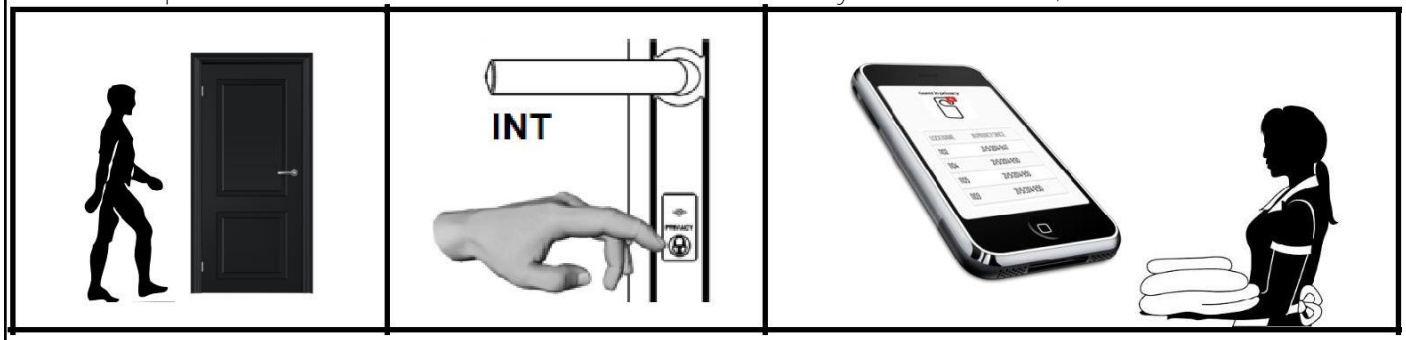
Los widgets "Llaves ULC cerraduras" (Chiavi ULC serrature) y "Llaves ULC codificadores" (Chiavi ULC codificatori) contienen también un recuadro que muestra información adicional relativa a la distribución de las llaves ULC: el número de cerraduras/codificadores que aún se deben actualizar y el formato de las llaves ULC.



WIDGET: RECEPCIÓN

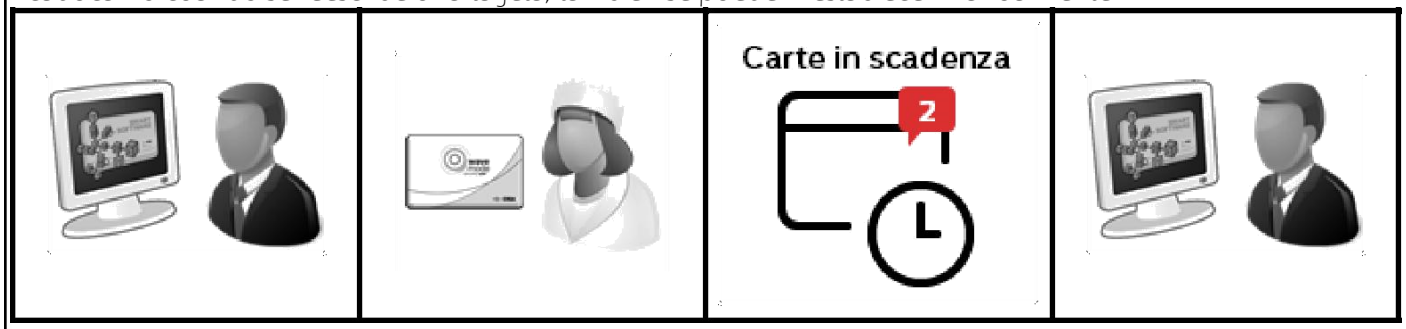


Este widget muestra el número de habitaciones en las cuales el estado Privacy está activo. Cuando se pulsa el widget, se muestra la lista de cerraduras de las habitaciones de los huéspedes que están en estado Privacy, ordenadas por el nombre de la cerradura. Cuando el estado Privacy está inhabilitado, la anotación se cancela.



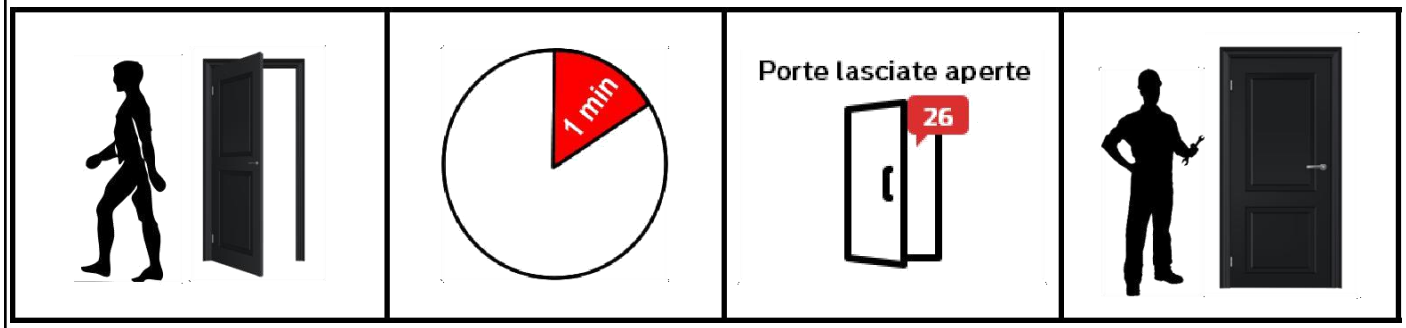


Este widget muestra el número de tarjetas de un tipo específico (Cliente, Servicio de 1 a 4, Operador) que caducarán en "H" horas. Cuando se pulsa el widget, se muestra la lista de tarjetas que tienen esta característica. Las anotaciones relativas a las tarjetas que están por caducar se cancelan automáticamente cuando las tarjetas caducan o cuando se reescribe una tarjeta; también se pueden restablecer manualmente.



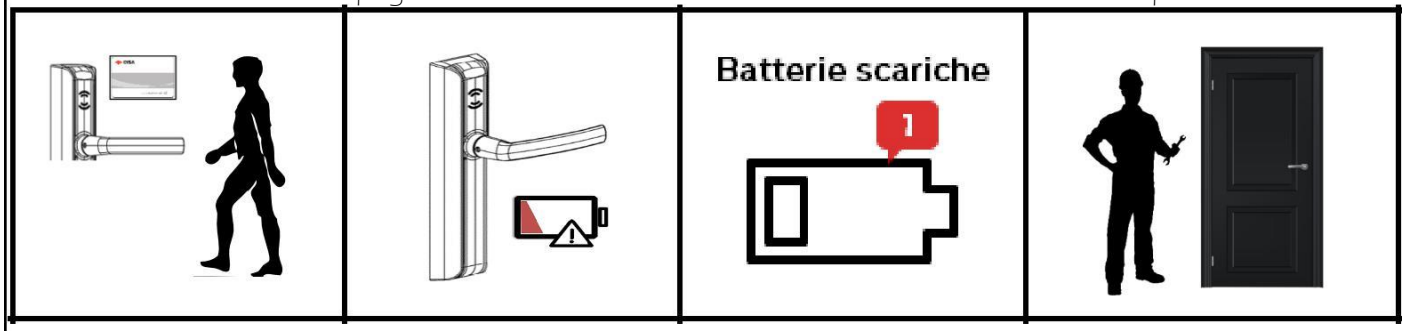


Este widget muestra el número de puertas dejadas abiertas por un tiempo superior al de acceso (generalmente, 1 minuto). Cuando se cierra la puerta, la anotación se cancela. Para poder activar esta alarma, las cerraduras deben tener un hardware de Informe Posición Puerta.



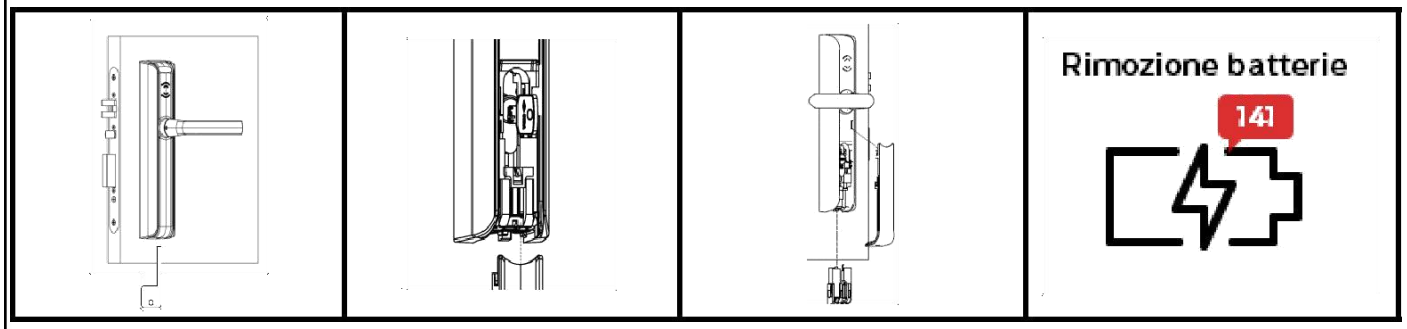


Esta alarma es activada por el bajo nivel de las baterías de la cerradura (menos del 25 % con respecto a las baterías cargadas). Para cada cerradura, se muestra solo el último evento correspondiente a las baterías, junto con la fecha/hora; si se produce un nuevo evento, se actualizan solo fecha/hora, sin añadir una nueva anotación. Esta alarma se apaga automáticamente cuando se detecta un nivel de baterías superior al 25 %.





Esta anotación se activa después de la extracción de las baterías. Esta vista muestra varias alarmas en la misma cerradura, en caso de varias acciones. En esta vista los eventos se deben cancelar manualmente.





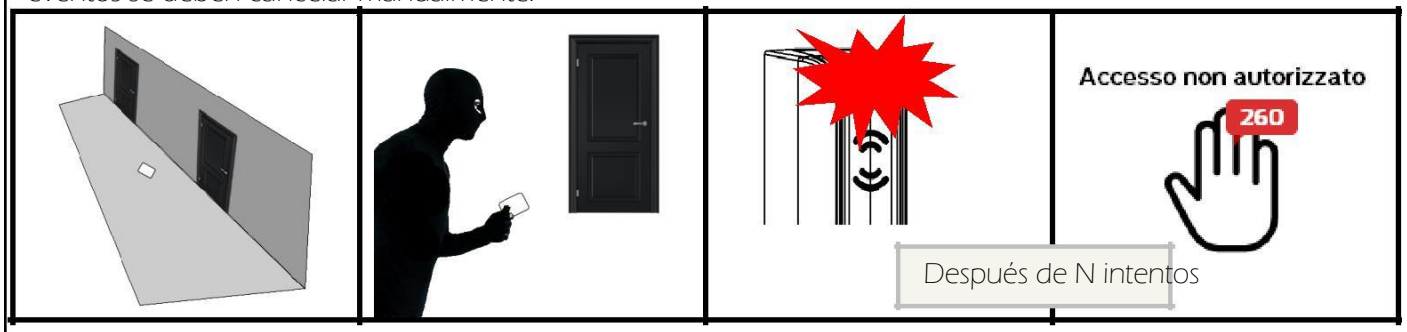
Este widget muestra las anotaciones relativas al estado de los componentes del sistema inalámbrico y de los controladores online. Esto incluye las alarmas de los componentes conectados (controladores, gateways, repetidores, lectores de pared online) que quedan offline. Las anotaciones se cancelan automáticamente cuando los componentes vuelven a estar online.



WIDGETS: SEGURIDAD

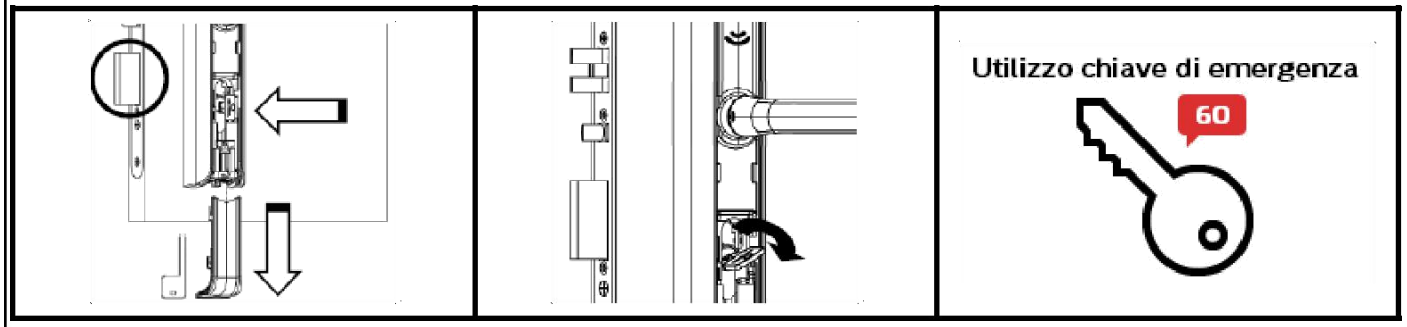


Este widget se activa cuando una tarjeta se utiliza "N" veces en puertas no autorizadas en un tiempo configurable "T" (los intentos después de un intervalo de tiempo superior no se consideran). Cuando se pulsa el widget, se muestra la lista de todas las puertas interesadas, junto con la fecha/hora del intento. En esta vista los eventos se deben cancelar manualmente.



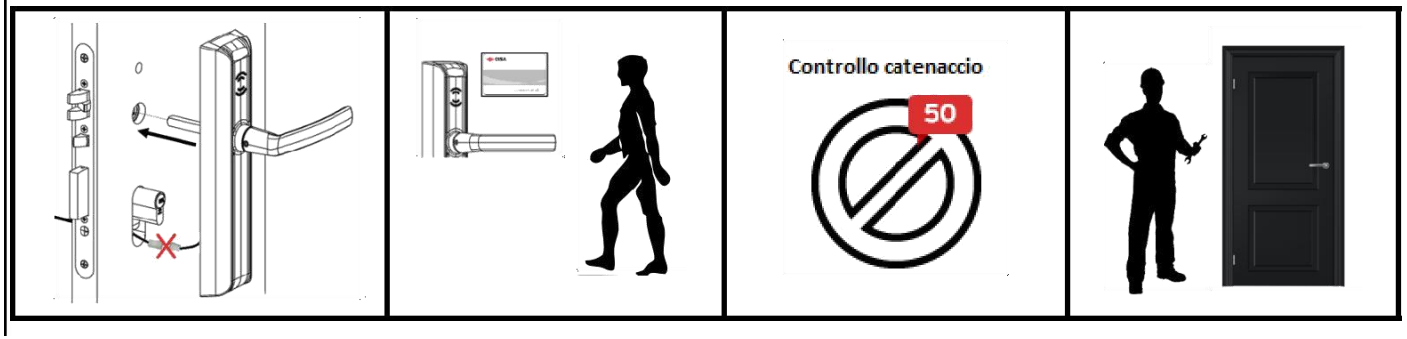


Esta alarma se activa cuando se abre una cerradura con una llave mecánica. Esta vista muestra alarmas múltiples en la misma cerradura, en caso de acciones múltiples.
En esta vista los eventos se deben cancelar manualmente.





Esta alarma se genera cuando el movimiento de la palanca de la cerradura mecánica no es captado correctamente. Esto puede ser causado por el hecho de que la palanca no pueda moverse libremente (a causa de una instalación incorrecta o de la puerta no alineada) o por un cable averiado en la mecánica. Esta vista muestra alarmas múltiples referidas a la misma cerradura, en caso de acciones múltiples. En esta vista los eventos se deben cancelar manualmente.

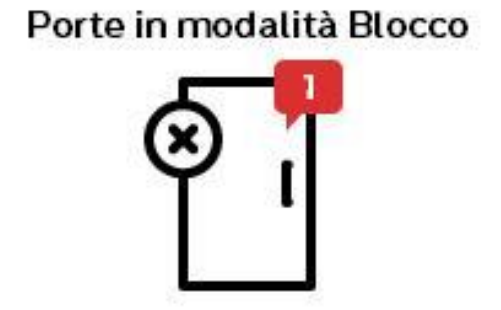


WIDGETS: INFORMACIÓN ADICIONAL

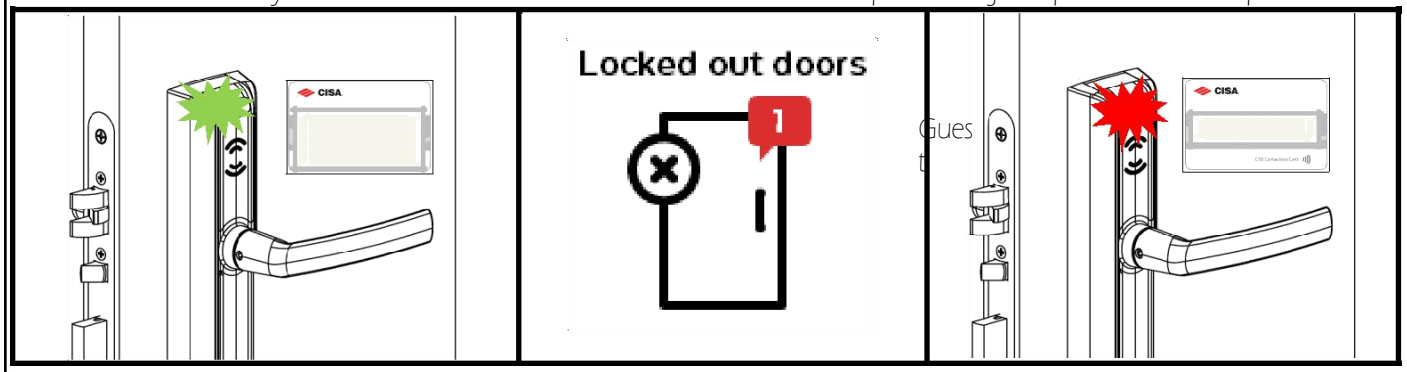


Este widget muestra el número de puertas que están en estado Peligro. Cuando una cerradura entra en estado Peligro, aumenta un contador y se agrega un evento en la vista. Cuando se utiliza una tarjeta de fin peligro, el contador se reduce y el evento se elimina.



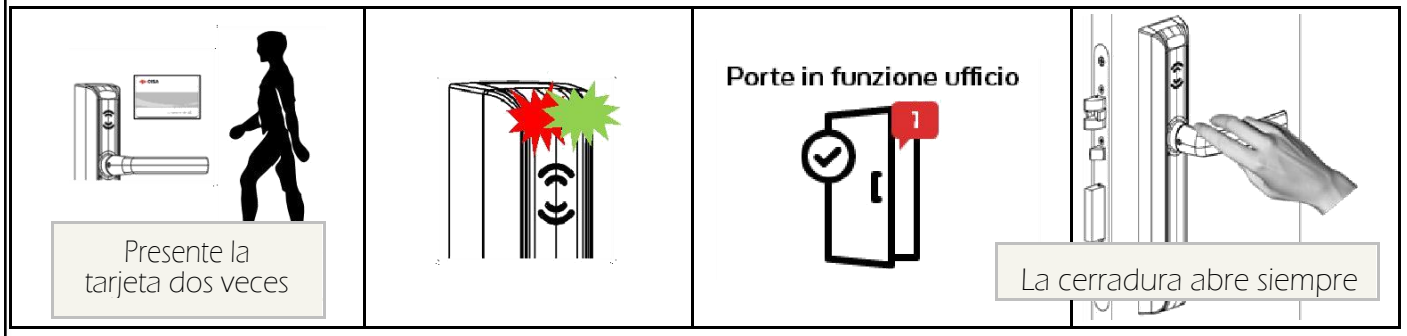


Este widget muestra el número de puertas en las cuales se ha bloqueado al menos una tarjeta. Cuando una puerta entra en estado de Bloqueo (Blocco), el contador aumenta y en la vista se agrega un evento. El contador se reduce y los eventos se cancelan solo cuando todos los tipos de tarjetas pueden abrir la puerta.





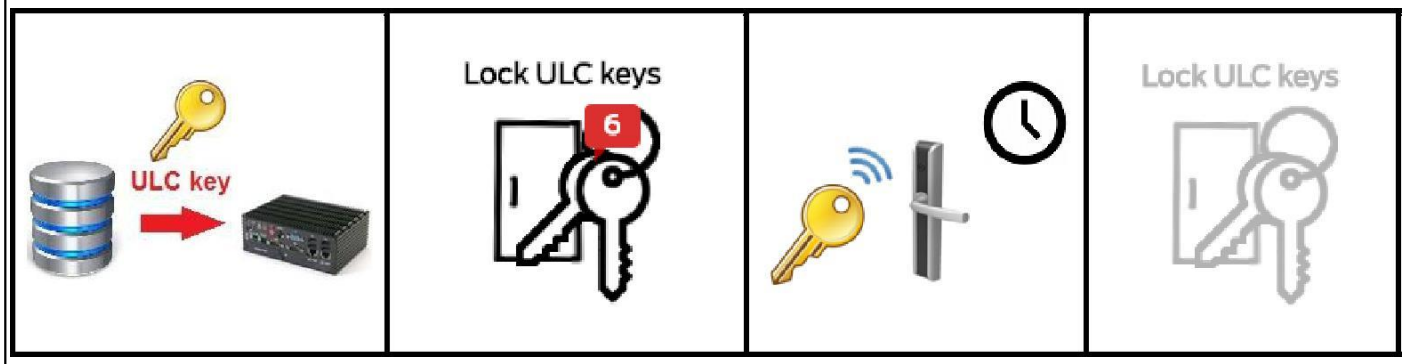
Este widget muestra el número de puertas en modo Oficina (Ufficio). Los eventos se cancelan automáticamente cuando la cerradura ya no está en modo Oficina (Ufficio).



WIDGET: ADMINISTRACIÓN SISTEMA

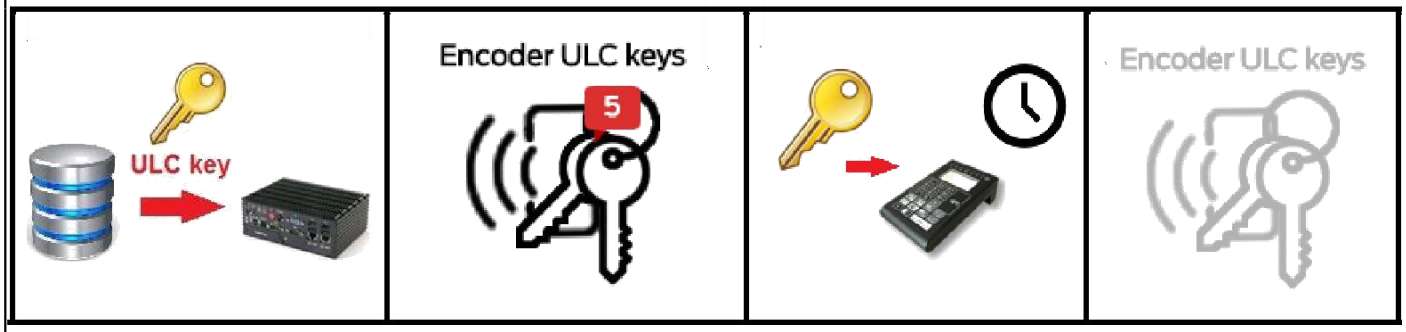


Este widget muestra el número de puertas en las que la nueva llave ULC enviada aún se debe actualizar.
La actualización se realiza en forma wireless para las cerraduras online, vía Ethernet para los lectores de pared online, vía HHI para las cerraduras offline.
Nota: Este widget considera solo las puertas marcadas como "activa".





Este widget muestra el número de codificadores en los que la nueva llave ULC enviada aún se debe actualizar.
La actualización se realiza vía Ethernet para todos los codificadores.



DASHBOARD VS. SMART SOFTWARE

El dashboard ofrece una panorámica rápida del campus, dado que muestra alarmas provenientes de sistemas diferentes conectados entre sí. Gran parte de la información se puede recopilar también mediante el Smart Software, pero exclusivamente para el sistema al que está conectado (y en forma menos inmediata).

Widget	Vista Smart Software	Dónde leer la información
Cliente en estado Privacy	Zonas de acceso	Para cada cerradura, controle el ícono XXX en la columna "Estado Privacy" (Stato Privacy)
Tarjetas que expiran	Tarjetas	Abra el filtro e introduzca la fecha deseada (por ejemplo, mañana) en la columna "Fin Validez" (Fine Validità)
Puertas dejadas abiertas	Zonas de acceso	Para cada cerradura, controle el ícono XXX en la columna "Estado Puerta" (Stato Porta)
Baterías descargadas	Zonas de acceso	Para cada cerradura, controle la columna "Nivel Batería" (Livello Batteria), con posibilidad de filtración
Extracción baterías	Historial cerradura	Abra el filtro y seleccione el evento "Extracción baterías" (Rimozione batterie)
Estado del sistema	Historial cerradura	Abra el filtro y seleccione el evento "Dispositivo Offline", donde el dispositivo puede ser controlador, gateway, repetidor, lector de pared o cerradura
Acceso no autorizado	Historial cerradura	Controle los eventos evidenciados en amarillo, pero no es posible verificar rápidamente si una tarjeta está intentando el acceso en múltiples puertas
Uso llave emergencia	Historial cerradura	Abra el filtro y seleccione el evento "Llave de emergencia" (Chiave emergenza)
Control palanca	Historial cerradura	Abra el filtro y seleccione el evento "Control palanca" (Controllo catenaccio)
Puertas en modo Peligro	Historial cerradura	Abra el filtro y seleccione el evento "Tarjeta de Peligro" (Carta Pericolo); la puerta está en modo peligro solo si no está presente también un evento "Tarjeta de fin peligro" (Carta Fine Pericolo)
Puertas en modo Bloqueo	Historial cerradura	Abra el filtro y seleccione el evento "Tarjeta de bloqueo" (Carta Blocco); la puerta está en modo peligro solo si no está presente también un evento "Tarjeta de desbloqueo" (Carta Sblocco)
Puertas en función Oficina	Zonas de acceso	Para cada cerradura, controle el ícono en la columna "Función Oficina" (Funzione Ufficio)
Llaves ULC cerraduras	Zonas de acceso	Para cada cerradura, controle la columna "Llave ULC" (Chiave ULC), donde el ícono verde significa Próxima llave
Llaves ULC codificadores	N/A	N/A

WIDGETS: RESUMEN

RESUMEN DATOS

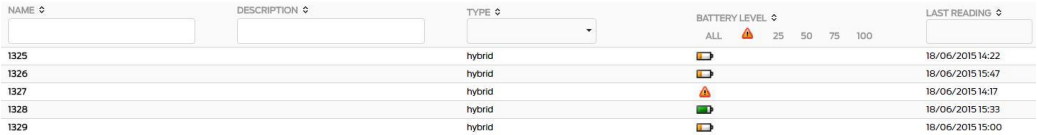
La barra en la parte inferior muestra, al lado del nombre del hotel, algunos datos adicionales sobre la instalación.

HOTEL	STANZE	OCCUPATE	LIBERE	CLIENTI	SERVIZIO	EVENTI	EVENTI PASSATI
HOTEL A	1468	0	1468	0	219	1484446	1440070

Estas conexiones se refieren a tres diferentes categorías de listas de registros.

Habitaciones

Pulsando las primeras 3 conexiones, se visualiza una lista detallada de las habitaciones seleccionadas (todas, ocupadas o libres). En la lista se indica también el nivel de las baterías; si la lista se filtra por el nivel de las baterías, se muestran todas las cerraduras con un nivel de las baterías equivalente al seleccionado; para ordenar en forma creciente o decreciente, pulse las flechas al lado del encabezamiento de la columna.



NAME	DESCRIPTION	TYPE	BATTERY LEVEL (ALL 25 50 75 100)	LAST READING
1325		hybrid		18/06/2015 14:22
1326		hybrid		18/06/2015 15:47
1327		hybrid		18/06/2015 14:17
1328		hybrid		18/06/2015 15:33
1329		hybrid		18/06/2015 15:00

Tarjetas

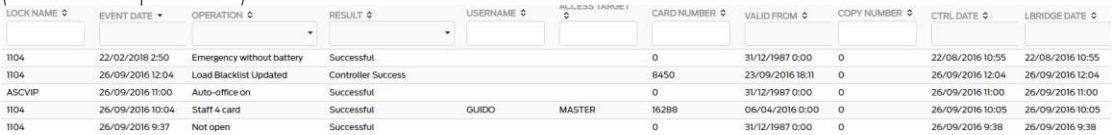
Pulsando las conexiones "Clientes" (Clienti) y "Servicio" (Servizio), se visualiza una lista detallada de las tarjetas seleccionadas (cliente o servicio).



CARD NUMBER	CARD TYPE	ACCESS ID	PRIMARY ACCESS	START VALIDITY	EXPIRATION
2	Operator	CISA	MASTER	01/01/1988 0:00	01/05/2023 0:00
1546	Staff	FIRE 33	MASTER	30/09/2014 0:00	07/01/2051 0:00
1548	Staff	FIRE 35	MASTER	30/09/2014 0:00	07/01/2051 0:00
6669	Operator	MT LEROY FREDERI	MASTER	26/03/2015 0:00	30/09/2016 23:59
6970	Operator	KLIVERANI	MASTER	08/05/2016 0:00	08/05/2017 23:59

Eventos

Pulsando las últimas 2 conexiones a la derecha, se visualiza una lista detallada de los eventos seleccionados (actuales o pasados).



LOCK NAME	EVENT DATE	OPERATION	RESULT	USERNAME	ACCESS TARGET	CARD NUMBER	VALID FROM	COPY NUMBER	CTRL DATE	LBRIDGE DATE
1104	22/02/2018 2:50	Emergency without battery	Successful			0	31/12/1987 0:00	0	22/08/2016 10:55	22/08/2016 10:55
1104	26/09/2016 12:04	Load Blacklist Updated	Controller Success			8450	23/09/2016 18:11	0	26/09/2016 12:04	26/09/2016 12:04
ASCVIP	26/09/2016 11:00	Auto-office on	Successful			0	31/12/1987 0:00	0	26/09/2016 11:00	26/09/2016 11:00
1104	26/09/2016 10:04	Staff 4 card	Successful	GUIDO	MASTER	16288	06/04/2016 0:00	0	26/09/2016 10:05	26/09/2016 10:05
1104	26/09/2016 9:37	Not open	Successful			0	31/12/1987 0:00	0	26/09/2016 9:38	26/09/2016 9:38

CAMPUS

Esta sección permite visualizar los datos de diferentes instalaciones o secciones de una instalación (por ejemplo, edificios).



HOTEL	STANZE	OCCUPATE	LIBERE	CLIENTI	SERVIZIO	EVENTI	EVENTI PASSATI
CISA V.ZARA	0	0	0	0	16	24422	0
NEW PORT BAY	1098	0	1098	0	405	654737	789040

Para visualizar los datos de una sola instalación, pulse el nombre de la instalación.

A continuación, para sumar los datos de la instalación visualizada A y de otra instalación B (presente en la tabla Campus), seleccione el cuadro cerca del nombre de la instalación B.

DASHBOARD
CHECK-IN\CHECK-OUT

CHECK-IN

Es posible utilizar el dashboard para realizar el check-in y el check-out de los clientes y para crear directamente las tarjetas de cliente. Para acceder a esta función, pulse el botón CREAR TARJETA (Crea carta) en la parte superior de la página:



La interfaz del dashboard permite especificar los siguientes datos para una tarjeta de cliente para crear, en forma similar al SSW:

- Una lista de habitaciones abiertas por la tarjeta de cliente
- Una lista de servicios abiertos por la tarjeta de cliente (se pueden utilizar solo los primeros 16 servicios definidos en el keyplan)
- La validez de la tarjeta de cliente (sección "Duración estadía"/"Durata soggiorno")
- El número de copias de la tarjeta para crear
- Codificador a utilizar para la creación de la tarjeta
- Información del cliente (como nombre y apellido)

El dashboard puede identificar si la habitación tiene una tarjeta de cliente válida. En este caso, se muestra un mensaje que pregunta si proseguir igualmente con el check-in (esta operación activará un check-out automático en la tarjeta anterior, aún válida para esa habitación).

Nota: Para poder utilizar el codificador seleccionado para esta función, el codificador no debe estar ocupado en una sección en curso con una instancia SSW (es decir, el usuario debe desconectarse del SSW).

CHECK-OUT

Se accede a la página de check-out pulsando el botón CANCELAR TARJETA (Cancella Carta) en la parte superior de la página. Esto permite especificar el número de la habitación correspondiente a la tarjeta a cancelar. Cuando el check-out ha terminado, la cerradura recibe la cancelación de la tarjeta de cliente, y la habitación se considera libre para una nueva tarjeta de cliente.

DASHBOARD: CONFIGURACIÓN

MENÚ CONFIGURACIÓN



Para acceder a los menús de configuración, pulse

Logout: para desconectarse del dashboard

Idioma: para seleccionar el idioma de visualización del dashboard. Actualmente están disponibles los idiomas inglés, francés, italiano y alemán

Configuraciones: para configurar los parámetros correspondientes a algunos widgets:

- Puertas monitorizadas a considerar para poblar el widget "Puertas dejadas abiertas" (Porte lasciate aperte).
- Acceso no autorizado: para configurar los valores "N" y "T" (este widget se activa cuando una tarjeta se utiliza "N" veces en puertas no autorizadas, en un intervalo de tiempo "T"). Además, permite seleccionar qué tipos de eventos se deben considerar accesos no autorizados.
- Tarjetas que expiran: para configurar los tipos de tarjetas a controlar (el widget muestra el número de tarjetas del tipo especificado que caducarán dentro de las 24 horas).
- Configuraciones visualización: para configurar el número de líneas a visualizar en cada lista.
- Configuraciones visualización widgets: para configurar qué widgets deben ser accesibles desde qué niveles/perfiles de operador. Por defecto, cualquier operador que puede realizar el login en el dashboard tiene los derechos para acceder a todos los widgets; esto puede ser modificado por un operador con capacidad para acceder al menú Configuraciones.
  El comportamiento de la vista de selección depende de la configuración del sistema:
  - Si el sistema trabaja con los niveles operador, las columnas están numeradas de 1 a 10 y son estrictamente jerárquicas. En este caso, para cada widget, si un cuadro de control está seleccionado, todos los cuadros de control para los niveles más elevados se seleccionan automáticamente;
  - Si el sistema trabaja con los perfiles Operador, las columnas están numeradas de 1 a 15 y pueden no ser estrictamente jerárquicas; esto significa que un operador 9 puede tener un cierto conjunto de derechos y un operador 8 puede tener más o menos, según la configuración de la instalación.

  Si uno cualquiera de los widgets no debe ser visualizado por un operador, el cuadro del widget no se carga en el dashboard y los cuadros que normalmente están a la izquierda suben a la derecha, quedando siempre en la línea correcta para no mezclar tipos diferentes de widgets (recepción, técnico, etc.).

DASHBOARD: CONFIGURACIÓN



- Configuraciones intervalo alarmas: para seleccionar si visualizar, en el contador externo de los widgets, solo las alarmas correspondientes a las últimas 24 horas (agregando así un límite temporal a las alarmas visualizadas) o todas las alarmas (sin límite temporal). Esta función se aplica a los siguientes widgets:
  - Extracción baterías
  - Acceso no autorizado
  - Uso llave de emergencia
  - Controlar cerradura

  Según la selección, un ícono diferente se visualiza en el ángulo inferior derecho del cuadro de widgets



DERECHOS DE ACCESO

Es posible regular las funciones accesibles a los diferentes operadores, en base a los niveles jerárquicos definidos en la puesta en marcha de la instalación (en el configurador):

Función	Etiqueta configurador
Login al dashboard y visualización solo de los widgets	System login
Funciones de check-in y check-out	Guest card issue
Acceso al menú Settings	System Menu
Acceso al contenido de los widgets y marcado registros leídos	Lock Audit Trails
Login a la Admin App	System Admin
Posibilidad de eliminar eventos dentro de los widgets	Clear events

HHI INSTRUMENTOS DE SERVICIO

El HHI es un dispositivo móvil eSIGNO utilizado para comunicarse con los dispositivos electrónicos del sistema (cerraduras, lectores de pared y cilindros electrónicos). Puede ser un dispositivo dedicado autónomo o puede estar integrado en el codificador SRV BKUP.

El HHI cumple las siguientes funciones, incluso cuando está offline (no conectado a la red Ethernet):

- Inicialización dispositivo
- Descarga firmware cerradura/lector de pared
- Descarga historial y visualización
- Sincronización dispositivo
- Lectura información dispositivo
- Lectura lista negra dispositivo

Nota: Funciones adicionales son controladas por las infraestructuras wireless.

Para cada instalación se pueden definir y utilizar hasta 5 dispositivos HHI (más el integrado en el codificador SRV BKUP). Durante la puesta en marcha de la instalación, los dispositivos HHI se proporcionan con:

- Firmware cerradura o lector de pared;
- Tablas hora legal.

Para acceder al HHI y utilizarlo, es necesario suministrar al HHI los siguientes datos:

- Datos inicialización instalación (por ejemplo, código de instalación)
- Keyplan (información relativa a las cerraduras y a las camas)
- Operadores del Smart Software que pueden realizar el login al HHI
- Fecha/hora actual

Para hacerlo,

1. Conecte el HHI en stand-by (READ HHI OP. C. en el display) a la red Ethernet
2. Abra la vista Zonas de acceso (Zone accesso) del Smart Software
3. Pulse el botón dedicado:



4. Seleccione el dispositivo HHI a sincronizar
5. Confirme la operación

Cuando la sincronización ha terminado, se puede desconectar el HHI de la red Ethernet.

A continuación, todos los operadores admitidos están habilitados para el login.
Para acceder:

1



Coloque la tarjeta de operador en el codificador.

Se visualizan fecha/hora de la última sincronización.
Para continuar, seleccione YES y pulse ENTER

2



Introduzca la contraseña y pulse ENTER: ahora está conectado.

3



Navegar a través de los menús deseados.

HHI: CERRADURA ESIGNO Y LECTOR DE PARED

La conexión con una cerradura o un lector de pared eSIGNO se puede obtener equipando a eSIGNO Mobile en modo HHI con eSIGNO Mouse.



Gracias a esta conexión, es posible:

- descargar el firmware en la cerradura;
- inicializar y sincronizar la cerradura;
- administrar la memoria de la cerradura (eventos de historial, datos);
- configurar las autoprogramaciones en la cerradura;
- variar los parámetros de la cerradura.

En alternativa, la comunicación entre eSIGNO Mobile y las cerraduras o el lector de pared eSIGNO se puede obtener usando las tarjetas de servicio (véase el párrafo siguiente).

COMUNICACIÓN ENTRE HHI Y CERRADURA O LECTOR DE PARED eSIGNO

Para comunicarse con un dispositivo eSIGNO (cerradura o lector de pared), conecte el ratón eSIGNO a la ranura correspondiente en eSIGNO Mobile.



Es posible comprender si el ratón eSIGNO está conectado correctamente, controlando la pantalla de eSIGNO Mobile:

```
HHI          #000
 26/03/09 10:27
     DISPLAY
      DATA
```

El ratón eSIGNO no está conectado a eSIGNO Mobile.

```
HHI [....]   #000
 26/03/09 10:27
     DISPLAY
      DATA
```

El ratón eSIGNO no está conectado correctamente a eSIGNO Mobile. (véase [....] en la primera línea).

Para obtener la comunicación real entre el dispositivo eSIGNO (cerradura o lector de pared) y el HHI, el ratón eSIGNO se debe presentar al dispositivo.

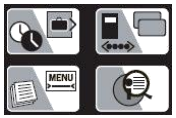
```
HHI [LINK]   #000
 26/03/09 10:27
     DISPLAY
      DATA
```

La conexión entre el dispositivo eSIGNO y HHI está activa (véase [LINK] en la primera línea).

Cuando la comunicación ha sido establecida, el dispositivo eSIGNO permanece encendido mientras el ratón eSIGNO permanece frente al lector. A partir de este momento, es posible usar los botones especiales en eSIGNO Mobile para ejecutar diferentes operaciones.

```
HHI [BOOT]   #000
 26/03/09 10:27
     DISPLAY
      DATA
```

Nota: En el momento de la conexión, si eSIGNO Mobile verifica la ausencia de firmware eSIGNO compatible en el dispositivo, en el display se visualiza el presente mensaje (véase [BOOT] en la primera línea).



BOTONES ESPECIALES

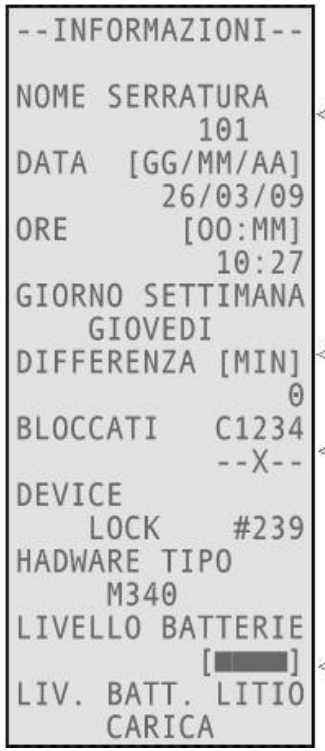


SINCRONIZACIÓN DE LA CERRADURA

El dispositivo HHI envía a la cerradura la fecha y la hora, además de las tablas para pasar a la hora legal. Después de la sincronización, la cerradura emite 2 destellos verdes.



INFORMACIÓN



Con esta función, es posible leer datos desde la cerradura.

Este campo representa el nombre de la cerradura dentro del keyplan; el número lógico de la cerradura se indica abajo.

Diferencia entre la hora de la cerradura y el del sistema de codificación.

Tipos de tarjetas bloqueados (sin acceso a la cerradura):

- C = tarjeta de cliente;
- 1, 2, 3, 4 = tarjetas de servicio tipo 1, 2, 3, 4.

En este caso, están bloqueadas las tarjetas de servicio tipo 2.

Estos son los niveles de carga de las baterías comunes y de la batería de litio de backup.



LECTURA DEL HISTORIAL DE LA CERRADURA



Con esta función es posible leer un determinado número de operaciones realizadas en una cerradura específica, eligiendo entre 10, 25, 50, 100 o TODAS. Después de la lectura, los datos se pueden imprimir en la tarjeta o visualizar en el HHI. Es posible leer operaciones memorizadas en diferentes cerraduras y cargarlas todas en el HHI, hasta alcanzar la máxima capacidad de la cerradura (hasta 1000 operaciones).



HHI: E-CYLINDER

La comunicación entre el HHI y el E-Cylinder no requiere la utilización del ratón eSIGNO: en efecto, esta se obtiene mediante la emisión de tarjetas de servicio especiales, que posteriormente se deben presentar al cilindro.

Nota: Estas tarjetas de servicio también se pueden utilizar como formas alternativas de comunicación entre eSIGNO Mobile y cerraduras o lectores de pared eSIGNO.

COMUNICACIÓN ENTRE HHI Y E-CYLINDER

Las tarjetas de servicio utilizadas para obtener una comunicación entre el HHI y el E-Cylinder (o cualquier dispositivo eSIGNO en general) se pueden emitir seleccionando la opción correspondiente en el menú HHI (menú Tarjetas de Servicio).

A continuación, explorando con , es posible elegir el tipo de tarjeta a emitir. Los diferentes tipos de tarjeta de servicio se describen en la tabla siguiente.

TIPO DE TARJETA	CUÁNDO SE UTILIZA
SINCRO	PARA SINCRONIZAR EL DISPOSITIVO Y EL CODIFICADOR
INIT	PARA INICIALIZAR EL DISPOSITIVO
RESET	PARA RESETEAR EL DISPOSITIVO
INFORMACIÓN DISPOSITIVO	PARA DESCARGAR DEL DISPOSITIVO LA INFORMACIÓN SOBRE LA INICIALIZACIÓN Y EL ESTADO OPERATIVO
AUTOPROGRAMACIONES (AUTOPROGRAMMI)	PARA ADMINISTRAR LAS AUTOPROGRAMACIONES EN EL DISPOSITIVO
CAMBIO DE BATERÍA (CAMBIO BATTERIA)	PARA CAMBIAR LAS BATERÍAS DEL CILINDRO (N. D. EN OTROS DISPOSITIVOS)
MONTAJE/DESMONTAJE (MOUNT/DISMOUNT)	PARA SEPARAR LA CABEZA DEL CILINDRO DEL CUERPO (N. D. EN OTROS DISPOSITIVOS)

Una vez emitida, la tarjeta se debe presentar al dispositivo:

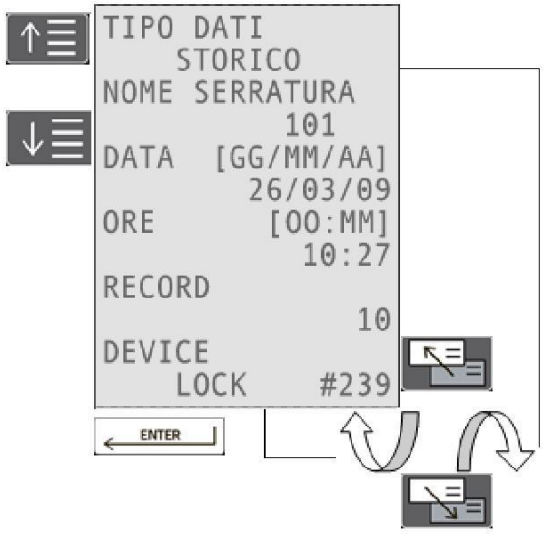
- si la operación se está desarrollando correctamente, el dispositivo emite una luz anaranjada; al final, emite dos destellos verdes, acompañados por dos tonos rápidos;
- si la operación no es posible (por ejemplo, cuando el dispositivo no está inicializado), el dispositivo emite tres destellos rojos, acompañados por dos tonos agudos (situación de error lógico);
- si la tarjeta de servicio se separa del dispositivo durante la ejecución de la operación, el dispositivo emite un destello rojo, acompañado por un tono agudo (error físico).

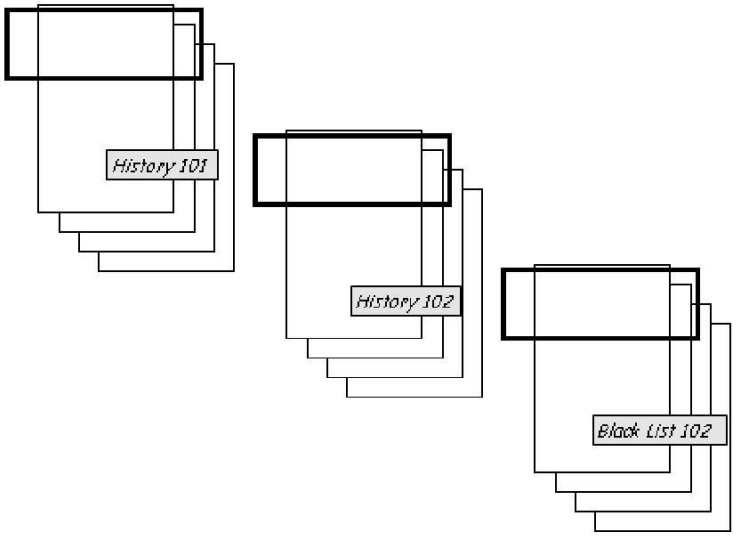
Por información adicional, consulte el párrafo menú Tarjetas de Servicio (Carte Servizio).

MENÚ PRINCIPAL HHI

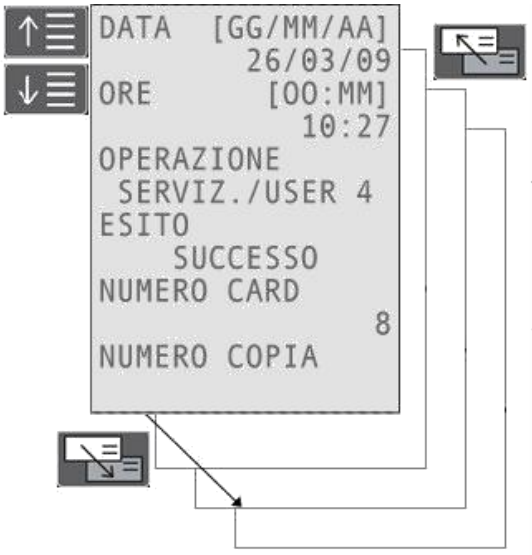
VISUALIZAR DATOS (1)

En este menú es posible visualizar diferentes páginas de lectura; en particular, el historial y la lista negra de las diferentes cerraduras. Los descriptores de los datos están ordenados del más reciente al más antiguo; cada descriptor consiste en un conjunto de registros.





VISUALIZAR DATOS DE HISTORIAL



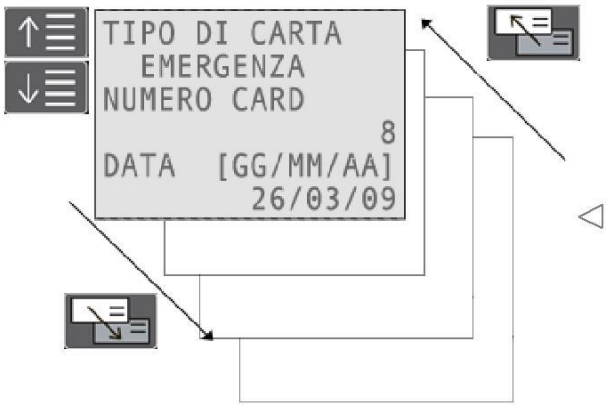
Se visualizan las operaciones realizadas en la cerradura, a partir de la más reciente.

Este es el tipo de operación; más abajo se encuentra el resultado.

Este es el número identificador representativo de la tarjeta.

VISUALIZAR DATOS (2)

VISUALIZAR DATOS LISTA NEGRA



Se visualizan las tarjetas anuladas en la cerradura, es decir, las tarjetas incluidas en la lista negra.

Inicio de la validez de la tarjeta.

PARÁMETROS SINCRONIZACIÓN CERRADURA

Este menú permite sincronizar una cerradura offline o un lector de pared con todos los parámetros guardados en el Smart Software.
A continuación se describe el procedimiento completo:

- En la vista Zonas de acceso (Zone accesso) del SSW, actualice los parámetros de la cerradura deseada (por ejemplo, tiempo de apertura, fechas de referencia personal/operador, autoprogramación, etc.) y confirme.
- Sincronice el HHI con estos últimos datos
- Presente a la cerradura el ratón conectado al HHI
- Seleccione el menú Sincronización Parámetros Cerradura (Sincronizzazione Parametri Serratura) para comunicar los parámetros a la cerradura (que emite 2 destellos verdes cuando la operación ha terminado)

INICIALIZAR CERRADURA

Cada cerradura se debe inicializar con un número específico y otros parámetros.

1



Para inicializar la cerradura pulse  ; a continuación, seleccione Programa Cerradura, pulsando ENTER.

2



Seleccione la opción Inicializar Cerradura, pulsando ENTER.

Nota: Si la cerradura ya está inicializada, es necesario realizar un reset antes de poder reinicializarla (opción Reset Cerradura en el menú Asistencia Cerradura).

Introduzca el número que desea asignar a la cerradura (por ejemplo, 101);
a continuación, pulse 

3



En alternativa, pulse simplemente  para navegar entre los números de 3 puerta disponibles.

Pulsando  es posible visualizar el número lógico asignado a la puerta.

Para confirmar y comenzar la inicialización, pulse 

4



Los datos de inicialización son transmitidos a la cerradura.
Si la comunicación es positiva, la cerradura emite una secuencia de dos destellos verdes, uno rojo y dos verdes.
Este procedimiento envía a la cerradura electrónica nombre, horario, grupos y tablas para el paso a la hora legal.



RESET CERRADURA

Se realiza un reset de la cerradura al estado de fábrica. Después de esta operación, la cerradura puede ser reinicializada.



DESCARGAR PROGRAMA CERRADURA

Para actualizar a una nueva versión el software dentro de las cerraduras, o en caso de pérdida del software en las cerraduras, es necesario descargar el programa en las mismas.



LEER LISTA NEGRA

Eligiendo esta opción, se carga la lista de tarjetas memorizadas en la lista negra de la cerradura (black-list); esta lista se puede visualizar en el display del eSIGNO Mobile.

MENÚ TARJETAS DE SERVICIO (1)

CREAR TARJETA DE SINCRONIZACIÓN HORARIO

Este menú permite crear tarjetas de servicio de sincronización. Con esta tarjeta es posible sincronizar el dispositivo con respecto al codificador que la ha emitido.

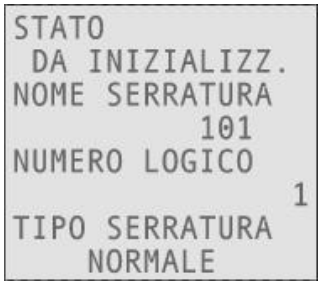
La operación se realiza emitiendo una tarjeta de sincronización y presentándola al dispositivo; una vez terminada, el dispositivo emite dos destellos verdes. Esta operación es necesaria durante la inicialización de la instalación o después de un cambio de las baterías del dispositivo.
En particular, una tarjeta de sincronización permite al dispositivo adquirir los siguientes datos:

- fecha y hora;
- los parámetros correspondientes a la hora solar y legal;
- los días festivos (qué días del año se consideran festivos).

Nota: Es importante presente la tarjeta de sincronización al cilindro inmediatamente después de haberla emitido, para preservar la función de alineación de la fecha y la hora entre el cilindro y el codificador. Una vez terminada la operación, el campo Diferencia [min] (Differenza [min]), en la Información Cilindro, debería contener el valor 0.

CREAR TARJETA DE INIT

Este menú permite crear tarjetas de servicio de inicialización. Con esta tarjeta es posible inicializar un dispositivo con el nombre de una de las cerraduras incluidas en el keyplan.



Explorando con , seleccione el nombre de la cerradura que el dispositivo asumirá después de la inicialización.

Pulsando 

se confirma la creación de una tarjeta de inicialización cilindro para la cerradura seleccionada.

A continuación, esta tarjeta debe ser presentada al dispositivo; una vez terminada la operación, el dispositivo emite dos destellos verdes.

Es necesario realizar un reset del dispositivo antes de presentar esta tarjeta; si el dispositivo ya está inicializado y se presenta una tarjeta de inicialización, emite tres destellos rojos, acompañados por dos tonos.

CREAR TARJETA DE RESET

Este menú permite crear tarjetas de servicio de reset. Con esta tarjeta es posible realizar el reset de un dispositivo, llevándolo al estado original de fabricación. Una vez terminada la operación, el cilindro puede ser inicializado y sincronizado nuevamente.

Nota: La única tarjeta aceptada por un dispositivo en estado de reset es una tarjeta de inicialización. Para activar las otras tarjetas, es necesario inicializar antes el dispositivo.



MENÚ TARJETAS DE SERVICIO (2)

CREAR TARJETA INFO DEVICE

Este menú permite crear tarjetas de información del dispositivo. Con esta tarjeta es posible descargar del dispositivo todos los datos correspondientes a inicialización, fecha y hora, nivel de las baterías y versión del software. La operación se realiza emitiendo una tarjeta de información del dispositivo y presentándola al dispositivo; una vez terminada, el dispositivo emite dos destellos verdes.
Para leer una tarjeta de información del dispositivo, es necesario usar el menú correspondiente (descrito más abajo).

LEER TARJETA INFO DEVICE



Los datos descargados en la tarjeta de información del dispositivo se pueden visualizar en la pantalla del codificador, seleccionando este menú y presentando la tarjeta al codificador.

- *Diferencia temporal entre el dispositivo y el codificador.*
- *Nivel de las baterías del dispositivo.*
- *Versión del firmware instalado en el dispositivo.*

CREAR TARJETA DE CAMBIO DE BATERÍA

Este menú permite crear tarjetas de cambio de batería. Con esta tarjeta es posible cambiar las baterías del cilindro. Presentando la tarjeta al cilindro, las dos trabas que mantienen bloqueada la cubierta de la cabeza del cilindro se vuelven retráctiles; de esta forma es posible extraer la cubierta del cilindro (utilizando la herramienta correspondiente) y sustituir las baterías. A continuación, la cubierta se puede colocar y bloquear nuevamente, presentando la tarjeta de cambio de batería una segunda vez.

CREAR TARJETA DE MONTAJE/DESMONTAJE

Este menú permite crear tarjetas de montaje/desmontaje. Con esta tarjeta es posible separar la cabeza del cilindro del cuerpo del mismo. Presentando la tarjeta al cilindro, la cabeza se fija a la leva; para desenganchar la cabeza del cuerpo del cilindro, es necesario girar la misma, tirando simultáneamente; la operación inversa se puede realizar colocando la cabeza y presentando la tarjeta de montaje/desmontaje una segunda vez.

CONFIGURACIÓN OPCIONES

Este menú permite configurar la duración (en días) de las tarjetas de servicio emitidas mediante los menús anteriores (Sincro, Init, Reset, Info Device, Autoprogramaciones, Cambio de Batería, Montaje/Desmontaje). La duración por defecto es de 365 días.

ESCENARIO FALLO

El escenario Fallo (Failure) se verifica cuando el sistema de codificación basada en ordenador está fuera de uso o cuando hay problemas en la conexión a la red Ethernet. En este caso se activa el sistema basado en el codificador Server Backup.

En modo Fallo (Ethernet o RS485), las características del codificador se limitan a las siguientes operaciones:

- Creación tarjetas de cliente (utilizando solo el módulo base)
- Leer y visualizar los datos de la tarjeta
- Copiar y/o hacer el check-out de las tarjetas de cliente

Modo Normal

El ordenador servidor en el que está trabajando el Smart Software y la red LAN funcionan correctamente; el codificador Backup Server trabaja solo como réplica de la base de datos del ordenador servidor. El display muestra:

```
CISA HOTEL

SRV BKUP#000dH00
  06/12/13 17:32 READ
  OPER.CARD
```

Modo Fallo

El ordenador servidor está fuera de uso; los ordenadores client en los que está trabajando el Smart Software no se pueden utilizar. El sistema puede rebajar de clase su funcionamiento, trabajando en modo Fallo a través del codificador Backup Server. Complete los siguientes pasos para activar el modo Fallo.

Codificador Backup Server

El codificador Backup Server se debe encender manualmente en modo Fallo. Coloque una tarjeta de operador en el codificador Backup Server e introduzca la contraseña. Cuando el display muestra el siguiente mensaje, pulse Enter (solo se admiten operadores de alto nivel).

```
* SYSTEM MENU *


>          ENABLE
     FAILURE MODE <
```

El codificador requiere el modo de comunicación a utilizar: para continuar con Ethernet, seleccione NO; para cambiar a RS485, pulse  y seleccione YES.

```
USE RS485 COMM.? >
NO <
```

Después de confirmar el modo de comunicación Failover, el codificador Backup Server se reinicia y visualiza los siguientes datos:

```
CISA HOTEL

SRV ETH #000dH00
  06/12/13 17:32 READ
  OPER.CARD
```

(La palabra ETH en el display es sustituida por 485, si se ha elegido el modo de comunicación RS485).

El modo de comunicación también se puede cambiar después, si la red LAN deja de funcionar: para cambiar el modo de comunicación, acceda al codificador Backup Server, pulse el botón MENÚ y seleccione esta opción:

```
* SYSTEM MENU *

> SWITCH TO RS485
  NETWORK <
```

Una vez más, el codificador se reinicia y visualiza esta información:

```
CISA HOTEL
SRV 485 #000dH00
  06/12/13 17:32 READ
  OPER.CARD
```

Codificadores Client

Durante las operaciones normales, los codificadores client trabajan como estaciones de codificación guiadas por las estaciones de trabajo PMS o por el Smart Software. En modo Fallo, cada codificador client debe estar conectado al codificador Backup Server. Complete los pasos siguientes para activar el modo Fallo.

```
CISA HOTEL
CLI ETH #002dH02
  06/12/13 17:32 READ
  OPER.CARD
```

Seleccione el mismo modo Fallo del codificador Backup Server. Por defecto, los codificadores client están configurados en modo comunicación Ethernet (véase la segunda línea del display, que muestra la palabra ETH). Si el codificador Backup Server cambia al modo de comunicación RS485, es necesario cambiar el modo de comunicación también en los codificadores client. Para cambiar a RS485, pulse ESC, luego pulse  y seleccione YES.

```
USE RS485 COMM.? >
NO <
```

Nota: Cuando se activa el modo Fallo RS485, verifique que todos los codificadores client estén registrados; de esta forma se pueden tener mejores prestaciones y evitar el apagado automático del codificador. La estimación de la duración de las baterías del codificador es de aproximadamente 1 hora (depende de las condiciones de las baterías).

Después de confirmar el modo de comunicación Failover, el codificador client se reinicia y visualiza los siguientes datos:

```
CISA HOTEL
CLI 485 #002dH02
  06/12/13 17:32 READ
  OPER.CARD
```

Un operador puede acceder. Siempre es posible conocer el modo de comunicación, controlando la información en el display (CLI ETH/485).

LOGIN AL CODIFICADOR

Antes de realizar cualquier operación, acceda al codificador eSIGNO con una tarjeta de operador válida.

1

```
CISA HOTEL
SERVER  #000dH00
 26/01/09 17:20
<READ OPER.CARD<
```

Coloque una tarjeta de operador válida en el codificador.

2

```
-   LOGIN TO   -
-   ENCODER    -
ENTER PASSWORD
       >
```

Introduzca la contraseña y pulse ENTER. ahora está registrado.

3

```
GUEST FOR

21/01/07    15:30
 < READ CARD <
```

Presente una tarjeta para visualizar los datos.

CREACIÓN TARJETAS DE CLIENTE

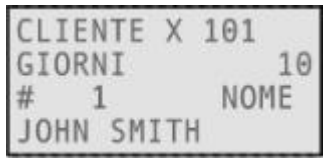
Nota: Cuando se reutiliza una tarjeta válida para codificar una nueva credencial, la credencial anterior se considera cancelada. Una vez restablecido el modo normal, el servicio de sincronización del Smart Software actualizará el estado de la base de datos.

1



Introduzca el número de habitación, la duración de la permanencia, el número de copias deseadas y el nombre del cliente, pulsando  después de cada campo.

2



Pulse

3



Coloque la tarjeta sobre el dispositivo de grabación del codificador y espere hasta oír una breve señal acústica.

 ¡La grabación de la tarjeta ha terminado!

GESTIÓN TARJETAS DE CLIENTE



COPIAR TARJETA CLIENTE

Presente al codificador la tarjeta a copiar y luego pulse este botón. Cuando el codificador emite un sonido, presente la nueva tarjeta al codificador. Si la función SmartMedia está habilitada, no es posible crear copias de tarjetas de cliente en modo Fallo.



CHECK-OUT TARJETA CLIENTE

Presente la tarjeta a cancelar al codificador y luego pulse este botón. Si se presenta nuevamente la tarjeta, se visualiza el mensaje "Checked out card".



MENÚ

Pulse este botón para habilitar/inhabilitar el modo Fallo o para cambiar las configuraciones de comunicación (Ethernet o RS485).

eKEY

La cerradura eSIGNO puede estar equipada con tecnología Bluetooth Low Energy (BLE), permitiendo funciones para la gestión de credenciales Mobile basadas en un servicio Trust Cloud, capaz de enviar derechos de acceso en forma segura.

BlueID es la tecnología que permite una comunicación BLE segura, en la que se basa eKEY.

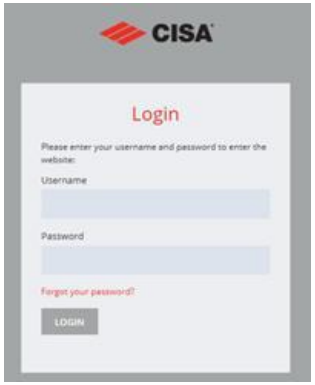
El aspecto comercial de esta función no será incluido en el presente manual; para cualquier pregunta, se ruega contactar con el representante comercial Cisa.

REGISTRO HOTEL

El hotel se debe registrar en la interfaz de administración gestgid proporcionada para clientes CISA: https://ifbck.com/admin/registration-gestgid/cisa



- El hotel debe especificar:
  - Correo electrónico (cuenta de login)
  - Datos del hotel
  - Sitio web de reserva
  - Material de marketing
- Un correo electrónico será enviado a la cuenta especificada para confirmar el registro
- Si la confirmación es aceptada, la cuenta de login se habilitará en: https://ifbck .com/admin/login/cisa



CONFIGURACIÓN DE SISTEMA

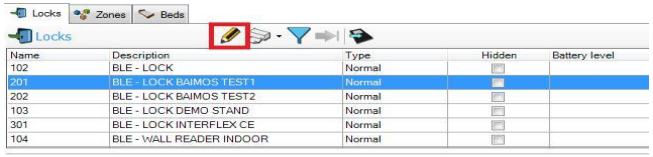
Los mismos detalles de la cuenta (es decir, el correo electrónico y la contraseña) utilizados para el registro del hotel se deben introducir en la sección correspondientes de la vista Preferencias (Preferenze), dentro de la instancia SSW4 instalada en el servidor de sistema. Una vez que estos detalles han sido introducidos, la conexión a la nube se puede probar con el botón TEST.



Las cerraduras y los lectores de pared eSIGNO BLE son producidos por CISA con una referencia unívoca SOID (Secured Object ID), registrada en el producto e impresa en la etiqueta correspondiente. Los dispositivos BLE pueden ser configurados mediante el Smart Software e inicializados utilizando el HHI (como cualquier otro dispositivo eSIGNO):

1) Desde cualquier vista, pulse 

.
2) Seleccione la puerta a asociar con el dispositivo BLE y pulse  (este paso se debe repetir para cada dispositivo BLE a inicializar)



Nota: No es recomendable modificar los parámetros BLE (advertisement, potencia, etc.) sin haberlo acordado previamente con Cisa.

3) Seleccione el cuadro "Activo BLE" (Attivo BLE) y confirme con
4) Sincronice el HHI pulsando
5) Realice el login en el HHI e inicialice los dispositivos desde el menú "Init Cerradura" (Init Serratura)
6) Realice el logout del HHI, conéctelo a la red Ethernet y sincronícelo nuevamente con

   Los siguientes campos vinculados a la funciones BLE se rellenarán con los datos leídos por los dispositivos

   a. "Object ID", correspondiente al SOID asociado en producción
   b. "Nombre local BLE", que se puede utilizar para identificar el dispositivo BLE, realizando un escaneo con la aplicación *nRFConnect* (véase más abajo)



   La aplicación *nRFConnect* puede realizar un escaneo de todos los dispositivos BLE en los alrededores e indicar los nombres locales de los mismos

7) La lista completa de los dispositivos BLE inicializados con los SOID asociados se puede obtener pulsando la flecha al lado del botón y seleccionando "Informe técnico". En alternativa, la referencia SOID está presente en las etiquetas asociadas a cada cerradura/lector de pared.
8) Realice el login al backend gestgid (Door Management → Locks) y cree las cerraduras asociando el nombre de la cerradura a la referencia SOID. Nota: El SOID distingue entre mayúsculas y minúsculas y se debe introducir en el back-end con precisión



HISTORIAL BLE

Cada apertura generada por un dispositivo móvil genera un registro de historial con el MOID (Mobile ID) correspondiente. Esta referencia unívoca está asociada a los datos de usuario registrados en el servidor gestgid.

RESERVA Y CHECK-IN

La aplicación gestgid está disponible para teléfonos iOs y Android.

Android versión 5.0 es recomendado como requisito mínimo.

PROCESO DE RESERVA

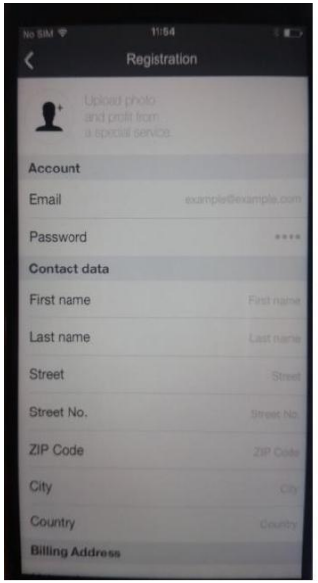
1) *El cliente se conecta al sitio web del hotel y reserva una habitación, introduciendo los datos estándar de reserva (nombre, apellido, correo electrónico, tarjeta de crédito, etc.)*

2) *El sitio web del hotel controla la reserva y envía un correo electrónico de confirmación al cliente*

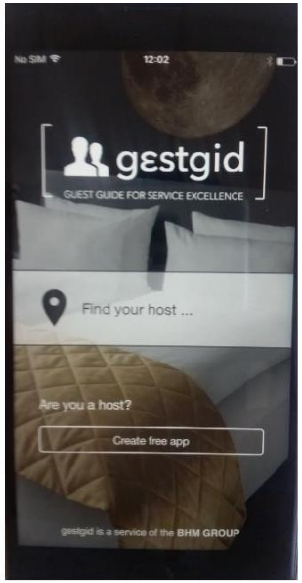
Gracias por haber reservado en Hotel Cisa.

Podemos ofrecer un servicio adicional con nuestra credencial de beneficios Mobile. Descargue la aplicación GESTGID en su smartphone (iOs/Android) en el siguiente enlace:
https://appsto.re/it/pD2G_.i
Enlace Android: https://play.google.com/store/apps/details?id=com.bhmgrp.gestgid
Regístrese en la aplicación con su correo electrónico y busque nuestro hotel.
Utilice todos nuestros servicios, incluida la apertura de la puerta mediante Mobile Key.

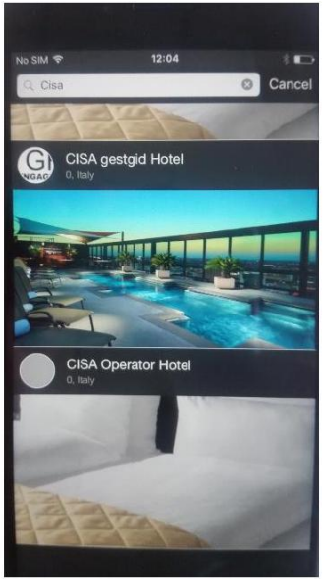
3) *El cliente descarga la aplicación gestgid y se registra*



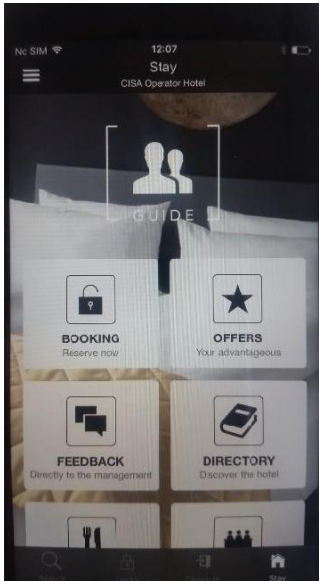
4) El cliente se registra introduciendo los datos personales, como correo electrónico



5) El cliente busca el hotel



6) El cliente selecciona el hotel para el cual ha realizado la reserva

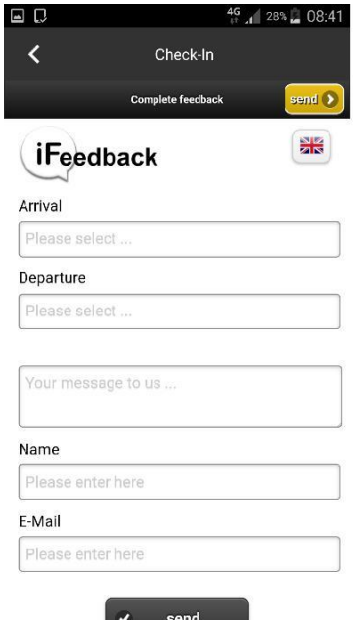


7) Desde esta vista, el cliente puede controlar la reserva (incluidas las credenciales)

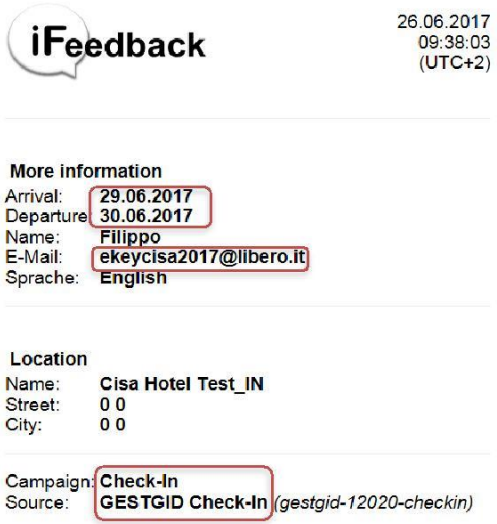
PROCESO DE CHECK-IN

El cliente puede:

a) llegar a la recepción del hotel y pedir una Mobile Key (y/o una tarjeta RFID): el encargado de la recepción preguntará el correo electrónico del cliente
b) contactar con el hotel para confirmar la reserva y comunicar el correo electrónico
c) usar el widget de check-in en la aplicación gestgid (véase más abajo)



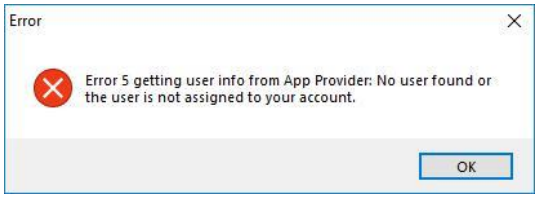
El cliente introduce los datos para el check-in



Se envía un correo electrónico al hotel.
El encargado asocia la solicitud de check-in a la reserva realizada online por el cliente.
El campo correo electrónico es la referencia principal para el envío de la Mobile key al cliente.

GESTIÓN CREDENCIALES MOBILE

Nota: Si el correo electrónico introducido para solicitar una nueva credencial (o la copia de una ya existente) no ha sido utilizado por el cliente para registrarse en la aplicación, el SSW4 restituye un mensaje de error y la credencial no se crea.



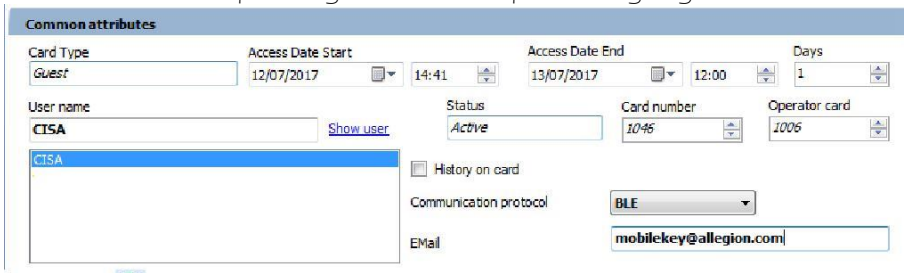
En este caso, verifique que todos los detalles hayan sido introducidos correctamente en el SSW4 y que el cliente haya completado correctamente el registro en la aplicación gestgid.

SMART SOFTWARE – NUEVA CREDENCIAL MOBILE

Para crear una nueva credencial Mobile:

1) Desde cualquier vista, pulse 

2) Pulse la flecha del botón 
3) Seleccione qué tipo de credencial Mobile se debe crear, entre
   - Cliente
   - Servicio
   - Usuario
4) Introduzca los parámetros deseados, según el tipo de credencial Mobile.
   En particular, seleccione el protocolo de comunicación "BLE" e introduzca el correo electrónico que el cliente ha utilizado para registrarse en la aplicación gestgid



5) Pulse  para aceptar. La credencial Mobile estará habilitada en el smartphone asociado.

SMART SOFTWARE – COPIA DE CREDENCIALES MOBILE

Esta operación permite la creación de una copia idéntica de una credencial de cliente, independientemente del formato de la credencial de cliente original (RFID o BLE). La nueva credencial no inhabilita el acceso de la original.

1. Desde cualquier vista, pulse 

2. Seleccione la credencial a copiar, eligiendo en la lista de las disponibles.
3. Pulse 
4. Seleccione el protocolo de comunicación "BLE", introduzca el correo electrónico que el cliente ha utilizado para registrarse en la aplicación gestgid y seleccione el parámetro "Superar Privacy" (Supera Privacy).



5. Pulse  para aceptar. La credencial Mobile estará habilitada en el smartphone asociado.

SMART SOFTWARE - CHECKOUT DE CREDENCIALES MOBILE

Esta operación permite la cancelación de una credencial de cliente, por ejemplo, cuando el cliente realiza el check-out del hotel.

1) Desde cualquier vista, pulse 

.
2) Seleccione la credencial de cliente a cancelar, eligiendo en la lista de las disponibles.
3) Pulse .
4) El estado de la credencial en la que se ha realizado el check-out está indicado con un ícono rojo. La credencial Mobile está inhabilitada en el smartphone asociado.

SMART SOFTWARE - CANCELACIÓN DE CREDENCIALES MOBILE

Esta operación permite la cancelación de una credencial. El software pregunta si crear una tarjeta de cancelación para presentar a las cerraduras offline. Las cerraduras online (especiales e wireless), por el contrario, se actualizan automáticamente.

1) Desde cualquier vista, pulse 

.
2) Seleccione la credencial a cancelar, eligiendo en la lista de las disponibles.
3) Pulse .
4) El estado de la credencial en la que se ha realizado el check-out está indicado con un ícono rojo. La credencial Mobile está inhabilitada en el smartphone asociado.

GESTIÓN DE LAS CREDENCIALES MOBILE DESDE PMS

Para la gestión de las credenciales Mobile Cliente se han introducido dos mandos PMS adicionales:

- Creación (Creazione)
- Copiar (Copia)

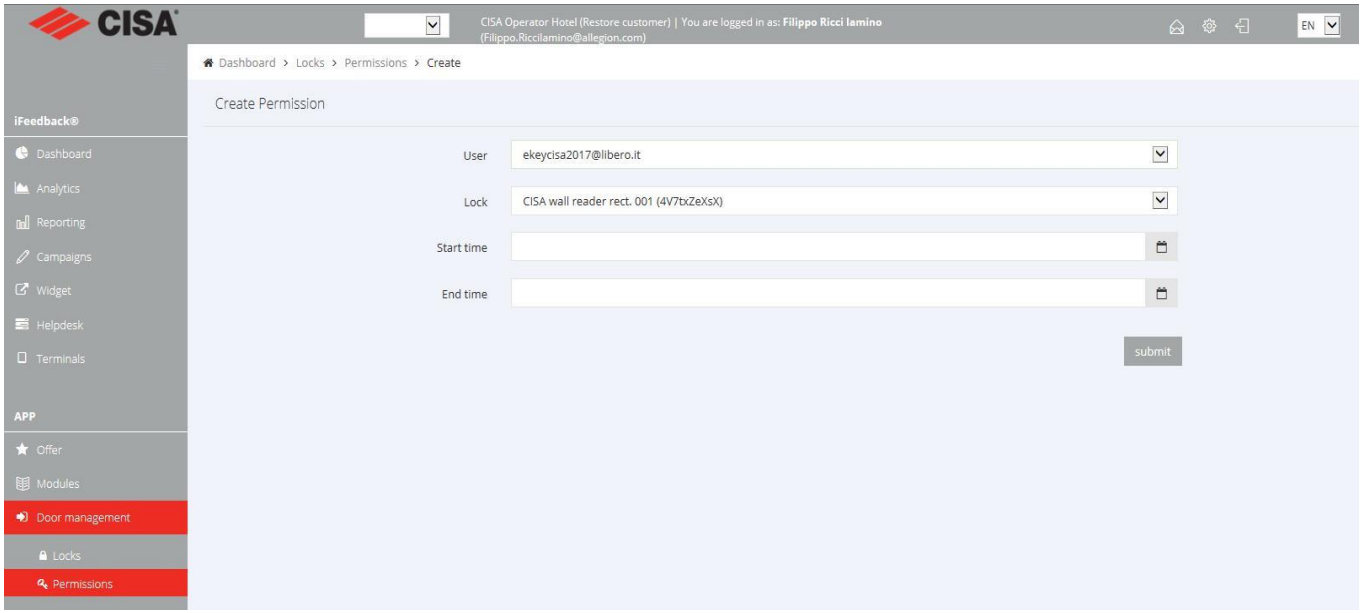
Estos dos nuevos mandos deben incluir el correo electrónico del usuario, dividido entre el campo Usuario Adicional #9 (nombre de usuario correo electrónico) y #10 (dominio)

Ejemplo: el correo electrónico mobilekey@allegion.com se debe dividir en "mobilekey" en el campo Usuario Adicional #9 (Utente Aggiuntivo #9) y "allegion.com" en el campo Usuario Adicional #10 (Utente Aggiuntivo #10).

BACK-END GESTGID

El gestor del hotel puede realizar el login en el backend gestgid, mediante la cuenta gestgid del hotel.

Para generar una credencial Mobile para un usuario específico, siga el procedimiento que se describe a continuación.



1) Realice el login en el backend gestgid.
2) Acceda al menú "Door management", seleccione "Permissions" y, a continuación, "Grant Permission".
3) Especifique el correo electrónico del usuario, las cerraduras a acceder e inicio/fin de validez.
4) Pulse el botón "submit". La credencial Mobile se habilitará en el smartphone asociado.

Atención: El backend gestgid no tiene ningún control sobre eventuales derechos de apertura duplicados; esto podría llevar a errores en la gestión de las credenciales.
Por este motivo, se recomienda encarecidamente utilizar SSW4 para controlar las credenciales.

GESTIÓN LLAVE ULC

Las llaves de criptografía ULC son controladas para aumentar la seguridad de las credenciales codificadas en soportes ULC.

Las nuevas llaves de criptografía ULC pueden ser introducidas en el sistema por un servidor externo de gestión de las llaves o manualmente por la Administration App.

Nueva llave desde un servidor externo

Un servidor externo de gestión de llaves envía una tripleta de llaves ULC PARA distribuir en el sistema CISA. Estas llaves se consideran llaves ULC anteriores, actuales y siguientes. La solicitud del servidor externo puede ser resuelta por el sistema CISA en las siguientes formas:

Código	Significado
0	El paquete de 3 llaves ha sido recibido correctamente por primera vez.
1	El paquete de 3 llaves tiene más de una llave de rotación (es decir, con respecto al paquete anterior, es diferente en más de 1 llave)
2	La llave siguiente en el paquete de 3 llaves es NULL o tiene un formato erróneo.
3	En la base de datos del sistema CISA no está la llave actual.
4	Se envía un nuevo paquete de 3 llaves, pero CISA aún no ha completado la distribución del anterior.
5	La llave anterior en el paquete de 3 llaves es NULL o tiene un formato erróneo.
6	La llave actual en el paquete de 3 llaves es NULL o tiene un formato erróneo.
20	Un aviso de error para informar que el sistema CISA ya ha recibido el mismo paquete de 3 llaves, que ha sido devuelto.

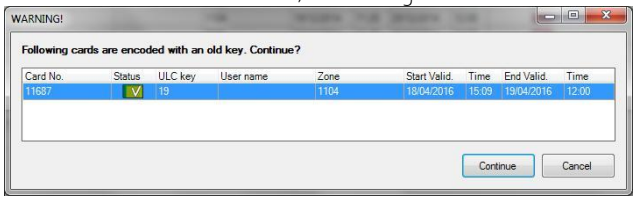
Nueva llave desde la Administration App

1. Conéctese a la Administration App (http://server_PC's_IP_address:8080/SmartSoftwareAdmin).
2. Pulse el menú *ULC Keys* y pulse *Add*.
3. Introduzca una llave en el campo *Key value (encrypted)* y pulse el botón *Save*. La columna *Key Type* muestra el tipo de llave entre Anterior (3), Actual (2) y Siguiente (1).

Confirmación de una nueva distribución

La distribución de una nueva llave de criptografía ULC comienza solo si la anterior distribución ha terminado, comenzando por los codificadores. Antes de comenzar la actualización de las cerraduras, se verifica si existen tarjetas válidas encriptadas con la llave ULC anterior (estas tarjetas ya no abrirán las cerraduras). La distribución de una nueva llave de criptografía ULC a las cerraduras comienza:

- Si no se ha encontrado ninguna tarjeta codificada con llave ULC anterior;
- Si el operador fuerza la actualización, pulsando el botón  en la vista Tarjetas del SSW. En este modo se muestran las tarjetas encriptadas con la llave ULC anterior. Si el usuario fuerza la distribución de la nueva llave ULC, estas tarjetas se vuelven inutilizables en las cerraduras.

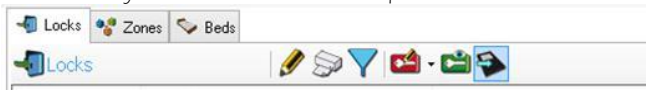


GESTIÓN LLAVES ULC

Distribución de una nueva llave ULC

La distribución de la nueva llave de criptografía ULC se realiza para todas las cerraduras y los lectores de pared marcados como *Activo* en el SSW. Mientras la llave de criptografía ULC se envía automáticamente en forma wireless a las cerraduras online y vía Ethernet a los lectores de pared online, debe ser enviada a las cerraduras y a los lectores de pared offline a través del HHI. Para hacerlo:

1. Conecte el HHI en stand-by (READ HHI OP. C. en el display) a la red Ethernet
2. Desde la vista Zonas de acceso (Zone accesso) del SSW, sincronice el HHI pulsando el botón dedicado y seleccionando el dispositivo HHI a sincronizar



3. Cuando la sincronización termina, se puede desconectar el HHI de la red Ethernet.
4. Acceda al HHI con una tarjeta de operador y presente el ratón a la cerradura/lector de pared.
5. Pulse el botón SYNCHRO  para comunicar la llave ULC a la cerradura (que emite 2 destellos verdes cuando la operación ha terminado).
6. Lea el historial de la cerradura pulsando el botón 

7. Desconéctese del HHI y conéctese nuevamente a la red Ethernet.
8. Desde la vista Eventos cerradura (Eventi serratura) del SSW, cargue el historial desde el HHI, pulsando el botón ; a continuación, seleccione el dispositivo HHI. Los eventos aparecen en la pantalla.

La actualización de la llave ULC en los dispositivos online se registra en el historial de la cerradura con 2 eventos (véase más abajo).

Lock Name	Event Date	Operation	Result	User name	Access Target	Card Number
1104	18/04/2016 16:24:34	ULC key updated (ctrl)	Successful			21
1104	18/04/2016 16:24:06	ULC key updated	Successful			Key: 21

Para los dispositivos offline, se muestra solo un evento ("Llave ULC actualizada"/"Chiave ULC aggiornata").

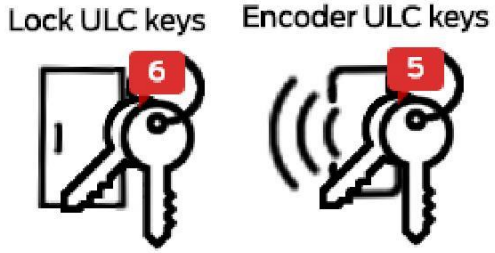
Controle la distribución de las llaves ULC

Cuando la nueva llave de criptografía ULC ha sido distribuida a todas las cerraduras y lectores de pared, después de 5 minutos (este intervalo de tiempo es configurable en la Administration App), se envía un correo electrónico a la dirección configurada en la Administration App. El texto del correo electrónico es el siguiente: "Todas las cerraduras han sido actualizadas correctamente con las llaves ULC".

Si algunas cerraduras aún no han sido actualizadas (por ejemplo, si hay cerraduras offline que deben ser actualizadas manualmente), la misma dirección recibe después de 1 hora (también este tiempo es configurable en la Administration App) un correo electrónico que contiene la lista de todas las cerraduras que aún se deben actualizar. El texto del correo electrónico es el siguiente: "¡Atención! Algunas cerraduras no han sido actualizadas con las llaves ULC. 1101, 1102..."

GESTIÓN LLAVE ULC

Es posible monitorizar la distribución de las llaves de criptografía ULC a través de dos widgets diferentes en el dashboard (véase el capítulo correspondiente):



Cuando una nueva llave de criptografía ULC se envía al sistema CISA, se activan ambos widgets con el número total de cerraduras activas y codificadores para actualizar. Abriendo un widget, es posible evaluar el estado actual de la distribución de las llaves de criptografía ULC (cuáles cerraduras ya han sido actualizadas, cuales aún deben ser actualizadas, cuál llave de criptografía ULC ha sido distribuida, etc.).

El widget "Llaves ULC codificadores" (Chiavi ULC codificatori) se desactiva primero, cuando todos los codificadores están actualizados; luego la distribución pasa a las cerraduras. Cuando ambos widgets se apagan, la distribución de la llave de criptografía ULC ha terminado.

Se puede ver el estado actualizado de las cerraduras en la vista Zonas de acceso (Zone accesso) del SSW. La columna *Llave ULC (Chiave ULC)* muestra uno de los siguientes íconos:

	Not updated
	Pending
	Updated

Cuando todas las cerraduras marcadas como *Activa* tienen el ícono verde, la distribución de la llave de criptografía ULC ha terminado.

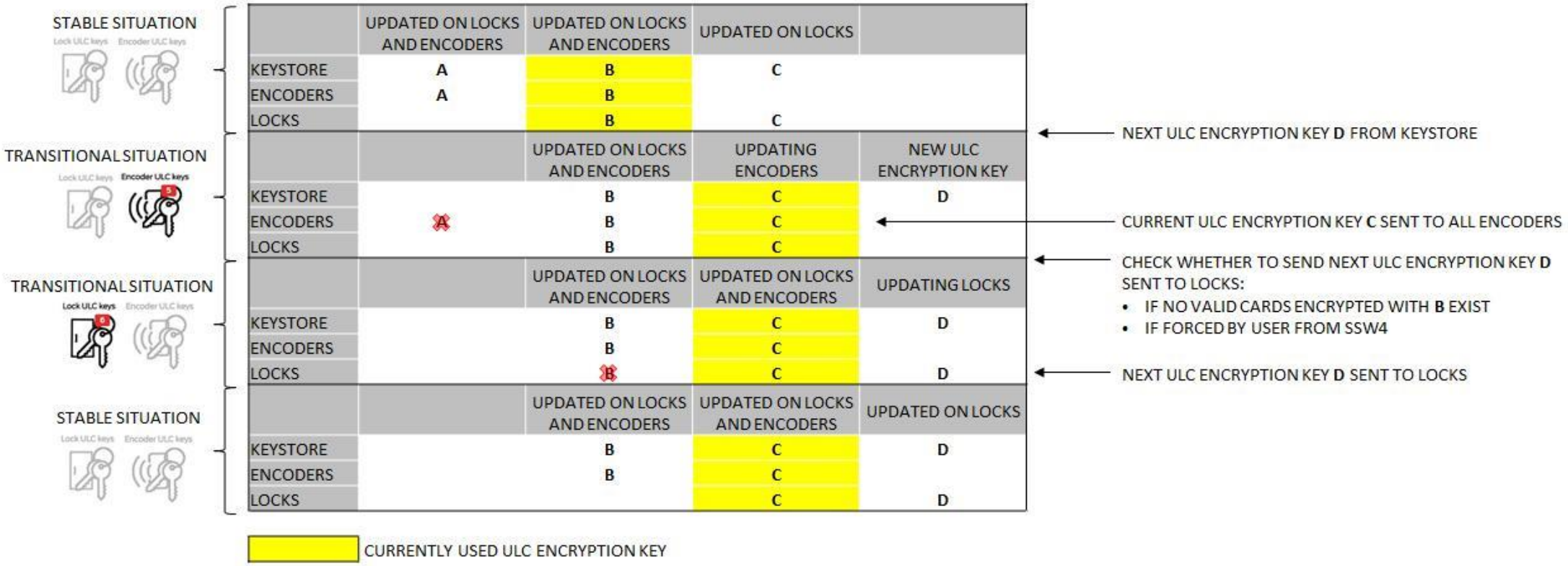
Codificación con llaves de criptografía ULC

Cuando la distribución de la nueva llave de criptografía ULC entre codificadores y cerraduras activas ha terminado, esta nueva llave se utiliza para encriptar las nuevas tarjetas ULC.

La llave de criptografía ULC utilizada para encriptar cada tarjeta de cliente puede ser visualizada en la vista Tarjetas del SSW. La columna *Llave ULC (Chiave ULC)* muestra uno de los siguientes íconos:

	Undefined (No ULC Key)
	Previous
	Current
	Next

Todas las tarjetas encriptadas con la llave actual ULC pueden ser leídas por las cerraduras, mientras que las codificadas con las llaves viejas ya no se pueden leer.



	UPDATED ON LOCKS AND ENCODERS	UPDATED ON LOCKS AND ENCODERS	UPDATED ON LOCKS	
KEYSTORE	A	B	C	
ENCODERS	A	B		
LOCKS		B	C	

← NEXT ULC ENCRYPTION KEY **D** FROM KEYSTORE

		UPDATED ON LOCKS AND ENCODERS	UPDATING ENCODERS	NEW ULC ENCRYPTION KEY
KEYSTORE		B	C	D
ENCODERS	~~A~~	B	C	
LOCKS		B	C	

← CURRENT ULC ENCRYPTION KEY **C** SENT TO ALL ENCODERS

← CHECK WHETHER TO SEND NEXT ULC ENCRYPTION KEY **D** SENT TO LOCKS:
- IF NO VALID CARDS ENCRYPTED WITH **B** EXIST
- IF FORCED BY USER FROM SSW4

		UPDATED ON LOCKS AND ENCODERS	UPDATED ON LOCKS AND ENCODERS	UPDATING LOCKS
KEYSTORE		B	C	D
ENCODERS		B	C	
LOCKS		~~B~~	C	D

← NEXT ULC ENCRYPTION KEY **D** SENT TO LOCKS

		UPDATED ON LOCKS AND ENCODERS	UPDATED ON LOCKS AND ENCODERS	UPDATED ON LOCKS
KEYSTORE		B	C	D
ENCODERS		B	C	
LOCKS			C	D

CURRENTLY USED ULC ENCRYPTION KEY

CONTROLADOR ONLINE

El controlador especial de accesos online, combinado con un máximo de dos lectores de pared, permite controlar un punto de acceso usando un dispositivo de mando estándar (por ejemplo, strike electrónico, cerradura eléctrica o motorizada); este controlador se puede inicializar como puerta estándar, común o de servicio.

Cuando se presenta una tarjeta, la decisión entre abrir o no se basa en la existencia de datos offline en el lector (no hay ninguna solicitud online para el controlador).



El controlador trabaja también como validador: si una tarjeta ha sido creada con un cierto intervalo de validación, después de dicho intervalo perderá sus derechos de acceso. La validación se renueva cuando la tarjeta se presenta al validador.

El controlador también se puede utilizar para actualizar los derechos de acceso y para extender la validez a las tarjetas de servicio, si en el Smart Software han sido configuradas para la recodificación.

Además, el controlador puede recoger los datos del historial en la tarjeta, si esta función ha sido activada en el momento de la creación de la instalación.

MANTENIMIENTO
CERRADURA eSIGNO

ESTADO DE LA BATERÍA

El control del estado de la batería se puede realizar utilizando cualquier tarjeta de servicio válida; existen 2 niveles diferentes de aviso:

- batería descargada: el led emite 3 destellos rojo + verde antes de la apertura;
- batería muy descargada: el led emite 6 destellos rojo + verde antes de la apertura;
- batería agotada: el led emite 12 destellos rojo + verde; la cerradura no se abre. Estos avisos se registran en el historial de la cerradura como eventos separados de las aperturas.

Procedimiento para el cambio de las baterías:

- con la herramienta correspondiente, extraiga el plástico inferior de la placa externa;
- desconecte el portabaterías presionando la traba central;
- sustituya las baterías (se requieren 3 pilas alcalinas AAA LR3). Atención: Riesgo de explosión si la batería es sustituida con otra de tipo incorrecto. Elimine las baterías usadas según las instrucciones







CILINDRO MECÁNICO DE EMERGENCIA

Las cerraduras electrónicas siempre están dotadas de un cilindro mecánico de emergencia.
El cilindro trabaja con 3 llaves diferentes (numeradas de 1 a 3):

- la llave número 1 se debe utilizar en primer lugar;
- si la llave número 1 se ha extraviado o no se considera segura, se puede usar la llave número 2. En este caso, el uso de la llave número 1 queda inhabilitado;
- de la misma forma, utilizando la llave número 3 se inhabilita la llave número 2.

Independientemente de la llave que se está utilizando, siga el procedimiento que se describe a continuación:

- acceda al cilindro mecánico quitando el plástico inferior de la placa externa, utilizando la herramienta correspondiente (véase la figura anterior);
- introduzca la llave mecánica y gírela 360° en sentido dextrógiro;
- gire el pomo (o la manilla externa).

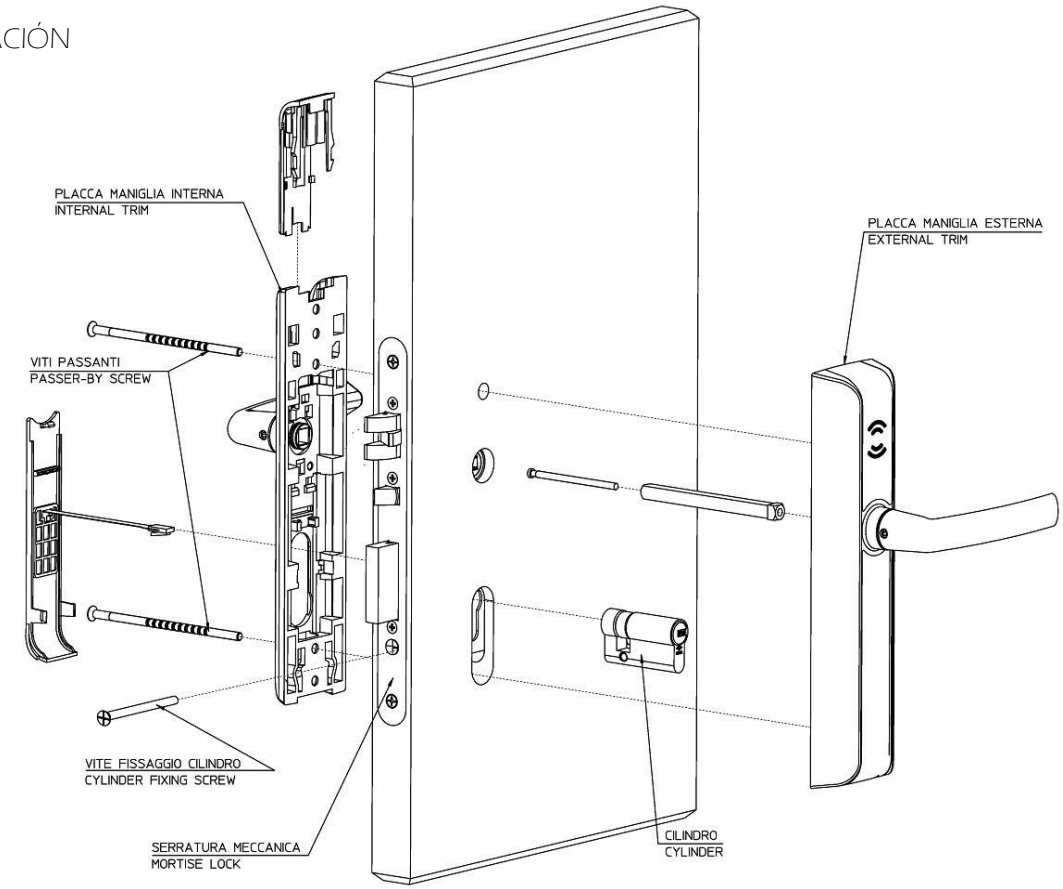
MANTENIMIENTO

MANTENIMIENTO Y LIMPIEZA

El incumplimiento de las siguientes indicaciones puede causar daños irreparables en el producto.

- Protección contra detergentes que contienen ácidos: limpie las cerraduras solo con un paño suave y detergentes con pH neutro diluido. No use detergentes agresivos que contengan ácidos.
- Protección contra el ácido tánico: este puede evaporar de puertas de roble u otras maderas con elevado contenido de tanino; verifique que la cerradura no esté en contacto directo con una superficie de madera no tratada.
- Protección contra selladores: no utilice selladores acéticos o que contengan otras sustancias agresivas (por ejemplo, ácido fórmico o acético, amoníaco, aldehídos, fenoles, cloro, etc.); tanto el contacto directo con el sellador como los vapores de estas sustancias pueden afectar la superficie de la cerradura.
- Durante las obras en general (demolición, remodelación, revoque y pintura), proteja las cerraduras del contacto con polvo, cal, revoque, pinturas y esmaltes. Ventile el local antes de quitar las protecciones. Consejo: coloque las cerraduras después de realizar los trabajos y de verificar que el local ha sido bien ventilado.

INSTALACIÓN



OPERACIONES DE SERVICIO

MANTENIMIENTO
CERRADURA eGO

ESTADO DE LA BATERÍA

El control del estado de la batería se puede realizar utilizando cualquier tarjeta de servicio válida; existen 3 niveles diferentes de aviso:

- batería descargada: el led emite 3 destellos rojo + verde antes de la apertura;
- batería muy descargada: el led emite 6 destellos rojo + verde antes de la apertura;
- batería agotada: el led emite 12 destellos rojo + verde; la cerradura no se abre. Estos avisos se registran en el historial de la cerradura como eventos separados de las aperturas.

Procedimiento para el cambio de las baterías:

- extraiga el plástico superior de la placa interna;
- desenrosque el tornillo superior de la placa interna;
- extraiga el portabaterías;
- sustituya las baterías (se requieren 4 pilas alcalinas AAA LR3). Atención: Riesgo de explosión si la batería es sustituida con otra de tipo incorrecto. Elimine las baterías usadas según las instrucciones;
- coloque el portabaterías, enrosque el tornillo superior y coloque el plástico superior en la placa interna







CILINDRO MECÁNICO DE EMERGENCIA

Siga el procedimiento que se describe a continuación:

- acceda al cilindro mecánico quitando el plástico inferior de la placa externa;
- introduzca la llave mecánica y gírela 360°;
- gire el pomo (o la manilla externa).

MANTENIMIENTO Y LIMPIEZA

Véase el párrafo en la sección "Cerradura eSIGNO"



OPERACIONES DE SERVICIO

MANTENIMIENTO
CERRADURA eFLEXO

ESTADO DE LA BATERÍA

El control del estado de la batería se puede realizar utilizando cualquier tarjeta de servicio válida; existen 3 niveles diferentes de aviso:

- batería descargada: el led emite 3 destellos rojo + verde antes de la apertura;
- batería muy descargada: el led emite 6 destellos rojo + verde antes de la apertura;
- batería agotada: el led emite 12 destellos rojo + verde; la cerradura no se abre. Estos avisos se registran en el historial de la cerradura como eventos separados de las aperturas.

Procedimiento para el cambio de las baterías:

- Desenrosque el plástico interno
- Sustituya las baterías (se requieren 4 pilas alcalinas AA LR3). Atención: Riesgo de explosión si la batería es sustituida con otra de tipo incorrecto. Elimine las baterías usadas según las instrucciones
- Enrosque el plástico interno





CILINDRO MECÁNICO DE EMERGENCIA

Siga el procedimiento que se describe a continuación:

- introduzca la llave mecánica y gírela 360°;
- gire el pomo (o la manilla externa).

MANTENIMIENTO Y LIMPIEZA

Véase el párrafo en la sección "Cerradura eSIGNO"

MANTENIMIENTO
E-CYLINDER ESIGNO

ESTADO DE LA BATERÍA

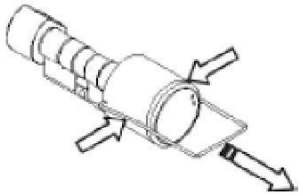
El control del estado de la batería se puede realizar utilizando cualquier tarjeta de personal (utilizada para el personal). En caso de batería descargada, el cilindro emite tres destellos rojos + verdes antes de abrir la puerta.

Nota: En caso de batería inutilizable (si no ha sido cambiada, no obstante las indicaciones ilustradas previamente), después de algunas aperturas el cilindro deja de reaccionar con las tarjetas válidas. Para reactivarlo, es necesario cambiar las baterías, utilizando el adaptador de alimentación externo.

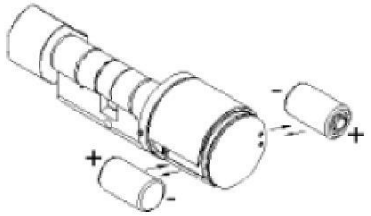
Procedimiento de sustitución de las baterías

1. Presente una tarjeta de cambio de baterías (emitida en modo HHI).
2. Las dos trabas que mantienen bloqueada la cubierta de la cabeza del cilindro se vuelven retráctiles; extraiga la cubierta del cilindro, utilizando la herramienta correspondiente.
3. Sustituya las baterías (2 x 3 V tipo CR-2 de litio); si la polaridad es correcta, el cilindro emite un tono. Atención: Riesgo de explosión si la batería es sustituida con otra de tipo incorrecto. Elimine las baterías usadas según las instrucciones
4. Presione las dos trabas y coloque la cubierta, verificando que las trabas queden en la posición correcta.
5. Presente nuevamente una tarjeta de cambio de baterías. Las dos trabas permanecen bloqueadas.
6. Presente una tarjeta de sincronización para comunicar al cilindro la fecha y la hora actualizadas.

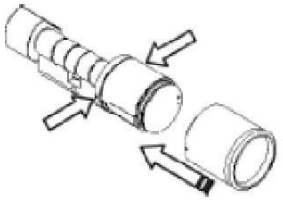
2



3



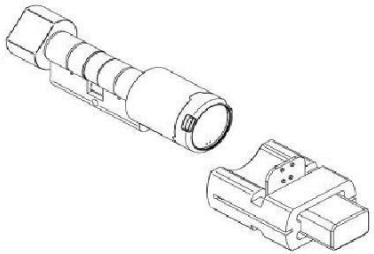
4



Adaptador de alimentación externo

Si las baterías son completamente inutilizables, es necesario usar el adaptador de alimentación externo para restablecer el funcionamiento del cilindro. Para hacerlo, quite el disco con el logotipo, utilizando la ventosa correspondiente, y conecte el adaptador, verificando que las patillas de alimentación coincidan con las de alimentación externa de la manilla. Si la posición es correcta y las baterías están agotadas, el cilindro emite un tono.

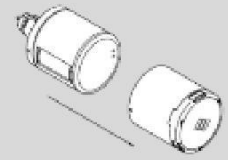




OPERACIONES DE SERVICIO

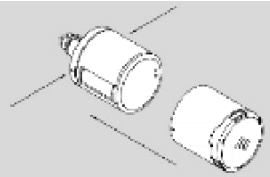
INSTALACIÓN E-CYLINDER

1. Extraiga la manilla electrónica del envase y quite el cárter de la manilla electrónica.

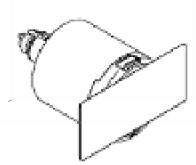


2. Extraiga la lengüeta de plástico del alojamiento de una de las dos baterías dentro de la manilla electrónica.

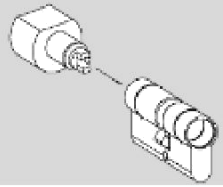
3. Coloque el cárter en la manilla electrónica, siguiendo las guías correspondientes. Presionando las trabas laterales de la manilla, complete la colocación del cárter. Verifique que las trabas laterales sobresalgan nuevamente dentro de los orificios presentes en el cárter.



4. Emita una tarjeta de inicialización con el codificador eSIGNO en modo HHI y preséntela inmediatamente al cilindro; mantenga la tarjeta delante del cilindro hasta visualizar la señal de inicialización (dos tonos y 3 destellos verdes, seguidos por un destello rojo).

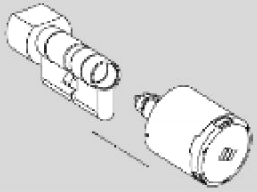


5. Coloque la manilla mecánica en el cuerpo del cilindro, rotando y ejerciendo una ligera presión, hasta oír el clic de enganche.
   Nota: Si se debe instalar una manilla electrónica en ambos lados, el cuerpo mecánico debe tener al menos 30-35 mm.

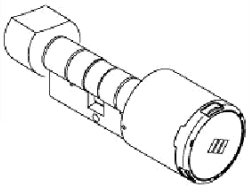


6. Introduzca el cuerpo del cilindro en el orificio de la puerta, fijándolo con el tornillo suministrado.

7. Introduzca la manilla electrónica (previamente inicializada) en el cuerpo del cilindro colocado en la puerta, y gírela hasta oír el clic de enganche.

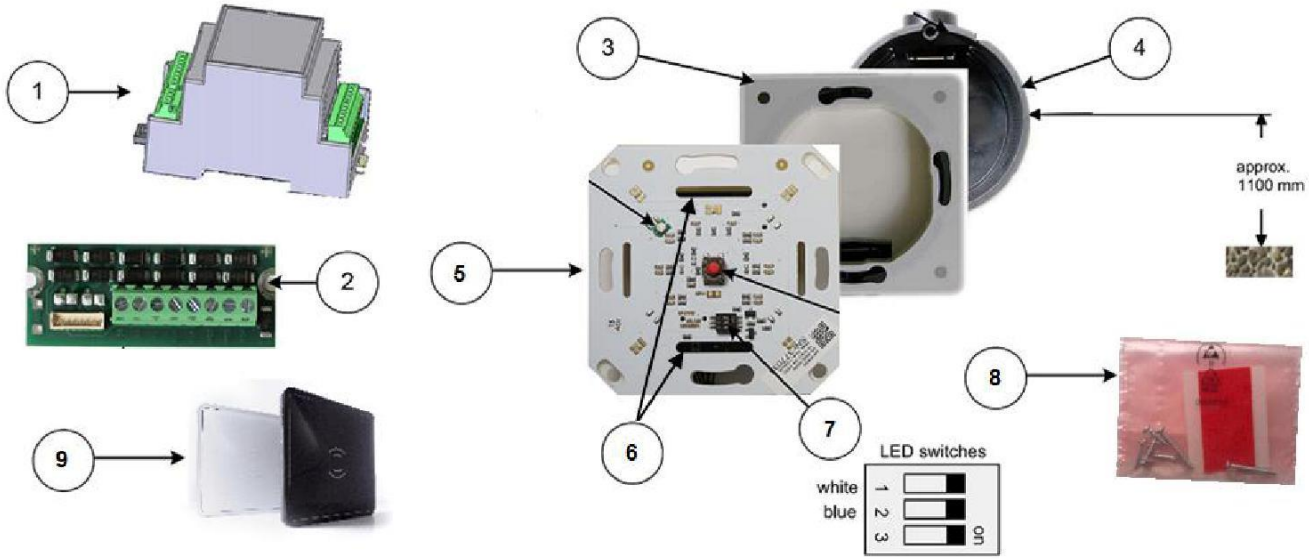


8. El cilindro electrónico está correctamente instalado.



MANTENIMIENTO
eSIGNO WALL READER GLASS

COMPONENTES



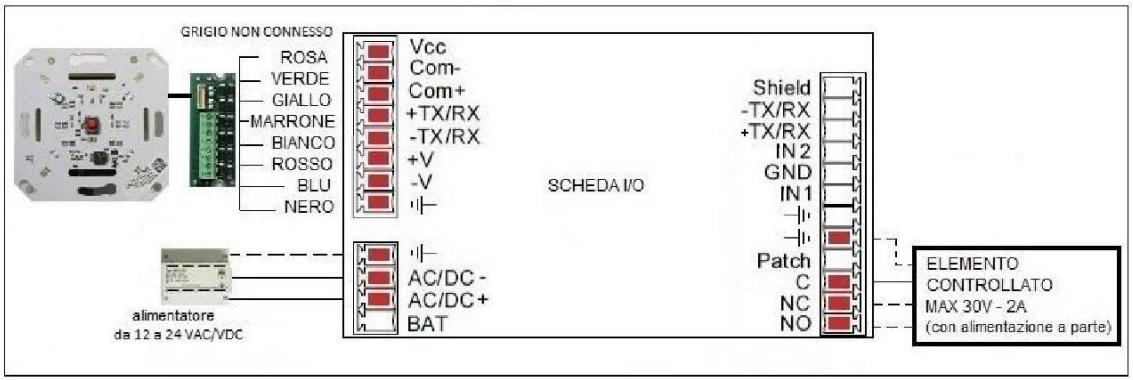
1	Tarjeta de I/O con relé	6	Orificios de fijación para la cubierta de vidrio
2	Tarjeta terminal con cinta adhesiva	7	Interruptor DIP para regulación led
3	Elemento de protección para lector RFID	8	Material para montaje en caja de empotrar
4	Caja de empotrar (por ejemplo, 502E, no incluida)	9	Cubierta de vidrio con clips metálicos de fijación
5	Lector RFID con cable de 7 polos		

INSTALACIÓN

1. Instale los cables. Para cumplir los valores EMC requeridos, es necesario utilizar los cables indicados en la tabla, conectándolos tal como se muestra en la figura. Verifique la longitud de los cables: eventuales extensiones pueden causar disfunciones.
2. Para este producto, utilice una caja de empotrar cuadrada (tipo 502E) o redonda (tipo PB502); instálela en la pared (a una altura recomendada de 1.1 m), de tal forma que los tornillos de fijación queden en la parte superior y en la parte inferior.
    - La distancia mínima con respecto a otros dispositivos RFID debe ser de 30 cm.
    - Si el dispositivo se fija en una superficie metálica, la distancia de lectura se reduce.
3. Fije la tarjeta terminal en la caja de empotrar, usando la cinta adhesiva incluida en el suministro.
4. Instale la tarjeta I/O en un lugar seguro para evitar manipulaciones (por ejemplo, dentro de una caja de derivación, junto con la alimentación).



OPERACIONES DE SERVICIO



5. Conecte la tarjeta terminal a la tarjeta I/O (véase la figura anterior).
6. Conecte el elemento controlado a la tarjeta I/O: esta puede controlar un elemento controlado de hasta 30 V - 2 A, con un contacto normalmente abierto (NA) o normalmente cerrado (NC). El elemento controlado requiere una alimentación aparte; no se debe utilizar la del lector de pared.
7. Conecte la alimentación a la tarjeta I/O: la alimentación se debe suministrar con un elemento de 12 a 24 Vca/Vcc (es posible utilizar el artículo CISA código 07302.08.0). Atención: La conexión a la red eléctrica a 230 V debe ser realizada por electricistas profesionales. En caso de conexión errónea, subsiste el peligro de descargas eléctricas, que pueden causar graves lesiones o la muerte.
8. Conecte el cable de 7 polos proveniente del lector RFID a la tarjeta terminal.
9. Coloque el lector dentro de la caja de empotrar, de tal forma que los orificios de fijación para la cubierta queden en la parte superior y en la parte inferior.
10. Active el lector de pared Glass eSIGNO, encendiendo la alimentación.
11. Ponga en la posición deseada los interruptores DIP que regulan los leds. A continuación se muestran los valores por defecto, según el color de la cubierta de vidrio.

Cubierta de vidrio	1 (Leds blancos – stand-by)	2 (Leds azules – stand-by)	3 (Leds verdes/rojos - funcionamiento)
Vidrio blanco	OFF	ON	ON
Vidrio negro	ON	ON	ON

12. Fije delicadamente la cubierta de vidrio en el lector RFID, usando los clips metálicos. No use objetos puntiagudos para quitar la cubierta (pueden destruir la cubierta); por el contrario, tire delicadamente.

SINCRONIZACIÓN

En caso de interrupción de la alimentación principal, el lector de pared mantiene su sincronización durante 2 días aproximadamente. Después de este tiempo, el lector de pared podría perder la referencia fecha/hora, mostrando 5 destellos rojos acompañados por un tono cuando se presenta una tarjeta cualquiera; en este caso, es necesario sincronizar de nuevo el lector de pared con el dispositivo HHI:

- Directamente con el ratón eSIGNO, pulsando el botón SYNCHRO;
- Creando una tarjeta de sincronización desde el menú Service Card y presentándola al lector de pared. Si la tarjeta se lee correctamente, el lector de pared emite 2 destellos rojo + verde, acompañados por 2 tonos.



OPERACIONES DE SERVICIO

MANTENIMIENTO
eSIGNO ENERGY SAVER

• Energy saver **multiestándar**. Funciona con tarjetas de proximidad CISA eSIGNO y Wave Mode CT2, CT3 y CT4, Mifare Classic (CT5 y CT6) y Mifare Ultralight;
permite interceptar e impedir el uso impropio de objetos o tarjetas diferentes de las indicadas.

• Identificación del tipo de tarjeta: las tarjetas de cliente activan dos salidas, que pueden controlar **dos telerruptores** (no incluidos); las tarjetas de personal controlan solo uno. Posibilidad de controlar un solo telerruptor (activado por ambos tipos de tarjeta).

• Por defecto, el energy saver controla las salidas como **normalmente sin tensión**; para modificar esta configuración, el dispositivo debe ser adecuadamente inicializado.

• Posible combinación con transformador (art. 07302.08.0) y telerruptores (art. 07302.10.0).

CARACTERÍSTICAS TÉCNICAS (versión B.02.01)

Energy saver multiestándar eSIGNO 1A0501.06.0(.45)	
Alimentación	24 Vca ± 10 % a 50 Hz
Tensión máx. de salida	24 Vca
Potencia absorbida máx.	1 VA
Potencia de salida	2 x 5 VA
Corriente máx. CMOS	500 mA por canal
Temperatura de funcionamiento	0-50 °C
Humedad relativa	0-90 %
Dimensiones (L x H x P)	70 x 60 x 30 mm
Espesor tarjeta máx.	0,75 mm
Transformador 07302.08.0	
Entrada/salida	220 Vca /12-24 Vca
Potencia	15 VA
Para barra DIN 35, tipo Omega y C	
Telerruptor 07302.10.0	
Alimentación	24 Vca a 40-60 Hz
Contactos	3 NA, 1 NC
Potencia máx. contactos	20 A AC1 - 2.2 kW AC3
Para barra DIN 35, tipo Omega y C	

Este energy saver está listo para ser instalado (véase el esquema) y utilizado, con las siguientes configuraciones:
- reconocimiento de todas las tarjetas eSIGNO y Wave Mode CT2, CT3 y CT4;
- reconocimiento de sector (01) y contraseña (FFFFFFFFFFFF) estándar para Mifare Classic;
- reconocimiento de desviación estándar (00) para Mifare Ultralight;
- ningún control sobre código de instalación y número de habitación;
- salidas controladas como normalmente sin tensión.

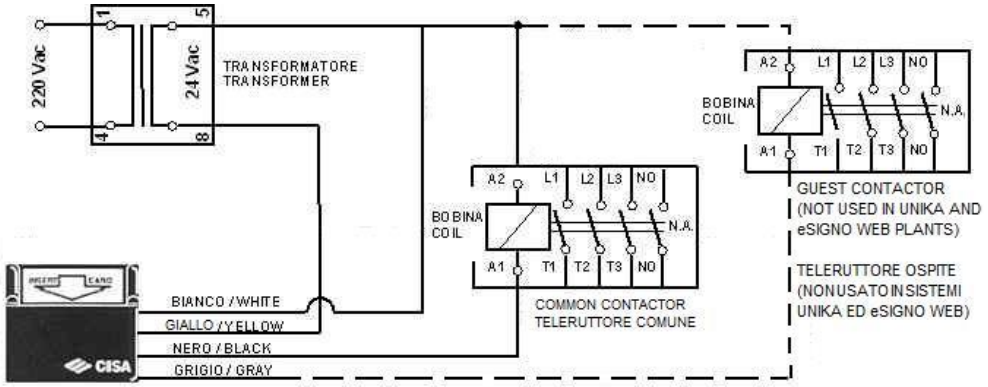
Si se requieren configuraciones diferentes, se ruega consultar el párrafo Inicialización, que puede verse a continuación.

INSTALACIÓN

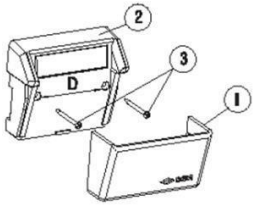
Cableado

Para controlar ambos telerruptores, siga el esquema que se muestra en la figura. Si no se debe conectar el telerruptor huésped, ignore la rama punteada (no conecte el cable gris).

Si el energy saver está conectado, los leds frontales se encienden.

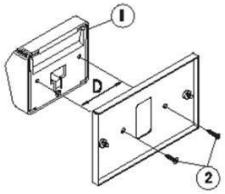


Fijación a la pared



- Quite la cubierta, forzándola lateralmente (1), para acceder a los dos orificios (2) pasantes Ø 3 mm.
- Fije con los dos tornillos (3) 2,9 x 32 mm suministrados.
- Coloque la tapa en su alojamiento.

Fijación en la caja de mecanismos



- Utilice los dos orificios Ø 2 mm (1).
- Fije el energy saver en la placa con tornillos autorroscantes de cabeza cilíndrica M 2,9 x 9,5 (UNI 6954) o equivalentes (2), no suministrados.

INICIALIZACIÓN

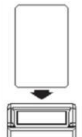
Esta operación se debe realizar si se requieren configuraciones diferentes de las configuraciones por defecto (por ejemplo, instalaciones con integraciones). En este caso, mediante un encoder CISA, es necesario crear una tarjeta init estándar con soporte CT4:

- las configuraciones personalizadas Mifare Classic y Ultralight se transfieren automáticamente del encoder a la tarjeta init;
- para controlar las salidas como normalmente en tensión, use una tarjeta init para cualquier cerradura con la función Oficina habilitada; para mantenerlas como normalmente sin tensión, use una tarjeta init para una cerradura con la función Oficina inhabilitada;
- una vez inicializado, el energy saver funciona solo con tarjetas emitidas para la instalación en cuestión. Para inicializar el energy saver con un número de habitación (que será tomado de la primera tarjeta de cliente presentada después de la inicialización), cree una tarjeta init para una cerradura cualquiera con la función Inhabilitar Privacy seleccionada.

La correcta inicialización está indicada por 5 destellos de los leds. Para volver a poner el energy saver a los valores de fábrica, presente una tarjeta de reset codificada con soporte CT4 (operación realizada correctamente indicada por 2 destellos de los leds).

USO

Con el energy saver encendido, la introducción de una tarjeta de huésped provoca la habilitación de ambos telerruptores, mientras que la introducción de una tarjeta de servicio provoca la habilitación de un solo telerruptor. Cuando se extrae la tarjeta, los telerruptores se inhabilitan después de 50 segundos. Si hay un solo telerruptor instalado, es habilitado por ambos tipos de tarjeta.



APÉNDICE

EVENTOS DE HISTORIAL

Esta tabla enumera las operaciones posibles, visualizables en los historiales de la cerradura:

Operaciones del historial de la cerradura	Descripción
Cliente	Una tarjeta del tipo indicado ha sido presentada a la cerradura
Servicio 1-4	
Usuario 1-4	
Tarjeta de emergencia	
Tarjeta de peligro	
Tarjeta de fin peligro	
Tarjeta monouso	
Tarjeta de bloqueo	
Tarjeta de desbloqueo	
Tarjeta de sincronización	
Cancelar cliente	Una tarjeta de cancelación para una tarjeta del tipo indicado ha sido presentada a la cerradura
Cancelar servicio 1-4	
Cancelar usuario 1-4	
Cancelar tarjeta de emergencia	
Tarjeta de cliente recodificada	La tarjeta de cliente ha sido recodificada
Función Privacy activa/inactiva	La función Privacy está activa/inactiva
Función Oficina activa/inactiva	La función Oficina está activa/inactiva
Preparación habitación	La función Preparación habitación ha sido activada
Apertura interna	La cerradura ha sido abierta desde adentro
Control palanca	Controlar palanca (véanse las indicaciones led)
Puerta no abierta	La puerta no ha sido abierta después de una tarjeta válida
Puerta cierre retardado	La puerta ha permanecido abierta durante al menos 1 minuto
Puerta abierta desde hace	En el momento del cierre, la puerta había estado abierta durante N minutos
Diagnóstico: estado cerr.	Eventos de diagnóstico de la cerradura
Diagnóstico: encendido	
Nivel de batería bajo	Las baterías de la cerradura están casi descargadas
Baterías descargadas	Las baterías de la cerradura están descargadas
Batería extraída	Las baterías han sido extraídas de la cerradura
Tarjeta recodificada	La tarjeta ha sido recodificada
Tarjeta validada	La tarjeta ha sido validada

Operaciones del historial de la cerradura	Descripción
Emergencia mecánica	La puerta ha sido abierta utilizando un cilindro mecánico
Emergencia sin baterías	La puerta ha sido abierta utilizando un cilindro mecánico sin baterías
Fin de emergencia	Cierre de la puerta después de la apertura con cilindro mecánico
Montar/desmontar	Cilindro electrónico en modo Montar/desmontar
Cambio de baterías	Cambio de baterías del cilindro electrónico
Manipulac. cil.	Cilindro electrónico manipulado
Err. motor cil.	Error en el movimiento del motor del cilindro
Auto-oficina activo/inactivo	Activación/desactivación de la autoprogramación indicada
Auto-bloqueo/desbloqueo	
Motor on	Activación del motor del dispositivo
Actualiz. autoprogramación	Los datos de la cerradura (autoprogramación, parámetros, tablas hora legal, días festivos, lista de cancelación o datos de recodificación) han sido actualizados en forma wireless .
Actualiz. parámetros	
Actualiz. DST	
Actualiz. días festivos	
Actualiz. lista cancelación	
Actualiz. datos recodificación	
Apertura remota cerradura	La cerradura ha sido abierta a distancia
Nuevo elemento lista cancel.	Un elemento ha sido agregado/quitado de la lista de cancelación de la cerradura
Elemento lista cancel quitado	
HHI apertura/init/sincro	Operaciones realizadas desde HHI
Carga historial	
Carga lista de cancelación	
Controlador online/offline	El dispositivo ha cambiado su estado a online/offline
Gateway online/offline	
Repetidor online/offline	
Puerta online/offline	
Lector de pared online/offline	
Campus Ack	Un registro ha sido cancelado manualmente desde el widget del dashboard especificado

EVENTOS DE HISTORIAL

Esta tabla enumera las operaciones posibles, visualizables en los historiales de codificación:

Operaciones historial de codificación	Descripción
Dispositivo encendido/apagado	Estado del dispositivo
Login	Se ha realizado la operación de login/logout
Logout	
Check-in cliente	Se ha realizado el check-in de un huésped (ahora su tarjeta es válida)
Check-out cliente	Se ha realizado el check-out de un huésped (su tarjeta ya no es válida)
Codificación tarjeta de operador	Una tarjeta del tipo indicado ha sido codificada
Codificación cliente	
Codificación servicio 1-4	
Codificación usuario 1-4	
Codificación tarjeta de emergencia	
Codificación tarjeta de fin peligro	
Codificación tarjeta de peligro	
Codificación tarjeta monouso	
Codificación tarjeta init	
Codificación tarjeta de bloqueo/desbloqueo	
Codificación tarjeta de cliente futura	Una tarjeta de cliente con validez futura ha sido codificada
Copia tarjeta de cliente	Se ha copiado una tarjeta de cliente
Cambio de contraseña operador	La contraseña de la tarjeta de operador ha sido modificada
Cancelar tarjeta de operador	Una tarjeta de cancelación para una tarjeta del tipo indicado ha sido codificada
Cancelar cliente	
Cancelar servicio 1-4	
Cancelar usuario 1-4 Cancelar emergencia	
Recodificación operador	Ha sido configurada la recodificación para una tarjeta del tipo indicado
Recodificación servicio 1-4 Recodificación usuario 1-4	
Tarjeta suspendida	La tarjeta ha sido suspendida
Tarjeta restablecida	La tarjeta ha sido restablecida

Operaciones historial de codificación	Descripción
Modificación recodificación operador	Ha sido modificada la recodificación para una tarjeta del tipo indicado
Modificación de recodificación servicio 1-4 Modificación de recodificación usuario 1-4	
Cancelar recodificación operador	
Cancelar recodificación servicio 1-4	Ha sido cancelada la recodificación para una tarjeta del tipo indicado
Cancelar recodificación usuario 1-4	
Tarjeta recodificada	La tarjeta ha sido recodificada
Conexión de tarjeta para crear	La tarjeta para crear ha sido generada, con enlace a la tarjeta original
Error de verificación	Se ha verificado un error de verificación durante la grabación de la tarjeta
Mantenimiento	Codificador en modo de mantenimiento
Reconstrucción	Reconstrucción de la base de datos del codificador
Apertura remota cerradura	La cerradura ha sido abierta a distancia
Actualiz. parámetros	Modificación de los parámetros de la cerradura
Actualiz. autoprogramación	Modificación autoprogramación de la cerradura

EVENTOS DE HISTORIAL

Esta tabla enumera los posibles resultados de las diferentes operaciones visualizables en los historiales:

Resultados operaciones	Descripción
Resultado	Operación realizada correctamente
Instalación errónea	La tarjeta es válida para otra instalación
Zona errónea	La tarjeta es válida para otra zona
Aún inválida	La tarjeta aún no es válida (futura)
Tarjeta caducada	La tarjeta ha caducado
Día de la semana erróneo	La tarjeta es válida en otros días de la semana
Tarjeta anterior	La tarjeta presentada ha sido invalidada por la emisión de una tarjeta de cliente más reciente
Bloqueo	La tarjeta presentada pertenece a un nivel bloqueado en la cerradura
Lista negra	La tarjeta presentada está en la lista negra de la cerradura
Número de tarjeta erróneo	La tarjeta presentada ha sido creada en el mismo minuto que la anterior (por lo tanto, no es válida). Esto puede ocurrir solo para tarjetas emitidas en modo Fallo
Fuera de los turnos horarios	La tarjeta es válida solo en otros turnos
Huésped en la habitación	La función Privacy está activa
No autorizado	Usuario no autorizado para ejecutar la operación
Error de comunicación	Operación no terminada a causa de un error de comunicación
Ya inicializado	El dispositivo ya está inicializado
No memorizado	Tarjeta no memorizada e intento de apertura con CLC
Crédito insuficiente	La tarjeta no contiene suficientes créditos para permitir el acceso.
Lista negra llena	La lista negra de la cerradura está llena
Historial en la tarjeta lleno	La memoria de la tarjeta está llena (en referencia a la utilización del historial)
Tarjeta no validada	La tarjeta no ha sido validada
Tarjeta suspendida	La tarjeta ha sido suspendida
Fallo	Operación no completada a causa de un fallo
Fallo (de 1 a 10)	Operación no completada a causa de un fallo (mensaje debug)

CAPACIDAD TARJETA DE HISTORIAL

La siguiente tabla indica el número máximo de operaciones que pueden estar contenidas como historial en cada tipo de tarjeta:

Tipo de tarjeta	Descarga historial (keyplan 1024)	Descarga historial (keyplan 2032)	Historial en la tarjeta (keyplan 1024)	Historial en la tarjeta (keyplan 2032)
CS3	15	5	30	12
CS4	0	0	0	0
CS7 Enhanced	15	5	30	12
CT3	0	0	0	0
CT4	15	5	30	10
CT5 (MIFARE 4KB)	200	188	392	372
CT6 (MIFARE 1KB)	30	18	56	36

CONFIGURACIONES DE SISTEMA

Las siguientes tablas indican los límites de cada configuración compatible con el Smart Software

WAVE MODE

	M201 512K Camas	M201 512K Camas 650 Habit
Ajustes	500	650
Common + Util.	50+1024	65+1024
Zonas	100	130
Suites (Guests)	25	33
Camas	1500	0
Historial	2000	2600
Tarjetas creadas	3250	3250
Operadores	183	208
Categorías	250	324

eSIGNO

M305 2 MB	M305 8 MB	M305 2 MB (Código cuenta)	M305 8 MB (Código cuenta)
1500	5000	1500	5000
2182	2389	2182	2389
300	1000	300	1000
75	250	75	250
4500	15000	4500	15000
10500	32766	10500	32766
12000	16382	12000	16382
350	933	350	933
749	2499	749	2499

About Allegion

Allegion (NYSE: ALLE) helps keep people safe where they live, work and visit. Allegion is pioneering safety as a provider of security solutions through 23 brands in more than 120 countries. For more, visit **allegion.com**

CISA ■ Interflex ■ LCN ■ SCHLAGE ■ VON DUPRIN

ALLEGION™

© 2013 Allegion

Publication number, Rev. XX/XX
allegion.com