KABA

USER'S GUIDE

Next Generation FDU

PK3514_06_07

Front Desk Unit Reference Manual

First Edition

A publication of
KABA ILCO Inc.
7301 Decarie Blvd.
Montreal, Quebec,
Canada H4P 2G7

Printed in Canada, 2007
Copyright by KABA ILCO Inc., 2007
All rights reserved.

No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without prior written permission from the Publisher.

The information contained in this publication is accurate to the best of KABA ILCO Inc.'s knowledge.

Specifications are subject to change without notice.

PK3514_04_07

CE

American User's Information – FCC Compliance Statement

Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
The user may find the following booklet prepared by the federal Communications Commission helpful: 'How to identify and Resolve Radio-TV interference Problems." This booklet is available from the Government Printing Office, Washington, DC, 20402. Stock # 004-000-00345-4.

European User's Information – Declaration of Conformity

This device complies with the EMC Directive 89/336/EEC (amended by 92/31/EEC and 93/68/EEC for a class A digital device. It has been tested and found to comply with EN50081-2: 1993 (EN55011:1991) and EN50082-2:1995 (EN61000-4-2:1995 & ENV50140:1993).

Foreword

This manual describes the features, implementation, and proper use of the Kaba Lodging Access Control System. It is meant for use by management personnel, as a complement to our on-site training program. Step-by-step instructions for Guest Service Attendants are found in the Kaba Lodging Access Control System Front Desk User's Guide.

Do not distribute this book or parts thereof for general use.

Chapter 1: Introduction

1.1 The Kaba Ilco Lodging Access Control System

Kaba Ilco designed its Lodging Access Control System specifically for use in lodging facilities (hotels, resorts, dormitories, etc.), where the control of keys is a major concern. This system replaces traditional mechanical keys and locks with reusable keycards that use a unique, encrypted combination to grant access to the correct electronic locks throughout the property. These keycards are difficult to copy and the number of data combinations is so vast that guessing the code is virtually impossible. The access levels have been designed to allow each guest or staff member to carry a single keycard, for their own convenience, and to simplify the management of keycards.

In addition to its key control benefits, the system includes an audit trail in the electronic locks, Remote Access Controllers and Front Desk Units, which are used to encode keycards. These audit trails allow managers to know who entered a room, when they entered it, and who made the card that was used to gain entry.

The system supports a variety of electronic lock and card reader models, including the Solitaire lock series, Generation E-760 locks, 770 locks, and Remote Access Controllers. Some menus and functions of the Front Desk Unit and details of lock operation may differ depending on the version and configuration of the equipment.

1.2 How to Use This Manual

This manual is intended to be a practical reference for the implementation and use of the Kaba Ilco Lodging Access Control System. It explains the principles of the system, and provides a reference for the step-by-step operation of the system, for the system features, and for each type of keycard. This manual does not replace the training or retraining provided by the manufacturer, which is strongly recommended for a complete understanding of the system. For further information or for assistance, contact Kaba Ilco (see chapter 12).

1.3 Who Should Use This Manual

The information in this manual is a vital part of the security of the system and contains information not intended for general staff. The manual should be kept under lock and key, and should not be circulated. It is intended for reference by upper management and the System Administrator. A separate Front Desk User's Guide is available for reference by Guest Service Attendants, providing instructions for all operations of the system accessible using a Front Desk Authorization keycard. Contact Kaba Custimer Service or technical Support for more information.

1.4 Abbreviations and Symbols

Throughout this manual, the abbreviation FDU is used for the term "Front Desk Unit".

The names for different types of keycards (e.g. Guest, Floor, Front Desk Authorization), feature settings in the FDU, or other important concepts in the system are capitalized for easy recognition as shown below.

Alphabetical List of Abbreviations

BMA	Bellman's Master Authorization
DST	Daylight Savings Time
FDA	Front Desk Authorization
FDU	Front Desk Unit
GMA	General Manager Authorization
GSA	Guest Service Attendant
MA	Master Authorization
PA	Programming Authorization
PIN	Personal Identification Number
RAC	Remote Access Controller

Within this manual, symbols to be used on the Front Desk Unit keypad are enclosed between the signs < >. As example: when <?> is shown, this indicates that the "?" key should be pressed on the FDU keypad.

Chapter 2: System Components

The system makes use of eight major components:

- Keycards
- Electronic Locks and Remote Access Control systems (e.g. Solitaire 710-II, Generation E-760, 770, RAC 4XT, etc)
- Front Desk Unit
- Lock Communication Cable
- Printer
- Time
- Audits
- Interfaces

2.1 Keycards

In the system, keycards replace keys. Each guest receives a new keycard, which gives them access to only the lock on their suite, and to any allowed Common Areas such as the main entrance and elevator, or paid services such as parking or sport facilities. Staff also carry keycards for their access needs throughout the property. Different master key levels are provided to manage staff access.

Keycards as used in the system have many advantages over mechanical keys:

- Each time a room is rented, the lock is re-keyed automatically.
- Locks can be instantly re-keyed by authorized staff without dismantling the lock.
- Locks recognize a variety of Guest and Staff access levels, which can be re-keyed individually.
- Keycards have an expiry date, after which a lost or stolen keycard poses no threat to security.
- Keycards can be cancelled at any time, without dismantling the lock.
- Keycards are inexpensive.
- Returned keycards can be re-encoded and re-used many times.
- The information on the keycard is encrypted, and there is no way to determine from the data the specific room the keycard opens.

Keycards supplied by Kaba Ilco are standard 0.030" thick cards similar to those used in the banking industry. The keycard media uses a magnetic stripe, which is encoded with a unique pattern of magnetic fields containing the encrypted code.

Two types of keycards are available depending on the model of FDU spurchased: Low Coercivity (Lo-C) and High Coercivity (Hi-C). A Hi-C keycard requires more magnetic energy to encode information to it than a Lo-C keycard does. This also means that a Hi-C

keycard is less susceptible to accidental demagnetization by strong magnetic fields than a Lo-C keycard, but also costs more for replacement cards.

If a property requires personnel or guests to maintain keycards for extended periods of time then a Hi-C system may be considered, otherwise the standard Lo-C FDU system is all that is required for the vast majority of properties.

NOTE: FDUs can only encode one type of keycard, which is dependent on the system purchased. It is not recommended to have both types of systems on a property. If unsure of what type of FDU has been purchased please contact Kaba Ilco.

Figure 2.1: *Magnetic stripe keycards (front and back)*

Keycards are subject to erasure by strong magnetic fields.

Keycards may be unreadable by locks or the Front Desk Unit if they are scratched, bent or dirty. Worn out keycards should be discarded.

Keycards should be treated with the same respect as mechanical keys, and should *never* be identified by writing the room number on the keycard. (For more keycard security information, see chapter 9).

2.2 Electronic Locks

2.2.1 Door Locks

Kaba Ilco locks are battery-operated units that are installed, without wiring, on each door to provide access control throughout the property. Each lock is controlled by a microprocessor with an internal clock that is synchronized with the FDU *(see Section 2.6 - Time)*. The lock can read keycards, process the information on a keycard to determine whether the card is valid for accessing the room, and lock and unlock the electromechanical hardware that controls access to the room.

On the outside of the door, the lock has a card reader, indicator lights, and a handle attached to the housing. An infrared transceiver is located behind the indicator light. The lock communicates with the FDU by infrared light using a lock communication cable, to receive its programming or to download the audit trail *(refer to Section 2.7 - Audits)*. The Solitaire line has a medallion that conceals access to an electrical or mechanical override for use in emergencies *(refer to Section 10.1 – If a lock will not open)*. Generation E-760 locks and 770 locks feature electrical override capability that is activated by the FDU using a communication cable, and a drill point override located in the outside handle.

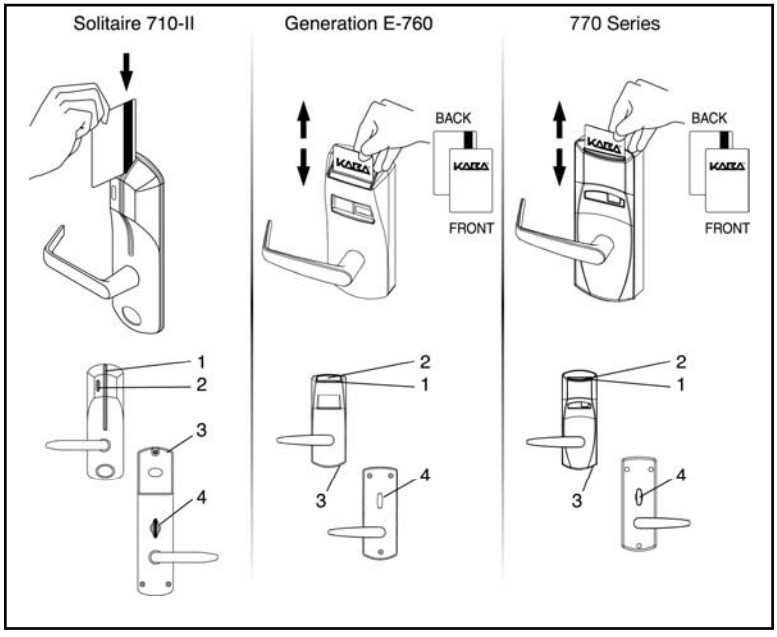


Figure 2.2.1: *Operating a door lock.*
Legend: (1) Reader Slot; (2) Indicator LEDs; (3) Battery Compartment; (4) Privacy Thumbturn

To operate the lock, the user simply inserts and removes their keycard as shown in the figure above, then turns the handle. The lock responds with visible and/or audible feedback *(refer to Section 5.2 – Lock Responses to Keycards)*.

The batteries, which are located in a compartment on the outside of the door for Generation E-760 & 770 locks, or on the inside of the door for other models, are standard alkaline AA batteries that are widely available, and can be purchased in a sealed pack from Kaba Ilco. The life of the batteries depends on the model and application of the lock. In general, they last two years, or approximately 80,000 insertions. Guest room doors are normally opened less frequently than Common Area doors or doors used primarily by staff, and their batteries tend to last longer.

2.2.2 Remote Access Controllers

For special doors that do not use a conventional lock, there are magnetic stripe card readers (figure 2.2.2) that can be mounted in a convenient location on a nearby wall. The card reader is connected to a Remote Access Controller (RAC) concealed in a panel box, which can control up to 8 relays (1 relay standard), in order to activate electronic devices such as elevator call buttons, magnetic locks or sliding doors.

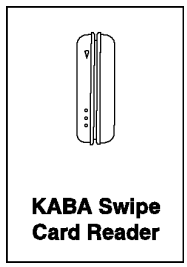


Figure 2.2.2

Card readers operate similarly to locks. In addition, RAC Models 3.5, 4 & 4XT card readers offer flexible time zones *(refer to Section 5.5 - Remote Access Controller Models 3.5 and 4 Flexible Time Zones)* for controlling access by Guest, Staff and Passage keycards. The most frequent application of card readers is for Common Area doors, such as the gym, pool & parking.

2.2.3 Exit Device Operators

An exit device operator is an electronic lock that connects with exit door hardware, such as a panic bar. Such a lock converts an exit-only door into a two-way door that permits guests and staff with a valid keycard to re-enter from the outside. The exit device is operated like any other lock, and is usually programmed as a Common Area door *(refer to section 2.2.5 – Types of Doors in the System)*.

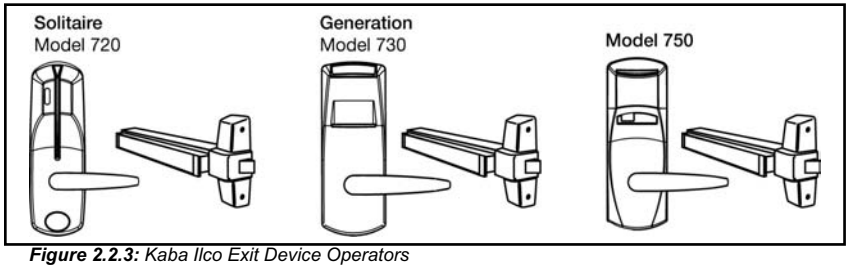


Figure 2.2.3: *Kaba Ilco Exit Device Operators*

2.2.4 Lock Addresses

Whatever the type of hardware (lock, card reader, exit device controller, etc.), each lock in the system contains a list of addresses in its memory that is programmed using the FDU. The addresses tell the lock the door that it controls and the lock opens only for keycards with the correct address, date and time. An incorrect address, date or time will result in access being denied. An example of the addresses in a lock is shown below. For more information, refer to *Section 5.3.1 – Lock Addresses*.

Address Level	Room #501	Room #502
Guest	501	502
Section	10	10
Floor	5	5
Group	2	2
Zone	10	10
Area	1	1

Table 2.2.4: *The lock or card reader on each door has its own unique set of addresses*

2.2.5 Types of Doors in the System

In addition to having a specific address, each lock in the system has a specific door type, or profile, according to the type of suite it controls. The FDU programs this profile when the addresses are set. The profile affects the pattern of addresses that must be programmed into the lock. For example, a Restricted Area door can only be opened by a Restricted Area keycard with the correct address or by the Emergency keycard, but guests, authorized staff, master keys and the Emergency keycard can open a guest room door. The same lock hardware can be used for both doors with the only difference between the two locks being in the programming set using the FDU *(refer to Chapter 5: Locks – Using and Programming)*.

The different types of doors used in the system are as follows:

Guest	*All guest room doors, except for Common Door Suites. Includes meeting and conference rooms, and suites that can be rented as a single unit.*
Common Door Suites/ Inner Doors	*Suites with a common door where the rooms inside can be rented separately or together.*

Guest Common Area	*Doors accessible by groups of guests, using the same keycard that also gives them private access to their own room or suite. Staff access can also be permitted. Examples: pool, parking, elevator.*
Staff Common Area	*Doors accessible by groups of staff, using the same keycard that gives them access to the doors they require for their work. Examples: locker rooms, cafeteria, staff lounge.*
Restricted Area	*Doors to sensitive areas such as computer rooms, General Manager's office, liquor storage rooms, etc.*

2.3 Front Desk Unit

The Front Desk Unit (FDU) is a portable computer console that runs the system. The FDU contains a 128 x 64 dot LCD display screen, a keypad, and a manual swipe card encoder for writing information to, and reading information from, magnetic stripe keycards. The encoder has no moving parts and requires very little service other than the occasional cleaning. The FDU operates on 9VDC power, which is supplied by the power pack provided by Kaba Ilco for either 110VAC/60Hz or 220VAC/50Hz electrical lines. For use away from a source of electricity or during a power failure, the FDU has an 8-hour battery backup.

Depending on the requirements of the property, there are different types of FDU available for use with either low coercivity or high coercivity keycards *(refer to Section 2.1 – Keycards)*, and for encoding keycards on 3 tracks together (triplewide) or on individual tracks (triple track), if the hotel wishes to put POS information on the keycard.

All keycards are made on the FDU. Once an Authorization keycard has been swiped through the encoder to activate the FDU, the user has access to the functions that are allowed for their security level. Additionally, a PIN may be assigned to specific users to provide the same functionality for encoding keycards *(refer to Section 4.2.6 - PIN Usage as an Alternative to Authorization Keycards)*. The FDU requests information for making a keycard using simple questions on the screen. The user enters their choices (e.g. the room number), and passes a blank keycard through the encoder at an even speed. Successful encoding is indicated by a confirmation message on the screen.

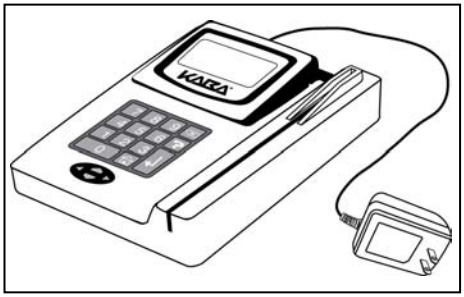


Figure 2.3: *FDU and plug-in power supply*

The other main function of the FDU is to communicate with the locks to program them to recognize the correct keycards for the door on which they are installed, to set the lock's internal clock, or to download the audit information stored in the lock.

Most properties operate with more than one FDU to ensure there are sufficient units available at all times for issuing keycards to guests, and to provide a backup in case one of the FDUs requires servicing or is in use programming or auditing locks. All of the FDUs on a property are equivalent, and can be used interchangeably by using one FDU to synchronize all other FDUs on a regular basis by transferring data between units *(refer to Section 3.5.4 – Transferring Data to Another FDU)*. Up to 64 FDUs can be used on a single property.

The portability, compact size and low weight of the FDU, plus the fact that it requires no database or computer network, makes it an extremely versatile and reliable tool.

2.4 Communication Cable

The FDU can be connected to the lock for programming or auditing using the communication cable, which has an infrared transceiver at the lock end. The transceiver end is constructed differently for each lock model, so that the transceiver is correctly positioned in front of the lock transceiver located behind the indicator light. The other end connects to Serial Port A on the rear of the FDU.

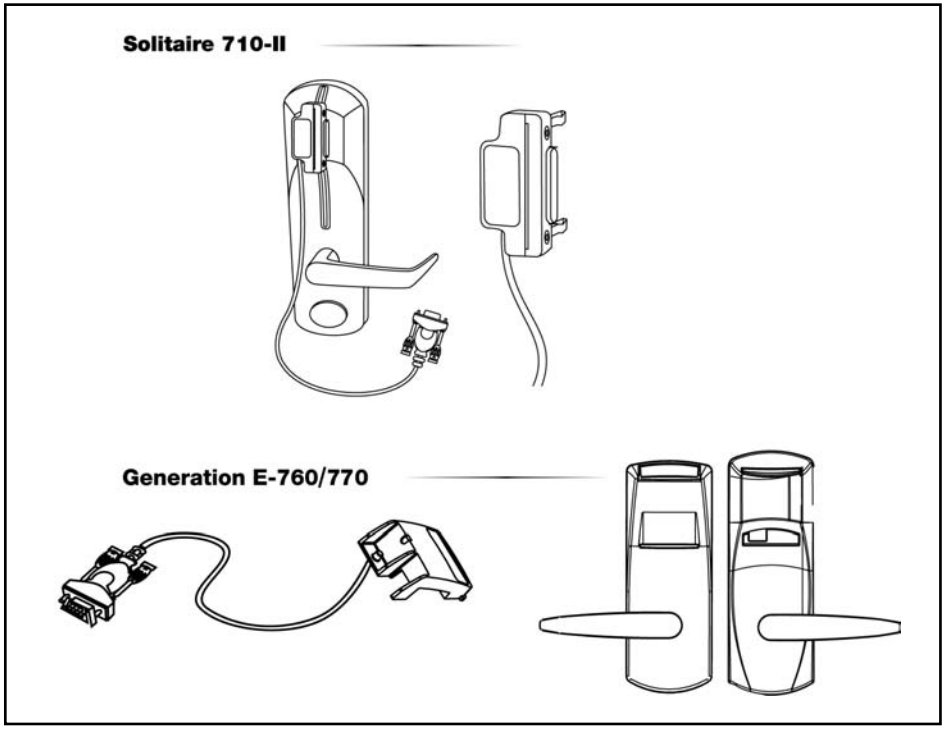


Figure 2.4: *Each lock requires a specific communication cable*

2.5 Printing

A serial or USB printer may be connected to the FDU to print the audit trail from a lock or from the FDU. These records are essential when investigating unauthorized entry to a room. Another time when it is important to use a printer is when Staff keycards are returned at the end of a shift and "logged off" using the readback function.

It is also possible to print out staff related information coming from the audits since most of the parameters involved in transactions are written in the audits.

NOTE: Some serial and USB printers may not be compatible with the FDU. Contact Kaba Ilco for assistance.

Audit Event	Description
03/14/2007 11:39A Firmware version: V0.920 FDU No.: 1 Encoder type: FDU-B Coercivity: Low C HCONF date: 01/01/2001 HCONF version: 0 Filter: All	Information on the FDU, including firmware revision, FDU number, type and date of hotel configuration. Note that the hotel configuration information itself is not shown for security reasons.
03/14/2007 11:38A 1 GUEST Encoding Room Number 101 Auth 22 NEW, Seq ID 1295-003 EXPIRY DATE 2007/03/17	Most recent activity (audit event 1). Shows the encoding of a Guest keycard, created on March 14th, valid until March 17th, using Authorized FDA keycard #22.
03/14/2007 11:38A 2 PIN CREATED EVENT Auth 200	2nd most recent activity, the creation of a PIN.
03/14/2007 11:38A 3 FDU AUTH. Encoding Auth 200 NEW, Seq ID 1295-001 EXPIRY DATE 2014/09/04	3rd most recent activity, the encoding of an FDA authorized keycard using a GMA keycard (Auth 200).

Table 2.5: *Explanation of sample FDU audit record information.*

A stand-alone computer may also be used to print the lock or FDU audit by first transferring the audit to a USB memory stick via the system's USB port. Once on a memory stick it can be transferred to a PC and printed via a standard text editor program.

For more details refer to sections *4.8 - Printing a Record of Staff Keycards*, *7.1.3 - Viewing, Printing or Sending the Lock Audit to an USB Memory Stick* and *7.2.1 - Viewing, Printing or Sending the FDU Audit to an USB Memory Stick*.

2.6 Time

Time is a major component of the Kaba Ilco Lodging Access Control System and a security advantage compared with systems that do not use time. Both the FDU and the

locks are time sensitive, meaning that they have an accurate internal clock and that time is used to determine whether a keycard is valid or not.

2.6.1 Keycard Creation Date and Time Stamp

When a keycard is encoded using the FDU, it's creation date and time are stamped in it, as well as an expiry time. The lock uses this information to grant or deny access to the keycard. Not only must the keycard be for the correct room (address), but also the current time in the lock must be earlier than the expiry time encoded on the keycard.

Furthermore, a table in the lock's memory records the time stamp of the most recently encoded keycard that has been inserted in the lock for each access level (e.g. Guest and Section/Floor/Group/Zone/Area levels for a standard guest room). The keycard is only considered valid by the lock if it was made at the same time as the value recorded in the table, or if it is more recent.

NOTE: When a more recent keycard is inserted, its date and time stamp replaces the previous information, automatically invalidating any keycard for the same access level that was created earlier (except if the keycard is a duplicate, see *Section 4.5 – New Versus Duplicate Keycards* for details).

In this way, the locking system ensures that, once a new guest or staff keycard is inserted in a lock, all previous keycards for the same level are cancelled automatically (and no longer have access). A Reset keycard can be used to update the time stamp without giving access to the room, providing another way to instantly cancel all previous keycards.

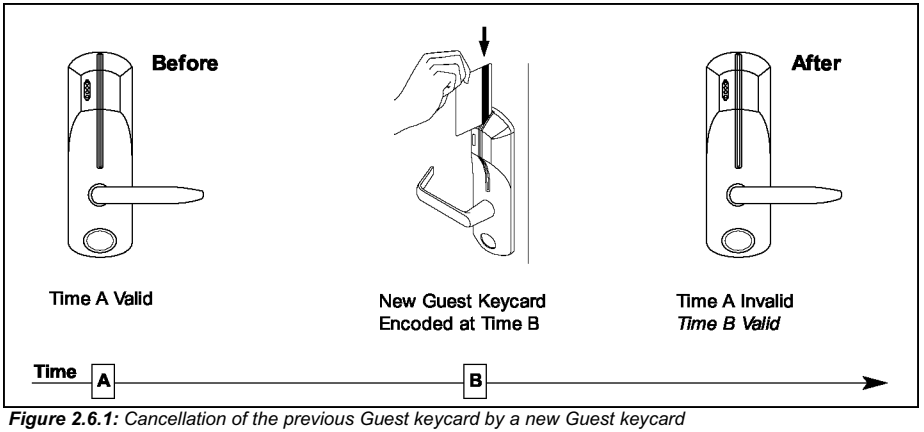


Figure 2.6.1: *Cancellation of the previous Guest keycard by a new Guest keycard*

Similarly, the FDU stores a table of the most recent Authorization keycards that have been used in the FDU. To cancel an Authorization keycard, all that is needed is to make a

new Authorization keycard with the same number as the Authorization keycard to be cancelled, and swipe it through each FDU. The time stamp of the new Authorization keycard becomes the current time stamp for determining whether an Authorization keycard with the same Authorization number is valid. (This cancels all previous Authorization keycards with that number.) This technique provides a high level of security.

2.6.2 Date and Time Stamped Audit Trail

When a keycard is inserted in a lock, the lock audit trail is updated, including information on the keycard that was inserted, and the date and time that the entry occurred. The time of each transaction is also recorded in the FDU audit.

2.6.3 Keycard Expiry Date and Time

Each keycard has an expiry time stored directly on the keycard, after which the keycard is no longer valid.

2.6.4 Keeping the System Synchronized

Because of the importance of time, it is recommended that all the FDUs on a property be synchronized periodically, usually twice a year, by transferring data from one FDU to the others. Each time an FDU is used to program a lock or reset lock addresses, and after every battery replacement in a lock, the lock's internal clock is reset by the FDU to ensure the entire system remains synchronized. The time in each lock should be reset twice per year, if the FDU has not communicated with the lock during the past six months. Refer to *Section 3.5.4 – Transferring Data to Another FDU* for more details.

Another situation where FDUs should be synchronized is when PINs are created as a substitute for certain types of authorization keycards. For more details please refer to sections *3.5.5 – Pin Management* and *4.2.6 – PIN Usage as an Alternative to Authorization Keycards*.

2.6.5 Daylight Savings Time

The local time shown on the FDU screen is not the same as the FDU's internal clock time (or the system time). The FDU's internal clock should be set only when the system is first installed. The local time can be set separately in the FDU features, and daylight savings time is handled by moving the local time ahead or back by one hour. Refer to *Section 3.6, part 10 – Current Time* for more details.

2.7 Audits

The lock audit can be consulted in the event of unauthorized access to determine which keycard was used, when entry occurred, and the identity of the operator who issued the keycard. The lock audit trail also records the use of special keycards such as Reset,

Lockout, Programming, Initialization and override usage. The FDU and communication cable are used to read the audit stored in the lock.

NOTE: Keycards that are rejected by the lock (wrong address, expired, locked-out by the privacy thumbturn or by a lockout keycard) are not recorded in the audit.

Solitaire locks store the last 350 audit records, while Generation E-760 & 770 locks store 200 audit records.

The lock audit is a strong deterrent to crime, particularly employee theft. It protects offices, storerooms and other back-of-the-house doors, as well as guest rooms, and can be useful to track the use of parking facilities. All keycards, including multiple copies of a keycard made at the same time, have different sequence ids that can be traced. ***All staff should be made aware of the audit trail in order to obtain the deterrent effect.***

In addition, the FDU maintains a detailed audit of the last 4,000 transactions to provide proof of inappropriate use.

NOTE: In order to use the audit trails as legal proof, Staff and Authorization keycards must be properly logged using the forms provided and a printout record done of these keycards when made.

The audits are stored in non-volatile memory, which means that they cannot be erased, even if power is interrupted.

2.8 Interfaces

The FDU can be connected to a stand-alone PC or to a computer network to provide additional features when used in conjunction with a PMS (Property Management System). A second interface mode, the POS (Point-of-Sale) interface, is also available.

2.8.1 PMS Interface

The PMS interface allows properties that use a computer to manage guest reservations and billing to transfer the information regarding the guest's keycard directly from the PMS computer to the FDU. By using this method, human error in re-entering the information in the FDU is eliminated. All that is required to encode a guest's keycard with the correct data is for the clerk to swipe a blank keycard through the FDU encoder when prompted to do so. The PMS interface saves time, makes registration more efficient and prevents double-selling of rooms.

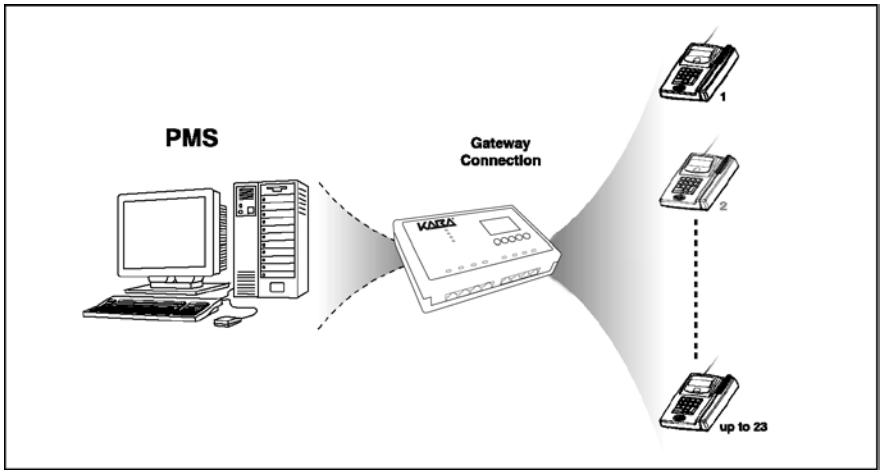


Figure 2.8.1: *PMS Interface, Gateway II configuration.*

2.8.2 POS Interface

For properties that wish to use keycards to post charges for restaurants, boutiques and other amenities to a guest's account, or to track the use of parking by guests, a special model of FDU with a triple-track encoder is available. In addition to encoding the encrypted keycard code that works with the locks on other tracks, POS Interface FDUs with triple-track encoders use track 2 to encode information in the worldwide ABA standard that is used on bankcards and credit cards. Point-of-Sale readers in cash registers or other equipment that use the ABA standard format can read this information from track 2 to post charges automatically to the room account over a network. The data used to post charges (e.g. the guest's folio number) can be either entered manually, or transferred ***automatically*** from the PMS when encoding the keycard.

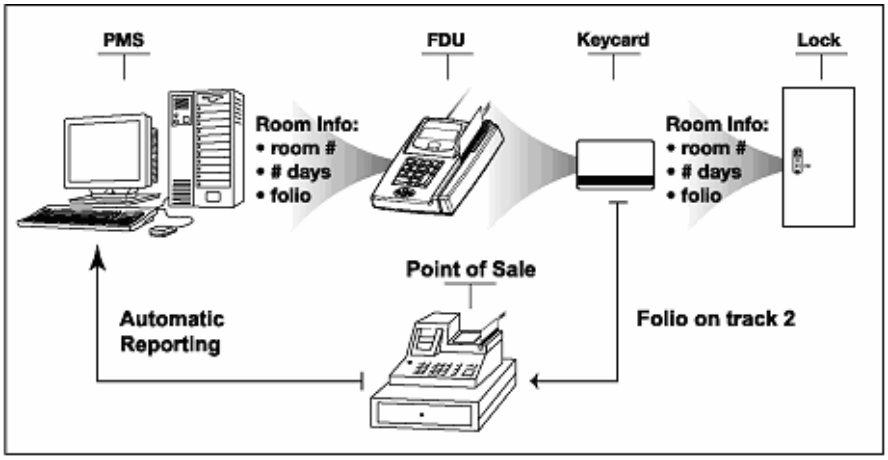


Figure 2.8.2a: *PMS and POS Interface of triple track FDU (automatic reporting of charges from the point of sale)*

As an alternative to the POS interface, the property can use an FDU in POS Verifier mode to post charges manually to the room account by reading the guest's room number (Please refer to *Section 3.3.2 – POS Verifier Mode*, and *Section 3.5.11 – Using the FDU in POS Verifier Mode* for details).

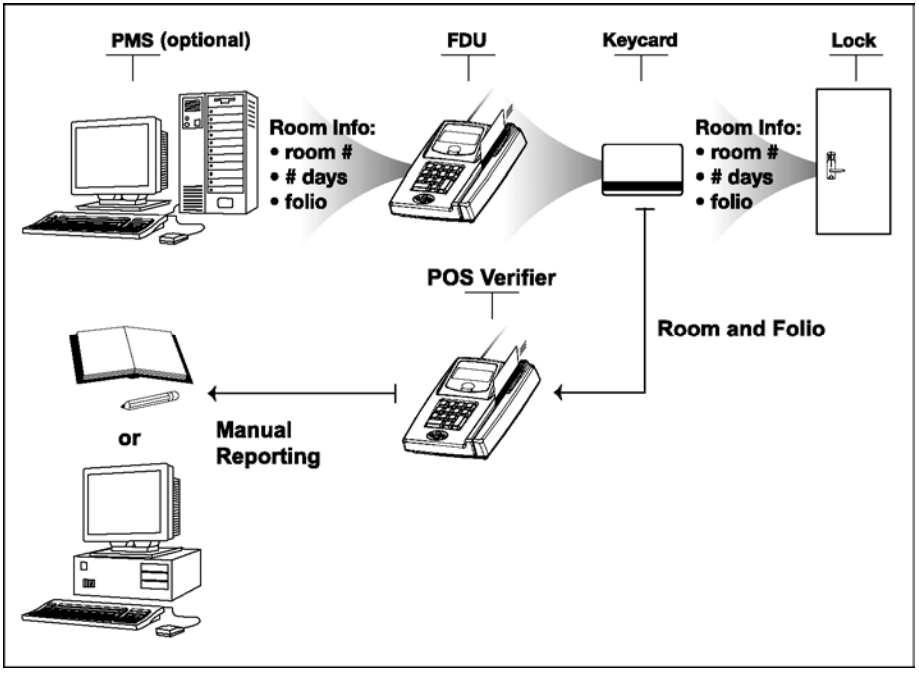


Figure 2.8.2b: *POS Verifier function of standard FDU (manual reporting of charges from the point of sale)*

Chapter 3: Front Desk Units - Using and Programming

3.1 First Use of an FDU

Before using an FDU, it must be charged overnight and properly configured. See *Section 6.4 – Starting the System After Installation* before using an FDU for the first time.

3.2 FDU Overview

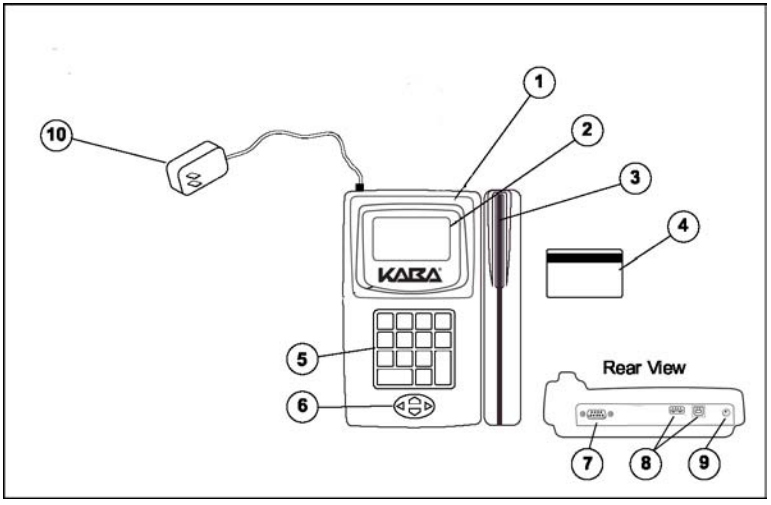


***Figure 3.2** • The FDU*

1. FDU - Front Desk Unit
2. LCD Screen
3. Magnetic Stripe Encoder
4. Magnetic Stripe Keycard
5. Keypad
6. Cursor Keys
7. Serial Port
8. USB Ports
9. 9 VDC Jack
10. Power Supply for FDU

3.2.1 The FDU Keypad and Cursor Keys

The following image shows the FDU keypad and the cursor keys. The keypad allows the user to enter numeric values, and special buttons permit navigation in the FDU menus or provide context sensitive help. Cursor keys allow movement within menus and input displays.

The <⌫> button is used to correct mistakes when entering numerical values. It is also used to go back to the preceding menu level when menus are displayed on the screen.

The <?> button provides context sensitive help when pressed. The FDU shows basic information on the selected menu item when this key is pressed.

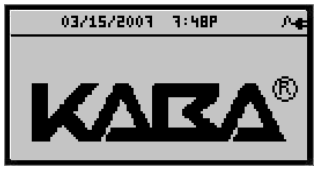
The <↵> button is used to activate or start an action on the FDU.

The <⌂> button has two purposes. The first is to provide a quick way to go back to the main menu, which is the starting point of all interactions with the FDU. The other purpose is to display, when pressed twice, the FDU information. For more details, refer to *Section 3.5.6 – Displaying the FDU Identification*.

The left <◀>, right <▶>, up <▲> and down <▼> arrow cursors are used to move in the appropriate direction within menus and input displays. The left arrow <◀> is also used to correct mistakes when entering numerical values.

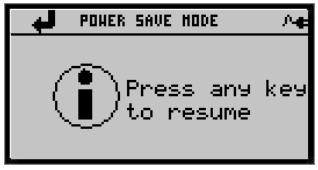
3.2.2 Authorizing the FDU

The FDU is normally unauthorized. The FDU will not operate until an Authorization keycard is swiped through the magnetic stripe encoder or a valid PIN is entered. The screen that is displayed when the FDU is unauthorized is:



After the FDU has been authorized, it will offer menu choices for making keycards or other actions according to the authorization level of the user. After one of the time-out periods has expired, the FDU will go back to the unauthorized mode for security issues. For more details, please refer to S*ection 3.6, part 9 – FDU Time-outs*.

When running on batteries, the FDU turns off the LCD backlight and enters a power saving mode after a period of inactivity to save on the batteries. Pressing any key will exit this mode, turn the backlight on and go to the main Kaba screen.



IMPORTANT: **For security purposes, all transactions performed by the FDU are audited, showing the authorization keycard used, the transaction details, date and time.**

DO NOT lend Authorization keycards to anyone.

DO NOT leave Authorization keycards unattended anywhere.

DO NOT leave the FDU unattended, and DO NOT allow another person to use the FDU, without first logging off the previous user's authorization by pressing <⌫> until the main screen is displayed.

Keycards, including Authorization keycards, can be erased by strong magnetic fields.

3.2.3 FDU Menus

The FDU menus are displayed on the FDU's LCD screen. As example, the main menu is shown below:

The upper line  is a status line that reports modes of operation and other information. The remainder of the screen consists of the page content. The display may show a lot of information to the user at the same time via the status line and the page content.

3.2.3.1 Status Line:

The status line is used strictly to report information to the user. It consists of 4 areas as detailed below.

The first area shows the scroll indicator. Depending on the number of items that need to be displayed, arrow(s) appear in this area to inform the user that remaining items extend below and/or above the screen. The possible values for the scroll indicator are:

Scroll indicator	Description
 (none)	All the required information is displayed. No need to use the arrow keys to see other information.
	The user can only press the up <▲> arrow as they are at the bottom of the list of menus or items.
	The user can only press the down <▼> arrow as they are at the top of the list of menus or items.
	The user can press the up <▲> or down <▼> arrow since they are between the top and the bottom of the list of menus or items.

The second area shows the action indicator. Each page has an action associated to it, which is performed when the <↵> key is pressed. This area contains a small icon representing the action. The possible values for the action indicator are:

Action indicator	Description
	Close the current page.
	Encode or read a keycard.
	Go to the selected page.
	Save changes made to the configuration.

The third area shows either the date & time, or a page title as text information. Note that when in Daylight Savings Time (DST) an asterisk (*) is shown at the end of the time shown.

The fourth area shows the power indicator. It indicates if the external power is connected, disconnected, if the battery is being charged, if the battery is running out or if the battery pack is not present or failed. The possible values for the power indicator are:

Power indicator	Description
	External power supply connected and battery fully charged.
	External power supply disconnected, running on battery.
 (flashing)	Battery nearly drained, requires immediate recharging.
 to 	External power supply connected, battery charging (the indicator will show that the battery voltage level is charging)
	External power supply connected, battery pack not present or failed.

3.2.3.2 Page Content:

The page content may display 3 different types of information: menus, inputs, and messages reported by the FDU.

The first type of information is a menu being shown. A menu is a page where the user must select one item from the selection displayed. Each item is a link o another page and has a label and a number associated to it. The user may select the desired item by entering the number using the keypad (no need to press <↵>) or using the up <▲> or down <▼> arrows to move the highlighted horizontal bar over the item and pressing <↵> to select the item. The <⌫> key is used to cancel an operation or move backward through the menus.

In the following example, the “Guest Keycard” item that is highlighted will be selected if 1 is pressed on the keypad or the <↵> key is pressed.

The second type of information available in the page content is a display of inputs. This is a page where the user inputs information on selected lines. The type of information can be a number, a date or a preset value available within the FDU.

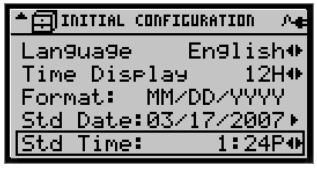
Numbers and dates are entered using the keypad, with the left <◀> arrow deleting the last digit entered if an error is made.

Preset values available are shown using the left <◀> or right <▶> arrows. In the example below, pressing left <◀> or right <▶> arrow will show all possible values for the "Type" parameter, which is highlighted within a rectangle.

The third type of information available in the page content is a message sent by the FDU to inform or warn the user of a specific event that is either in progress or has completed.

3.2.3.3 Entering Time:

When the 12 hours format is used, the time has to be entered within 1 and 12 hours along with the AM or PM indicator. Use the keypad to enter the desired hour and the right <▶> arrow to toggle between AM and PM.



When the 24-hour format is used the right <▶> arrow has no effect, and the user must enter values between 00:00 and 23:59 using the keypad.

In both formats, the left <◀> arrow deletes the last digit entered, as in any digital input in various menu items.

3.2.4 Reading and Encoding Keycards

The FDU's built-in magnetic stripe encoder has been developed to read and encode keycards reliably. Keycards must be passed through the entire length of the slot, and at as consistent a speed as possible to ensure correct reading and encoding every time.

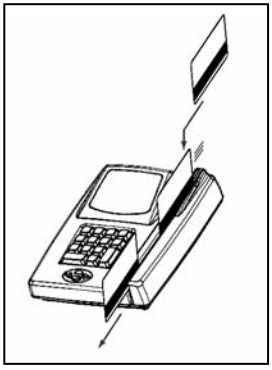


Figure 3.2.4: *Magnetic stripe keycards should be placed in the slot with the magnetic stripe down and facing away from the keypad.*

3.3 Software Version and Operation Modes

The FDU has built-in software, which determines the menu functions. The FDU software supports the following lock series:

- System 700-II Locks
- System 710 Locks
- System 710-II Locks
- System 760 Locks
- System 770 Locks
- RAC 3.5, 4 & 4XT Access Control Systems

3.3.1 Manual Mode

Manual Mode is the normal mode of operation of the FDU, in which the first screen following the insertion of a valid Authorization keycard or input of a valid PIN entered is eitehr the Main Menu, or the “Guest Keycard” menu if using an FDA Authorization:

The Main Menu offers access to all the functions for which the user is authorized. An exception is the Bellman's Authorization keycard, which has only one function, encoding a Bellman's Master keycard. Since there is only one menu item, the Main Menu does not appear in this case.

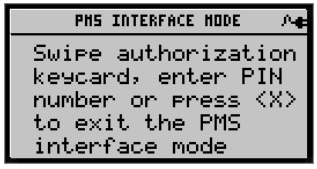
3.3.2 POS Verifier Mode

POS Verifier Mode is accessed using a POS Authorization keycard. As soon as the POS keycard is swiped, the FDU is put in POS Verifier Mode and the user is prompted to swipe a Guest keycard to validate the room information of the guest. This is the only function available to this keycard.

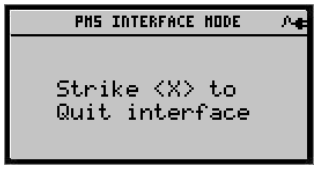
To perform other operations, the user must return the FDU to manual mode by pressing <⌫> then swiping a valid Authorization keycard (other than a POS Authorization, e.g. Front Desk Authorization, Master Authorization, etc.).

3.3.3 PMS Interface Mode

PMS Interface Mode is used for encoding guest level keycards using data transferred from a Property Management System computer. Choosing option 3 from the Main Menu accesses the PMS mode and then presents the following Authorization screen.



After a valid Authorization keycard is inserted or a valid PIN entered, the FDU waits for a request from the PMS to encode a keycard. The following screen is displayed:



To perform other operations, the user must return the FDU to manual mode. For more information, please refer to *Chapter 8 - Interfaces*.

3.4 Battery Back-up

The FDU can operate for up to 8 hours without external power, using its internal rechargeable battery back-up. The FDU switches to the battery back-up automatically when external power is interrupted. When the battery back-up is too low, the FDU will shut itself down to prevent any operations and it must be plugged into an AC outlet in order to resume operation. Before shutting down, the Power indicator, (top right corner indicator) will flash to indicate that the FDU voltage level is low.

NOTE: When the Power indicator flashes, immediately stop using the FDU and connect the FDU to its external power supply to recharge it. In the event the unit stops responding y recharging the battery pack in a short time-frame will restore the system settings, including time.

When the FDU is operating via the external power supply, the "external power supply connected" indicator *(see Section 3.2.3.1 – Status Line:)* appears at the far right of the status line. When running on internal batteries, the "running on battery" indicator *(see Section 3.2.3.1 – Status Line:)* will appear at the far right of the status line. When possible, the FDU should always be powered using the accompanying power supply to ensure reliable operation. Operation under battery power should be limited only to certain situations, such as: lock programming, printing of the audit or encoding of Staff keycards in management offices (away from the Front Desk power supply), or for remote registration of tour or convention groups on a bus, etc.

IMPORTANT: Never remove both the AC power and the battery pack from the FDU. If the battery is removed from the FDU and the system is not connected to the AC power supply, the settings of the FDU will be lost. Power can only be restored to the system with the AC power supply, which will reset the system back to the factory default settings. If this occurs there is a high probability that synchronization problems will exist with other FDUs and locks on the property. For assistance if this situation occurs please contact Kaba Technical Support.

3.5 FDU Procedures

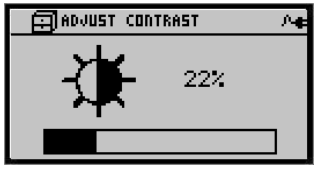
3.5.1 Adjusting the Contrast and Volume.

3.5.1.1 Adjusting the Contrast:

The contrast may be adjusted via the initial Kaba screen or the main menu.

1. From the initial Kaba screen:

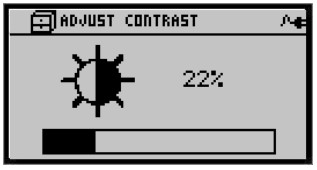
Press the left <◀> or right <▶> arrow to reach the contrast menu:



2. Press the left <◀> arrow to decrease the contrast or right <▶> arrow to increase the contrast. Press <↵> to save the new contrast level.

1. For the main menu, swipe a keycard wih a GMA or MA authorized user level.

2. As a shortcut press 7 followed by 5. Alternatively use the down <▼> arrow followed by <↵> to reach the "FDU Setup" menu, followed by the down <▼> arrow and <↵> to reach the "Contrast" menu:



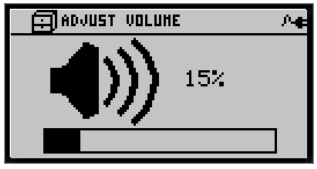
3. Press the left <◀> arrow to decrease the contrast or right <▶> arrow to increase the contrast. Press <↵> to save the new contrast level.

3.5.1.2 Adjusting the volume:

The volume may be adjusted via the initial Kaba screen or from the main menu.

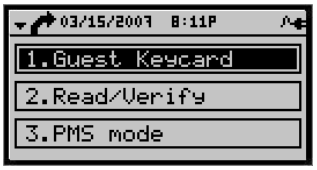
1. From the initial Kaba screen:

Press the up <▲> or down <▼> arrow to reach the volume menu:

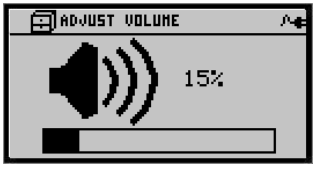


2. Press the up <▲> arrow to increase the volume level or the down <▼> arrow to decrease the volume level. Press <↵> to save the new volume level.

1. For the main menu, swipe a keycard wih a GMA or MA authorized user level.



2. As a shortcut press 7 followed by 4. Alternatively use the down <▼> arrow followed by <↵> to reach the "FDU Setup" menu, followed by the down <▼> arrow and <↵> to reach the "Volume" menu:



3. Press the up <▲> arrow to increase the volume level or the down <▼> arrow to decrease the volume level. Press <↵> to save the new volume level.

3.5.2 Setting Keycard Expiry Values

3.5.2.1 Selectable Expiry:

All keycards except Guest level keycards *(see Section 3.5.2.2 – Variable Expiry:)* expire after the period set using the Expiry menu. Because these values can be selected using a GMA or MA keycard, they are referred to as "selectable". Use the procedure described below in *Section 3.5.2.3 – Setting the Expiry Values:* to set the selectable expiry period desired for each type of keycard. The allowed expiry range for each keycard is designed to fit the keycard's function. For example, all Reset keycards expire after 1-24 hours, since these keycards are designed for immediate use to reset locks.

Refer to *Appendix A – Keycard Quick Reference Chart* for more details on the selectable expiry for each type of card.

3.5.2.2 Variable Expiry:

The System offers two types of expiry times for Guest level keycards, selectable expiry as defined above, or variable expiry. If variable expiry is enabled when a keycard is being encoded staff can either use the default setting of the selectable expiry, or they can enter a custom expiry value each time they encode a Guest level keycard.

The Variable Expiry feature applies to the following types of guest entry keycards only: Guest, Adjoining Suite, Common Door Suite, Convention Suite and Pre-Registered. (To enable Variable Expiry, see *Section 3.6, part 2 – Variable Expiry*.)

3.5.2.3 Setting the Expiry Values:

Purpose: To set the selectable expiry values to be used when encoding keycards.

Minimum Keycard Required: Master Authorization (MA) or General Manager Authorization (GMA), depending on which keycard expiry is to be set. Refer to *Appendix A –Keycard Quick Reference Chart* for more details.

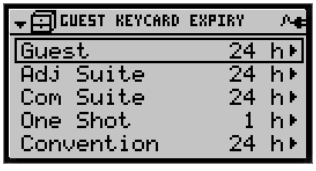
Steps to set the expiry for a keycard:

1. Swipe a keycard having a GMA or MA authorized user level.

2. Press 7 as a shortcut or use the down <▼> arrow to reach the “FDU Setup” menu and press <↵>.

3. Press 1 or <↵> to reach the “Keycard Expiry” menu.

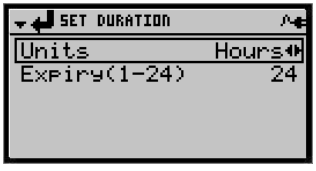
4. Press 1 or <↵> to select the "Guest Keycards" menu. All guest keycards types will be displayed along with their actual expiry value and the unit used (hours or nights). Select the type of keycard for which the default expiry is to be set. Once the type of keycard is selected, press the right <▶> arrow to access the corresponding menu.



5. The units of the expiry value and the valid range are displayed. Some keycards can be set to operate in hours or nights, while others are only hours or only nights *(refer to Appendix A –Keycard Quick Reference Chart)*.

   To change the expiry units, highlight the "Units" field and press the left <◀> or right <▶> arrow.

   To change the expiry duration, highlight the "Expiry" field, set the new desired value, and press <↵> to save the change.



Example: *A large tour group will check in who will be staying three nights, and the Hotel Default is one night for all Guest levels. An employee with an MA keycard can change the value for Guest keycard expiry to 3 nights. The Front Desk clerk will then be able to encode the three night keycards in a large batch. To return the Guest expiry to 1 night it must be changed back using the previous steps.*

NOTES: **Pre-registered keycards can be encoded up to 10 days in advance. These keycards become valid at the start time entered during card encoding; the expiry is added to the validity start time.**

An expiry value of one month is recommended for staff Sub-master level keycards (Section, Floor, Group, Zone, Area).

3.5.3 Saving and Loading the Default Expiry Values and Features

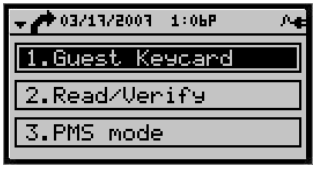
3.5.3.1 Saving the Default Expiry Values and Features:

All Default Expiry Values and Features are automatically saved when they are entered with the FDU menus.

3.5.3.2 Loading the Default Expiry Values and Features:

If required, the factory default expiry values can be reloaded into the FDU.

1. Swipe a keycard having a GMA or MA authorized user level.



2. Press 7 or use the down <▼> arrow followed by <↵> to reach the “FDU Setup” menu.

3. Press 1 or <↵> to reach the “Keycard Expiry” menu.

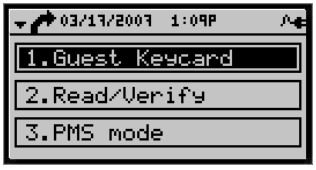
4. Press 5 or use the down <▼> arrow followed by <↵> to reach the “Load Factory Expiries” menu.

Press <↵> to load the factory expiries defaults.

3.5.3.3 Loading the Default Features values:

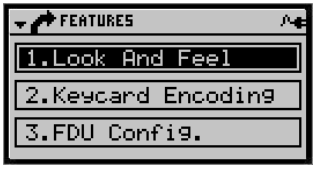
If required, the factory default features can be reloaded into the FDU to overwrite any changes previously done.

1. Swipe a keycard having a GMA or MA authorized user level.



2. Press 7 or use the down <▼> arrow followed by <↵> to reach the “FDU Setup” menu.

3. Press 2 or use the down <▼> arrow followed by <↵> to reach the “FDU Features” menu.



4. Press 6 or use the down <▼> arrow followed by <↵> to reach the “Load Factory Features” menu.

Press <↵> to load the factory features defaults.

3.5.4 Transferring Data to Another FDU

Purpose:

To transfer current data from one FDU to another to ensure that all FDUs in a facility are set to the same time, recognize the same Authorization keycards, and have the same feature settings. This procedure is used when first installing the system, and should be performed periodically afterward to ensure that all the FDUs in the facility remain synchronized. This procedure can also be used to transfer settings from a damaged or defective FDU to a replacement unit. Twice a year, it is recommended to perform a lock time reset on all hotel locks.

The data that is transferred from one FDU to another includes:

- **Current date and time**
- **External Hotel Code**
- **Current selection of features and expiries**
- **Valid Front Desk Units and the identity of any stolen FDUs that have been cancelled**
- **Valid Authorization keycards**
- **Any valid PINs in the transmitting FDU, as well as records of any previously assigned/revoked PINs. (see Note)**

NOTE: If performing an FDU to FDU transfer with a previous version of Kaba Ilco's FDU system, no PIN information is transmitted between the units since the previous generation FDU system does not support the PIN feature. For further information please contact Kaba Technical Support.

Minimum keycard required: Master Authorization

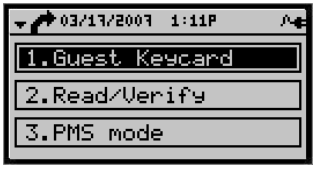
Steps to transfer data to another FDU:

1. Label the two Front Desk Units to differentiate the one that must receive the data (new) from the one that must send the data (old or Master FDU).
2. As a property may have previous versions of Kaba's FDU system as well as the new generation model different types of cables may be required for the FDU to FDU transfer. If the version of FDU is unknown please contact Kaba Technical Support.

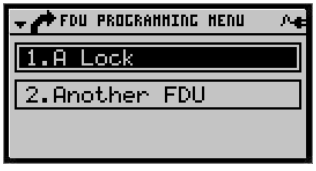
   Based on the table below, connect the required FDU to FDU communication cable to the Serial Port on the rear panel of each Front Desk Unit.

Sending FDU version	Receiving FDU version	Required cable
Previous Generation	Previous Generation	Straight serial cable
Previous Generation	Next Generation	Straight serial cable
Next Generation	Previous Generation	Null modem cable
Next Generation	Next Generation	Null modem cable

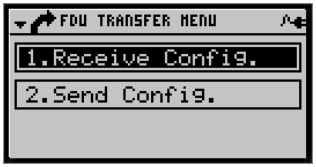
3. On the FDU that will receive data, swipe a keycard having a GMA or MA authorized user level.



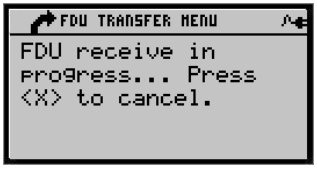
4. Press 8, or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



5. Press 2, or use the down <▼> arrow followed by <↵> to reach the "Another FDU" menu.

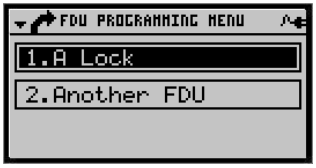


6. Press 1, or use the down <▼> arrow followed by <↵> for “Receive Configuration” to put the receiving FDU in receive mode.

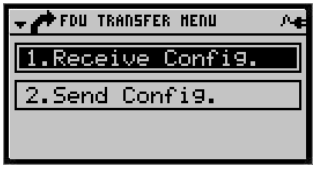


7. On the FDU that will transmit the data, swipe a keycard with a GMA or MA authorized user level.

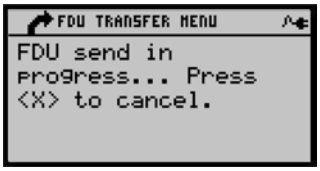
8. Press 8, or use the down <▼> arrow followed by <↵> to reach the “Programming FDU/Lock” menu.



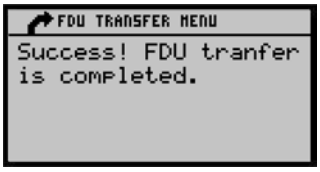
9. Press 2, or use the down <▼> arrow followed by <↵> to reach the “Another FDU” menu.



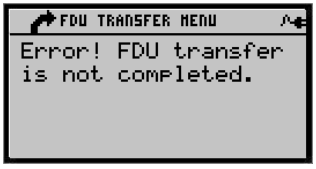
10. Press 2, or use the down <▼> arrow followed by <↵> for “Send Configuration” to put the transmitting FDU into send mode.



After the data is transmitted, both FDU screens will give the following message



If an error occurred, the following message is displayed and the receiving FDU will maintain it's previous configuration.



NOTE: The information shown above is when both FDUs are of the latest generation model. An FDU to FDU transfer using one FDU of previous generation will be slightly different. For any required support please contact Kaba Technical Support.

3.5.5 Pin Management.

The PIN can be used by new or existing employees if agreed to by the administrator, as an alternative to using an authorization keycard. The PIN is a 4 to 8 digit code selected by either the administrator or the employee, or can be suggested by the FDU.

To ease access to the FDU, an employee having a PIN may access the FDU without their authorization keycard. Instead of swiping a keycard, the PIN is entered using the FDU keypad. If the entered PIN matches one defined in the FDU, the access will be granted, otherwise the FDU will display an "Invalid PIN entered" message. The usage of an authorization keycard can continue to be used to log into the FDU if the employee prefers it to the usage of a PIN.

The following table shows the different authorization levels to create and manage PINs. For example, a Master can create a PIN for a Front Desk but cannot create one for a Bellman.

Type of creator	Type of FDU users allowed to have a PIN
General Manager	Programming, Bellman, Front Desk, POS
Master	Front Desk, POS

Table 3.5.5: *PIN management access table.*

NOTE: For security, the General Authorization and Master Authorization levels cannot have PINs assigned

When a property has multiple FDUs, only one unit should be used for the management of PINs. As there is no real-time communication between multiple FDUs on a property, using a master FDU for PIN management will minimize any potential issues with the same PIN being used for different authorization levels on 2 different FDUs in the same property.

The FDU offers the following options to manage PINs, which are detailed below:

- Create/Assign a PIN for a new or existing employee
- Read-back/verify a PIN
- Modify a PIN
- Revoke a PIN

NOTE: To either create or use PINs the FDU must first be configured for to use one, or both, of these features. Please refer to *Section 3.6 part 18 – Accept PIN* and *Section 3.16 part 19 – Create PIN* for more details.

IMPORTANT: For security reasons, if a Hotel Restart is done *(see Section 3.5.9 – Hotel Restart)* all current PINs will be invalidated and an error message of "Invalid keycard, the authorization has expired" will be displayed. Previously assigned PIN values will remain in memory to warn the administrator if a new user requests the same sequence.

3.5.5.1 Create/Assign a PIN – New employees:

If the FDU has been configured to accept the creation of PINs a PIN may be assigned to certain employee levels as an alternative to their keycard.

1. Swipe a keycard having a GMA or MA authorized user level.

2. Press 6, or use the down arrow <▼> and press <↵> to reach the "Staff Keycard" menu.

3. Press 2 or use the down arrow <▼> to and press <↵> to reach the "FDU Authorization" menu.

4. Enter the authorization mumber of the staff keycard being created, and select the "Assign Pin ?" line with the down <▼> arrow. Press the left <◀ > or right <▶> arrow to set the "Assign PIN" value to YES.

   The FDU will suggest a PIN that provides maximum level of security based on its internal database.

5. If the suggested PIN is acceptable, press <↵> and swipe the staff keycard to encode the PIN to this authorized level user.

5. ***It is highly recommended to always use the PIN suggested by the FDU,*** however, if a different PIN is desired, press the down <▼> arrow to select the "PIN code" option and enter a 4 to 8 digit code.

If the code is already assigned in the FDU memory an error message will appear and a new code will have to be selected.

Additionally, if the PIN was already used in the past but is now revoked *(see Section 3.5.5.5 - Revoke an Existing PIN)* a warning message will be displayed.

When completed, press <↵> and swipe the staff keycard to encode the PIN to this authorized level user.

IMPORTANT: **For security, a PIN that is written down should be kept in a safe place to prevent unauthorized people from knowing it.**

IMPORTANT: **To ensure ex-employees are unable to access the system, it is highly recommended to NOT re-enable previously used codes. The suggested PIN provided by the FDU should always be used.**

3.5.5.2 Create/Assign a PIN – Existing employees:

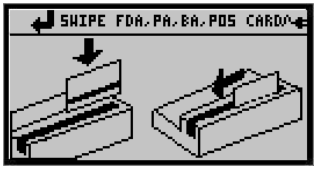
Existing employees of certain authorization levels can have a PIN assigned to the keycard already assigned to them.

1. Swipe a keycard having a GMA or MA authorized user level.

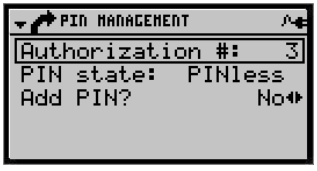
2. Press 7, or use the down <▼> arrow followed by <↵> to reach the "FDU Setup" menu.

3. Press 3, or use the down <▼> arrow followed by <↵> to reach the "PIN Management" menu.

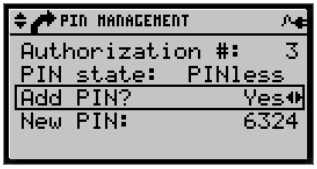
   Swipe the keycard corresponding to the authorized user for whom a PIN is to be created. ***Keep in mind that only certain authorization levels can have PINs.***



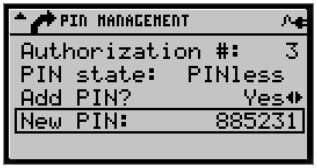
   The following menu will be displayed:



4. To create a PIN, select the "Add PIN" option using the down <▼> arrow and press the left <◀> or right <▶> arrow to set the YES value.



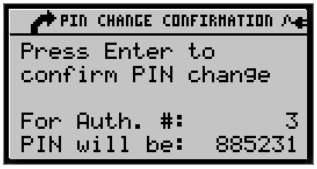
The FDU suggests a new PIN value that was never supplied to date. Otherwise, the user may decide to choose another PIN. If this is the case, the "New PIN:" option must be selected with the down <▼> arrow and the new PIN code can be entered using the keypad. A 4 to 8 digit code must be entered.



It is highly recommended to always use the suggested PIN provided by the FDU.

NOTE: If the PIN is already in use by another authorized user the FDU will refuse the duplicate PIN. Additionally, if the PIN was previously revoked a warning message will be given. *Refer to Section 3.5.5.1 - Create/Assign a PIN – New employees:*

5. Once the PIN is acceptable, press <↵> to reach the confirmation screen.



Press <↵> to assign the new PIN to the authorized keycard or press <⌫> to go back to the previous menu. If accepted, the following message appears:

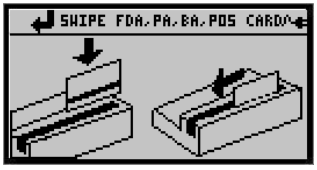
3.5.5.3 Read-back/Verify a PIN:

If required, a PIN assigned to a particular authorized keycard can be verified.

1. Swipe a keycard having a GMA or MA authorized user level.

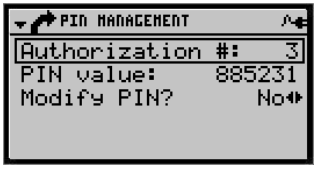
2. Press 7, or use the down <▼> arrow followed by <↵> to reach the "FDU Setup" menu.

3. Press 3, or use the down <▼> arrow followed by <↵> to reach the "PIN Management" menu.



Swipe the keycard corresponding to the authorized user.

4. The PIN information on the keycard will be displayed.



5. Press <⌫> twice to exit.

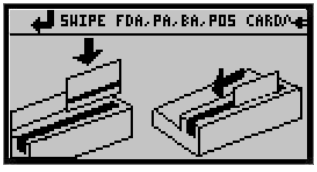
3.5.5.4 Modify an existing PIN:

If an employee wishes to change their PIN or the PIN in use has become compromised, the currently assigned PIN can be modified.

1. Swipe a keycard having a GMA or MA authorized user level.

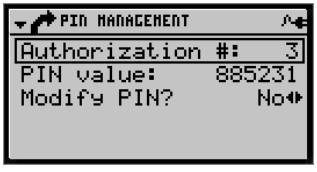
2. Press 7, or use the down <▼> arrow followed by <↵> to reach the “FDU Setup” menu.

3. Press 3, or use the down <▼> arrow followed by <↵> to reach the “PIN Management” menu.

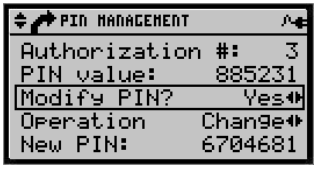


Swipe the keycard corresponding to the authorized user who’s PIN is to be modified.

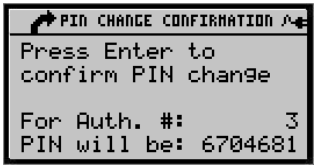
4. The screen will display the current PIN information.



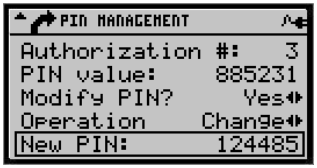
5. To modify the PIN value, press the down <▼> arrow and select the “Modify PIN?” value. Use the left <◀> or right <▶> arrow to set the value to YES.



The FDU suggests a new PIN value that was never supplied to date. If the value shown is acceptable press <↵>.



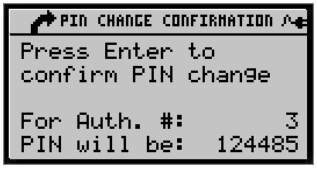
If a custom value is desired select "New PIN:" and enter the PIN value. Press <↵> to assign the new PIN to the authorized user.



It is highly recommended to always use the suggested PIN provided by the FDU.

NOTE: If the PIN is already in use by another authorized user the FDU will refuse the duplicate PIN. Additionally, if the PIN was previously revoked a warning message will be given. *Refer to Section 3.5.5.1 - Create/Assign a PIN – New employees:*

6. Once the PIN is acceptable, press <↵> to reach the confirmation screen.



Press <↵> to assign the new PIN to the authorized keycard or press <⌫> to go back to the previous menu. If accepted, the following message is displayed:

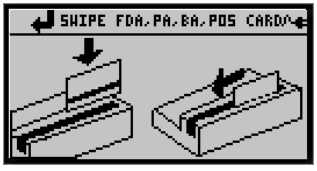
3.5.5.5 Revoke an existing PIN:

Under certain conditions, the administrator may decide to remove the PIN of an employee. In the event an employee is leaving or being dismissed, refer to the standard procedure described in *Section 10.7 – If an employee leaves or is fired.*

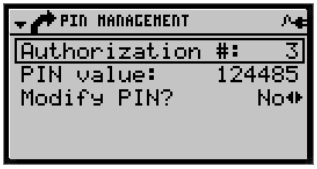
1. Swipe a keycard having a GMA or MA authorized user level.

2. Press 7, or use the down <▼> arrow followed by <↵> to reach the “FDU Setup” menu

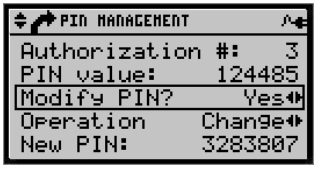
3. Press 3, or use the down <▼> arrow followed by <↵> to reach the “PIN Management” menu.



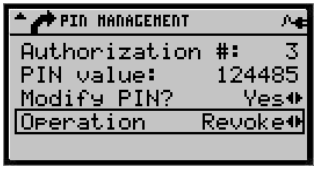
4. Swipe the keycard corresponding to the authorized user whose PIN is to be revoked.



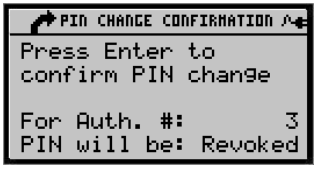
5. To revoke the PIN, select the “Modify PIN?” option with the down <▼> arrow and press the left <◀> or right <▶> arrow to set the YES value.



6. Select the “Operation” option with the down <▼> arrow and press the left <◀> or right <▶> arrow to set the value to Revoke.



7. Press <↵> to confirm revoking of the PIN from the FDU for that authorization level.



Press <↵> to revoke the PIN or <⌫> to go back to the previous menu. When <↵> is pressed, a confirmation message is given:

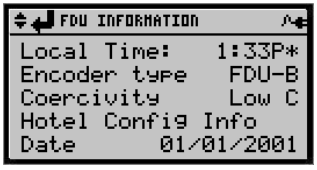
3.5.6 Displaying the FDU Identification

To find out basic system information for the FDU, such as the type of FDU (A or B), coercivity of encoding (Low C vs High C), firmware version and other parameters the FDU Identification screen is available to show this basic information.

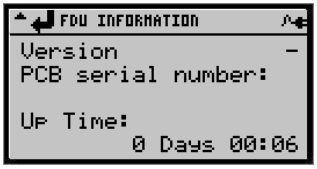
1. Press the <⌂> button, which is available from any menu. Depending on which menu the FDU is currently on, a second press of the <⌂> button may be required.

   Note that the time shown is the system time of the FDU and ***not*** the local time.

2. Press the down <▼> arrow as needed to see the remaining parameters.



   The time shown in the image above is the Local Time, adjusted for Daylight Savings Time *(see Section 2.6.5 Daylight Savings Time)*



   The Version & PCB serial number may be helpful when discussing any issues with Technical Support.

   The Up Time represents how long the unit has been in operation since the last time a reset of the unit was done. This information may also be helpful when troubleshooting issues with Kaba Technical Support.

3.5.7 Hiding the Language, Date and Time Prompts

Purpose: This feature hides the language, date and time configuration options that appear if the FDU is reset. The date and time are very important system

parameters that should not be changed inadvertently. If these are parameters are changed the FDU may lose the ability to make keycards that work properly in the locks and other FDUs on the property. ***It is strongly recommended to set this feature to hide the language, date, and time prompts.***

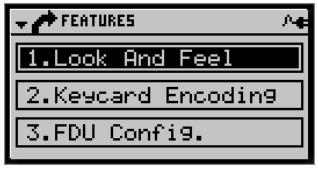
Minimum keycard required: General Manager Authorization

Steps required to hide the prompts:

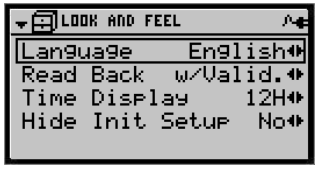
1. Swipe a keycard having a GMA authorized user level.

2. Press 7 or use the down <▼> arrow followed by <↵> to reach the "FDU Setup" menu.

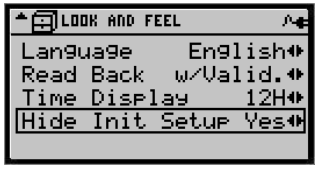
3. Press 2 or use the down <▼> arrow followed by <↵> to reach the "FDU Features" menu.



4. Press 1 or <↵> to reach the "Look and Feel" menu.



5. Choose the "Hide Init Setup" option and press the left <◀> or right <▶> arrow to set it to YES, then press <↵> to save it.



3.5.8 FDU Cancel

Purpose: If an FDU is stolen from the property, all the remaining FDUs and all the locks on the property must be notified to reject all keycards made by the stolen FDU. To do this an FDU Cancel is performed with an FDU Cancel keycard.

NOTE: The number of the stolen FDU must be known in order to perform an FDU Cancel. Always maintain an up-to-date list of the FDU numbers on the property, and keep it in a safe with any other sensitive information and spare GMA keycards. In the event that an FDU is stolen, use the <⌂> function to display the FDU identification on the remaining FDUs (refer to *Section 3.5.6 - Displaying the FDU Identification*), in order to confirm the number of the stolen FDU.

IMPORTANT: The PINs assigned by the stolen FDU may be still valid throughout the property. It is highly recommended to revoke all known PINs and assign new ones for all users. Please refer to *Section 3.5.5 – PIN Management* for further details.

The FDU Cancel procedure can be done quickly, as soon as an FDU is reported stolen. However, for complete security it is recommended that a Hotel Restart be performed at the earliest convenient time after an FDU is stolen, using a new external Hotel Code. The Hotel Restart completely neutralizes the stolen FDU.

Minimum keycard required: General Manager Authorization

Expiry: 1 to 24 hours (default 24 hours)

Steps to perform an FDU Cancellation

IMPORTANT: Call Kaba Ilco for assistance. A special code is required to make the FDU Cancel keycard. Please call Kaba Ilco Technical Support who will provide the guidance required for the remaining steps.

The entire procedure must be completed within the expiry time.

1. Create 3 FDU Cancel keycards. Swipe one of these cards in every FDU on the property, including the FDU used to encode the FDU Cancel keycard. The FDU will now no longer accept Authorization keycards encoded using the missing FDU.

2. Insert the FDU Cancel keycard once in each lock on the property. The locks will respond with one green flash to indicate the card has been accepted. This action notifies the lock to reject keycards from the missing FDU.

3. Re-issue all Guest, Staff and Authorization keycards that were encoded using the missing FDU. A printout of each new Staff keycard issued should be done in order to record the sequence id of each keycard (Please refer to *Section 4.8 – Printing a Record of Staff Keycards* for more information).

3.5.9 Hotel Restart

The Front Desk Units have been assigned an **internal** Hotel Code at the factory. In addition, the system administrator specifies a confidential **external** Hotel Code. Together, the internal and external Hotel Codes ensure that each installation is unique, and secure. Each component of the system (locks, card readers, FDUs, and every type of keycard) makes use of the Hotel Code to prevent tampering. The FDUs transfer the correct Hotel Code to the locks when the locks are first programmed, and each keycard is automatically encoded with the correct Hotel Code by the FDU.

IMPORTANT: The property should assign its own external Hotel Code and make new General Manager Authorization keycards when the system is first installed, or if security is compromised by the theft of an FDU or disclosure of the Hotel Code.

To choose a new code and transfer it to all the locks, FDUs and keycards requires a Hotel Restart. Once changed, the external Hotel Code is classified information and only select staff members should know the code. Typically, GMA cardholders should know what the code is.

NOTE: Consult Kaba Ilco Technical Support if in doubt concerning the need to perform a hotel restart. Because the procedure is somewhat complex and involves all the locks, FDUs and keycards, it is recommended that the Hotel Restart be performed at night.

Write down the external Hotel Code and keep it in a secure place!

The Hotel Restart procedure is divided into several tasks:

- Selecting a new external Hotel Code
- Making a Hotel Restart keycard
- Using the Hotel Restart keycard in the first FDU

- Making new General Manager Authorization, Emergency and Initialization keycards on the first FDU
- Storing the new Hotel Code and spare GMA, Emergency and Initialization keycards in a safe.
- Synchronizing the remaining FDUs on the property with an FDU to FDU transfer.
- Inserting the Hotel Restart keycard in all locks on the property
- Re-issuing all Authorization, Staff and Guest keycards

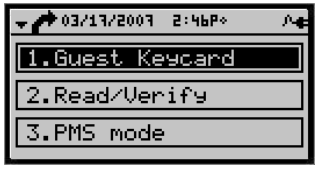
The Hotel Restart keycard has a factory default 24-hour default expiry, so before making the keycard be sure that there is sufficient manpower to pass this card through each lock in the property. If necessary, make more than one Hotel Restart keycard. The keycard is valid only once in each lock and FDU.

Purpose:	To perform a Hotel Restart to protect the property with a personalized external Hotel Code.
Minimum keycard required:	General Manager Authorization Expiry: 1 to 24 hours (default 24 hours)

NOTE: The entire procedure must be completed within the expiry time.

Steps to perform a Hotel Restart

1. Swipe a keycard having a GMA authorized user level in the FDU.

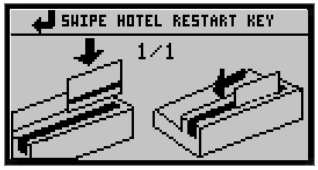


2. Press 4 or use the down <▼> arrow followed by <↵> to reach the “Lock Action Card” menu.

3. Press 6 or use the down <▼> arrow followed by <↵> to reach the “Hotel Restart” menu.

4. Select a new external Hotel Code, write it down and keep the information in a secure location. Enter the new external Hotel Code in the FDU with the keypad, then press the down <▼> arrow to enter the number of Hotel Restart keycards required (more than one is recommended, so that there will be sufficient time to insert one in each lock on the property).

   Press <↵>.



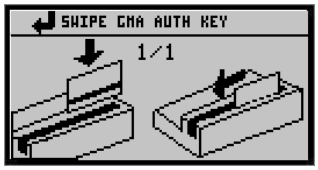
5. Swipe the required amount of blank keycards through the FDU until the requested number of cards is encoded.

NOTE: Hotel Restart keycards should only be handled by upper management or other persons in a position of trust.

6. On the FDU used to make the Hotel Restart key-card, press <⌫> until the Authorization prompt is displayed:

7. Swipe the Hotel Restart keycard through the FDU.

8. Press 1 on the keypad to go forward with the change and create a new GMA keycard or 2 to exit.



9. Swipe a blank keycard through the FDU to create the new General Manager Authorization keycard (number 200).

IMPORTANT: **A magnetic field could erase the GMA keycard. IMMEDIATELY MAKE TWO SPARE GMA KEYCARDS USING THE RESTARTED FDU AND STORE THEM IN A SAFE FOR USE IN EMERGENCIES. The two spare GMA keycards should have two different Authorization numbers (eg: 198 and 199), and these numbers should not be used for any other GMA keycards in use on the property. This ensures that the two spare GMA keycards will always be valid if they are required for emergency use.**

IMPORTANT: **Encode two new Initialization keycards and two Emergency keycards using the restarted FDU, and store them in the safe along with the spare GMA keycards. These keycards may be required in the future to service the system.**

10. If the property has additional FDUs an FDU to FDU transfer must be done to set all FDUs to the same external code (refer to *Section 3.5.4 - Transferring Data to Another FDU* for details on transferring between FDUs).

    Do NOT swipe the hotel restart keycard in a second FDU as a new GMA card will have to be made which will overwrite the GMA keycard made in steps 3 and 4 above.

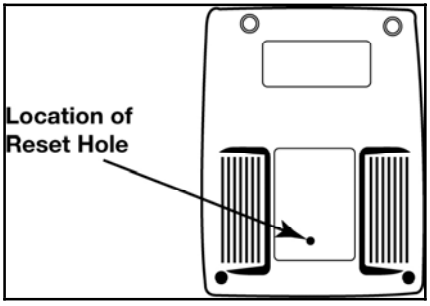
11. Notify the locks of the new Hotel Code by swiping a Hotel Restart key-card through every lock in the property. The keycard is valid only once in each lock. The lock will provide a response by flashing green once but will remain closed.

IMPORTANT: **The Hotel Restart has now been completed. Because the previously issued keycards used a Hotel Code that is no longer recognized by the locks or the FDUs, all required keycards including Emergency, Staff, Guest, Authorization, Passage, etc., required to operate the system must be re-encoded and re-issued. Previous PINs are now revoked and should be reassigned. When encoding Staff keycards, remember to print out the information of each keycard created in order to record each sequence id.**

3.5.10 Resetting the FDU

Purpose: To reset the FDU if it becomes frozen (permanently stuck at one step or screen).

Minimum keycard required: N/A



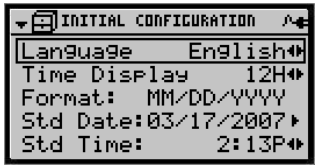
To reset the FDU, use a pin or flattened paper clip to depress the reset button located behind the hole on the bottom of the FDU as shown in the image above.

If the system has been configured to hide the date, time and hotel prompts, as per *Section 3.5.7 - Hiding the Language, Date and Time Prompts*, then the FDU will reset and after a few seconds the main screen will appear and the system is ready to function as before.

If the system has not been configured to hide the language, date, time and hotel prompts, the FDU will reset, and after a few seconds show the initial configuration screen,

indicating the current parameters. No changes should be done, as the FDU maintains these settings for an extended period of time. Without changing any of the information, press <↵> to ensure that the FDU will continue to function correctly with the other FDUs and the locks on the property.

IMPORTANT: **If the date or time is changed the system may no longer function with other FDUs or locks on the property.**



3.5.11 Using the FDU in POS Verifier Mode

In previous versions of the system the FDU and the POS (Point-of-Sale) were separate units. As of the latest FDU model, any FDU in the facility can be used as a Point-of-Sale verifier, to post charges manually to the guest's room or folio.

For this to occur the POS Verifier mode must be enabled. Refer to *Section 3.6 part 17 – Enable POS* for details on setting this feature. Each employee using POS verifier mode should have a unique POS Authorization keycard with a different number from 1 to 200. The POS function is the same as the Read Card function described in *Section 4.9.2 – Reading a Guest Keycard*. The POS Authorization keycard gives access to only that function. The FDU audit records each use of a POS Authorization keycard to read guest information.

Minimum keycard required: POS Authorization

3.6 FDU Feature Reference

Certain features found within various menus in the FDU have different settings available to a GMA authorized user level keycard. Shortcuts via the FDU keypad are indicated to access each feature indicated in this section.

Options that are encoded on keycards are enabled or disabled based on the choice of YES, NO or AUTO. The definitions of YES, NO or AUTO are:

YES: The FDU will offer the user the chance to add this option to the keycard (if applicable).

NO: This FDU will not prompt the user for this feature and it will NOT be added to the keycard.

AUTO: This option will ALWAYS be added to keycards (if applicable). The user will not be prompted.

For example, each Guest Common Area can be set to YES, NO or AUTO. Guest Common Areas, which are paid for separately from the room, should be set to YES, allowing the GSA to add the Guest Common Area to the guest's keycard if they have paid for access. Guest Common Areas, which are open to all guests, such as washrooms accessible from the lobby, should be set to AUTO, to be given to all guests automatically. Guest Common Areas that are unused or linked to specific rooms should be set to NO.

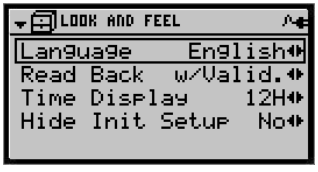
3.6.1. Language

Purpose: Sets the language for the FDU display.

Shortcut: Swipe a GMA keycard, press 7, 2 and 1

Default: The language is set when the FDU is initialized.

Options: The FDU can be configured to operate in different languages (English, French, Spanish, etc). This feature allows the user to select one of the languages for all the screens and menus. For example:



Use the left <◀> or right <▶> arrow to select the language desired. Press <↵> to save the setting.

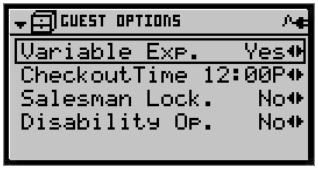
3.6.2. Variable Expiry

Purpose: Guest level keycards can be automatically encoded with the selected default expiry value (Variable Expiry disabled), or the expiry can be specified each time a Guest level keycard is encoded (Variable Expiry enabled).

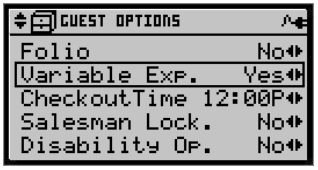
Shortcut: Swipe a GMA keycard, press 7, 2, 2, 1 and 1

Default: Enabled

Options:
YES: Enabled
NO: Disabled



FDU-A



FDU-B

By default the variable expiry is set to YES indicating that each time a guest level keycard is encoded the user can specify a time period for the encoded keycard to be valid.

If set to NO then every guest keycard encoded will be valid only for the default expiry time set within the FDU. The system default is 1 night, please refer to *Section 3.5.2.3 – Setting the Expiry Values:* for details on changing the default value.

Use the left <◀> or right <▶> arrow to select the value desired. Press <↵> to save the setting.

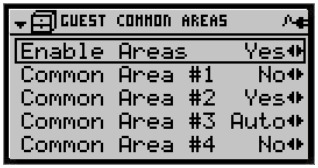
3.6.3. Enable Guest Common Areas

Purpose: There are eight Guest Common Areas available. Guests may be granted access to all or only to some of these areas. Admission to the common areas can be granted automatically when the keycard is encoded. Alternatively, each time a keycard is made, the areas to which guests will be admitted can be selected. Each common area can be set to offer one of these choices.

Shortcut: Swipe a GMA keycard, press 7, 2, 2, 1 and 2

Default: Disabled

Options:
YES: Enabled
NO: Disabled
AUTO: Automatic (only for “Common Area” when “Enable Areas” set to YES)



If the "Enable Areas" option is YES, specify YES, NO or AUTO for each Guest Common Area.

By default the "Enable Areas" option is set to NO, indicating that no Guest Common Areas will be offered when a Guest keycard is encoded.

If the Common Area(s) are to be offered each time a keycard is made, enter YES and when encoding a guest keycard the user will be prompted each time as to whether this specific common area is to be provided to the guest or not.

If the area is not to be offered or if the area is linked automatically to certain rooms, enter No for the specific Common Area(s).

If the area is to be encoded automatically on all guest keycards, enter AUTO for the specific Common Area(s).

Notes:

Do not press <↵> after each entry. Press the up <▲> or down <▼> arrow keys to select the Common Area and the left <◀> or right <▶> arrow to choose between, YES, NO and AUTO. Press <↵> to save the changes or <⌫> to return to the previous menu without saving the changes.

3.6.4. Salesman's Lockout

Purpose:

This feature can be added to any Guest or Suite keycard so the guest can control staff access to his room by locking out Sub-Master, Bellman's Master, and Grand Master keycards. The Emergency keycard is never locked out.

Shortcut:

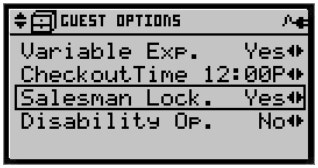
Swipe a GMA keycard, press 7, 2, 2, 1 and 1

Default:

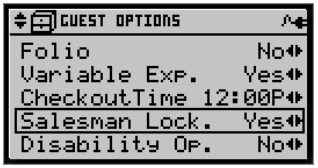
Disabled

Options:

YES: Enabled
NO: Disabled
AUTO: Automatic



FDU-A



FDU-B

When the "Salesman Lock." Is set to YES each time a Guest keycard is encoded the FDU will prompt the user as to whether or not this option is to be encoded on the keycard.

By default the Salesman's Lockout feature is set to NO, indicating that no keycards will be encoded with this option.

If set to AUTO, "Salesman Lock" feature is to be encoded automatically on all guest keycards.

Notes: This feature is not supported on Generation E-760 locks or 770 locks.

3.6.5. Staff Access to Guest Common Areas

Purpose: Staff can be given automatic access to a selection among the eight Guest Common Areas available. When this option is enabled, the selected Guest Common Areas are encoded on each staff keycard.

Shortcut: Swipe a GMA keycard, press 7, 2, 2, 2 and 2

Default: Disabled

Options:

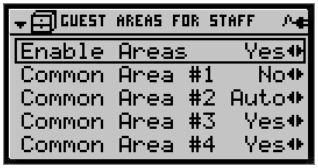
YES: Enabled

NO: Disabled

AUTO: Automatic (only for "Common Area" when "Enable Areas" is set to YES)

By default the "Enable Options" is set to NO, indicating that no cards will be encoded with access to guest common areas.

If the "Enable Areas" option is set to YES, specify YES, NO or AUTO for each Guest Common Area available.



If staff access to specific guest common areas is to be offered each time a staff keycard is made, enter YES. The user will then be prompted for each keycard being encoded as to whether access to those specific Common Areas is to be encoded on the keycard or not.

If the area is not to be offered or if the area is linked automatically to certain rooms, enter NO.

If the area is to be encoded automatically on all staff keycards, enter AUTO. For the Bellman Master keycard type, when AUTO is set, the guest common areas will still be displayed when this type of keycard will be created.

Notes:

Do not press <↵> after each entry. Press the up <▲> or down <▼> arrow keys to select the Common Area and the left <◀> or right <▶> arrow to choose between, YES, NO and AUTO. Press <↵> to save the changes or <⌫> to return to the previous menu without saving the changes.

3.6.6. Staff Common Areas

Purpose:

There are sixteen Staff Common Areas available. Staff may be granted access to all or only some of these areas. Admission to the common areas can be granted automatically when the keycard is encoded. Alternatively, each time a keycard is made, the areas to which personnel will be admitted can be selected. Each common area can be set to offer one of these choices.

Shortcut:

Swipe a GMA keycard, press 7, 2, 2, 2 and 1

Default:

Disabled

Options:

YES: Enabled

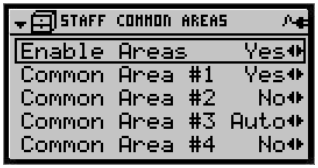
NO: Disabled

AUTO: Automatic (only for “Common Area” when “Enable Areas” is set to YES)

By default the “Enable Areas” is set to NO, indicating that no cards will be encoded with access to these areas.

If the “Enable Areas” option is set to YES, specify YES, NO or AUTO for each Staff

Common Area available.



If the Common Area is to be offered each time a keycard is made, enter YES. For each keycard being encode the user will be prompted as to whether or not access to that specific Common Area is to be provided.

If the area is not to be offered, enter No for the specific common area.

If the area is to be encoded automatically on all staff keycards, enter AUTO for the specific common area.

Notes:

Do not press <↵> after each entry. Press the up <▲> or down <▼> arrow keys to select the Common Area and the left <◀> or right <▶> arrow to choose between, YES, NO and AUTO. Press <↵> to save the changes or <⌫> to return to the previous menu.

3.6.7. Time Zones

3.6.7.1 Fixed Time Zones

Purpose:

There are six fixed time zones that can be used to limit staff access to any lock in the system, except for the RAC Model 3.5, 4 & 4XT Card Readers *(see Section 3.6 part 7.2 – Flexible Time Zones)*.

Time zone 0	00:00 to 04:00 hrs
Time zone 4	04:00 to 08:00 hrs
Time zone 8	08:00 to 12:00 hrs
Time zone 12	12:00 to 16:00 hrs
Time zone 16	16:00 to 20:00 hrs
Time zone 20	20:00 to 24:00 hrs

Each time zone may be given to all staff, to certain staff, or to no staff. When a time zone is encoded on a staff keycard, the locks grants access only during the Time Zone period. More than one Time Zone can be encoded on a staff keycard.

Shortcut: Swipe a GMA keycard, press 7, 2, 2, 2 and 3

Default: Disabled: No time restrictions on staff access.

Options:

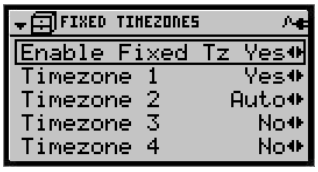
YES: Enabled

NO: Disabled

AUTO: Automatic (only for "Timezone" when "Enable Fixed Tz" is set to YES)

By default the "Enable Fixed Tz" is set to NO, indicating that the staff has access to the specific areas encoded on their card 24 hours a day.

If the "Enable Fixed Tz" option is set to YES, specify YES, NO or AUTO for each Timezone.



If the Time Zone is to be offered each time a keycard is made, enter YES. The user will be prompted for each keycard being encoded as to whether or not each Timezone set to YES is to be encoded on the keycard or not.

If the Time Zone is not to be offered, enter No (no staff will have access during that Time Zone).

If the Time Zone is to be encoded automatically on all staff keycards, enter AUTO (all staff will have access during that Time Zone.

Notes:

Do not press <↵> after each entry. Press the up <▲> or down <▼> arrow keys to select the Time Zone and the left <◀> or right <▶> arrow to choose between, YES, No and AUTO. Press <↵> to save the changes or <⌫> to return to the previous menu.

The locks function on internal time only, and do not know when time changes from Standard Time to Daylight Savings Time. Fixed time zones are actually five hours long to compensate for the time change. In Standard time, keycards will be valid from one hour before the start of the selected time zone to the exact end time of the time zone. In Daylight Saving time, keycards will be valid from the exact start time until one hour following the end of the selected Time Zone (see figure 4.6.7-1).

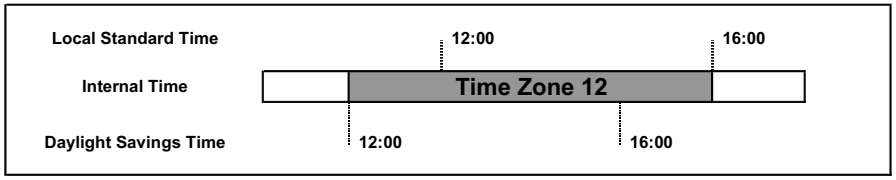


Figure 3.6.7-1: *Daylight Saving Time and Standard Time coverage of Fixed Time Zone 12.*

3.6.7.2 Flexible Time Zones

Purpose:

The RAC Models 3.5, 4 & 4XT do not use the Fixed Time Zones that can be encoded on a Staff keycard. Instead, the RAC models have their own set of 8 Flexible Time Zones, which are defined in the settings of the FDU and downloaded to the memory of the RAC when it is programmed.

Guest, Staff and Passage keycards can be assigned to one of the Flexible Time Zones that are programmed into the Model 3.5, 4 & 4XT RACs.

Each Flexible Time Zone consists of four intervals that can be individually selected. All keycards of the appropriate type (Guest, Staff or Passage) will be valid during the intervals in the assigned Flexible Time Zone, and are not valid (access denied) outside of those intervals. The Passage keycard swiped outside the intervals will put the door in Passage mode at the proper time.

Shortcut:

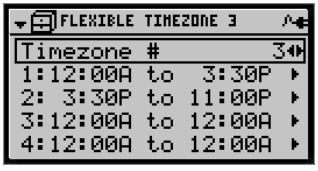
Swipe a GMA keycard, press 7, 2 and 5

Default:

No restrictions, access provided 24 hours a day.

Options:

The Features Menu allows setting up of the time intervals for the 8 Flexible Time Zones, NOT to implement them. There is no option to set each Flexible Time Zone to YES, NO or AUTO, since the choice of which Flexible Time Zone will apply to each Guest, Staff and Passage keycards is made when the RAC is programmed *(see Section 5.5 - Remote Access Controller Models 3.5 and 4 Flexible Time Zones)*.



The FDU shows all defined intervals for a specific time zone. Use the direction keys

and the number keys to change the values.

To remove a time interval, enter a 12:00A to 12:00A interval.

To edit the next interval, continue pressing the <▼> key. Press <↵> when finished to save the settings.

To select a different Timezone # press the left <◀> or right <▶> arrow when the "Timezone #" is highlighted and make changes as desired.

The times entered in the Time Zone will be the times that keycards of the specific type (Guest, Staff or Passage) that the user assigns to that time zone will be valid after the RAC is programmed.

Notes:

The RAC Models 3.5, 4 & 4XTFlexible Time Zones represent the internal time, not the local time. There is no one-hour "grace period" built-in to allow for the change from Standard Time to Daylight Saving Time. Reprogram the RAC twice per year to compensate when clocks are changed.

3.6.8. Checkout Time

Purpose:

The property checkout time can be set to any hour, from 00:00 to 23:00, in one-hour intervals. While the expiry date can be different for each level of guest keycard (Guest, Adjoining Suite, etc.), the checkout time is standard.

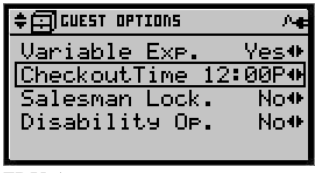
Shortcut:

Swipe a GMA keycard, press 7, 2, 2, 1 and 1

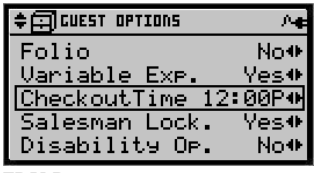
Default:

12:00 (noon); all guest keycards will expire at noon on their respective expiry date.

Options:



FDU-A



FDU-B

If desired, enter a different checkout hour desired using the keypad. Press <↵> to save the setting.

If a mistake is made and <↵> has not been pressed, the left <◀> arrow key can be used to make a correction.

3.6.9. FDU Time-outs

Purpose:

The time-out is the period of time between operations during which the Front Desk Unit remains authorized, before returning to the main screen and requiring the swipe of a new authorization keycard or PIN.

As long as the FDU remains authorized, it can make keycards or access any other function available to the Authorization keycard that was last used. Once timed out, an Authorization keycard must be swiped or a PIN entered again to access any functions of the FDU.

The timeouts should be set to relatively short values, except for special situations requiring a longer "grace period", such as programming a number of locks in sequence or performing a Hotel Restart. The Front Desk Unit time-out selection varies as described below.

Bellman's Authorization:
Time-out occurs automatically after each encoded keycard.

Front Desk, Master, Programming, and General Manager Authorization:
Time-out can be up to 20 minutes. To avoid illicit/unauthorized usage of the FDU by someone other than intended users, it is recommended to set time-outs to a low value.

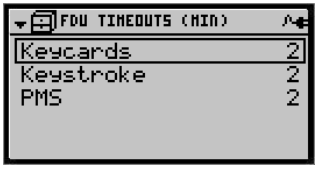
Shortcut:

Swipe a GMA keycard, press 7, 2, 3 and 2

Default:

2 minutes for all time-outs

Options:



Select each timeout, and enter the number of minutes desired with the keypad. Press <↵> to save the settings.

3.6.10. Current Time (DST adjustment)

Purpose:

The internal time on the Front Desk Unit is set when it is initialized. The FDU maintains this time, which is always local Standard Time, which it encodes on

keycards and can download to the locks as required. ***Do not*** ***adjust internal time according to seasonal time changes.***

The FDU also keeps current time. ***Current time*** ***is used to display expiries and audit information in local time. This time is changeable so the FDU may be adjusted to seasonal time changes.***

An example of the use of the current time is in making pre-registered keycards. The arrival time of the guest is specified in the current time, and the FDU automatically encodes the correct internal time on the keycard so that the keycard becomes valid at the time expected by the staff member using the FDU.

Shortcut: Swipe a GMA keycard, press 7, 2, 3 and 1

Default: Disabled

Options:

YES: Enabled

NO: Disabled

When set to YES as shown above, 1 hour is added to the system time to account for daylight savings time. An asterisk (*) on “Local Time” indicates daylight savings time is active. When set an asterisk (*) will also be shown next to the time on the status line from the main screen.

By default the DST adjustment is set to NO and the current time shown in the FDU will be standard time.

Press the left <◀> or right <▶> arrow to toggle between daylight savings time (YES) and standard time (NO). Press <↵> to save the setting.

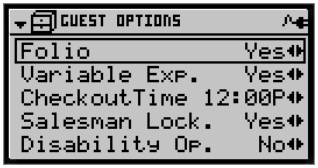
3.6.11. Folio Number

Purpose: Certain properties may use Folio Numbers for guests to make POS purchases. The Folio Number feature must be enabled in order for a folio number to be entered and encoded when issuing a Guest keycard.

Shortcut: Swipe a GMA keycard, press 7, 2, 2, 1 and 1

Default: Disabled

Options:



Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

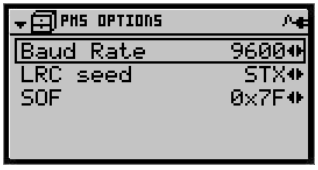
When set to YES as shown in the image above, the Front Desk Unit will provide an option for each guest keycard being encoded to add a folio number of up to 19 digits.

By default the Folio is set to NO and no option will be shown for adding a guest folio number to the guest keycards.

Notes: Folio numbers are only available on triple track FDU systems (FDU-B).

3.6.12. PMS Interface Options

Purpose: Allows the FDU to be used with various Property Management Systems available by third party vendors. These options are to be used only for the Standard (direct) interface configuration, and only by the technician installing the interface. For the Gateway II (indirect) interface configuration, the factory default value must be used.



Take note that those parameters are crucial to have a communication between the PMS and the FDU. Call Kaba Ilco before changing those parameters.

Shortcut: Swipe a GMA keycard, press 7, 2, 3 and 3

Notes: To use the FDU with PMS interfaces the unit must be configured during the hotel's initial configuration at Kaba Ilco.

3.6.13. Programming Authorization (PA) Enable

Purpose: Enables or disables the PA level (Authorization numbers 101 to 120).

The programming authorization function allows certain Front Desk Authorization level staff keycards to also be used to authorize certain staff to program locks, as well as perform lock audits.

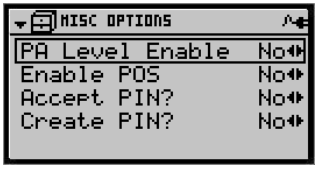
If there are Front Desk Authorization keycards in circulation with addresses between 101 and 120 prior to enabling the PA level, these Authorization keycards become Programming Authorization keycards automatically. If the PA level is disabled, any PA keycards in circulation automatically become Front Desk Authorization keycards.

Shortcut: Swipe a GMA keycard, press 7, 2, 3 and 4

Default: PA level disabled

Options: YES: Enabled

NO: Disabled



When “PA Level Enable” is set to YES, Programming Authorization keycards (Authorization numbers 101 to 120) can be created for staff.

By default “PA Level Enable” is set to NO and Programming Authorization keycards cannot be created. In this situation Authorization numbers 101-120 can be used for Front Desk Authorization keycards.

Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

3.6.14. Guest Keycard Read Back Enable without Room

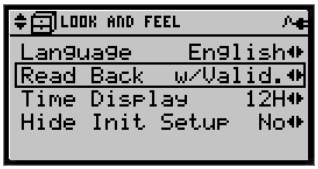
Purpose: Enables the FDU to read the information on a Guest level keycard without knowing the room number beforehand.

Shortcut: Swipe a GMA keycard, press 7, 2 and 1

Default: With validation (room number required)

Options:

With validation (w/Valid):	Enabled (room number required)
Without validation (w/o Valid):	Disabled (room number not required)



When set to "w/o Valid" (without validation) this feature allows GMA and MA authorization level keycards to read back the information on Guest level keycards without having to enter the room number encoded on the card.

When set to "w/Valid" (with validation), anytime a keycard is read back by a GMA or MA authorized user the encoded room number must also be entered to show the information on the Guest keycard.

Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

3.6.15. Disable Prompts

Purpose: To hide or show language, date & time initialization prompts when the FDU is reset.

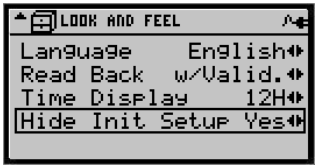
After the system has been installed and configured, it is preferable that the prompts for these important parameters be disabled to avoid the possibility of any changes being done to the system on an FDU reset. After the locks and FDUs on the property have been programmed any changes to the date or time on the FDU has a high probability of affecting the synchronization between the property locks and encoded keycards, as well as between FDUs.

Shortcut: Swipe a GMA keycard, press 7, 2 and 1

Default: Disabled

Options: YES: Hide the prompts

NO: Show the prompts



When "Hide Init Setup" is set to YES, on a FDU reset the system will not show, or allow changes to the language, date & time settings of the FDU.

When "Hide Init Setup" is set to NO, on a FDU reset the system will show the language, date & time settings and allow the user to modify these values. ***Any changes to the date and time settings may affect the reliability of keycards encoded and the property locks.***

Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

3.6.16. Disability Option

Purpose: Intended for guests who may require extra time to turn the handle on a door, the Disability Option allows the time a lock remains open to be extended to 15 seconds if desired. ***Only available on Generation E-760 & 770 series locks.***

Shortcut: Swipe a GMA keycard, press 7, 2, 2, 1 and 1

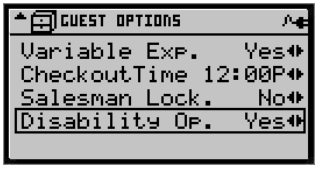
Default: Disabled

Options:

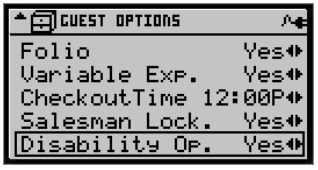
YES: Enabled (prompt the user when encoding keycards)

NO: Disabled (always allow 4 seconds to open the door)

AUTO: Automatic (always allow 15 seconds to open the door)



FDU-A



FDU-B

When the "Disability Op." is set to YES as shown above, for a guest keycard being

encoded, the user is prompted by the FDU as to whether this feature is to be encoded on the keycard or not.

By default the “Disability Op.” is set to NO and this feature is not encoded on any guest keycard being encoded.

When the “Disability Op.” is set to AUTO all guest keycards will be encoded with this feature. Locks will remain open for 15 to allow more time for the user to turn the handle and open the door.

Use the left <◀> or right <▶> arrow to toggle between YES, NO and AUTO. Press <↵> to save the setting.

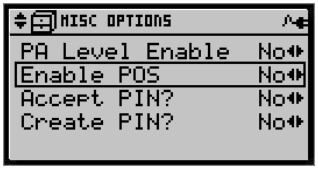
3.6.17. Enable POS

Purpose: Enables or disables the POS verifier mode.

Shortcut: Swipe a GMA keycard, press 7, 2, 3 and 4

Default: Disabled

Options:
YES: Enabled
NO: Disabled



When “Enable POS” is set to YES the FDU can create POS Verifier Mode keycards. Additionally if the FDU is to be used for POS verification this setting must be YES.

By default the “Enable POS” is set to NO and the FDU cannot create the POS Verifier Mode keycards, or be used for POS verification.

Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

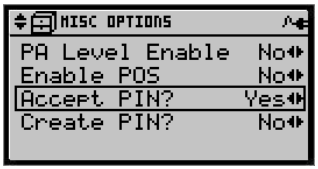
3.6.18. Accept PIN

Purpose: Enables the FDU to allow the use of PINs as a replacement for certain levels of keycards.

Shortcut: Swipe a GMA keycard, press 7, 2, 3 and 4

Default: Disabled

Options:
YES: Enabled
NO: Disabled



When “Accept PIN” is set to YES as shown above the FDU will allow the use of PINs as a replacement for certain authorization levels.

By default “Accept PIN” is set to NO and the FDU will not allow the use of PINs to access the system. In this configuration an authorization keycard is always required to access the FDU.

Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

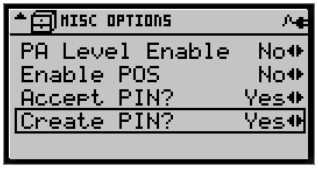
3.6.19. Create PIN

Purpose: Enables the FDU to allow the creation of PINs for certain authorization level keycards.

Shortcut: Swipe a GMA keycard, press 7, 2, 3 and 4

Default: Disabled

Options:
YES: Enabled
NO: Disabled



When “Create PIN” is set to YES the FDU will be able to be used for assigning PINs to certain authorization level keycards.

By default “Create PIN” is set to NO and the FDU will not be able to assign PINs.

Use the left <◀> or right <▶> arrow to toggle between YES and NO. Press <↵> to save the setting.

3.6.20. Time Display

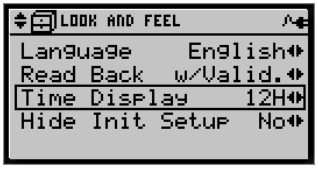
Purpose: To allow the time displayed on the FDU to being either a 12H or 24 H format.

The date format will also be changed dependent on the format selected.

Shortcut: Swipe a GMA keycard, press 7, 2, and 1

Default: 24H

Options:
12H: Time format is 4:35P, date format is mm/dd/yyyy
24H: Time format is 16:35, date format is yyyy-mm-dd



Use the left <◀> or right <▶> arrow on “Time Display” to toggle between 12H and 24H formats. Press <↵> to save the setting.

3.6.21. Privacy Override

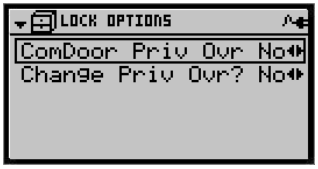
Purpose: This is an alternative to mechanical and electrical overrides for 760, 770, and 710-II lock models in countries that do not typically use deadbolts for privacy features (ex:

Australia). Allows the guest and section keycards to override the thumbturn privacy for given doors.

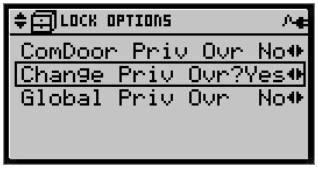
Shortcut: Swipe a GMA keycard, press 7, 2, and 4

Default: Disabled

Options:
YES: Enabled
NO: Disabled



Select the "Change Priv Ovr" option, and use the left <◀> or right <▶> arrow to toggle between YES and NO. NO will preserve any setting on the locks and YES will allow modifications.



Select the "Global Priv Ovr" option, and use the left <◀> or right <▶> arrow to toggle between YES and NO. NO will disable the privacy override and YES will enable it.

Notes: The Global Privacy Override allows the Australian Privacy functionality. This allows Section and Guest to override the deadbolt.

For use only with 710-II locks with firmware version 1.25 or higher, and 760 locks & 770 locks with firmware version 1.35 or higher.

Chapter 4: Keycards

4.1 The Secure Keycard Combination

The Front Desk Unit can encode a virtually endless stream of combinations on the keycards for each keying level in the property. The combinations are based on time, so they will not repeat during the useful life of the product. The combination is encrypted so that even by analyzing many keycards in sequence, it cannot be deciphered and a future combination projected.

The combination contains information which distinguishes the level of the keycard, the property to which it belongs (the "Hotel Code"), the Front Desk Unit on which the keycard was encoded, the keycard's time stamp, the expiry date and time, the sequence id of the keycard and the identity of the person whose Authorization keycard was used to make the keycard. This encrypted information has billions of possible combinations, which prevents a keycard from opening a door for which it has not been programmed.

4.2 The Major Categories of Keycards

There are 5 major categories of keycards, each with a distinct function according to the following table. All keycards are encoded using the FDU. The individual keycards in each category are fully described in *Section 4.10 – Keycard Reference*. Individual keycards are also listed in *Appendix A - Keycard Quick Reference Chart*.

Keycard Category	Function
Entry	Grants guests or staff access to permitted doors.
Authorization	Grants staff access to the menus of the FDU.
Lockout	Locks out specific rooms or combinations of rooms.
Special Purpose	Used to program locks and perform other procedures.
Reset	Cancels a circulating keycard or changes variable lock addresses (Section/Floor/Group/Zone/Area).

Table 4.2: *Major categories of keycards*

4.2.1 Entry Keycards

Entry keycards grant access to a door at one of the Guest, Restricted Area, Sub-Master or Master access levels. These access levels are set up according to the needs of lodging properties, as follows:

Access Level	Sub-Levels	Used by
Guest	Guest	Guests
	Common Door Suite	Guests
	Convention Suite	Guests
	Common Area	Guests and/or Staff
Restricted Area	n/a	Staff
Sub-Master	Section	Staff
("Staff")	Floor	Staff
	Group	Staff
	Zone	Staff
	Area	Staff
Master	Bellman's	Staff
	Grand Master	Top level Staff and/or Management
	Emergency	Top level Staff and/or Management

Table 4.2.1: *Entry keycards*

Each lock is programmed with the access levels that apply to the specific door it controls *(see also section 5.3 – Programming Locks and Remote Access Controllers)*. The lock accepts Entry keycards if their date and time stamp is valid, if they have not expired, and if their Room, Sub-Master or Master level address matches the addresses programmed in the lock.

The Master level address is the same for all locks, so that it gives access to all doors throughout the property. The security of the Master level is provided by controlling the encoding and distribution of the keycards, and by the presence of the audit trail. Master and Sub-master level keycards should be treated like master keys in a mechanical key system.

Suggestions on how to use these levels are given in the following sections of the manual:

- Section 4.10 – Keycard Reference
- Chapter 6 – Implementing the System
- Chapter 9 – Security Procedures
- Chapter 10 – Emergency Procedures

The Sub-master levels are sometimes referred to as the Staff level.

The Section, Floor, Group, Zone and Area Sub-master levels are considered variable address levels, since the address for each of these levels in the lock can be reassigned using a Reset keycard in order to manage staff access.

Example:
A lock can be changed from Group 1 to Group 2 instantly by inserting a Group 2 Reset keycard in the lock. The Guest and Restricted Area level addresses can only be changed by programming the lock using the FDU, and are known as fixed addresses. *(See Chapter 5 – Locks – Using and Programming)*

4.2.2 Authorization Keycards

The Authorization keycards grant access to specific menus of the FDU (see the FDU Menu Chart at the back of this manual). The FDU cannot be used until a valid Authorization keycard is swiped in the magnetic stripe encoder. Menus that are not accessible at the Authorization level in use will not appear on the screen of the FDU.

Authorization keycards are hierarchical. The higher levels include access to all the functions of the lower levels, as follows:

Auth. #s	Authorization Level		Main Applications
1 - 100	**FDA**	**Front Desk**	Making Guest keycards
101- 120*	**PA**	**Programming**	+ Communicating with locks
161 - 180	**MA**	**Master**	+ Most FDU functions and settings
181 - 200	**GMA**	**General Manager**	+ All FDU functions and settings
121 - 160**	**BA**	**Bellman's**	Making Bellman's Master keycard
1-200***	**POS**	**Point-of-Sale**	Puts FDU in POS Verifier Mode

The keycards below the line do not fit within the hierarchy.

* If the Programming Authorization level is disabled in the Features Menu, Authorization nos. 101-120 are available for Front Desk Authorization use.

** The Bellman's Authorization only allows the encoding of a Bellman's Master keycard. The General Manager Authorization keycard also has access to this function. *See section 4.10 part B2 – Bellman's Authorization.*

*** The POS Authorization only gives access to the Read Card Function, for setting the FDU as a Point-of-Sale Verifier for posting charges to a guest's account *(see section 3.5.11 - Using the FDU in POS Verifier Mode)*. Although the POS Authorization uses the same numbers as other Authorization keycards, its use will not invalidate the other keycard or

	vice-versa.

Table 4.2.2: *Authorization keycards*

4.2.3 Lockout Keycards

Lockout keycards always prevent access to a room by some, or all, types of keycards, with the exception of the Emergency keycard, which can open any door on the property, even if it is double-locked from the inside.

The Group Lockout is intended specifically to lock out the Guest level *(see Section 4.10 part C.5 – Group Lockout)*.

The feature known as the Salesman's Lockout is a privacy option that can be encoded on the guest's keycard *(see Section 3.6, part 4 – Salesman's Lockout)*. By activating the Salesman's lockout, a guest can prevent staff or other personnel from entering the room when away.

Lockout Level	Room(s) Affected	Access Levels Locked Out	Lockout Removal
Room	Specific room	All except Emergency	Room Unlock or Hotel Unlock keycard
Hotel	Any room	All except Emergency	Hotel Unlock keycard or specific rooms with Room Unlock keycard
Group	Rooms in a specific Group	Guest only	New Guest keycard
Salesman's	Specific guest room	All except Emergency and Guest	Guest keycard or whenever the Guest keycard used to set the lockout expires.

Table 4.2.3: *Categories of Lockout Keycards*

4.2.4 Special Purpose Keycards

These keycards are used to prepare a lock for programming, to change the Hotel Code, and for other purposes important to the management of the system. *Refer to Section 4.10, part D – Special Purpose Keycards.*

4.2.5 Reset Keycards

Reset keycards have two purposes:

i. To invalidate a circulating keycard for a specific access level

and/or

ii. To change the variable addresses (Section/Group/Floor/Zone/Area Sub-Master levels) in a lock.

Each Entry keycard level has a corresponding Reset keycard that cancels any keycard for the specified level encoded prior to the Reset keycard. A circulating Passage keycard can also be cancelled by its corresponding Reset keycard.

A Reset keycard can be used in one or more locks, depending on its function. New keycards must be made after the Reset keycard is encoded in order for them to work in the locks that have been reset.

Example 1: To cancel all circulating guest keycards for a specific room, use a Guest Reset keycard in the specific guest room lock.

The Sub-master (Section, Floor, Group, Zone and Area) levels and the Convention Suite level are variable addresses, which can be changed by inserting the corresponding Reset keycard in the lock. These levels allow a lock to be adapted to a different pattern of staff assignments, or temporarily assigned to a combination of rooms forming a Convention Suite, without using the FDU *(see Sections 4.10 parts E.1 through E.5)*.

Since the Reset keycard also updates the time stamp table in the lock, it cancels the previous Guest (Convention Suite) or Sub-master (Section/Floor/Group/Zone/Area) level keycard.

Example 2: To cancel all circulating Section 2 keycards, use a Section 2 Reset keycard in all the locks which are currently set to Section 2. New keycards will then have to be issued for Section 2. ***Caution: Do not use the Section 2 Reset keycard in locks that should not be set to Section 2, or the Section variable address will be changed (see example 3 below).***

Example 3: To change all Section 3 locks to Section 2, use a Section 2 Reset keycard in all the locks that are currently set to Section 3. New keycards will have to be issued for Section 2.

Authorization keycards do not have a corresponding Reset keycard. To cancel Authorization keycards, encode a newer Authorization keycard with the same Authorization number and swipe it in all the FDUs on the property *(see Section 4.3 – Updating and Cancelling Keycards)*.

4.2.6 PIN Usage as an Alternative to Authorization Keycards

For certain authorization levels, the FDU can be configured to allow the usage of a PIN as an easier method to access the FDU. Instead of swiping a keycard, the PIN is entered using the FDU keypad. If the entered PIN matches one defined in the FDU memory, access is granted as if the authorization keycard was swiped. If the system is configured to not accept PINs, or the PIN is invalid, a message indicating "Invalid PIN" will be displayed and access to the FDU denied.

Existing and new employees may receive a PIN if the administrator agrees to supply them with one and the system is configured for PIN usage.

Even when an authorization level has a PIN assigned and the FDU is configured to accept PINs, the user's authorization keycard will always be able to log into the FDU if desired.

The usage of a PIN is recorded in the FDU audit as per the usage of an authorization keycard.

NOTES: **In order to create a PIN with an FDU, the system must be configured to allow this function. Refer to *Section 3.6 part 19 – Create PIN* for further details.**

In order to accept the usage of PINs on an FDU, the system must be configured to allow this function. Refer to *Section 3.6 part 18 – Accept PIN* for further details.

IMPORTANT: **With the exception of doing a FDU-FDU synchronization *(see Section 3.5.4 – Transferring Data to Another FDU)* there is no direct communication between FDUs. As such, for sites that have more than one FDU it is strongly recommended to only use one FDU as a "Master FDU" for the creation of PINs. If more than one FDU is used for PIN creation there is a risk that 2 users with differing authorization levels could create the same PIN in 2 different units. This would pose the risk of each user being able to log into the other FDU with the other user's authorization level.**

The following table shows the different authorization levels that can create and manage PINs. For example, a Master can create a PIN for a Front Desk but cannot manage one for a Bellman.

Type of privilege	Authorization levels allowed to have a PIN
General Manager Authorization	Programming, Bellman, Front Desk, POS
Master Authorization	Front Desk, POS

Table 4.2.6: *PIN management access table*

NOTE: For security reasons, the General Manager and Master Authorization levels cannot have PINs assigned.

Once a PIN has been created, the FDU offers some options to manage it afterwards. An authorized user can verify, modify, revoke and copy the PIN to another FDU as detailed below.

4.2.6.1 Creating a PIN:

The PIN assignment is an optional part of the normal authorization keycard creation process. In the case of a new employee, after having specified the authorization type and number, the administrator enters the desired PIN and then creates a new keycard. The PIN is a 4 to 8 digit code and may be chosen by the employee or suggested by the FDU. Refer to *Section 3.5.5.1 – Create/Assign a PIN – New employees:* for detailed steps.

Additionally, an existing employee who does not currently have a PIN assigned to their authorization level can also have one created without having to recreate a new keycard Refer to *Section 3.5.5.2 – Create/Assign a PIN – Existing employees:* for detailed steps.

NOTES: The administrator has the responsibility to manage the choice of the PIN being used. The administrator must avoid PINs being easy to identify such as "1234" or the birthdate of the user.

The administrator has the responsibility to manage the duplication of PINs when more then one FDU is used for assigning PINs within the same property.

If the requested PIN is not already allocated to another employee, it becomes a valid substitution to the users' authorization keycard. For security purposes if a PIN is written down it should be kept in a safe place to prevent unauthorized people from seeing it.

If the PIN is already in use by the FDU, it is rejected and the administrator must choose another one. If the PIN has been revoked in the past, the administrator will have the choice to go forward with the assignment of this PIN or retry with another one which has not been previously used by an employee.

NOTE: Using a PIN that was revoked in the past can lead to security issues as an ex-employee may come back and find out that his old PIN is still valid.

4.2.6.2 Modifying, verifying and revoking a PIN:

In the event an employee forgets their PIN, the system allows an administrator with the right authorization level to swipe the keycard of the employee, and the PIN, if there is

one associated to the keycard, will be displayed. Refer to *Section 3.5.5.3 – Read-back/Verify a PIN:* for details on how to read back the PIN from a keycard.

If the privacy of a PIN has been compromised and other people potentially know the number, it must be replaced by a new one. The current PIN must be revoked and a new one created. Refer to *Section 3.5.5.4 – Modify an existing PIN:* on how to modify a PIN.

Since a PIN may not be reclaimed like a keycard, it must be revoked in certain situations, such as when an employee leaves, is fired, or if the administrator decides to have it revoked for other reasons. Refer to *Section 3.5.5.5 – Revoke an existing PIN* for details on how to revoke a PIN.

4.2.6.3 Transferring a PIN to another FDU:

When a hotel is equipped with more than one FDU, the PINs created can be copied to another FDU. This is not automatically performed at PIN creation since there is no direct communication between multiple FDUs on a site.

There are two options to transfer a PIN to another FDU. Assuming all FDUs are configured to create PINs, the administrator can create the PIN access on each FDU for a given user using the same PIN.

The other option for transferring the PIN to another FDU is to perform a FDU to FDU transfer (refer to *Section 3.5.4 – Transferring Data to Another FDU*). All configuration information as well as PINs defined within the source FDU will overwrite those in the destination FDU.

4.3 Updating and Cancelling Keycards

The lock accepts a keycard only if the following conditions are met.

a) The keycard access level and address are the same as that of the lock.

b) The keycard's time stamp is the same as, or later than, the currently accepted keycard.

c) The keycard has not expired.

As soon as a valid Entry or Reset keycard (one that is more recent than the time stamp for the corresponding level that is stored in lock memory) is used in the lock, its time stamp replaces the previous one. These conditions for acceptance guarantee that no previous keycard is valid once a newer Entry keycard or corresponding Reset keycard has been used in the lock, even if the older keycard has not expired.

IMPORTANT: Encoding a new keycard on the FDU does not cancel the previous keycard until the new keycard is inserted into the lock. The new Entry or Reset keycard must be inserted in all the locks affected by

the cancellation, in order to invalidate all previous keycards with the same address.

IMPORTANT: **To cancel an Authorization keycard, encode a new Authorization keycard with the same Authorization number, and then swipe it in every FDU at the property, including the FDU used to encode the new Authorization keycard. (See example 3.)**

Example 1: New Guest Keycard

Imagine that a guest checks out, and the room is rented to a new guest. The previous guest's keycard was created at the beginning of their registration (Time A). The current guest's keycard is created at a later time (Time B). The following figure illustrates how the new guest's keycard invalidates all previous Guest level keycards when it is first used in the lock.

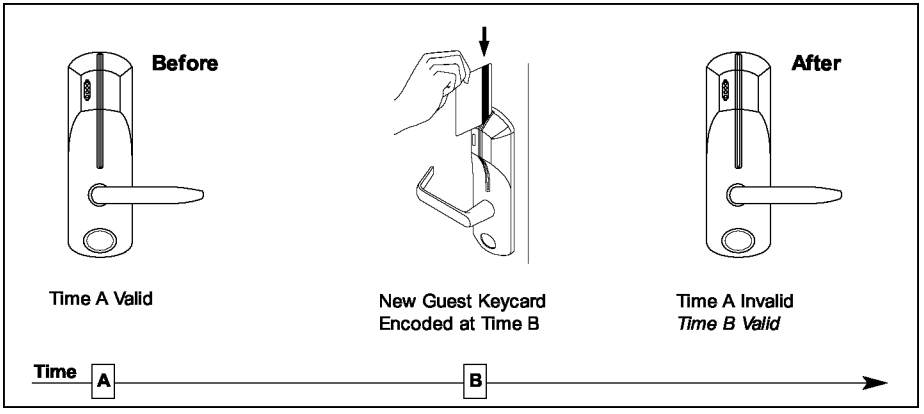


Figure 4.3-1: *Cancellation of previous Guest keycards*

Example 2: Grand Master Reset Keycard

The Grand Master keycard is always a duplicate (see *Section 4.5 – New Versus Duplicate Keycards* and *Section 4.10, part A.16 – Grand Master*), so that more Grand Master keycards can be made at any time without invalidating all the previous Grand Master keycards.

To cancel all the circulating Grand Master keycards, a Grand Master Reset keycard is made, and inserted in every lock on the property before it expires. In the following figure, a Grand Master Reset encoded at Time B changes the valid time for all future Grand Master keycards from A to B. Any Grand Master keycard made after Time B will be accepted but those made at time A will now be refused.

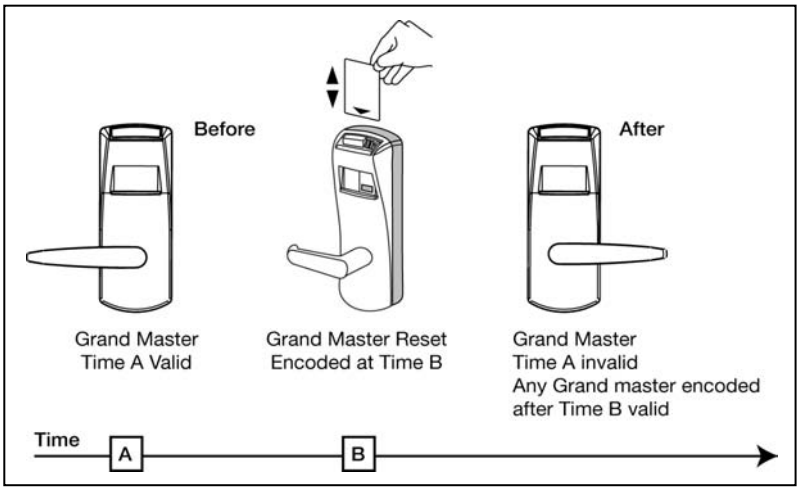


Figure 4.3-2: *Cancellation of previous Guest keycards*

Example 3: New Authorization Keycard

Suppose a Front Desk Authorization (FDA) has been lost (eg: Authorization #20). A new FDA #20 keycard should be encoded immediately on any FDU. The new FDA #20 keycard will invalidate the usage of the lost keycard as it has a more recent time stamp. ***Immediately swipe the new FDA #20 keycard in every FDU in the facility, including the FDU used to encode the new keycard.*** The time stamp for FDA #20 will thus be updated in every FDU, and the lost keycard will no longer be accepted, throughout the property.

4.4 Keycard Expiry

When a keycard is encoded, the expiry date and time after which it will no longer be valid is encoded on the keycard. There are two types of expiries, variable and selectable. The Guest levels have a variable expiry, meaning that the expiry may be chosen when making a keycard, if the Variable Expiry option is enabled in the Features Menu *(see Section 3.6, part 2 – Variable Expiry)*.

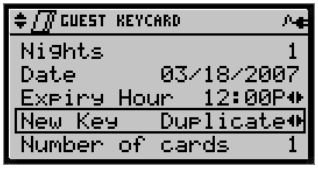
For all other types of keycards, or if the Variable Expiry option is disabled, the default expiry is encoded automatically. This is referred to as the selectable expiry, since the expiry value can be selected for each type of keycard using a General Manager Authorization keycard *(see Section 3.5.2 – Setting Keycard Expiry Values)*. The selectable expiry ranges and the default value loaded in the factory default settings of the FDU are summarized in *Appendix A - Keycard Quick Reference Chart*.

4.5 New Versus Duplicate Keycards

The FDU can make New or Duplicate keycards. When making a Guest keycard, the choice between New and Duplicate is possible after the room or suite number has been chosen. To toggle between both choices, select "New Key" and use the Left <◀> and Right <▶> arrows as shown below.

For a New keycard:

For a Duplicate keycard:



Pressing <↵> will encode a New or Duplicate keycard depending on the choice selected.

For a detailed description on the screen and menus functionality, keypad and arrow keys usage, refer to *Section 3.2 – FDU Overview*.

4.5.1 New Keycards

Whenever a keycard designated as New is made and used in the lock, the time stamp in lock memory is updated for that level and all previous keycards (New or Duplicate) are cancelled.

4.5.2 Duplicate Keycards

The system provides for the addition of users in situations where invalidating existing keycards is not wanted. Duplicate keycards should be made in situations where it is necessary to add a user (for example, an additional occupant arriving to join an existing guest in the same room).

A Duplicate keycard is accepted only when all the following conditions are met:

a) The keycard access level and address are the same as that of the lock;

b) The time stamp of the Duplicate keycard is more recent than the most recently used New keycard;

c) The keycard has not yet expired.

The Duplicate keycard does not invalidate the existing keycards at that level. Both the New keycard and the Duplicate keycard remain valid until they expire, or until a more recent New keycard is inserted in the lock.

4.5.3 When to Use New or Duplicate Keycards

New guests must always receive New keycards, thereby assuring that the previous guest's keycard is invalidated after they insert their keycard in all locks leading to their room. When a guest registers, the quantity of keycards needed by the guest's party are encoded together, and they are all identical New keycards (e.g. a family of three staying in a single suite would receive three New keycards made together). As soon as one of the New keycards is used in the lock, the previous guest's access is cancelled. Any Entry keycards made to invalidate keycards that have been lost must also be New keycards.

NOTE: The Bellman's Master, Grand Master and Emergency keycards are always Duplicates in order to avoid a situation in which a New Master level keycard could invalidate other Master keycards in some or all of the locks, leading to confusion in an emergency. To invalidate these keycards, a Reset keycard must be used in all locks.

To avoid the mistake of invalidating current keycards, ensure that New keycards are not issued when a Duplicate is required.

Situation	Keycards to Issue
Lost keycard*	New or Reset
Stolen keycard*	New or Reset
New guest registration	New
Replacement keycard**	Duplicate**
Add guests to an existing registration	Duplicate
Add staff to a Sub-master level	Duplicate

* For specific information on lost or stolen keycards, refer to *Chapter 10 – Emergency Procedures*.

** Only issue a Duplicate keycard if the damaged or defective keycard is returned. If the old keycard is not returned, issue a New or Reset keycard.

Table 4.5.3: *When to use New or Duplicate Keycards*

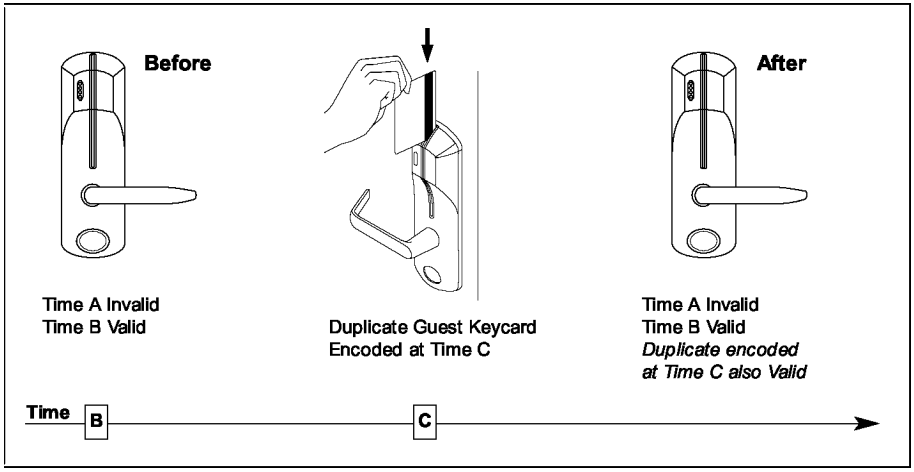


Figure 4.5.3: *Duplicate keycards made after the currently valid keycard (time B) are accepted without invalidating any other keycard.*

4.6 Options When Making Keycards

Certain options are available on the FDU when making certain types of keycards. In order for the options to appear on the screen when making a keycard the specific features must be enabled in the system. Refer to *Section 3.6 – FDU Feature Reference* for configuring the FDU system with specific features or options desired. If an option is not enabled, it will not appear on the display when keycards are being made, and the default value for that feature will automatically be encoded on the keycard.

Many of the options are enabled or disabled based on the choice of YES, NO or AUTO as the feature setting. In these cases, the definitions of the choice of YES, NO or AUTO is as follows:

YES: The FDU will prompt the user as to whether or not this option is to be added to each keycard being encoded (if applicable).

NO: This FDU will not prompt the user for this feature which will not be encoded on the card.

AUTO: This option will ALWAYS be added to keycards of the correct type. The user will not be prompted.

Example:

Each Guest Common Area can be set to YES, NO or AUTO (see *Section 4.6.1.2 – Guest Common Areas*). Guest Common Areas which are paid for separately from the room

should be set to ***YES***, allowing the Front Desk Clerk to add the Guest Common Area when encoding the guest's keycard if the guest has paid the supplement.

Guest Common Areas which are open to all guests, such as washrooms accessible from the lobby, should be set to ***AUTO***, to be given to all guests automatically.

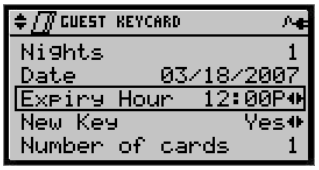
Unused Guest Common Areas or Guest Common Areas that are linked automatically to specific rooms should be set to ***NO***.

4.6.1 Options for Guest Level Keycards

4.6.1.1 Variable Expiry

Applicable Keycards: Guest, Adjoining Suite, Common Door Suite, Convention Suite, Pre-registered Guest, Pre-registered Adjoining Suite, and Pre-registered Common Door.

Description: When this option is enabled, Front Desk staff and others can change the number of nights and the check-out time, after which a Guest level keycard automatically becomes invalid. The default time is displayed in the following format:



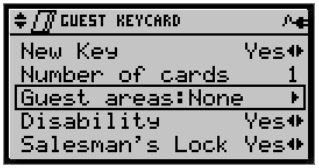
In 12H mode, the right <▶> arrow alternates between AM and PM, in 24H mode it is not used. Using the numeric keypad a new Expiry Hour can be entered. When all other parameters (nights, number of cards, etc) are set, press <↵> to encode the keycard.

4.6.1.2 Guest Common Areas

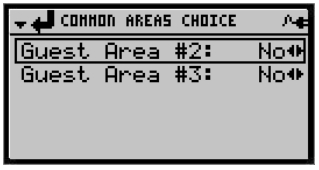
Applicable Keycards: Guest, Adjoining Suite, Common Door Suite, Convention Suite, Pre-registered Guest, Pre-registered Adjoining Suite, and Pre-registered Common Door.

Description: There are 8 Guest Common Areas available in an FDU. These are low security zones that may include services for which the guest has paid an extra fee, such as a pool or parking, which should be encoded on the keycard only if applicable. Each Guest Common Area is set to YES, NO or AUTO in the Features menu. When it is set to YES, the FDU will ask whether to include that specific common area for the guest before encoding a Guest Entry keycard.

For example, if the Guest Common Areas #2 and #3 are set to "YES" in the Guest Common Area (refer to section 3.6 part 3 – Enable Guest Common Areas) the user must select whether the Guest card being encoded will have access to this specific common area.



Press the right <▶> arrow to access the available common areas that can be selected. By default, access to the available common area(s) will be set to NO:



Press the left <◀> or right <▶> arrow to set access to desired areas to YES. Press <↵> to return to the Guest Keycard Menu.

4.6.1.3 Salesman's Lockout

NOTE: Not available on E-760 & 770 Series locks and RAC models 3.5, 4 & 4XT. If this option is encoded on the keycard it will not have any effect on these products.

Applicable keycards: Guest, Adjoining Suite, Common Door Suite, Convention Suite, Pre-registered Guest, Pre-registered Adjoining Suite, and Pre-registered Common Door.

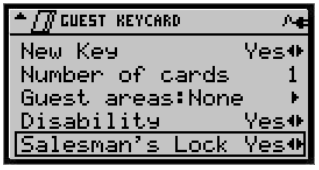
Description: The Salesman's Lockout feature offers increased protection for the guest's privacy and valuables when the guest is not in the room. When added to the guest's keycard, the guest can control staff access to their room by locking out all but their own keycard and the emergency keycard.

The Salesman's lockout is engaged by the guest by inserting their keycard after leaving the room, without turning the handle. The lock will respond with a single green flash. When the guest returns and enters their room, the Salesman's Lockout is automatically removed.

To ensure privacy when occupying the room, the guest may activate the inside thumbturn to throw the deadbolt. Only the Emergency keycard can override a thrown deadbolt.

The Salesman's Lockout is an example of a feature made possible by using keycards instead of traditional keys.

If the Saleman's Lockout is enabled in the Saleman's Lockout menu *(refer to section 3.6.4 – Salesman's Lockout)*, the Saleman's Lock item will be displayed in the applicable keycard menus.

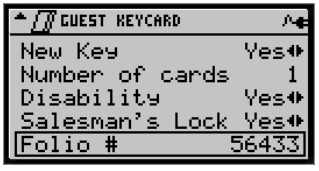


Press the left <◀> or right <▶> arrows to change between available values. When set to NO the Salesman's Lockout feature will not be encoded on the keycard. When set to YES (default value when enabled), the Salesman's Lockout feature will be encoded on the keycard.

4.6.1.4 Guest Folio Number

Applicable Keycards: Guest, Adjoining Suite, Common Door Suite, Convention Suite and Pre-registered

Description: Some properties use a folio number to track guest preferences, or to post charges from Point-of-Sale locations such as restaurants, bars, casinos or other paying services to the correct guest account. If folio numbers is enabled *(refer to Section 3.6 part 11 – Folio Number)*, the Folio will be displayed in this menu. Enter the guest's folio number of up to 19 digits when making each Guest Entry keycard:



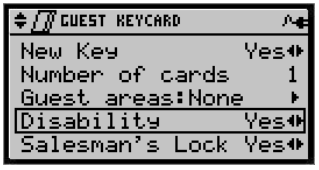
Enter the desired folio number. If an error is made, pressing the left <◀> arrow will delete the last digit entered.

4.6.1.5 Disability Option

Applicable Keycards: Guest and Pre-registered Guest

Description: Available on Generation E-760, 770, and E-710-II locks only, the Disability Option changes the time delay during which the door can be opened after a valid Guest level keycard is swiped from 4 seconds to 15 seconds. This assists guests who may have difficulty turning the handle or opening the door. If the Disability Option is set to "YES" in the Disability Option *(refer to section 3.6 part 16 – Disability Option)*, the Disability item will be displayed in the applicable keycard menus.

The Disability Option has no effect when the keycard is used in locks other than the Generation E-760, 770, and E-710-II locks.



Press the left <◀> or right <▶> arrows to change between available values. When set to NO the Disability Option will not be encoded on the keycard and doors will open only for the standard 4-second delay. When set to YES (default value when enabled) the Disability Option will be encoded on the keycard and applicable doors will open for 15 seconds.

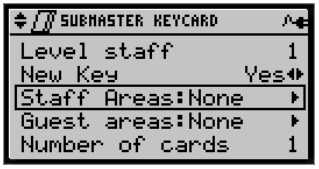
4.6.2 Options for Staff Level Keycards

4.6.2.1 Staff Common Areas

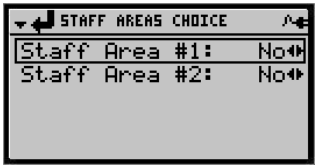
Applicable Keycards: Section, Floor, Group, Zone, Area

Description: There are up to 16 Staff Common Areas available in the FDU. These are low security zones that may include the cafeteria, staff locker rooms, service elevators, entrances, etc. that could be encoded on the staff keycard only if applicable. Refer to S*ection 3.6 part 6 – Staff Common Areas* for details on Staff Common Areas configuration.

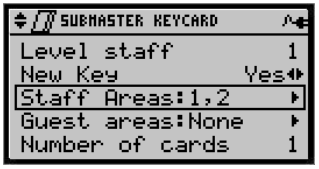
For example, if Staff Common Areas #1, #2 and #3 are set to YES in the Staff Areas menu, the user must select whether the staff keycard being encoded will have access to these specific staff common area(s).



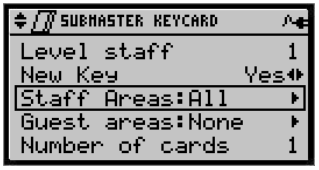
Press the right <▶> arrow to access the available Staff Areas that can be encoded on the keycard. The available Staff Areas will be listed, defaulting to NO.



Use the up <▲> or down <▼> arrows to select each Staff Area and press the left <◀> or right <▶> arrow to set the value to YES if it is to be encoded on the staff keycard. When the areas are set accordingly, press <↵>. The following is displayed when ready to encode specific Staff Areas to a Staff card:



If all 16 Staff Areas are available and set to YES for a Staff keycard the following is shown:



When all required parameters are set, press <↵> to encode the keycard with access to the selected Staff Common Area(s).

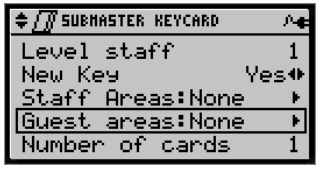
4.6.2.2 Guest Common Areas encoding for staff keycard

Applicable Keycards: Section, Floor, Group, Zone, Area, and Bellman's Master

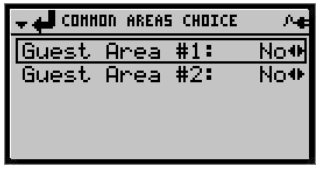
Description:

There are 8 Guest Common Areas available in the FDU, which may also be required for the staff to access. These are low security zones such as a pool or parking, and should be encoded on the keycard only if applicable to the specific staff. Each sub-master level keycard may have access to any guest common area, depending on the administrator decision. Refer to *Section 3.6 part 5 – Staff Access to Guest Common Areas* for configuration details.

For example, the FDU is set to grant staff access to guest common areas. Guest Common Areas #1, and #2 are set to AUTO, and Guest Common Areas #3 and #4 are set to YES. When encoding applicable staff keycards the user selects whether or not to grant access to the available Guest Common Areas.



Press the right <▶> arrow to choose the Guest Common Area(s) to encode on the staff keycard:



Use the up <▲> or down <▼> arrows to select each Guest Common Area available. By default the value is set to NO. Press the left <◀> or right <▶> arrow to set the value to YES if the particular Guest Common Area is to be encoded on the staff keycard. Note that the applicable staff card being encoded will automatically get access to Guest Common Areas #1 and #2 (as they are set to AUTO).

When encoding a Bellman Master keycard, all guest common areas set to AUTO will still appear in the list, defaulted to NO, so they will have to be entered manually staff access is desired.

4.6.2.3 Fixed Time Zones

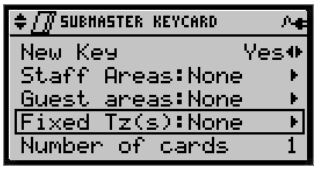
These time zones are available in all locks programmed as Guest or Staff Common Area locks, where flexible time zones apply. Some RAC 3.5 card readers equipped with

specific firmware versions will support time zones (for details please contact Kaba Technical Support). All RAC 4 & 4XT card readers support time zones.

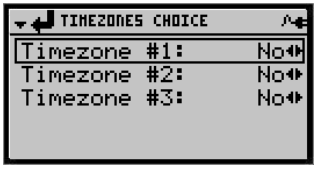
Applicable Keycards: Section, Floor, Group, Zone, Area and Grand Master

Description: Up to six time zones can be used to limit the validity of staff keycards to certain hours:

1) Time Zone 0 00:00 to 04:00 hrs.
2) Time Zone 4 04:00 to 08:00 hrs.
3) Time Zone 8 08:00 to 12:00 hrs.
4) Time Zone 12 12:00 to 16:00 hrs.
5) Time Zone 16 16:00 to 20:00 hrs.
6) Time Zone 20 20:00 to 24:00 hrs.



Press the right <▶> arrow to access the available timezones.



Each Timezone that is set to "YES" in the Fixed Time Zone Menu (refer to section 4.6 part 7.1 – Fixed Time Zones) will be displayed and defaulted to NO. Press the left <◀> or right <▶> arrow to set the value for any desired Timezone to YES. When the keycard is encoded the staff will only have access to locks during the timezone periods set to YES.

Use the AUTO option in the FDU Features Menu to give access to a time zone on all staff keycards. ***Note that if time zones are enabled, but no time zones are selected using the AUTO or YES options, the keycard will never be valid, and the FDU will warn the user with an error message.***

4.6.3 Options for Authorization Level Keycards

4.6.3.1 Accepting PIN

Applicable keycards: Front Desk, POS, Bellman's, and Programming authorization levels.

Description: Allows the FDU to accept the use of PINs for certain keycards as an alternative to using authorization keycards.

Refer to *Section 3.6 part 18 – Accept PIN* for details.

4.6.3.2 Create PIN

Applicable keycards: Front Desk, POS, Bellman's, and Programming authorization levels.

Description: Allows the FDU to create PINs for certain keycards

Refer to *Section 3.6 part 19 – Create PIN* for details.

It is strongly recommended to only use one FDU for the creation of PINs to avoid the same PIN being used by different users on different FDUs on the same property.

4.6.3.3 Assigning a PIN when making an authorized keycards

If the FDU has been configured to accept the creation of PINs (see 3.6.3.1) a PIN may be assigned to certain employee levels as an alternative to their keycard.

Applicable keycards: Front Desk, POS, Bellman's, and Programming authorization levels.

Description: Allows a PIN to be assigned to an authorized level user.

Refer to *Section 3.5.5.1 – Create/Assign a PIN – New employees:* and *Section 3.5.5.2 – Create/Assign a PIN – Existing employees:* for details.

4.7 Making and Resetting Keycards

Purpose: To encode or reset any of the keycards used in the system.

Minimum keycard required: Refer to *Section 4.10 – Keycard Reference*, *Appendix A – Keycard Quick Reference Chart*, or the fold-out *"FDU Menu Chart"* at the end of this manual.

Steps to encode a keycard:

1. Swipe a keycard or enter a PIN having a valid authorization user level.

2. Depending on the user level, from the main menu, the “Guest Keycard” and “Reset Keycard” options are accessible.

   Keycard menu:

   Reset Keycard menu:

3. Press <↵> or **1** to select the “Guest Keycard” menu, or scroll down to the “Reset Keycard” menu with the <▼> arrow and press <↵> or by pressing **5**.

4. The FDU will display a list of the keycards that are available at the Authorization level that was used to activate the FDU.

   Guest Keycard:

   Reset Keycard:

A complete list of all the possible keycards that can be encoded along with their shortcuts is given in *Table 4.7 – Available keycards*.

Shortcut	Level	Reset Keycard Available (Shortcut)
	Guest Level Access	
1,1	Guest	Yes (5,1,1)
1,2	Adjoining Suite	Yes (5,1,2)
1,3	Common Door Suite	Yes (5,1,3)
1,4	One-Shot	Yes (5,1,4)
1,5	Convention Suite	Yes (5,1,5)
1,6	Pre-registered Guest	Yes (5,1,6)
1,7	Pre-registered Adjoining Suite	Yes (5,1,6)
1,8	Pre-registered Common Door Suite	Yes (5,1,6)
	Lock Action Card	
4,1	Battery Test	No
4,2	Programming	No
4,3	Installation	
	– Initialization	No
	– Test Lock	No
4,4	Passage	
	– Guest Room	Yes (5,2)
	– Guest Common Area	Yes (5,2)
	– Staff Common Area	Yes (5,2)
	– Restricted Area	Yes (5,2)
4, 5	Lockout/Unlock	
	– Group	No
	– Room	No
	– Hotel	No
4,6	Hotel Restart	No
	Sub-Master Level Access (staff)	
6,1	Section	Yes (5,3,1)
6,1	Floor	Yes (5,3,1)
6,1	Group	Yes (5,3,1)
6,1	Zone	Yes (5,3,1)
6,1	Area	Yes (5,3,1)
	FDU Authorization (staff)	
6,2	Front Desk (FDA)	No

6,2	POS	No
6,2	Bellman's (BA)	No
6,2	Programming (PA)	No
6,2	Master (MA)	No
6,2	General Manager (GMA)	No
	Restricted (staff)	
6,3	Restricted Area	Yes (5,2)
	Master Level Access (staff)	
6,4	Bellman's Master	Yes (5,3,3)
6,5	Grand Master	Yes (5,3,4)
6,6	Emergency	Yes (5,3,5)

Table 4.7: *Available keycards that can be encoded*

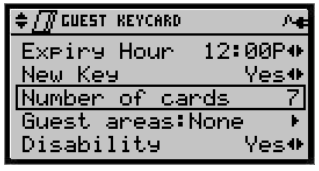
The shortcuts displayed in the table are applicable from the main screen accessed after a valid keycard or PIN is used to access the FDU. Additionally the Home key <⌂> could be pressed in any sub-menu to return to the main access screen for the authorization level and the shortcut keys can then be used.

5. Access the desired keycard type. A series of questions may be asked, or various options configured, dependent on the keycard type selected.

   For example:

   When Guest keycards are made, the FDU asks for the room number. In addition some fields can be manually changed, such as the number of nights, expiry hour, if the keycard is New or a Duplicate, and the number of cards desired. Other fields may also be available dependent on the FDU features set (ex: Salesman's Lockout, Guest Common Areas, etc.).

   For most types of keycards, a choice can be made to encode one or more copies of the keycard:



   When all values are entered for the keycard to be encoded, press <↵> to proceed to encoding the keycard with the options set.

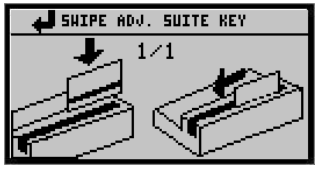
NOTE: If New Key is selected, all of the keycards encoded will be identical New keycards and will have the same date and time stamp, to ensure that they will not cancel each other when used in a lock. Any of the identical

keycards can be inserted in the lock to cancel previously encoded keycards of the same level.

If Duplicate keycard is selected, all of the keycards encoded will be identical Duplicate keycards (for more information, see section 4.5 – New Versus Duplicate Keycards). Some keycards, such as Grand Master and Emergency keycards are always duplicates, so that they can never cancel each other when used in locks.

6. The keycard(s) can now be encoded. The FDU will identify the type of keycard, and request that a blank keycard be swiped.

   For example, for an Adjoining Suite, the FDU screen will show:



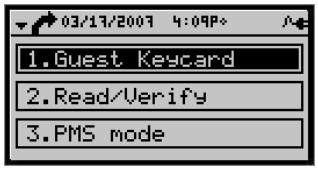
   Insert and swipe the first keycard.

   If more than one keycard has been requested the FDU will prompt for additional keycards to be swiped. Continue encoding blank keycards until the number requested have been done.

NOTE: Keycards must be passed evenly through the encoder, with the magnetic stripe down and to the right (away from the keypad and the screen). A wide range of speeds is accepted, and the FDU will indicate if encoding was successful or not.

Example: Making a Guest keycard for Guest Room 101 with a GMA authorized user.

1. Swipe a GMA authorized level keycard. *(Note that if a FDA keycard or PIN was used to access the system the screen shown in Step 3 would be the initial display).*



2. Press <↵> or press 1 to select the “Guest Keycard” menu.

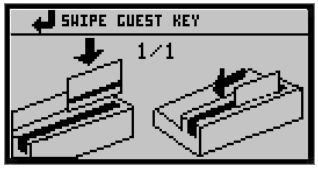
3. Press <↵> or press 1 to select the “Guest” menu.

Enter room number 101 (as example).

Other options can be changed such as Expiry Hour, New or Duplicate Key, and any other options enabled in the FDU.

Press <↵> when all options are set to encode the keycard.

4. The FDU will request a keycard to be swiped.



Insert and swipe a keycard.

A Guest keycard has now been created for room 101.

4.8 Printing a Record of Staff Keycards

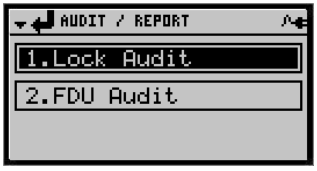
After creation of a staff keycard, the information should be printed out from the FDU and stored with the employee's file. The audit can be printed with either using a serial or USB line printer or with a USB memory stick and a PC with a text editor or standard spreadsheet program.

NOTE: Some serial or USB line printers may not work properly with the FDU. Call Kaba Ilco for assistance.

To print out the staff information from the FDU audit, follow the steps described below.

1. Swipe a keycard having a GMA or MA authorized user level

2. Use the down <▼> arrow followed by <↵> to reach the "Audit/Report" menu, or simply press 9 as a shortcut.



3. Use the down <▼> arrow followed by <↵> to reach the "FDU Audit" menu, or simply press 2 as a shortcut.

The default media is “Screen” which is the FDU’s LCD. To choose the Serial or USB line printer, select the “Media” option and use the left <◀> or right <▶> arrows to set it to “Serial Printer” or “USB Printer” dependant on the printer connected to the FDU.

The default Filter option is “All”, which will print all the different audit types available within the FDU. To print only the staff information select “Filter” with the down <▼> arrow and use the left <◀> or right <▶> arrow to set it to “Staff”.

4. Press <↵> to start the printing of the staff audit.

4.9 Verifying and Reading Keycards

4.9.1 Verifying a Guest Keycard

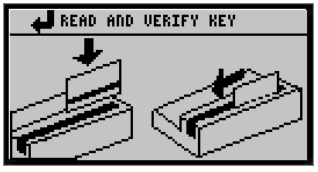
Purpose: If a Guest level keycard is not functioning properly, it can be verified using the “Read/Verify” function. The guest’s room number encoded on the keycard must be known for this function, unless the FDU is configured to not require it *(see Section 3.6 part 14 – Guest Keycard Read Back Enable without Room for details)*.

Minimum authorization level: Front Desk Authorization

Steps to Verify a Guest Keycard:

1. Swipe a keycard or enter a PIN value having a Front Desk authorized user level. If the user level is FDA, press the <⌂> key to reach the main screen.

2. Use the down <▼> arrow and press <↵> to reach the "Read/Verify" menu, or simply press **2** as a shortcut.



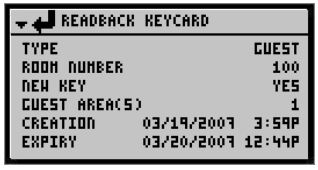
3. Swipe the keycard to be verified.

   If the keycard is not a Guest keycard type the FDU will display an error message of "Invalid Keycard Type" and return to the previous menu. Otherwise the user will be prompted for the room number if required.

4. Enter the room number of the keycard being verified, then press <↵>. For a room that is part of a Common Door Suite, enter the Common Door number.

   If the keycard does not match the room number entered the FDU will display an error message of "Invalid Keycard Type" and return to the previous menu.

   If the keycard matches the room number entered, the details of the keycard will be displayed on the screen.



5. To see the remaining information of the keycard, use the down <▼> arrow. If the FDU is a triple track system allowing Folio numbers, and the keycard has no folio defined, the field will be left blank.

If the FDU is a triple track system allowing Folio numbers, and the keycard has a folio defined, the folio number will be indicated as shown below.

6. Press any key to return to the Main Menu.

4.9.2 Reading a Guest Keycard

Purpose:

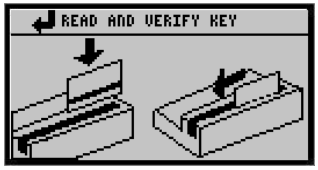
A Guest keycard can be read without knowing the room number if the "Read Back without Verification" option is enabled. Refer to *Section 3.6 part 14 – Guest Keycard Read Back Enable without Room* for details. This procedure allows the room number to be determined, and can have an adverse impact on security if misused. For security reasons, this function is audited, carrying the Authorization number of the person reading the keycard, the date and time, and the room number of the keycard read. If a printer is connected to the FDU, a record is automatically printed.

Minimum authorization keycard: Front Desk Authorization

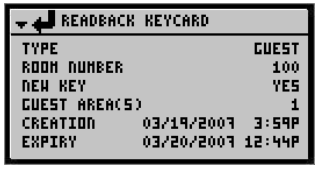
Steps to Read a Guest Keycard

1. Swipe a keycard or enter a PIN value having a Front Desk authorized user level. If the user level is FDA, press the <⌂> key to reach the following menu.

2. Use the down <▼> arrow to reach the Read/Verify menu and press <↵>, or as a shortcut simply press 2.



3. Swipe the keycard to be verified. The information encoded on the keycard is shown on the screen.

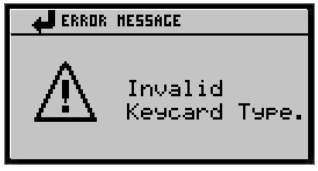


4. To see the remaining information, use the down <▼> arrow.

   If the FDU is a triple track system allowing Folio numbers, and the keycard has no folio defined the information shown will have a blank information for the Folio:

   If the FDU is a triple track system allowing Folio numbers, and the keycard has a folio number defined, the information shown will include this number:

5. If the keycard is not a Guest keycard, the FDU displays:



6. Press any key to return to the Main Menu.

4.9.3 Verifying a Staff Keycard

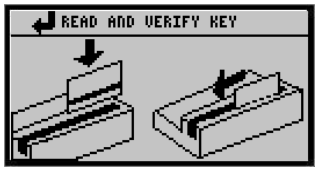
Purpose: When a Staff keycard is returned, it can be verified (or "logged off"). This procedure does not invalidate the Staff keycard, which can be signed back out for usage again on another shift. Verifying a Staff keycard is intended to provide proof that a Staff keycard was returned, and that it was the same Staff keycard issued to the employee, for which they signed the corresponding entry in the log. It can also be used to verify the Staff keycard if it is malfunctioning. This function is audited in the FDU and a record can be printed if required.

Minimum authorization level: Master Authorization

Steps to verify a Staff Keycard:

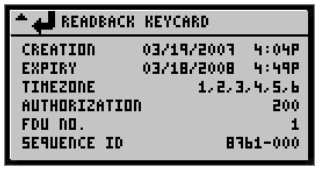
1. Swipe a keycard with a minimum MA authorized user level.

2. Use the down <▼> arrow to reach the “Read/Verify” menu and press <↵>, or simply press **2** as a shortcut.



3. Swipe the staff keycard.

To see the remaining of the information, use the down <▼> arrow.



4. Press any key to return to the Main Menu.

4.10 Keycard Reference

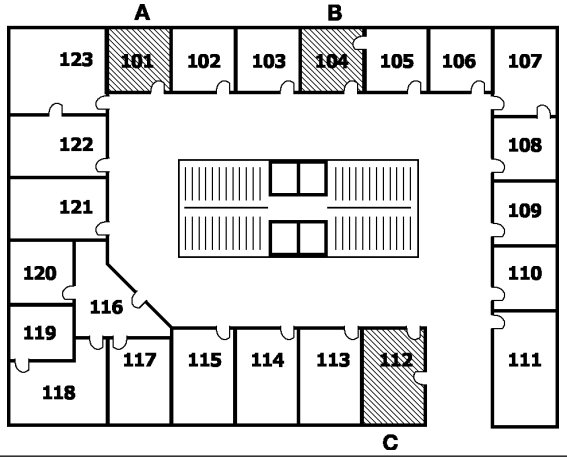
This section contains details on all the possible keycards that may be created with the FDU. The shortcuts indicated are based on being at the main screen after logging in with a keycard having the minimum authorization level, with the exception of the FDA authorization level. For the FDA level, after logging into the FDU the home <⌂> key must be pressed to use the short cut indicated.

Parameters indicated are fields that are always available for the inputting of values, or for the selection of available values, based on the FDU options being configured with the factory default configuration.

Options indicated are fields that may or may not be available for the inputting of values, or for the selection of available values, based configuration options available within the FDU.

A. Entry Keycards

A.1 Guest

Purpose:	Opens the door or doors that lead to an area that is normally rented as a single unit (room, suite or apartment).
Example:	
Minimum keycard:	Front Desk Authorization
Shortcut:	Swipe authorized keycard, press 1 and 1.
Expiry:	From 1 hour to 2730 nights
Factory default expiry:	1 night

Parameters:	Room number	Nights	Expiry Hour
	New/Duplicate	Number of cards	
Options:	Guest Common Areas	Disability Option	Salesman's Lockout
	Folio Number		

A.2 Guest One-shot

Purpose:	Opens a specific room only once, for use by walk-ins, maintenance by an external contractor, etc.
Minimum keycard:	Front Desk Authorization
Shortcut:	Swipe authorized keycard, press 1 and 4.

Expiry:	From 1 to 4 hours, or until the card is used once, whichever is first.
Factory default expiry:	1 hour
Parameters:	Room number
Options:	None
Notes:	A one-shot keycard for Guest Common Areas or Common Door Suites **cannot** be made.

A.3 Adjoining Suite

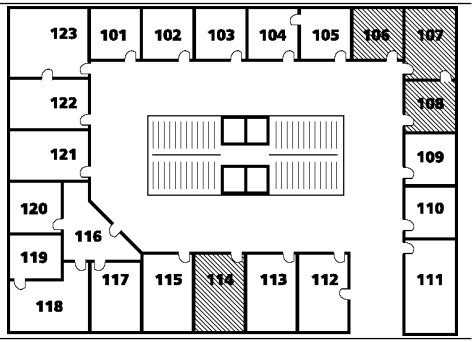
Purpose:	Opens each door of a combination of up to 15 individual guest rooms, within a 15 room number range. No resetting of the individual door locks is required.

Example:

Possible	Not Possible*	Not Possible**
106	**101**	**116**
107	**122**	**117**
108	**123**	**118**
114		

**Rooms not within a 15-room number range. See "Convention Suite Keycard"*

*** Rooms belong to a Common Door Suite.*



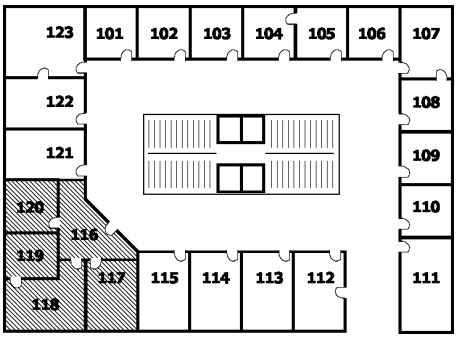
Minimum keycard:	Front Desk Authorization		
Shortcut:	Swipe authorized keycard, press 1 and 2.		
Expiry:	From 1 hour to 2730 nights		
Factory default expiry:	1 night		
Parameters:	Main Room	Add Room	Nights
	Expiry Hour	New/Duplicate	Number of cards
Options:	Guest Common Areas	Salesman's Lockout	Folio Number
Notes:	Enter all the room numbers using the up <▲> or down <▼> arrows and set the desired rooms to YES using the left <◀> or right <▶> arrows. After entering the last room number in the suite, press <↵> to continue. Cannot include doors of a Common Door Suite		

A.4 Common Door Suite

Purpose: Opens the common door and up to 8 inner doors that apply to a guest occupying a Common Door Suite. Multiple guests can have access to the common door, and to any non-overlapping combination of inner doors. Guests renting different inner rooms of a Common Door Suite do not cancel each other's keycards in the Common Door. Each Guest receives a New keycard when they check in, with access to the appropriate inner doors.

Example:

Guest 1	Guest 2	All to same guest
116	116	116
117	120	117
118		118
119		119
		120



Minimum keycard:	Front Desk Authorization		
Shortcut:	Swipe authorized keycard, press 1 and 3.		
Expiry:	From 1 hour to 2730 nights		
Factory default expiry:	1 night		
Parameters:	Common Door #	Add Room	Nights
	Expiry Hour	New/Duplicate	Number of cards
Options:	Guest Common Areas	Salesman's Lockout	Folio Number
Notes:	When enabled, the FDU will ask for the suite number of the common door and provide the option to specify the inner doors to provide access to as well.		

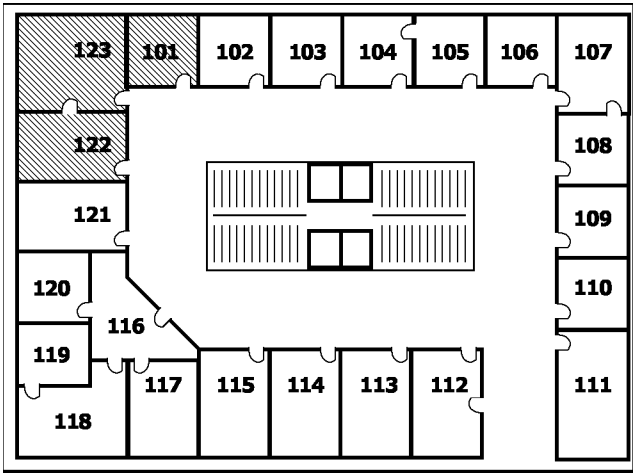
A.5 Convention Suite

Purpose: Opens each door of a Convention Suite. Convention suites are used when the rooms to be keyed alike do not fit within a 15 room number range *(see A.3 – Adjoining Suite)*. The lock on each door of the convention suite must be assigned a convention number using a Convention Suite Reset keycard (prepared with a minimum of a Master Authorization keycard). After use of a door as part of a Convention Suite, the next new Guest level keycard inserted in the lock cancels the convention number and returns the

lock to normal operation.

Example:

Guest rooms 101, 122, 123. (Cannot be in an Adjoining Suite because they span more than 15 room numbers.)



Minimum keycard:	Front Desk Authorization		
Shortcut:	Swipe authorized keycard, press 1 and 5.		
Expiry:	From 1 hour to 2730 nights		
Factory default expiry:	1 night		
Parameters:	Convention Number	Nights	Expiry Hour
	New/Duplicate	Number of cards	
Options:	Guest Common Areas	Salesman's Lockout	Folio Number

A.6 Pre-registered Guest

A.7 Pre-registered Adjoining Suite

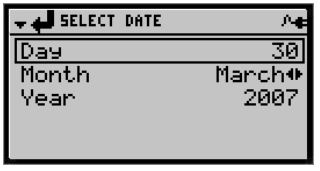
A.8 Pre-registered Common Door Suite

Purpose:

Pre-registered keycards for a Guest Room, Adjoining Suite or Common Door Suite can be made up to 10 days before the guest's registration begins. This feature is intended to speed check-in during peak periods or for large groups who have booked in advance.

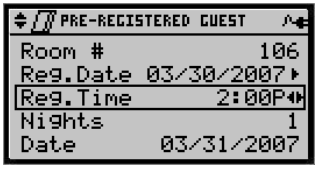
Pre-registered keycards only become valid at the selected registration date and time. Other Guest level keycards for the room or suite can be encoded as usual, until the Pre-registered keycard becomes valid and is inserted in the lock. A new Guest level keycard made after a Pre-registered keycard becomes valid will cancel the Pre-

	registered keycard, just like any normal Guest level keycard. The expiry of a Pre-registered keycard applies starting from the registration date and time.
Minimum keycard:	Front Desk Authorization
Shortcut:	Swipe authorized keycard, press 1 and 6.
Expiry:	From 1 hour to 2730 nights from the registration date and time (same as for the corresponding Guest level keycard).
Factory default expiry:	1 night
Parameters:	Same as for the corresponding Guest level keycard.
Options:	Same as corresponding Guest level keycard.
Notes:	The Pre-registered keycard may become valid up to one hour before its selected registration time, which is kept only in hours and is added to the time in hours and minutes that the card was made. (For example, a Pre-registered keycard, which is made at 08:25, with a registration time of 16:00, will become valid at 15:25 on the appropriate date, in order to ensure that it is valid before 16:00.). Enter the registration date and time when requested. After the room number is entered, select the “Reg. Date” and press the right <▶> arrow to enter the planned arrival date.



Press <↵> to go back to the previous menu level.

Select the “Reg. Time” and enter in the registration time.



A.9 Restricted Area

Purpose:	This keycard is intended for rooms that do not fit into the normal master-keyed structure of a property (e.g. GM office, computer room, and liquor storage areas). Locks programmed as Restricted Area doors accept only two types of entry keycards: Restricted Area and Emergency.		
Minimum keycard:	General Manager Authorization		
Shortcut:	Swipe authorized keycard, press 6 and 3.		
Expiry:	From 1 to 2730 nights		
Factory default expiry:	1 night		
Parameters:	Restricted Area #	New/Duplicate	Number of cards
Options:	None		

A.10 Section
A.11 Floor
A.12 Group
A.13 Zone
A.14 Area

Purpose:	Opens doors with the appropriate Sub-master level and address (e.g. Zone 3, Group 2, etc.). The Sub-master levels (Section, Floor, Group, Zone and Area) are used for access by staff who should not have master key privileges (e.g. office staff, housekeepers and housekeeper managers, maintenance workers, laundry, room service, etc.) Each Sub-master level is divided into 255 addresses. Rooms to which the same staff member or team of staff members require access should be keyed alike.
Example:	There is no hierarchy of Sub-master levels. For example, if Section addresses are used to divide the property according to the housekeeper who is assigned to clean a combination of rooms, then in high season there may be more than one Section per floor. Conversely, in low season a single Section may span more than one Section per floor. The section addresses would be reset at the start of either season using a Section Reset keycard. For more examples of the use of Sub-master levels, see *Section 5.3.1 – Lock Addresses*.
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 6 and 1.

Expiry:	From 1 to 2730 nights		
Factory default expiry:	365 nights		
Parameters:	Type (Section, Floor, Group, Zone or Area)		
	Level Staff (from 1 to 255)	New/Duplicate	Number of cards
Options:	Staff Common Areas	Guest Common Areas	Time Zones
Notes:	The Group Sub-master level should be reserved for housekeepers and/or housekeeper managers, allowing housekeeper managers to use a Group Lockout keycard *(see section 4.10 part C.5 Group Lockout)* to prevent the previous guest from returning to a room after it has been prepared and inspected. Properties with one or two FDUs may wish to reserve the Area sub-master level for use with the Back-up Keycard Kit (part # BK-7911). Enabled Guest Common Areas can be selectively assigned to all Staff keycards. Refer to *Section 4.6.2.2 – Guest Common Areas encoding for staff keycard* for details. To enable and set up Fixed Time Zones that apply to Staff keycards, see *Section 3.6 part 7-1 Fixed Time Zones*.		

A.15 Bellman's Master

Purpose:	Opens every room on the property, except for Restricted Areas or rooms that have been locked out using the deadbolt or privacy lock, the Salesman's Lockout, a Room Lockout keycard or a Hotel Lockout keycard. The Bellman's Master keycard operates at the room and suite levels only. There are no Time Zones with this keycard, because the expiry should be set to the length of a shift (or less) in the Expiry Menu. ***The Bellman's Master is always a duplicate keycard, so that it cannot be cancelled unintentionally by a more recently encoded keycard if more than one Bellman is on duty.*** ***If it is necessary to cancel this keycard, use a Bellman's Reset keycard in every lock in the facility before issuing replacements. If a valid Bellman's Master keycard is lost, cancel it immediately.***
Minimum keycard:	Bellman's Authorization (BA) or General Manager Authorization (GMA)*
Shortcut:	Swipe authorized keycard, press 6 and 4.
Expiry:	Selectable, 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	Guest Common Areas**

Options:	None
Notes:	* If a BA is used, the only option available is to encode one Bellman's Master keycard. If a GMA is used, select option 13 from the Keycard Menu. ** All enabled Guest Common Areas can be selectively assigned to all Bellman Master keycards.

A.16 Grand Master

Purpose:	Opens every room on the property, except for Restricted Areas or rooms that have been locked out using the deadbolt or privacy lock, the Salesman's Lockout, Room Lockout or Hotel Lockout. The Grand Master keycard opens all Common Area doors, but may be restricted to specific Time Zones. Use of the Grand Master keycard should be tightly restricted since it can open any room in the property and is usually set for a relatively long expiry. ***The Grand Master is always a duplicate keycard, so that it cannot be cancelled unintentionally by a more recently encoded keycard if Grand Master keycards are issued to more than one employee.*** ***If it is necessary to cancel this keycard, use a Grand Master Reset keycard in every lock in the facility before issuing replacements. If a valid Grand Master keycard is lost, cancel it immediately.***
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 6 and 5.
Expiry:	From 1 to 2730 nights
Factory default expiry:	365 nights
Parameters:	Number of cards
Options:	Time Zones
Notes:	This is an entry keycard, not a General Manager Authorization keycard used for encoding keycards.

A.17 Emergency

Purpose:	The Emergency keycard can open ANY door in ANY situation, if the lock is working properly. The Emergency keycard overrides the deadbolt or privacy lock, as well as the Room, Hotel and Salesman's Lockouts. ***Use of the Emergency keycard is usually restricted to the security staff and is strictly controlled because a lost keycard can open any room in the property.*** ***The Emergency keycard is always a duplicate keycard. It does not invalidate previous issued keycards. If an Emergency keycard is lost, it is absolutely necessary to issue an Emergency Reset keycard and insert this keycard in all locks. Replacement Emergency keycards may then be issued.***
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 6 and 6.
Expiry:	From 1 to 2730 nights
Factory default expiry:	365 nights
Parameters:	Number of cards
Options:	None

B. Authorization Keycards

Authorization keycards are not valid in locks and are required for accessing the FDU and specific functions related to the level of the authorization keycard.

B.1 Front Desk Authorization (FDA)

Purpose:	Grants access to menus of the Front Desk Unit intended for Front Desk Staff, primarily Guest Service Attendants concerned with encoding Guest level keycards and their corresponding Reset keycards, as well as Battery Test keycards.
Authorization #s:	1 to 100 if the Programming Authorization level is enabled 1 to 120 if the Programming Authorization level is disabled
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 6 and 2
Expiry:	None

B.2 Bellman's Authorization (BMA)

Purpose:	For encoding a Bellman's Master keycard only. Intended to be issued to each bellman to encode their own Bellman's Master keycard during their shift as needed, on any FDU in the facility. Since the Authorization keycard used to make the Bellman's Master is audited, the identity of the bellman who enters a room can be determined from the audit trail.
Authorization #s:	121 to 160
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 6 and 2
Expiry:	None
Notes:	Alternatively, a Bellman's Authorization can be held by one person on each shift and used to encode all the Bellman's Master keycards, but in this case a printer would have to be connected to the FDU to provide a record of the sequence id of each Bellman's Master keycard issued. (This approach is not recommended.)

B.3 Master Authorization (MA)

Purpose:	Grants access to menus of the Front Desk Unit intended for management (head of security, front desk manager). This keycard allows the user to make most Entry keycards, Front Desk Authorization keycards, all Reset keycards and some special purpose keycards, as well as to change most expiries and perform all functions under the Programming Menu. The MA cannot be used to audit FDUs, or to change FDU features. The MA can access all the functions of an FDA. Not valid in locks.
Authorization #s:	161 to 180
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 6 and 2
Expiry:	None

B.4 Programming Authorization (PA)

Purpose:	Grants access to all FDU functions needed to program or audit locks. In addition, grants access to the same functions as the FDA keycard.
Authorization #s:	101 to 120
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 6 and 2
Expiry:	None
Notes:	The Programming Authorization feature must first be enabled in the FDU features. When it is disabled, authorization #s 101-120 become available for FDA keycards, and any existing PA keycards become FDA keycards.

B.5 General Manager Authorization (GMA)

Purpose:	Grants access to all functions of the FDU. Intended for the highest level of user, including the Chief of Security, the General Manager and the System Administrator.
Authorization #s:	181 to 200
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 6 and 2
Expiry:	None
Notes:	***It is extremely important to make two spare GMA keycards in case of accidental erasure of the GMA keycard in general use. The spare GMA keycards must have two different authorization numbers that are not used for any other GMA keycard in the facility. These spare keycards should be stored in a safe. If it is necessary to use one of the spare GMA keycards, immediately make another spare and lock it in the safe.***

B.6 POS Authorization

Purpose:	Grants access to the functions of the Point-of-Sale Verifier mode of the FDU. There are no menus associated with the POS mode. Simply swipe the POS Authorization keycard to put the FDU in POS Verifier mode that can be used to verify a guest's keycard in order to post charges to their room.
Authorization #s:	1 to 200
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 6 and 2
Expiry:	None
Notes:	The POS verifier must be enabled in the FDU features. POS Authorization keycards are completely separate from the other Authorization levels. A POS Authorization keycard can share the same Authorization number as an FDA, PA, MA, BA or GMA keycard without cancelling the other keycard, and vice-versa.

C. Lockout Keycards

Lockout keycards are used in emergencies to protect property or evidence in a room or to prevent illicit entry in closed parts of the property (see *Section 4.2.3 – Lockout Keycards* and *Section 10.9 – If an FDI is stolen*).

C.1 Hotel Lockout

Purpose:	Locks out all but the Emergency keycard. The Hotel Lockout keycard is valid throughout the property. Locks that are swiped with this keycard will deny access to all authorized keycards in circulation, except the Emergency keycard. Access to authorized keycards can only be restored by swiping a Hotel Unlock keycard. Specific rooms may be unlocked using a Room Unlock keycard.
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 4 and 5
Expiry:	Selectable, from 1 hour to 65,535 hours (7 years)
Factory default expiry:	24 hours
Parameters:	Number of cards

C.2 Hotel Unlock

Purpose:	Unlocks any room locked-out by the Hotel Lockout or Room Lockout keycard.
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 4 and 5
Expiry:	Same as Hotel Lockout setting
Factory default expiry:	24 hours
Parameters:	Number of cards

C.3 Room Lockout

Purpose:	Locks out all but the Emergency keycard for a specific room. The Room Lockout keycard is valid for a specific room only. The lock specified will deny entry to all valid keycards until unlocked by a Room Unlock or Hotel Unlock keycard.
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 4 and 5
Expiry:	Selectable, from 1 hour to 24 hours
Factory default expiry:	24 hours
Parameters:	Room number Number of cards

C.4 Room Unlock

Purpose:	Unlocks a specified room locked-out by a Room Lockout keycard.
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 4 and 5
Expiry:	Same as Room Lockout keycard
Factory default expiry:	24 hours
Parameters:	Room number Number of cards

C.5 Group Lockout

Purpose:	Invalidates the previous Guest level keycard and prevents guests from returning to rooms from which they have checked out. This keycard is made for the Group address assigned to the lock and is intended to be used by the housekeeper supervisor after inspecting the room. For this reason, Group addresses are usually assigned according to the duties of each housekeeper supervisor.
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 4 and 5
Expiry:	From 1 to 2730 nights

Factory default expiry:	365 nights
Parameters:	Group Number Number of cards
Notes:	The Group Lockout keycard does not work in the common door of a Common Door Suite. The Group Lockout keycard will not invalidate Guest keycards issued up to 45 minutes prior to its use in the lock.

D. Special Purpose Keycards

D.1 Battery Test

Purpose:	This keycard prompts a low battery indicator in locks when the battery is below acceptable voltage. If the red and green lights flash together when the Battery Test keycard is inserted in the lock, the battery is low. This should occur within 2 to 4 weeks prior to battery failure. There is a single green flash if the battery is still good.
Minimum keycard:	Front Desk Authorization
Shortcut:	Swipe authorized keycard, press 4 and 1
Expiry:	No Expiry
Factory default expiry:	None
Parameters:	Number of cards
Notes:	The Battery Test keycard does not give access to the door. Weekly battery testing is recommended. Any Sub-master or Master keycard will also prompt the low battery indicator just before giving access to the door, and the same sequence of indicator lights will be displayed (i.e. a low battery is indicated by red and green lights flashing together). No battery indication is available for any guest keycards.

D.2 Programming

Purpose:	Prepares the lock for communication with the Front Desk Unit.
Minimum keycard:	Programming Authorization
Shortcut:	Swipe authorized keycard, press 4 and 2
Expiry:	From 1 to 2730 nights
Factory default expiry:	2730 nights
Parameters:	Number of cards
Notes:	***If the lock has never been initialized, or following a battery replacement, the Initialization keycard must be inserted prior to the Programming keycard.*** If the FDU is not connected and/or communication with the lock does not begin within 30 seconds, the lock will return to its normal state with no changes to its programming.

D.3 Passage

Purpose:	Puts the lock in Passage mode, in which a keycard is no longer required to open the door. Passage mode is removed by re-inserting the Passage keycard. Passage mode capability must be enabled for each specified room number when the FDU is programmed at the factory (*see Chapter 6 – Implementing the System*). Typically, rooms such as Common Areas and meeting rooms are appropriate for the use of Passage mode. Rented Guest rooms should not be put in Passage mode.
Minimum keycard:	General Manager Authorization for Staff Common Areas and Restricted Areas Master Authorization for Guest Common Areas and other rooms.
Shortcut:	Swipe authorized keycard, press 4 and 4
Expiry:	From 1 to 2730 nights
Factory default expiry:	1 night
Parameters:	Type (Guest room, Guest Common Area, Staff Common Area, Restricted Area)
Notes:	***For security reasons, when a lock is in passage mode, the lock will not indicate give any indication that it is set in this state. All valid keycards will provide the same indications as if the lock was in its regular state.***

D.4 Hotel Restart

Purpose:	Used to set or change the Hotel Code when installing the system or if an FDU is stolen. ***If a Hotel Restart keycard is swiped in the FDU, a series of menus appears. Consult the instructions in Section 3.5.9 – Hotel Restart before continuing.*** ***All assigned PINs of the FDU will be cancelled.***
Minimum keycard:	General Manager Authorization
Shortcut:	Swipe authorized keycard, press 4 and 6
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	Hotel Code Number of cards
Notes:	***Call Kaba Ilco for assistance.***

D.5 FDU Cancel

Purpose:	Used if an FDU is stolen. Once inserted in all locks, all keycards made by the specified Front Desk Unit will be invalid. Once swiped through all FDUs in the system, no Authorization keycards made by the stolen FDU will be accepted.
Minimum keycard:	General Manager Authorization
Shortcut:	***Enter a PIN of 5222 to reach the Technical Support Menu then call Kaba Ilco for assistance.***
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	FDU number (of stolen unit)
Notes:	***Call Kaba Ilco for assistance.***

D.6 Initialization

Purpose:	Initializes the lock during a first-time installation, or after an interruption of battery power (e.g. during a battery replacement, or whenever the battery power is temporarily disconnected).
Minimum keycard:	Programming Authorization
Shortcut:	Swipe authorized keycard, press 4 and 3.
Expiry:	No Expiry
Factory default expiry:	None
Parameters:	Number of cards

D.7 Test Lock

Purpose:	Tests locks before they are initialized. Used by the lock installers to access rooms during the installation. Test Lock keycards do not work after a lock has been initialized. (Refer to lock installation instructions.)
Minimum keycard:	Programming Authorization
Shortcut:	Swipe authorized keycard, press 4 and 3
Expiry:	No Expiry
Factory default expiry:	None
Parameters:	Number of cards

E. Reset Keycards

E.1 Guest Reset
E.2 Adjoining Suite Reset
E.3 Common Door Suite Reset
E.4 One-Shot Reset

Purpose:	Invalidates the corresponding room or suite entry keycard. ***The Reset keycard must be inserted in all locks leading to the specified guest room or suite.*** Once done, all entry keycards for the same level encoded before the Reset keycard was encoded will be denied entry in the lock.
Example:	(i) Suppose that one of the rooms in an Adjoining Suite is to be dropped from the reservation but that the guests require continued access to the remaining rooms of the Adjoining Suite. Access to the room being dropped from the reservation can be revoked by inserting a valid Adjoining Suite Reset keycard in the lock for the affected room. Alternatively, a valid Group Lockout keycard can be inserted in the affected lock *(see Section 3.10 part C.5 – Group Lockout).* (ii) Suppose that a guest has lost their keycard and is away from the property. To cancel their lost keycard without giving access to the room and without encoding a new keycard until they return, the corresponding Reset keycard should be encoded and inserted in the lock to the guest's room.
Minimum keycard:	Front Desk Authorization
Shortcut:	For Guest Reset: Swipe authorized keycard, press 5, 1 and 1 For Adjoining Suite Reset: Swipe authorized keycard, press 5, 1 and 2 For Common Door Suite Reset: Swipe authorized keycard, press 5, 1 and 3 For One-Shot Reset: Swipe authorized keycard, press 5, 1 and 4
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	Room/Suite number(s) Number of cards
Options:	None

E.5 Convention Suite Reset

Purpose:	Assigns a Convention Address to a group of guest rooms. Once the Convention Suite Reset keycard has been inserted in all doors, the doors will accept a Convention Suite keycard with the same address number, as long as the Convention Suite keycard was encoded **after** the Convention Suite Reset keycard.

	The doors will also reject any guest level entry keycard that was valid before the Convention Suite Reset keycard was inserted. Doors return to normal operation when a new Guest level entry keycard other than a Convention Suite keycard is inserted.
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 5, 1 and 5
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	Convention number Number of cards
Options:	None
Notes:	Swipe the keycard through the doors to be included in the Convention Suite as soon as convention guests register.

E.6 Pre-registered Reset

Purpose:	Invalidates any pre-registered keycard before it becomes valid. (The Pre-registered Reset keycard must be encoded after the Pre-registered keycard it is intended to cancel). ***The Reset keycard must be inserted in all locks leading to the specified guest room or suite.*** ***If the pre-registered keycard is already valid, use a Reset keycard for the corresponding guest room.***
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 5, 1 and 6
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	Number of cards
Options:	None

E.7 Restricted Area Reset

Purpose:	Invalidates the corresponding Restricted Area entry keycard. Restricted Area keycards encoded before the Reset keycard was encoded will not work in the lock. ***The Reset keycard must be inserted in all locks leading to the specified Restricted***

	Area.
Minimum keycard:	Master Authorization
Shortcut:	Swipe authorized keycard, press 5, 3 and 2
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	Restricted Area number
Options:	None

E.8 Section Reset
E.9 Floor Reset
E.10 Group Reset
E.11 Zone Reset
E.12 Area Reset

Purpose:	(i) Invalidates Sub-master entry keycards for the corresponding Section, Floor, Group, Zone or Area ***and/or*** (ii) Assigns a new Sub-master address to the lock. The Sub-master levels are known as variable addresses since they are designed to be easily changed using the corresponding Reset keycard to adapt to changes in staff assignments, or to high and low season needs of the property.		
Example:	(i) If a housekeeper for Section 1 loses their keycard, insert a Section 1 Reset keycard in all Section 1 locks ***and issue new Section 1 keycards***, or make new Section 1 keycards and insert one of them in all Section 1 locks (ii) If the season changes from high to low, and the rooms in Sections 1 and 2 need to be combined into one larger Section to be served by a single housekeeper, insert a Section 1 Reset keycard into the locks with Section address 2, then issue new Section 1 keycards. The new Section 1 now includes all the locks that were formerly in Section 2		
Minimum keycard:	Master Authorization		
Shortcut:	Swipe authorized keycard, press 5, 3 and 1		
Expiry:	From 1 to 24 hours		
Factory default expiry:	24 hours		
Parameters:	Type (Section, Floor, Group, Zone, Area)	Level (1-255)	Number of cards

Options:	None

E.13 Bellman's Master Reset
E.14 Grand Master Reset
E.15 Emergency Reset

Purpose:	Invalidates all of the circulating Entry keycards for the corresponding Master key level (Bellman's Master, Grand Master or Emergency). Since these Master level keycards have access to every room in the property, and since they are always duplicates, ***if one of the keycards mentioned above is lost it is absolutely necessary to encode the corresponding Reset keycard and insert it in every lock and card reader on the property. Replacement Master level keycards can then be issued.***
Minimum keycard:	Master Authorization
Shortcut:	For Bellman's Master Reset: Swipe authorized keycard, press 5, 3 and 3 For Grand Master Reset: Swipe authorized keycard, press 5, 3 and 4 For Emergency Reset: Swipe authorized keycard, press 5, 3 and 5
Expiry:	From 1 to 24 hours
Factory default expiry:	24 hours
Parameters:	None
Options:	None

E.16 Passage Reset

Purpose:	Invalidates a Passage keycard in locks leading to a specific room, Restricted Area or Common Area.
Minimum keycard:	Front Desk Authorization
Shortcut:	Swipe authorized keycard, press 5 and 2
Expiry:	From 1 to 2730 nights
Factory default expiry:	1 night
Parameters:	Room, Guest Common Area, Staff Common Area, or Restricted Area number
Options:	None

Notes:

Does not cause the lock to revert from Passage mode to Normal mode.

Chapter 5: Locks - Using and Programming

5.1 Lock Installation

Kaba Ilco locks are shipped with installation instructions. Keep a copy of these instructions for each type of lock on the property, in case there is a need to service or replace a lock.

5.2 Lock Responses to Keycards

After a lock has been initialized and programmed as part of the system, it gives an audible and visible response when a keycard is inserted, providing valuable information about the lock status.

Possible responses from the visible indicator and actions where applicable:

Indicator Light	Condition and Action Required
Flashing Green	Access granted. **Turn handle to open door.**
Flashing Red	Access granted to Emergency keycard while a lockout is in place. **Turn handle to open door.**
Single Green	Input from Reset or Lockout keycard accepted. (Access is not granted.) Follows a FDU cancel, a hotel restart, Passage or battery test. **No action required.**
Single Red	Keycard valid but locked out. Out of time zone. **Unlock the deadbolt from inside the room, or remove security lockout (*see Section 3.2.3 – Lockout Keycards*).**
No light	Invalid keycard or misread. **Verify the keycard *(see Section 4.9 – Verifying and Reading Keycards)*.**

Flashing Green & Red	Low battery indicator when using Staff keycard. **Change the battery *(see Section 11.4 – Replacing a Battery)*.**
Single Green & Red	Low battery indicator when using Battery Test keycard. **Change the battery *(see Section 11.4 – Replacing a Battery)*.**
Green, then Red (locks)	Lock not programmed or card misread. **Try again. If this response continues, troubleshoot the card and/or lock.**
Single green, then Red (RACs only)	Passage activated and out of time zone.
Red LED always on	Halt Mode (Batteries are too low to continue operation). **Batteries need to be changed. ***
Red LED flashes every half second	Power-on or reset while mechanical override is on. **Disengage mechanical override & reconnect the batteries (cam not engaged).**
Double short flash of Red LED every 4 sec.	Advanced fail mode (memory failure). **Lock circuit board needs to be changed.**
Green and Red (single flash together) then green once	Successful initialization.
Green and Red (single flash together) then red once	Unsuccessful initialization.
Green and Red together (single flash together for 6 seconds)	Test card.

* Can also happen during installation. Solution: Disconnect the batteries, wait 5 seconds and reconnect the batteries.

5.3 Programming Locks and Remote Access Controllers

Locks and RAC's have the same or similar functions in the system, and are programmed in the same way, with the exception of flexible Time Zones available in RAC models 3.5,

4 & 4XT. ***Either a lock or a RAC can be used on any door, to accommodate the door hardware.***

Locks and RACs arrive from the factory with the operating system installed, but without an identity as belonging to a particular Guest room, Common Area or Restricted Area. The lock's internal clock also needs to be set to the internal time of the FDU when first initialized or following a battery replacement. These settings are programmed by the FDU using the lock communication cable and a Programming keycard that prepares the lock to receive data from the FDU. Note that RACs don't require the programming keycard. A Programming Authorization or higher keycard is required to access the programming functions of the lock.

IMPORTANT: **Do not attempt to read or encode any keycard (including Authorization, Programming and Initialization keycards) while the communication cable is connected between the FDU and the lock or RAC. Connect the cable just before sending or reading the information.**

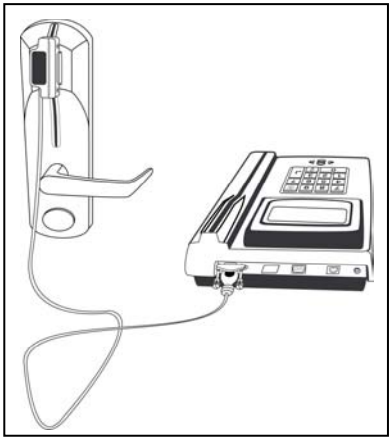


Figure 5.3: *The communication cable is connected to Serial Port A on the rear of the FDU, and then inserted in the reader slot of the lock or card reader so that the infrared communication device is level with the indicator window.*

5.3.1 Lock Addresses

As explained in *Section 4.2.1 – Entry Keycards*, each lock has a set of levels that determines which keycards will be accepted by the lock. Access is divided into the Guest, Restricted Area, Sub-master and Master levels, corresponding to the types of keycards by the same name. Addresses are a sub-division of the level. For example, the Guest levels may be divided into 16,000 addresses, one for each access type. The Sub-Master levels may each be divided into 255 addresses (e.g. Section 1 to Section 255). The Master level has only one address since these keycards are valid throughout the property. The different

levels are independent of each other, so that invalidation of a keycard at one level does not affect the other levels. For example, the Guest level keycard can be changed daily without affecting housekeepers, maintenance personnel, or the Emergency keycard, which normally have access to the same room.

Access Level	Sub-Levels	Used by
Guest	Guest	Guests
	Common Door Suite	Guests
	Convention Suite	Guests
	Common Area	Guests and/or Staff
Restricted Area	n/a	Staff
Sub-Master ("Staff")	Section	Staff
	Floor	Staff
	Group	Staff
	Zone	Staff
	Area	Staff
Master	Bellman's	Staff
	Grand Master	Top level Staff and/or Management
	Emergency	Top level Staff and/or Management

Table 5.3.1: *Access levels*

The Guest or Restricted Area address can only be set by the FDU and should be different for every lock on the property, unless there is more than one door to the same room. The Sub-master levels are variable addresses, meaning that they can be changed without the use of the FDU by a Reset keycard, allowing the room assignments of staff throughout the property to be changed easily. Master level keycards have access to all locks automatically, and the Master level address does not have to be programmed.

When the FDU is in programming mode, the addresses are set at each level prior to programming a lock. The list of addresses remains in memory while the FDU is still in the Programming menu, and can be changed as required for the next lock.

Example: *Addresses for rooms 501 and 502, two different guest rooms.*

Address Level	#501	#502
Guest	501	502
Section	10	10
Floor	5	5

Group	2	2
Zone	10	10
Area	1	1

The Sub-master levels in the example are the same for the adjacent rooms 501 and 502, so that only the Guest address needs to be specified when programming room 502 immediately after room 501.

NOTE: No address exists for the One Shot, Adjoining Suite, or Pre-registered Guest levels, as these keycards use the Guest address. For example, Adjoining Suite keycards are simply keycards that are encoded with up to 15 Guest addresses in a consecutive block.

If an address is programmed as "0", the lock will not respond to any key-card at that level. For example, to prevent any Zone keycard from opening the door, set the Zone to 0. Likewise, the linen storage on Floor 2 to be used only by Floor 2 keycard holders can be programmed as Room 0 and Floor 2.

5.3.2 Programming Guest Room Locks

Purpose: To program the addresses of a lock that is a normal guest room or other room (i.e. not a room in a Common Door Suite, a Restricted Area or a Common Area). Most doors in the facility are programmed as guest rooms.

	Level	Available Addresses	Example
Guest**	Guest	16,000 available: 1-99,999*	501
	One-Shot	-	
	Pre-registered	-	
	Adjoining Suite	-	
	Convention Suite***	1-1,100	0
Sub-Master	Section	1-255	10
	Floor	1-255	5
	Group	1-255	2
	Zone	1-255	10
	Area	1-255	1
Master	Bellman's Master	-	All

	Grand Master	-	All
	Emergency Master	-	All

* **The FDU can be ordered in standard configuration, with available Room level addresses from 1 to 16,000, or in a custom configuration, with a specified room range from 1 to 99,999** ***(see Chapter 6 – Implementing the System).***

** **Note that each guest room in the facility should have a unique address at the Guest level. The Guest level for a guest room door includes just one address for Guest, One-Shot, Pre-registered, and Adjoining Suite keycards, all of which can give access to the same guest room, but have different expiries or other features associated with the keycard. These keycards are for different access levels that share the same address.**

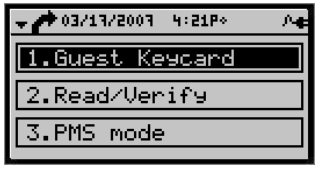
*** **The Convention Suite address is set using a Convention Suite Reset keycard at the time the room becomes a part of a Convention Suite** ***(see section 4.10 part E.5 – Convention Suite Reset)*****. Other types of doors do not have a Convention Suite address and cannot be part of a Convention Suite.**

Equipment required: FDU
Lock communication cable
Initialization keycard
Programming keycard (Not required for RAC)
Completed Planning Forms

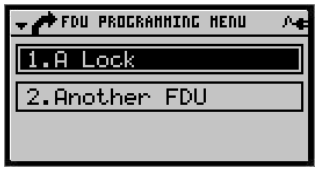
Minimum keycard required: Programming Authorization

Steps to program the Guest Room lock addresses:

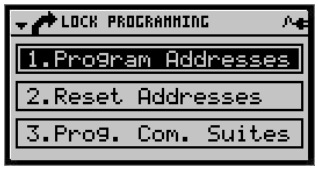
1. On the lock side, if this is a first time installation, or if power to the lock has been interrupted, insert the Initialization keycard in the lock. The red and green indicators should light, then only the green indicator should flash. Re-insert the Initialization keycard if the pattern of indicator lights described is not observed.
2. On the FDU, swipe a keycard, or enter a PIN value having a Programming authorized user level.



3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



4. Press 1 or <↵> to reach the “Lock Programming” menu.



5. Press 1 or <↵> to reach the “Program Addresses” menu.

6. The FDU displays a list of the current addresses in memory for programming guest room locks. Consult the Planning Form to determine the desired addresses for the lock.

   Enter a room number. Scroll through the list using the <▲> and <▼> keys to view the Guest, Section, Floor, Group, Zone and Area addresses. To move to a different line, use the up <▲> or down <▼> arrow. Press <↵> when ready to program the lock.

7. Insert the Programming keycard in the lock, after which the green indicator light should be lit. Connect the communication cable from the FDU to the lock and press any key on the FDU to send the programming to the lock. After the configuration is transferred to the lock, the following message is displayed:

The addresses are now assigned. Every time lock addresses are programmed, the FDU sets the lock's internal clock to the correct time, so there is no need to reset the lock time. Remove the communication cable from the lock.

5.3.3 Programming Locks in a Common Door Suite

Purpose: To program the addresses of a lock on an inner door or common door of a Common Door Suite.

Common Door Suites are multi-room configurations with a common door and several inner doors to a maximum of 8 (see S*ection 4.10 part A.4 – Common Door Suite* for an example). If the inner doors are to be rented separately and are fitted with electronic locks, the common door and the inner doors require a special program. The common door must recognize keycards for the inner doors. If the inner doors are rented to different guests, their New keycards DO NOT invalidate each other in the Common Door.

	Level	Available Addresses	Example
Guest	Common Door Suite	1,000 available: 1-99,999	116
	Inner Door	1-99,999	117
	Inner Door	1-99,999	118
	Inner Door	1-99,999	119
	Inner Door	1-99,999	120
Sub-Master	Section	1-255	10
	Floor	1-255	5
	Group	1-255	2
	Zone	1-255	0
	Area	1-255	1
Master	Bellman's Master	-	All
	Grand Master	-	All
	Emergency Master	-	All

Table 5.3.3a: *Addresses for common door #116, part of a Common Door Suite that includes inner doors #117, 118, 119 and 120.*

	Level	Available Addresses	Example
Guest	Inner Door	1-99,999	117
	Common Door Suite	1,000 available: 1-99,999	116
Sub-Master	Section	1-255	10
	Floor	1-255	5
	Group	1-255	2
	Zone	1-255	0
	Area	1-255	1
Master	Bellman's Master	-	All
	Grand Master	-	All
	Emergency Master	-	All

Table 5.3.3b: *Addresses for Inner Door #117. The Common Door Suite level is specified so that a keycard for inner doors with the same number in a different Common Door Suite will not give access. The lock confirms both Guest levels before granting access.*

None of the doors in the suite may be part of an Adjoining Suite. Like Guest room doors, doors in a Common Door Suite are programmed with addresses for the five Sub-master levels to permit staff access.

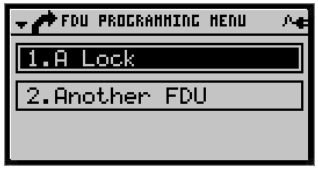
Equipment required: FDU
Lock communication cable
Initialization keycard
Programming keycard
Completed Planning Forms

Minimum keycard required: Programming Authorization

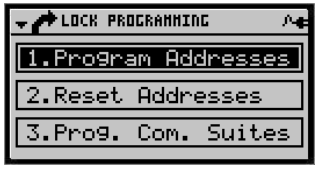
Steps to program the Common Door Suite lock addresses:

1. If this is a first time installation, or if power to the lock has been interrupted, insert the Initialization keycard in the lock. The red and green indicators should light, and then only the green indicator should flash. Re-insert the Initialization keycard if the pattern of indicator lights described is not observed.
2. Swipe a keycard or enter a PIN value having a Programming authorized user level.

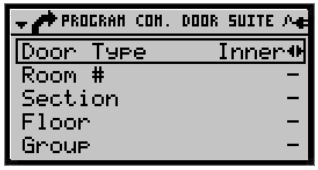
3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



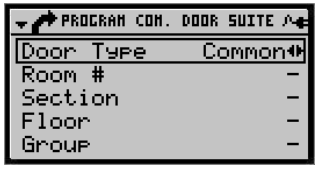
4. Press 1 or <↵> to reach the "Lock Programming" menu.

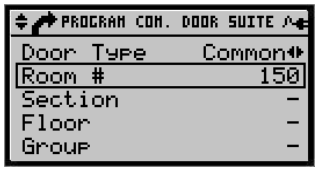


5. Press 3 or use the down <▼> arrow followed by <↵> to reach the "Program Common Suites" menu.

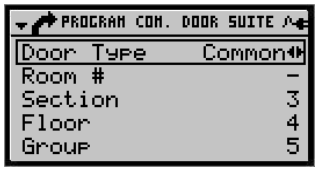


6. Using the left <◀> or right <▶> arrow, select the **Common Door** option, then press < ▼> and enter the room number.





7. Scroll through the list of addresses using the <▲> and <▼> keys to view the Common Door, Section, Floor, Group, Zone and Area Addresses.

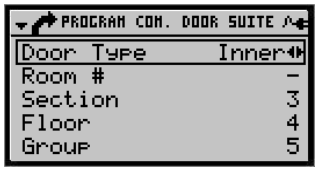


NOTE: The Common Door address must match the list of addresses programmed at the factory for the Common Doors of Common Door Suites.

8. Enter the new address. Change other addresses if necessary, and press <↵> when ready to program the lock.

9. Insert the Programming keycard in the lock, and ensure the green indicator is lit. Connect the communication cable from the FDU to the lock and press any key on the FDU to send the programming to the lock.

The addresses are now assigned. Every time lock addresses are programmed, the FDU sets the lock's internal clock to the correct time, so there is no need to reset the lock time. Remove the communication cable from the lock. The FDU will return to the Common Door Suite menu and shows the previous values used for the lock.



10. Continue programming other Common doors of the Common Door Suite (the addresses will be kept in memory, and likely only the address of the inner door will need to be changed), or press <⌫> to return to the previous menu.

5.3.4 Programming Inner Door Locks in a Common Door Suite

Purpose: To program the addresses of a lock on an inner of a Common Door Suite.

Common Door Suites are multi-room configurations with a common door and several inner doors to a maximum of 8 *(see Section 4.10 part A.4 – Common Door Suite for an example)*. If the inner doors are to be rented separately and are fitted with electronic locks, the common door and the inner doors require a special program. The common door must recognize keycards for the inner doors. If the inner doors are rented to different guests, their New keycards DO NOT invalidate each other in the Common Door.

	Level	Available Addresses	Example
Guest	Common Door Suite	1,000 available: 1-99,999	116
	Inner Door	1-99,999	117
	Inner Door	1-99,999	118
	Inner Door	1-99,999	119
	Inner Door	1-99,999	120
Sub-Master	Section	1-255	10
	Floor	1-255	5
	Group	1-255	2
	Zone	1-255	0
	Area	1-255	1
Master	Bellman's Master	-	All
	Grand Master	-	All
	Emergency Master	-	All

Table 5.3.4a: *Addresses for common door #116, part of a Common Door Suite that includes inner doors #117, 118, 119 and 120.*

	Level	Available Addresses	Example
Guest	Inner Door	1-99,999	117
	Common Door Suite	1,000 available: 1-99,999	116
Sub-Master	Section	1-255	10
	Floor	1-255	5
	Group	1-255	2
	Zone	1-255	0
	Area	1-255	1
Master	Bellman's Master	-	All
	Grand Master	-	All
	Emergency Master	-	All

Table 5.3.4b: *Addresses for Inner Door #117. The Common Door Suite level is specified so that a keycard for inner doors with the same number in a different Common Door Suite will not give access. The lock confirms both Guest levels before granting access.*

None of the doors in the suite may be part of an Adjoining Suite. Like Guest room doors, doors in a Common Door Suite are programmed with addresses for the five Sub-master levels to permit staff access.

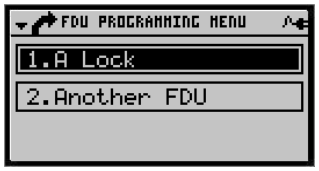
Equipment required:
FDU
Lock communication cable
Initialization keycard
Programming keycard
Completed Planning Forms

Minimum keycard required: Programming Authorization

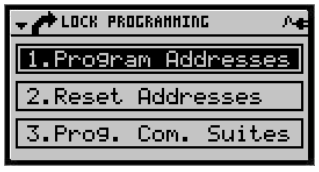
Steps to program the Inner Door lock addresses:

1. If this is a first time installation, or if power to the lock has been interrupted, insert the Initialization keycard in the lock. The red and green indicators should light, and then only the green indicator should flash. Re-insert the Initialization keycard if the pattern of indicator lights described is not observed.
2. Swipe a keycard or enter a PIN value having a Programming authorized user level.

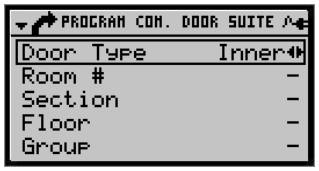
3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



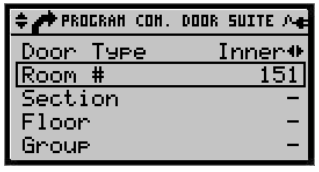
4. Press 1 or <↵> to reach the "Lock Programming" menu.



5. Press 3 or use the down <▼> arrow followed by <↵> to reach the "Program Common Suites" menu.

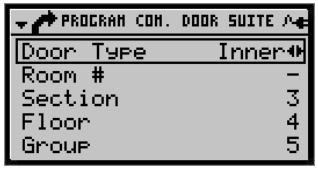


6. Press the down <▼> arrow to enter the room number.



Scroll through the list of addresses using the <▲> and <▼> keys to view the Common Door, Inner Door, Section, Floor, Group, Zone and Area Addresses.

Enter a number from 1 to 255 (eg: 2 for Inner Door) to change the addresses selected.

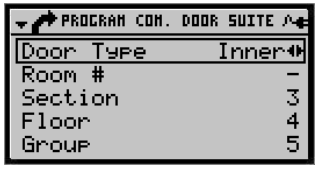


Note: The Inner Door address must match the list of addresses programmed at the factory for the Inner Doors of Common Door Suites.

7. Enter the new address. Change other addresses if necessary, and press <↵> when ready to program the lock.

8. Insert the Programming keycard in the lock, and ensure the green indicator is lit. Connect the communication cable from the FDU to the lock and press any key on the FDU to send the programming to the lock.

The addresses are now assigned. Every time lock addresses are programmed, the FDU sets the lock's internal clock to the correct time, so there is no need to reset the lock time. Remove the communication cable from the lock. The FDU will return to the menu for the Common or Inner Door Suite menu and shows the previous values used for the lock.



Continue programming other Inner or Outer doors of the Common Door Suite (the addresses will be kept in memory, and likely only the address of the inner door will need to be changed), or press <⌫> to return to the previous menu.

5.3.5 Programming Common Area Locks and RAC's

Purpose: To program the addresses of a Guest Common Area or Staff Common Area lock. Common Area locks may have more than one address (eg: Guest Common Area #1, 2 and 3). When a Common Area lock is audited, it displays "M" if it has multiple addresses and the address number if it has a single address. New RAC Models 3.5, 4 & 4XT support Flexible Time Zones, which are programmed separately *(see Section 5.5 – Remote Access Controller Models 3.5, 4 & 4XT Flexible Time Zones)*.

Common Area locks recognize any Guest level or Staff level keycard that was encoded with the corresponding Common Area, as long as it has not expired. The lock does not maintain a table of the most recent keycard used. There are no Sub-Master or Bellman's Master levels available in a Common Area lock. Staff can selectively be given access to any of the Guest Common areas *(see Section 3.6 part 5- Staff Access top Guest Common Areas)*.

Level	Available Addresses	Example
Staff Common Area	16	9, 10, 11, 16
Grand Master, Emergency Master	-	All

Table 5.3.5a: *Addresses for a Staff Common Area lock with multiple addresses.*

Level	Available Addresses	Example
Guest Common Area	8	1
Grand Master, Emergency Master	-	All

Table 5.3.5b: *Addresses for a Guest Common Area lock with a single addresses.*

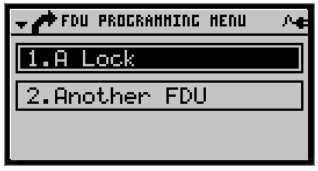
Equipment required: FDU
Lock communication cable
Initialization keycard
Programming keycard
Completed Planning Forms

Minimum keycard required: Programming Authorization

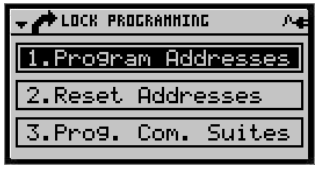
Steps to program the Common Area lock addresses or RACs:

1. On the lock side, if this is a first time installation, or if power to the lock or RAC has been interrupted, insert the Initialization keycard in the lock or RAC. The red and green indicators should light, and then only the green indicator should flash. Re-insert the Initialization keycard if the pattern of indicator lights described is not observed.
2. On the FDU, swipe a keycard or enter a PIN value having a Programming authorized user level.

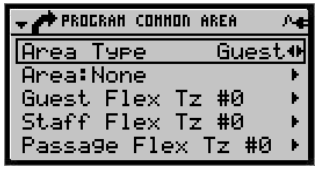
3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



4. Press 1 or <↵> to reach the "Lock Programming" menu.



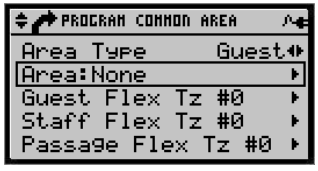
5. Press 4 or use the down <▼> arrow followed by <↵> to reach the "Program Common Areas" menu.



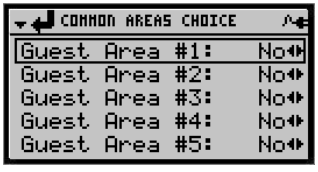
Follow the instructions in the correct column:

NOTE:
Only one type of Common Area (Guest or Staff) can be chosen per lock.

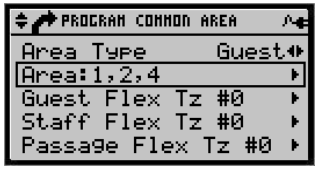
6. Select **Guest Common Area** option, and then press < ▼>.



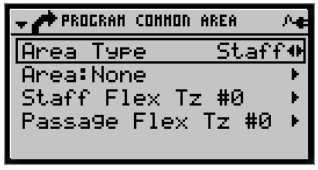
Press the right <▶> arrow to display all Guest Common Areas.



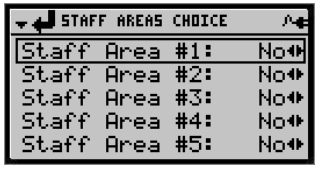
7. More than one or all 8 Guest Common Area addresses may be assigned to a single lock. Select the Guest Common Area, from 1-8 (e.g. 1,2,4), and then press <↵>.



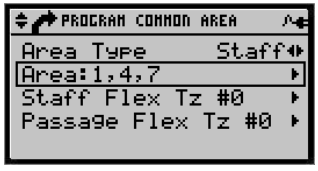
6. Using the left <◀> or right <▶> arrow, select the **Staff Common Areas** option and then press <▼>.



Press the right <▶> arrow to display all Staff Common Areas.



7. More than one of all 16 Staff Common Area addresses may be assigned to a single lock. Select the Staff Common Area, from 1-16 (e.g. 1,4,7), and then press <↵>.



8. Press <↵> when ready to program the lock.

9. Only for a lock, insert the Programming keycard in the lock, and ensure the green indicator is lit. For a RAC, use the Initialization keycard instead of the Programming keycard to initialize communication.

10. Connect the communication cable from the FDU to the lock and press any key on the FDU to send the programming to the lock.

The addresses are now assigned. Every time lock addresses are programmed, the FDU sets the lock's internal clock to the correct time, so there is no need to reset the lock time. Remove the communication cable from the lock.

5.3.6 Programming Restricted Area Locks

Purpose: To program the address of a lock for a Restricted Area. The only keycards accepted by Restricted Area locks are the correctly addressed Restricted Area keycard, and the Emergency keycard. Only one address needs to be programmed into the lock, which is the Restricted Area number (from 1 to 200).

Level	Available Addresses	Example
Restricted Area	1-200	169
Emergency Master	-	All

Table 5.3.6: *Addresses for a Restricted Area 169 lock.*

Equipment required: FDU
Lock communication cable
Initialization keycard
Programming keycard
Completed Planning Forms

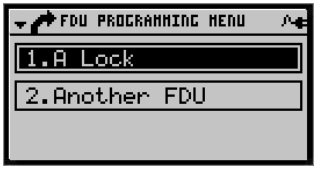
Minimum keycard required: Programming Authorization

Steps to program the Restricted Area lock addresses:

NOTE:
The initialization keycard starts up the PCB. It does not prepare the board for programming

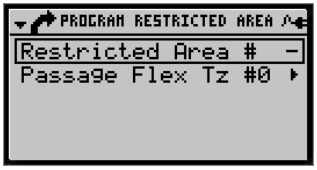
1. If this is a first time installation, or if power to the lock has been interrupted, insert the Initialization keycard in the lock. The red and green indicators should light, then only the green indicator should flash. Re-insert the Initialization keycard if the pattern of indicator lights described is not observed.
2. Swipe a keycard or enter a PIN value having a Programming authorized user level.

3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



4. Press 1 or <↵> to reach the "Lock Programming" menu.

5. Press 5 or use the down <▼> arrow followed by <↵> to reach the "Programming Restricted Areas" menu.



Consult the Planning Form to determine the desired addresses for the lock. Enter the new address and press <↵>.

6. Insert the Programming keycard in the lock, and ensure the green indicator is lit. Connect the communication cable from the FDU to the lock and press any key on the FDU to send the programming to the lock.

The address is now assigned. Every time lock addresses are programmed, the FDU sets the lock's internal clock to the correct time, so there is no need to reset the lock time. Remove the communication cable from the lock.

5.4 Resetting Lock Addresses

This function allows the FDU to download the addresses and the table of valid keycards from a lock, and to transfer the information to another lock. The address information can be edited before sending it to another lock, but not the valid keycard information. The FDU can send all or only selected Sub-Master addresses to the receiving lock.

5.4.1 Lock Replacement or Retrofit

When a lock is replaced, the replacement lock needs to be programmed with the same addresses as the old lock, and to accept the same keycards at the Guest and all Sub-master levels. If the old lock is still able to communicate this information to the Front Desk Unit, this can be accomplished by resetting the addresses with the data copied from the old lock. The new lock must first be programmed with the room number of the lock it

is replacing, since the Guest level address is not transferred when resetting lock addresses. The Guest keycard will continue to function in the replacement lock.

If the old lock is not able to communicate with the FDU, then the addresses can be copied from the lock of the next guest room. In all likelihood, this lock contains all of the same Sub-master addresses as the defective lock.

5.4.2 Expanding a Sub-Master Address

The Sub-Master addresses (Section, Floor, Group, Zone and Area) are also known as Variable addresses because they can be modified to reflect changes in staff access patterns. Variable addresses can be altered without affecting the valid keycards for other levels in two ways:

(i) Using a Reset keycard *(seeSsection 4.2.5 – Reset Keycards)*

or

(ii) Using the FDU to Reset the lock addresses, as explained below.

Occasionally, it may be desired to expand a Sub-Master level address to include several new rooms. For example, it may be decided that Group 2, which currently includes Floors 10-15, should also include Floors 16-20. There may be several keycards already in circulation for Group 2 that would be inconvenient to replace. If Group 2 is expanded by using a Group 2 Reset keycard in locks on Floors 16-20, these locks will recognize a later time stamp for Group 2 than the locks on Floors 10-15. Consequently, the Group 2 keycards currently in circulation will work on Floors 10-15, but not on Floors 16-20.

Alternatively, Group 2 can be expanded without needing to issue new Group 2 keycards, by resetting the addresses in locks on Floors 16-20 using the valid keycard data from a lock that is already in Group 2, taken from one of the locks on Floors 10-15. ***The FDU allows the selection of which Sub-master addressesare to be sent to the receiving lock. In this example, it is important to deselect all but the Group Sub-master level, so that other address levels, such as the Floor, are not changed.***

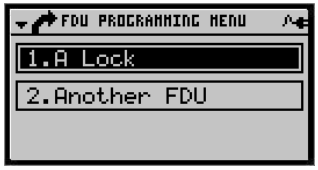
5.4.3 Procedure for Resetting Lock Addresses

Purpose:	To reset the addresses in one lock based on data downloaded from another lock.
Equipment required:	FDU Lock communication cable Initialization keycard Programming keycard Completed Planning Forms
Minimum keycard required:	Programming Authorization

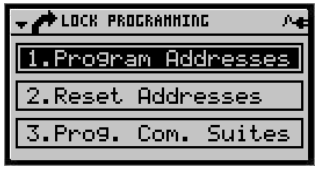
Steps to reset the lock addresses:

1. Program the new lock with the room number only. Refer to Sections 5.3.2, 5.3.3 or 5.3.4 and skip the steps for setting the Sub-Master addresses (Section, Floor, Group, Zone and Area).
2. Swipe a keycard or enter a PIN value having a Programming authorized user level.

3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "Programming FDU/Lock" menu.



4. Press 1 or <↵> to reach the "Lock Programming" menu.

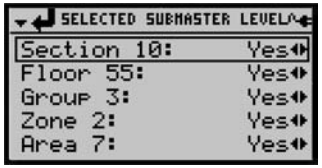


5. Press 2 or use the down <▼> arrow followed by <↵> to reach the "Reset Addresses" menu.

6. Insert the Programming keycard in the lock that is to be the source for the addresses (old lock or a neighbouring lock), and ensure the green indicator is lit. Connect the communication cable from the FDU to the source lock and press any key on the FDU to read the addresses and valid keycards.

Remove the communication cable from the lock.

7. The correct addresses and keycard data are now stored in the FDU. The FDU will display a list of the Sub-master addresses obtained from the source lock.



The Yes indicate Sub-master addresses that will be sent to the destination lock (the new or replacement lock). A Sub-Master level may be deselected by pressing the corresponding YES or NO value. ***Deselect any levels that are not to be sent to the new lock.***

8. Press <⌫>.

9. Insert the Programming keycard in the lock that is to be the destination for the addresses (new or replacement lock), and ensure the green indicator is lit. Connect the communication cable from the FDU to the source lock and press any key on the FDU to send the valid addresses and keycards.

The addresses have been sent. Remove the communication cable from the lock.

5.5 Remote Access Controller (RAC) Models 3.5, 4 & 4XT Flexible Time Zones

The Remote Access Controller (RAC) Models 3.5, 4 & 4XT support eight flexible time zones for restricting Guest access, Staff access and the hours during which Passage Mode can be active. The RAC Flexible Time Zones are first defined in the FDU Features menu using a General Manager Authorization keycard (see section 3.6 part 7.2 – Flexible Time

Zones). One of the eight Time Zones (1-8) or no time zone (0) can be selected for each of the following types of keycards when the RAC is programmed:

Time Zone Level	Applicable Keycards
Guest keycards	Guest, One-shot, Adjoining Suite, Common Door Suite and Convention Suite
Staff access keycards	Section, Floor, Group, Zone, Area, Bellman's Master and Grand Master
Passage mode	Passage

Using these time zones, RACs, which are often used for common areas such as a pool or other amenities or in other high traffic situations, can be customized to offer a higher degree of security based on the hours when access should be permitted. Guest, Staff, and Passage Mode access can all be restricted individually on each card reader.

NOTE: The six Fixed Time Zones that are encoded on Staff Sub-master level keycards to restrict access to other locks are not available on the RAC.

5.5.1 Guest and Staff Level Flexible Time Zones

When an otherwise valid entry keycard is swiped in the card reader of RAC Models 3.5, 4 or 4XT 4 at a time of day that does not fall in one of the intervals of the selected time zone, access will be denied, and the red indicator will flash once. If no time zone is selected, the RAC will accept valid keycards regardless of the time of day. The use of the Emergency keycard is not restricted by time zones. Staff and Guest access can be controlled by the same or different time zones.

5.5.2 Passage Mode Level Flexible Time Zone

The Passage keycard is used in the normal way when a Passage Time Zone is selected. The RAC is put in Passage mode by inserting a valid Passage keycard once. The RAC remains in Passage mode until the Passage Time Zone interval ends, or until a Passage keycard is swiped a second time in the reader of the RAC. The remainder of the time, a keycard will be required to gain access to the RAC.

5.5.3 Programming Flexible Time Zones

Purpose: To associate a Flexible Time Zone with a type of keycard (Guest, Staff or Passage) in the programming of RAC Models 3.5, 4 & 4XT. The addresses and the time zones can be programmed in one operation.

Equipment required: FDU
Completed Planning Forms

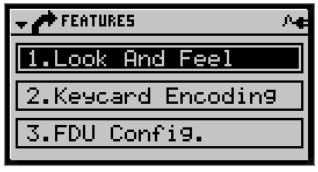
Minimum keycard required: Programming Authorization

Steps to program RAC Time Zones:

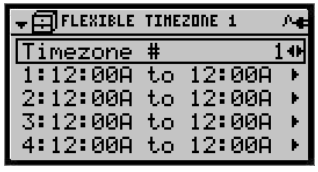
1. Swipe a keycard or enter a PIN value having a Programming authorized user level.

2. Press 7 or use the down <▼> arrow followed by <↵> to reach the "FDU Setup" menu.

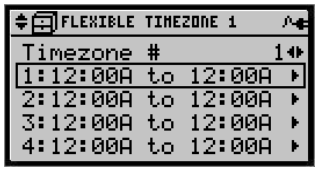
3. Press 2 or use the down <▼> arrow followed by <↵> to reach the "FDU Features" menu.



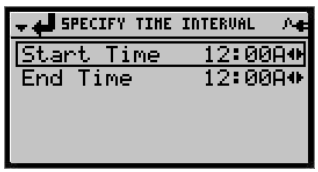
4. Press 5 or use the down <▼> arrow followed by <↵> to reach the "Flexible Timezones" menu.



The Timezone #s to be modified is selected using the left <◀> or right <▶> arrows. To change the intervals select the Timezone to be modified using the up <▲> or down <▼> arrows.



5. Press the right <▶> arrow to change the starting or ending hour.



6. Press <↵> when the interval is defined.
7. Program the RAC as per the *Section 5.3 – Programming Locks and Remote Access Controllers.*

5.6 Resetting Lock Time

Purpose:

The internal clock inside each lock should be reset whenever the battery power has been disconnected, or twice per year to eliminate time drift between the locks and the FDUs.

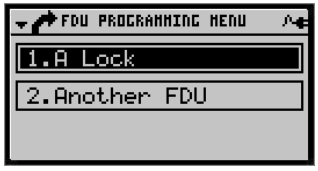
A lock which has been taken off battery power for more than a few seconds will not function until its time is reset, even when the batteries are replaced. This is a precaution to ensure that the time stays accurate. All the lock addresses, the table of valid keycards and the lock audit are retained in memory even during a battery failure, and the lock does not need to be reprogrammed following a battery replacement. Every time the FDU communicates with a lock, it sets the lock's internal clock to the correct time, so there is no need to reset the lock time if the lock addresses have just been reset or programmed or if the lock has just been audited.

Equipment required:	FDU Lock communication cable Initialization keycard Programming keycard Completed Planning Forms
Minimum keycard required:	Programming Authorization

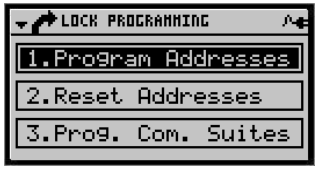
Steps to reset lock time:

1. If power to the lock has been interrupted, insert the Initialization keycard in the lock. The red and green indicators should light, and then only the green indicator should flash. Re-insert the Initialization keycard if the pattern of indicator lights described is not observed.
2. Swipe a keycard or enter a PIN value having a Programming authorized user level.

3. Press 8 or use the down <▼> arrow followed by <↵> to reach the "FDU Programming" menu.



4. Press 1 or <↵> to reach the "Lock Programming" menu.



5. Press 6 or use the down <▼> arrow followed by <↵> to reach the "Reset Time" menu.

6. Insert the Programming keycard in the lock, and ensure the green indicator is lit. Connect the communication cable between the FDU and the lock and press any key on the FDU to send the programming to the lock.

The lock's internal time is now set. Remove the communication cable from the lock.

5.7 The Emergency Override

Locks are equipped with an override located behind the decorative medallion, for use in an emergency. These overrides may be mechanical, or electrical in nature.

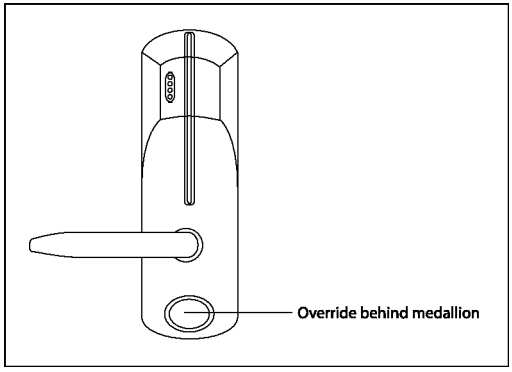


Figure 5.7: *Override location.*

Generation E-760 & 770 locks can be overridden electronically using the FDU and communication cable, or by drilling the handle.

5.7.1 The Mechanical Override

Locks with a mechanical override are equipped with a highly pick-resistant key cylinder which provides a mechanical bypass should the electronics fail. This cylinder is opened

using a high-security key, made with a factory-restricted key blank. This blank cannot be purchased and replacements are only available to an authorized agent of the property.

The mechanical key should not be in circulation since it will rarely be used. However, it should be available at all times in case of an emergency. The key will open a lock even if the deadbolt/privacy lock is engaged. Use of the override key is registered in the audit trail of the lock.

All override cylinders in the property are keyed alike and are different from the cylinders of any other property. Some models of mechanical override have interchangeable core-type cylinders, which can be removed with a special change key. This should only be done when replacing a defective lock, at which time the same cylinder should be placed in the replacement lock. Follow the instructions that were shipped with the lock. It is very important that keys and cylinders be secured at all times. In the event that a mechanical key is lost or stolen, please notify Kaba Ilco immediately.

5.7.2 The Electronic Override

Purpose: If the lock reader fails, the E-760, 770, and 710-II locks can be opened by the FDU using the communication cable. The lock must have been previously initialized by a valid FDU from the hotel where it is installed.

Equipment required: FDU

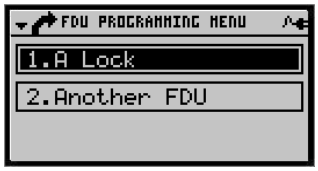
Lock communication cable

Minimum keycard required: Programming Authorization

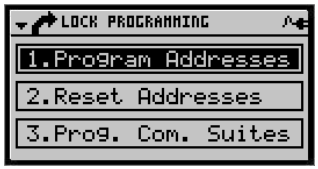
Steps to performing an electronic override:

1. Swipe a keycard or enter a PIN value having a Programming authorized user level.

2. Press 8 or use the down <▼> arrow followed by <↵> to reach the “FDU Programming” menu.



3. Press 1 or <↵> to reach the “Lock Programming” menu.



4. Press 7 or use the down <▼> arrow followed by <↵> to reach the “Electronic Override” menu.

5. Press <↵> to communicate with the lock and perform the override.

5.7.3 Overriding a RAC Card Reader

RACs control electrical devices such as magnetic locks, motorized doors and elevators, using relays. There is an ON/OFF override switch built into the RAC panel box. Each individual device should have an appropriate override installed to meet safety codes. An elevator, for example, should have a stop button.

5.8 The FDU Override

As an alternative to mechanical and electrical overrides, the FDU provides an easier way to override the privacy of 760, 770, and 710-II lock models. When the lock is programmed with the override privacy feature, any staff employee may unlock this lock. This is known as the “Global Australian Privacy Override” as this is typically only for

door configurations as found in International locations. Refer to *Section 3.6 part 21 – "Privacy Override"* for more details.

Chapter 6: Implementing the System

6.1 Introduction

The success of the property's Kaba Ilco Lodging Access Control System depends on good practices, from evaluating the needs of the property, to following the start-up and operating procedures correctly. This chapter provides an overview of the process of planning and implementing the system, with references to the detailed procedures elsewhere in this manual and instructions for using the forms in the Appendices.

6.2 System Administrator

For the best results in smoothly implementing and operating the system, a System Administrator should be appointed. The System Administrator is a person in a position of responsibility, who oversees all aspects of the system, including planning and implementing the system with the assistance of a qualified installer, arranging training, issuing Authorization keycards, controlling PINs, deciding the keying structure, FDU setup (language, staff accesses, POS, etc…) and maintaining good security practices.

In short, the System Administrator will become the "in-house expert" on the system. All major operations that underlie the security of the system, such as programming locks, maintaining records, issuing the more powerful keycards, and performing critical procedures such as a Hotel Restart should only be done in consultation with the System Administrator.

Whenever the assistance of Kaba Ilco is required, the System Administrator is the logical person to describe the problem to Kaba Ilco's support staff, and to obtain and implement advice and solutions. Over the years, Kaba Ilco has found that having one direct contact at a property helps provide the best service.

6.3 Planning the Property's System

In order to fulfill an order for the system, Kaba Ilco requires information about the rooms, suites and Common Areas in the property. The planning forms provided in Appendix B are an excellent way to prepare for ordering and installing the system, including creating the keying structure for the Sub-master (Section/Floor/Group/Zone/Area) Staff levels which will be used throughout the property. Consult a qualified Kaba Ilco vendor/installer for assistance in performing a "site survey" of the property and for help with filling in the forms.

A. Guest Common Areas:

There are eight Guest Common Area (GCA) numbers available. Use part A.1 of the form to plan how these eight GCA numbers will be used to provide access to the Guest Common Areas throughout the property for guest and staff. If eight numbers are insufficient, group all the areas that have the same keying into a single Common Area. For example, if all guests will have access to the side door, the elevator, the parking garage, and the sauna, simply group these four services into one Guest Common Area.

Circle AUTO if a Common Area is to be automatically given to all guests.

Circle YES if the Guest Service Attendant should be able to decide to allocate the Common Area to each guest's keycard.

If a Common Area is to be automatically encoded for a selected group of guest rooms only, this feature will be configured in the FDU at the factory. Enter the range of linked rooms, and circle NO for the default selection, so that other rooms will never be given this Common Area.

Example of Form B-A, part 1:

	Description	Given To	Default	Linked Rooms
1	*Elevator and side entrances*	*All guests*	Yes/No/(Auto)	
2	*Pool and tennis*	*All guests*	Yes/No/(Auto)	
3	*Parking gate*	*Paying guests*	(Yes)/No/Auto	
4	*Penthouse elevator access*	*Penthouse*	Yes/(No)/Auto	*2201 - 2204*
5	*Unused*		Yes/(No)/Auto	

Use the second part of the form to plan the address and lock or RAC model for each individual door that will be programmed as a Guest Common Area lock. Note that Common Area locks can have more than one address. For example, if GCA #1 is for guests in one wing of the property, including all the entrances to that wing, and GCA #2 is for guests in another wing of the property, the RAC for a lounge in the main lobby between the two wings can be programmed as Guest Common Area 1 and 2, thus giving access to all the guests in both wings, without using another Common Area address.

If desired, use the final column to plan how the RAC timezones will be used (for applicable doors).

Example of Form B-A, part 2:

2. Guest Common Area Doors

GCA	Door	Lock / Reader Model	(RAC 3.5/4/4XT) Time Zone (1-8) Guest	Staff	Passage
1	*Elevator, B to 6th floor relay*	*RAC 4*	*n/a*	*2*	*n/a*
2	*Health Club, door from lobby*	*RAC 4*	*1*	*2*	*4*
2	*Tennis, door from club*	*Solitaire 710-II*			
2	*Weight room, door from club*	*Solitaire 710-II*			
3	*Parking gate, West lot*	*RAC 4*	*n/a*	*n/a*	*n/a*
3	*Parking gate, East lot*	*RAC 4*	*n/a*	*3*	*4*
4	*Elevator, 7th floor relay*	*RAC 4*	*n/a*	*3*	*4*

B. Staff Common Areas:

There are 16 Staff Common Area numbers available. Staff Common Areas work similarly to Guest Common Areas but only for staff employees.

C. Sub-Master Levels:

This form is an opportunity to clarify how the Section, Floor, Group, Zone and Area levels may be used to manage staff access. Note that there is no hierarchy or link among these levels and they can be used as preferred. For example, if the system administrator prefers to use the Floor level because it represents the best representation, it is fine with the FDU system; another system administrator having to define the same access as the first one may prefer to use the Zone level, which is also correct. It is not mandatory to use all 5 levels if only some of them are required.

NOTE: The Group level is designed for housekeeping staff assignments, because of the Group Lockout keycard *(see Section 4.10 part C.5 – Group Lockout)*, which is normally given to housekeeper managers to invalidate the current valid guest rooms access after housekeeping staff have completed their work.

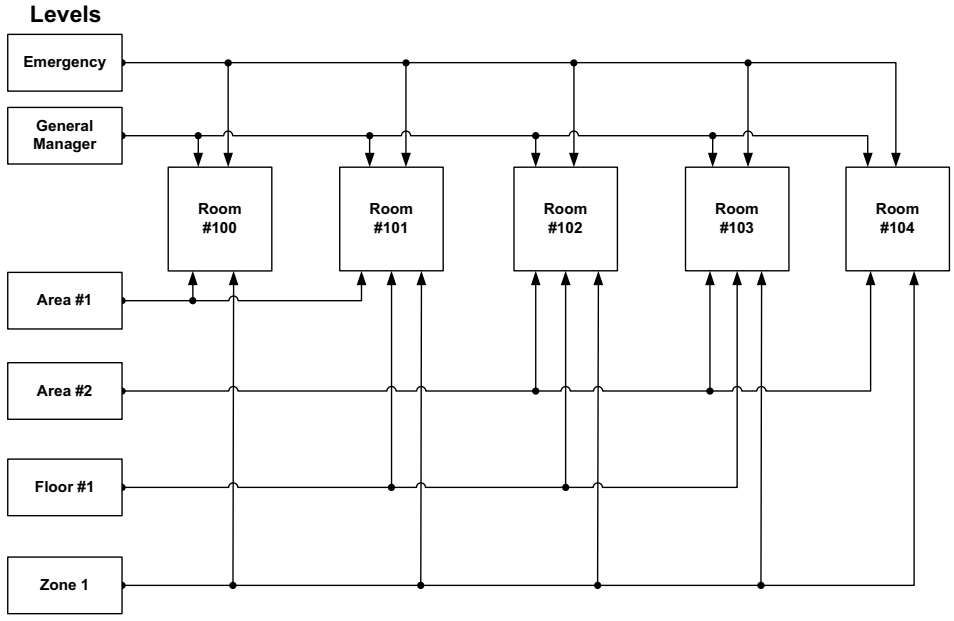
If the Backup Keycard Kit (part #BK-7911-E) is planned to be used, for properties up to 100 rooms, keep the Area level free for use with the backup kit, and program all locks as Group 1. Read the instructions that are shipped with the backup kit before continuing.

Each door may have an address from 1 to 255 for each of the Sub-master levels. They should be set up according to the needs of each property. Following are two examples

which illustrate how to use the Sub-master levels. If desired, draw a diagram on the back of the form to summarize the keying structure the property plans to use.

The Sub-Master levels are totally independent of each other. There is no need to program a certain number of Floors into each Section, or a certain number of Sections into each Group, etc. In fact, though Section always appears as a “lower” level than Floor, this need not be the case.

The following example shows some rooms along with the levels used to access the rooms. Both the Emergency and General Manager level access all rooms. Area #1 accesses rooms #100 and #101, area #2 accesses rooms #102, #103 and #104, Floor #1 accesses rooms #101, #102 and #103 and Zone 1 accesses all rooms.



Example of Form B-C:

	Description
Section	***Divides the rooms for housekeeping***
Floor	***Same as actual floor for outside maintenance contracts, etc***
Group*	***Whole property as Group 1 for use with backup kit***
Zone	***Unused***
Area**	***Same as Guest level, for use with backup kit***

D. Guest Rooms; E. Common Door Suites; F. Special Rooms; G. Restricted Areas

Once the keying structure has been decided, also known as the mapping of the hotel, the type of lock hardware, and the addresses that will be programmed into the lock, van easily be determined. Fill out planning forms D through G with this information to assist in programming the locks. For a description of each type of door, refer to *Section 5.3 – Programming Locks and Remote Access Controllers*.

Example of Form B-D (Guest Rooms):

Guest Address 1 - 16,000		Sub-Master Addresses 1 - 255					Lock / Reader Model	Passage Option	Linked G.C.A.	Programmed
Starting Room	Ending Room	Section	Floor	Group	Zone	Area				
101		1	1	1	n/a	101	Solitaire 710-II	NO	1, 8	
	110	1	1	1	n/a	110				
111		2	1	1	n/a	111	Solitaire 710-II	NO	1, 8	
	120	2	1	1	n/a	120				
201		3	2	1	n/a	201	"	NO	2, 8	
	210	3	2	1	n/a	120				
211		4	2	1	n/a	211	"	NO	2, 8	
	220	4	2	1	n/a	220				

Example of Form B-E (Common Door Suites)

	Guest Address 1 - 1,000		Sub-Master Addresses 1 - 255					Lock / Reader Model	Linked G.C.A.	Programmed
	Common Door	Inner Doors	Section	Floor	Group	Zone	Area			
	130		13	1	1	n/a	130	Solitaire 710-II	1, 8	
1		131	13	1	1	n/a	131	Solitaire 710-II	1, 8	
2		132	13	1	1	n/a	132	"	1, 8	
3		133	13	1	1	n/a	133	"	1, 8	
4		134	13	1	1	n/a	134	"	1, 8	
5										
6										
7										
8										

Example of Form B-F (Special Rooms)

Guest Address 1 - 16,000	Sub-Master Addresses (1 - 255)								
Door	Section	Floor	Group	Zone	Area	Lock / Reader Model	Passage Option	Linked G.C.A.	Programmed
415	*45*	*4*	*1*	*n/a*	*415*	*RAC 4XT*	*YES*	*none*	
Description: *Meeting Room A*									
420	*45*	*4*	*1*	*n/a*	*420*	*RAC 4XT*	*YES*	*none*	
Description: *Meeting Room B*									
425	*45*	*4*	*1*	*n/a*	*425*	*RAC 4XT*	*YES*	*none*	
Description: *Meeting Room C*									

The Special Rooms category (form F) exists for rooms which do not fit the normal Guest Room structure, but which are also not Common Areas or Restricted Areas. Examples include meeting rooms, lounges etc. Passage mode is not usually allocated to guest rooms, including Common Door Suites. Special room locks are programmed like Guest Room locks, but they can be put in Passage Mode if this option is requested for the specific room when ordering the system. Since they are programmed as Guest Rooms, rooms entered on the Special Rooms planning form can be rented as part of an Adjoining Suite, or Convention Suite *(see Sections 4.10 part A.3 – Adjoining Suite and 4.10 part A.5 – Convention Suite)*.

Example of Form B-G (Restricted Areas):

Door Identification		Restricted Area Access (1 - 200)	Lock / Reader Model	Passage Option	Programmed
Door	Description	Restricted Area			
B15	*Liquor Storage, basement*	*1*	*Solitaire 710-II*	*YES*	
B16	*Computer room, basement*	*2*	*RAC 4XT*	*YES*	
B30	*General Manager's Office*	*3*	*Solitaire 710-II*	*YES*	

H. Keycard Expiries

Fill in the expiry values planned to be used for each type of keycard, and a brief reason why. This information will be useful when setting the expiry values in the first FDU and for consultation if required to solve an expiry-related problem with the system. Filling in this form also provides continuity for explaining the system to others, for example if a new System Administrator is appointed.

Example of Form B-H:

		Selectable Expiry	Factory Default	Hotel Default Setting	Reason
Guest Level Access					
1	Guest	1 hr to 2730 nights	1 night	*1 night*	*Short stay property*
2	One-Shot	1 hr to 4 hrs	1 hr	*1 hr*	*Typical walk-in*
3	Adjoining Suite	1 hr to 2730 nights	1 night	*7 nights*	*Adj. Suite usually rents for 1 week*
4	Common Door Suite	1 hr to 2730 nights	1 night	*7 nights*	*Comm. door suite usually rents for week*
5	Convention Suite	1 hr to 2730 nights	1 night	*7 nights*	*Conv. Suite usually rents for 1 week*

I. FDU Features

After reading *Section 3.6 – FDU Feature Reference*, and understanding the use of each feature, use this form to enter the selections planned to be used as the Hotel Defaults. This information will be useful when setting the features in the first FDU, and for consultation if required to solve feature-related problems with the system. Filling in this form also provides continuity for explaining the system to others, for example if a new System Administrator is appointed.

Example of Form B-I:

Features		Comment	Factory Default	Hotel Set Default	Reason
1	Language	1 or 2	1	*1*	*English per our order*
2	Variable Expiry	YES or NO	YES	*YES*	*Length of guest stay may differ*
3	Guest Common Areas	YES or NO	NO	*YES*	*GCAs are used for user-pay spa*
		See Appendix C-A.1 for planned use of each Guest Common Area			
4	Salesman's Lockout	YES/NO/AUTO	NO	*NO*	*Not required by clientele*
5	Staff Access all Guest Common Areas	YES or NO	NO	*YES*	*For cleaning, evacuation plan*

J. Initial set of Keycards

Consult the plan for the Sub-master levels, and estimate the number and type of keycards required for staff use (Section, Floor, Group, Zone, Area, Restricted Area, Passage, Emergency, Grand Master, Authorization level keycards, etc.). List these keycards in form J. Determine how many copies are needed of each keycard. For example, if there are four employees who need to carry a Floor 2 keycard, enter four copies. These four

keycards will be made in the same transaction on the FDU, so that all the keycards will have the same time stamp.

Example of Form B-J:

All copies should be encoded as identical NEW keycards in one transaction of the FDU.

All copies should be encoded as identical NEW keycards in one transaction of the FDU

Keycards	Used by	Copies
Section 1	*Housekeepers, rooms 101-110*	*3*
Section 2	*Housekeepers, rooms 111-120*	*3*
Group 1 Lockout	*Housekeeper Managers*	*2*
Emergency	*Security staff on duty, & stored in safe*	*2*
Group 1	*Housekeeper Managers*	*2*
Restricted Area 3	*General Manager (for her office)*	*1*
Grand Master	*Maintenance Manager*	*2*

6.4 Starting the System After Installation

The System is usually started with the assistance of a Kaba Ilco installer. The System Administrator should participate closely in the startup to ensure his or her full understanding of how the system is configured, and to ensure that the choices made during the startup procedure are appropriate for the security and key control needs of the property.

In general, starting the System consists of the following major steps:

1. **Install the lock hardware:**

   This step is performed by a Kaba Ilco certified installer, who installs the correct type of lock or RAC to serve each door, according to the plan previously established. While the locks are being installed and before they are programmed, the Test Lock keycard can be used to test and open any door.

2. **Initialize the first FDU and set the options that will affect the operation of the system:**

   The first FDU is charged and the system time and language are selected. This FDU is then restarted with a secret external Hotel Code chosen by the management of the property, which ensures the security of the system. The remaining options for keycard expiries and FDU operation are selected, and a set of spare keycards for use

in emergencies or for servicing the system in future are encoded and placed in a safe. This step can be performed by the installer or the System Administrator.

3. **Initialize the remaining FDUs:**

   The first FDU is used to set up the system parameters of all the remaining FDUs (by performing an FDU to FDU data transfer as per *Section 3.5.4 – Transferring Data to Another FDU*), so that all the FDUs operate identically.

4. **Program all the locks on the property:**

   The FDUs are used to program the addresses of all the locks and card readers on the property. At the same time, the FDU automatically sets the internal clock of each lock to be in synch with the internal system time in the FDUs.

5. **Encode the keycards needed for staff and management:**

   An initial set of staff keycards for each access and authorization level is prepared. A printer is connected to the FDU throughout this operation to provide a printed record of the sequence ids of the keycards for use in conjunction with the audit trail if there is ever an investigation of illicit use of the FDU or a lock.

6. **Train the staff and issue them keycards:**

   The System Administrator initiates the process of training the staff in the use of the system, and should supervise the signing out of the previously encoded keycards to staff.

6.4.1 Starting the FDUs

Each FDU arrives from the factory with the software required in its permanent memory. This includes the hotel configuration like common door suites, guest common areas and other information specified in the planning forms. The FDU's batteries must be charged before they can be first used.

The first FDU must be configured with the external Hotel Code, the local standard time and date ***(ensure that DST is NOT entered at this stage)***, and the desired features including the selectable expiry times for each type of keycard. The system start-up prompts must be hidden from other users. This first FDU is then used to encode emergency keycards and spare GMA and Initialization keycards.

The remaining FDUs are initialized and the setup information from the first FDU is transferred to each other FDU using the serial port on the rear of the unit. This way, all the valid authorization keycards, the time and the FDU settings are identical on all FDUs.

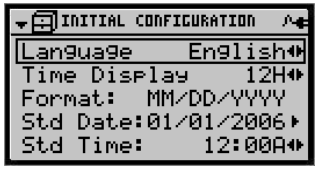
IMPORTANT: All FDUs must be plugged in and charged at least 24 hours in an AC outlet before their first use in battery back-up mode.

6.4.1.1 Initializing the First FDU

Purpose:	To start the first FDU in the system
Minimum keycard required:	GMA keycard that shipped with the FDU
Required condition:	FDU has been charged a minimum of 24 hours

Steps to initialize the first FDU:

1. The screen will show an hourglass. After a brief pause, the following screen will appear to perform language, date and time adjustment. ***If the screen does not come up please contact Kaba Technical Support.***

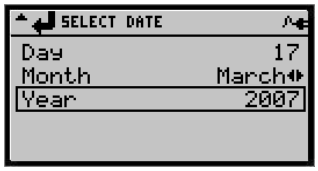


   Use the left <◀> or right <▶> arrow to select the desired language. When the appropriate language is chosen, use the down <▼> arrow.

2. To change the time display format, press the up <▲> or down <▼> arrow to select the "Time Display" option and press the left <◀> or right <▶> arrow to toggle between 12-hour and 24-hour format as desired. Based on the selected time format the date format will also change. The following shows the differences between the 2 formats:

	12-hour format	**24-hour format**
Standard Date:	MM/DD/YYYY	YYYY-MM-DD
Standard Time:	12 hrs + A (AM) or P (PM)	24 hours

3. To change the date, press the up <▲> or down <▼> arrow to select the "Std Date:" option, and press the right <▶> arrow to change the date.

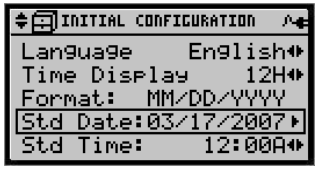


Use the keypad to enter the day of the month. To correct a mistake done using the keypad, use the left <◀> arrow; this applies for all numeric entries done in this section.

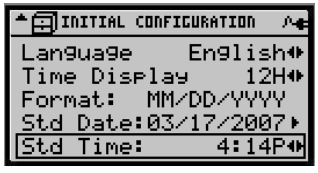
Select the Month option with the down <▼> arrow. Use the left <◀> or right <▶> arrow to select the correct month.

Finally select the Year option if needed and enter the year with the keypad.

When all 3 parameters are correct, press <↵>.



4. To change the time, use the up <▲> or down <▼> arrow to select the "Std Time:". Change the time to the correct **LOCAL STANDARD TIME** (NOT daylight saving time). Refer to *Section3.2.3.3 – Entering Time:* for how to enter the time.



Press <↵> to save the parameters. The time shown will be STNADARD TIME. If required, dependent on the time of year, set DST when the FDU features are set in Step 6.

5. ***Perform a Hotel Restart on the first FDU only. Follow the instructions in section 3.5.9 – Hotel Restart.*** Only one Hotel Restart keycard is needed. The Hotel Code should be different from **1000**. Ensure that the two Emergency, Initialization and GMA keycards mentioned in step 13 are made, and lock them in a safe along with a record of the Hotel Code chosen.

6. ***Set all keycard expiries and FDU features (see sections 3.5.2 – Setting Keycard Expiries and 3.6 – FDU Feature Reference), using the values previously chosen on planning forms H and I.*** Pressing <↵> saves each value set automatically.

   When setting the features, ensure that the Disable Prompt feature is set to YES (see Section 3.6 part 15 – Disable Prompts. This setting prevents accidental changes to the internal system time as a result of resetting an FDU *(see also section 3.5.10 – Resetting the FDU)*.

7. If many FDUs are to be configured, perform an FDU to FDU transfer *(see Section 3.5.4 – Transferring Data to Another FDU)*. Discard the GMA that came with the FDU and retain the new GMA 200 for use in initializing the remaining FDUs.

6.4.1.2 Taking a Census of the FDUs

Each FDU has an identifying number, which must be written down and stored in the safe along with the spare keycards and the Hotel Code. This information becomes important to the security of the property if ever an FDU is stolen. Make a list of all the FDU numbers on the property using the FDU Identification function, as described in *Section 3.5.6 – Displaying the FDU Identification*. The FDU number is located at the right of the "FDU #" option:

Update the list of FDU numbers if additional or replacement FDUs are ordered.

6.4.2 Programming the Locks

All Kaba Ilco locks and RACs arrive from the factory with the operating system necessary to perform the functions of any door in the system (Guest room, Common Door Suite, Common Area, Restricted Area). Before a lock can be used with any keycard except the Test Lock keycard and Initialization keycard, it must be initialized and programmed with the correct addresses for the door on which it is installed, and its internal clock must be set. ***Program each lock on the property according to the***

instructions in Section 5.3 – Programming Locks and Remote Access Controllers. Consult the planning forms previously prepared to assign the correct Room, Section, Floor, Group, Zone and Area address to the lock, or the correct Guest Common Area, Staff Common Area or Restricted Area address. The lock's internal time is automatically set to match the FDU when the addresses are successfully sent.

NOTE: Since a large number of locks need to be programmed in succession, set the FDU timeouts for "between keystrokes" and "between keycards" to their maximum values of 20 minutes *(see Section 3.6 part 9 – FDU Time-outs)*. The FDU will remain authorized for up to 20 minutes between operations. The addresses sent to the most recently programmed lock will remain in memory during that time, allowing the user to program the next lock more easily, by changing only the lock addresses which differ from the previous lock. Once finished programming, return the timeout values to the Hotel Defaults.

Once programmed, the lock will not accept the Test Lock keycard. To enter the room, make a valid keycard for that room.

The RAC flexible time zones (for Common Area doors only) are programmed-when the RAC addresses are programmed. Set up the time intervals in the flexible time zones in the FDU settings before programming the RAC as a Common Area lock *(see Section 5.5 – Remote Access Controller (RAC) Models 3.5, 4 & 4XT Flexible Time Zones)*.

6.4.3 Making the Initial Set of Staff Keycards

With the locks programmed, the system is fully operational. The System Administrator should now encode Authorization, Entry and Passage, Group Lockout, etc. keycards for staff members as required.

NOTE: When prompted to select NEW or DUPLICATE keycards, select NEW. If more than one copy of a Staff Sub-master level keycard (Section/Floor/ Group/Zone/Area) is required, DO NOT encode them one at a time. Instead, enter the exact number of keycards that is required when the FDU asks for the number of keycards:

All the keycards will be NEW keycards with the same time stamp, which will not cancel each other when used in the locks. Their “sequence ids” however will be different, so that the employees can be identified individually from the audit trail. If an employee is to be

added to a level for which a number of keycards has already been made this can be done with selecting DUPLICATE.

Example: Group 1 will be used by a team of 3 housekeepers, supervised by one housekeeper manager with a Group 1 lockout keycard for canceling the previous guest's access when one of the rooms prepared by their team of housekeepers has been inspected.

These four employees all need access to the doors in Group 1, and need to carry a Group 1 keycard.

NOT TO DO: If the keycards are encoded in four separate operations, then each one will have a different time stamp. The housekeeper with the most recent Group 1 keycard will cancel all the others when they first use their keycard in one of the Group 1 locks.

TO DO: If the keycards are encoded together in one operation as four identical copies, then all four will remain valid until they expire or are reset, and any of the three housekeepers or the housekeeper manager will have access to any of the rooms in Group 1.

If after making the first four Group 1 keycards, another two Group 1 keycards are required for two other employees, encode two DUPLICATE Group 1 keycards that will not cancel the first four.

6.5 Training Staff

IMPORTANT: This manual contains sensitive security information and is for management use only.

The System Administrator should provide copies of the Front Desk User's Guide to Guest Service Attendants. That booklet provides a handy reference for all the features of the system accessible using a Front Desk Authorization keycard, as well as relevant background that is sufficient for most non-management staff.

Training materials and seminars are available to help with the introduction of staff and management to the system.

For more information, contact Kaba Ilco.

6.6 Issuing Keycards to Staff

For the future integrity of the audit trail, it is important that each staff keycard issued to a staff member or manager (i.e. given out to any employee for their use) be recorded in the Keycard Issuing Log provided in Appendix C. The System Administrator should ensure that each staff member has the minimum number of keycards (usually only one keycard

per person) for all their access needs, and an Emergency keycard should be available on every shift. Each keycard must be "signed out" for legal proof of the identity of the authorized card holder.

Example of how to use the Keycard Issuing Log:

Many properties prefer to manage Staff keycards by signing them out to each staff member for each shift. In addition, Staff keycards have an expiry date. Many properties choose an expiry for Staff keycards of one month. This choice of expiry ensures that unreturned keycards are invalidated after a reasonable period of time, in the event of staff turnover, but it is also far enough in the future to allow an efficient daily sign-out procedure as follows.

Sample daily sign-out procedure:

1. Encode the new Staff keycards needed for the entire month. If this is not the first time these keycards are being made, the choice is available to re-encode the keycards currently carried by staff, or to encode new blank keycards, and collect the previous month's keycards for re-use at a later date.
2. Complete the Staff Keycard Issuing Log for the upcoming month. Enter each "sequence id", the type of keycard, and the ID code written on the card (if any), but leave the employee name and the other spaces blank.

IMPORTANT: Never identify a keycard with the rooms it opens. The ID code written on the keycard, if any, should help to identify the keycard, but be meaningless to others. A good example would be a number that designates the month for which the keycard is valid, followed by a number that is not related to the doors opened by the keycard.

Employee **MUST** sign for Restricted Area, Sub-Master and Master level entry keycards and all Authorization keycards*

ID Code	Keycard	Sequence id	Employee Name	Date	Time OUT	Signature	Date	Time IN	Signature
12011	*Group 1*	*35597-031*							
12422	*Floor 5*	*35598-055*							
12103	*Floor 5*	*35598-057*							
12054	*Section 3*	*35599-083*							
21604	*FDA 12*	*44234-021*							

12231	*PA 102*	*45345-001*							
12252	*PA 103*	*45345-201*							
12006	*MA 161*	*46909-021*							
12027	*MA 162*	*46909-023*							
12010	*GMA 199*	*47008-003*							
12024	*GMA 198*	*47008-069*							

3. Make as many copies of the partially completed log as there are shifts. Enter the employee names for each keycard for each shift. By making 31 copies of these master lists, a binder can be prepared for the entire month, ready for each employee to sign for their keycard at the beginning of each shift.

Employee **MUST** sign for Restricted Area, Sub-Master and Master level entry keycards and all Authorization keycards*

ID Code	Keycard	Sequence id	Employee Name	Date	Time OUT	Signature	Date	Time IN	Signature
12011	*Group 1*	*35597-031*	*Charles Jones*						
12422	*Floor 5*	*35598-055*	*Sarah Collins*						
12103	*Floor 5*	*35598-057*	*Terry Langevin*						
12054	*Section 3*	*35599-083*	*Cora Hart*						
21604	*FDA 12*	*44234-021*	*Sophie Lamorey*						
12679	*FDA 20*	*44235-008*	*Allan Grant*						
12231	*PA 102*	*45345-001*	*Thomas Hardy*						
12252	*PA 103*	*45345-201*	*Sergei Kaminsky*						
12006	*MA 161*	*46909-021*	*Greta Talbot*						
12027	*MA 162*	*46909-023*	*Amergio Rotili*						
12010	*GMA 199*	*47008-003*	*Christian Houle*						
12024	*GMA 198*	*47008-069*	*Jane Liu*						

6.7 Updating the configuration file

In the event new doors or suites need to be added to an existing configuration, help from Kaba Ilco is required.

The new configuration must be described to Kaba Ilco who will generate a new hotel configuration file and provide details for updating the system.

Contact Kaba Technical Support for full details.

Chapter 7: Auditing

In the event of suspected illicit entry to a room or use of the FDU, the audit trails can be read by following the instructions in this chapter. In addition, the lock audit is useful for verifying the lock firmware version, addresses and battery voltage (Generation E-760, 770, and 710-II locks only), if the lock appears to be malfunctioning.

According to the privileges of the user, the audit options available will vary as shown in the following table:

User	Type of audits that can be exported.
General Manager	Lock and FDU audits
Master	Lock audits
Programming	Lock audits
All others	None

Table 7: *Users with audit transfer abilities*

7.1 Auditing a Lock

The lock audit is stored in non-volatile memory, and cannot be erased by disconnecting the batteries, or by any programming function. Locks store the most recent 350 entries in FIFO (First-In-First-Out) format, with the following information:

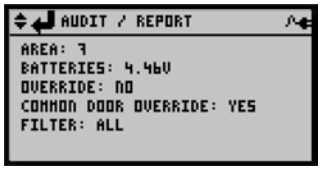
- Lock firmware version
- Type of lock
- Lock adresses
- Data for each recorded entry
    - Keycard level
    - Issuer's Authorization number
    - ID (serial) number
    - Date and time of entry

Generation E-760 & 770 locks store the most recent 200 audit entries.

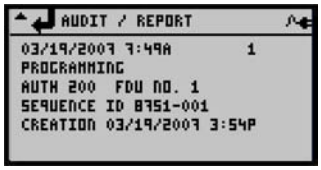
Example of a 760K lock audit:

The first screen displayed by the FDU when showing a lock audit contains information about the lock type, PCB, firmware version and addresses.

Subsequent screens contain information like the battery voltage level, featres encoded on the card, and the individual audits, numbered by most recent entry.



Audit #1 below shows the information on the programming keycard used to program the lock information.



In order to view the lock audit, the audit data must be transferred to the FDU for display, printing or saving. This can be accomplished by swiping a Programming keycard in the lock, waiting for a green LED to display on the lock, connecting the FDU to the lock using the communication cable and following the on-screen directions.

A sample print-out of a lock audit is shown below.

Audit Event	Description
760 (LCB9) Version: 1.35 Guest Room: 100 Section: 10 Floor: 55 Group: 3 Zone: 2 Area: 7 Batteries: 4.46V Override: YES Common Door Override: NO Filter: All	Information on the lock itself, including room number, addresses, battery level and audit filter information.

03/20/2007 7:49A 1 PROGRAMMING Auth 200 FDU No. 1 Sequence ID 8751-001 Creation 03/19/2007 3:54P	Most recent audit entry in memory, showing that a programming keycard was used (to download the audit), and the sequence ID of the keycard (to identify the staff).
03/20/2007 7:48A 2 GUEST Auth 200 FDU No. 1 Sequence ID 9705-005 Creation 03/20/2007 7:48A	Second most recent audit entry showing the usage of a guest keycard, time of entry, and the user authorization level that created the guest keycard.
03/20/2007 7:46A 3 OVERRIDE Auth 200 FDU No. 1	Third most recent audit entry showing the usage of the FDU to perform an override on the lock, and the user.

Figure 7.1: *Sample of printed lock audit, includes access and automation information.*

The FDU can store the full audit trail from up to 10 locks at a time. Each audit may be selected individually, scrolled on the screen, printed, saved on a PC or deleted from FDU memory as required. If a lock is audited twice, the top audit in the Front Desk Unit will always be the older one.

Auditing a RAC is done in the same manner as auditing a lock.

7.1.1 Auditing Locks Using the FDU

IMPORTANT: Do not attempt to read or encode any keycard (including Authorization, Programming and Initialization keycards) while the communication cable is connected between the FDU and the lock or RAC. Connect the cable just before sending or reading the information.

Purpose: To obtain the audit trail stored in the lock's non-volatile memory.

Minimum keycard required: Programming Authorization

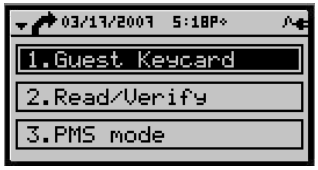
Equipment Required: FDU

FDU to lock communication adapter

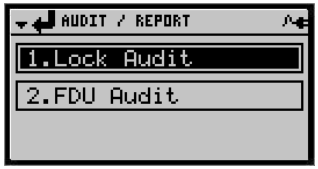
Programming keycard

Steps to obtain the audit trail from a lock

1. Swipe a keycard or enter a PIN having a Programming authorized user level.

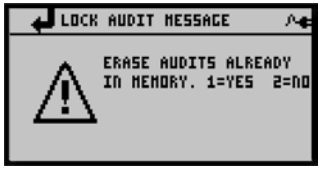


2. Press 9 or use the down <▼> arrow followed by <↵> to reach the "Audit/Report" menu.



3. Press 1 or <↵> to reach the "Lock Audit" menu.

4. Press 1 or <↵> to select the "Audit Lock" option. If there are other audits already stored in memory, the following message will appear.



The FDU can store up to 10 lock audits in memory. To keep the existing audits, enter 2. The new audit will be added to the audit list. To erase the existing audits, enter 1. The following screen will then be shown:

5. Connect the FDU to lock communication cable to serial port “A” on the back of the FDU.
6. Use the Programming keycard on the lock. Make sure that the solid green indicator is lit, and then insert the communication cable into the lock.
7. Press any key to start the communication.

If the SUCCESSFUL message is not displayed, the FDU has not received the data from the lock. Repeat Steps 3 to 6.

8. Once the data has been transferred to the Front Desk Unit, remove the communication adapter.

   The audit information is now stored in the Front Desk Unit.

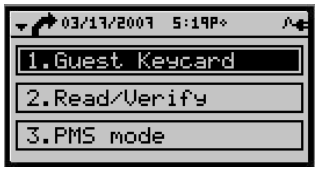
7.1.2 Clearing the Lock Audit from the FDU Memory

Purpose: To clear the lock audit from the Front Desk Unit

Minimum keycard required: Programming Authorization

Steps to clear the lock audit data from the Front Desk Unit

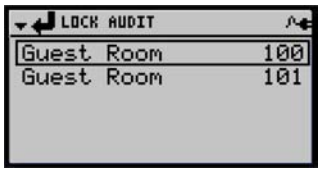
1. Swipe a keycard or enter a PIN having a Programming authorized user level.



2. Press 9 or use the down <▼> arrow followed by <↵> to reach the "Audit/Report" menu.

3. Press 1 or use <↵> to reach the "Lock Audit" menu.

4. Press 2 or the down <▼> arrow followed by <↵> to reach the "Clear Lock Audit" menu. The list of locks found in the FDU memory is displayed on the FDU screen.



5. Select the lock to clear using the room number using the up <▲> or down <▼> arrow then press <↵>.

   The audit trail has been cleared from the Front Desk Unit.

If there is no lock audit in the FDU memory, the following message is displayed:

7.1.3 Viewing, Printing or Sending the Lock Audit to an USB Memory Stick

Purpose:

Once the lock audit is in the FDU memory, it can be viewed, printed or sent to a USB memory stick in whole or in part. The Front Desk Unit can create a lock audit according to:

- Sequence of entries (all, previous 100, etc.)
- Authorization number used to encode the keycard used for entry
- Type of keycard used for entry (Guest, Grand Master, etc.).

In order to print, a serial printer must be connected to the FDU and properly configured (see section 2.5).

Minimum keycard required: Programming Authorization

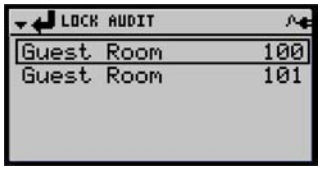
Steps to view or print the lock audit entries stored in the Front Desk Unit

1. Swipe a keycard or enter a PIN value having a Programming authorized user level.

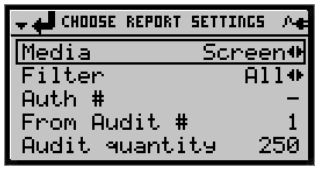
2. Press 9 or use the down <▼> arrow followed by <↵> to reach the "Audit/Report" menu.

3. Press 1 or <↵> to reach the “Lock Audit” menu.

4. Press 3 or use the down <▼> arrow followed by <↵> to reach the “Lock Report” menu.



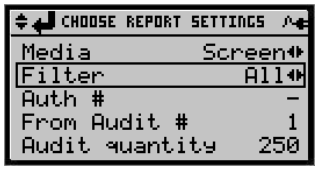
5. Select the lock to audit with the room number using the down <▼> arrow then press <↵>.



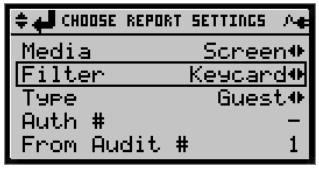
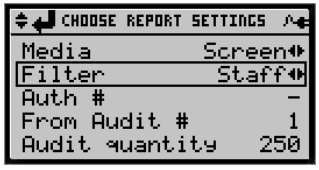
6. Select the media on which the audit will be sent. Use the left <◀> or right <▶> arrow to toggle between the Screen (FDU display), USB Drive (USB memory stick option), Serial (serial line printer connected to the serial port), or USB printer (USB line printer connected to the USB port).

   For this example, the desired media is Screen but the next steps apply to any media.

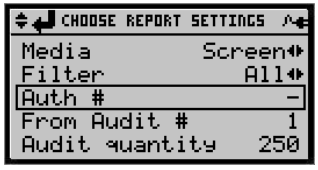
7. Use the down <▼> arrow to select the Filter option.



The following options for filtering the Audit entries are available:

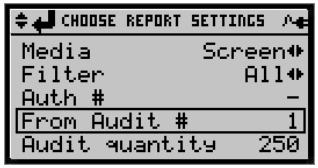
Option	Result
All	The entire audit will be displayed in reverse chronological order, from the newest entry to the oldest.
Keycard	When this choice is selected, the new option Type is displayed. Only the selected keycard type entries will be displayed.  To select the keycard type, select the Type option with the down <▼> arrow and the desired keycard type with the left <◀> or right <▶> arrow.
Staff	Only staff entries will be in the audit result. 

8. Use the down <▼> arrow to select the “Auth #” option.



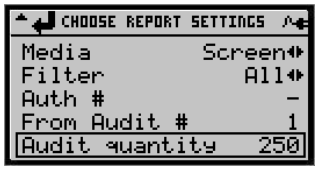
Specify the Authorization number. All entries by keycards encoded using the specified Authorization will be displayed.

9. Use the down <▼> arrow to select the “From audit #” option.



Enter the starting entry in the audit. The default value is 1, which is the newest one.

10. Use the down <▼> arrow to select the “Audit quantity” option.

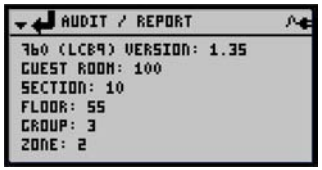


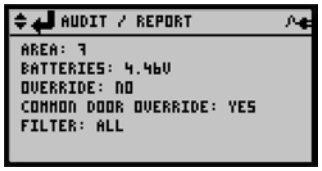
11. Enter the maximum number of entries in the audit to print. Only the most recent entries will be displayed, up to the specified number of entries. If an audit appears more than once, then the last entry is the most recent.

    Depending on the media that will receive the result of the audit, the following steps differ. The 3 following sections describes the particularity of the audit sent to the FDU screen, to a line printer or to a USB memory stick.

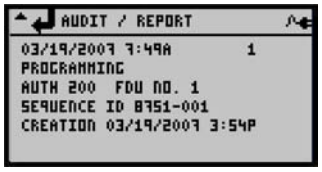
Lock Audit sent to the FDU screen

Press <↵> to start the audit report. When viewing the audit on the FDU screen, use the <▲> and <▼> keys to scroll through the list of entries. The first two screens will show information about the lock itself.





The following screens show information on the audit of the lock.

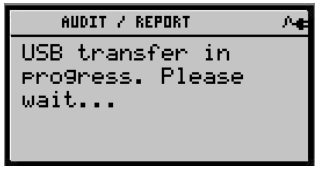


Lock Audit sent to the printer

Connect a serial line printer to the FDU serial port, or a USB line printer to the USB port. Press <↵> to start the audit report. The result of the audit will be sent to the connected printer.

Lock Audit sent to a USB memory stick.

1. Connect a USB memory stick to the FDU USB port.
2. Select the USB Drive as the media.
3. Press <↵> to start the audit transfer to the USB stick.



When the transfer is completed, a message is displayed to the user.

When the transfer is done, from this moment, the USB stick may be removed and plugged into a PC.

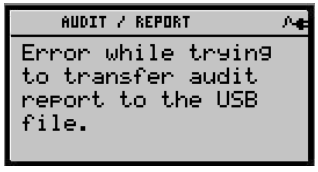
Most modern operating systems will automatically detect the USB stick and show its contents upon detection. The file containing the lock audit is called LockAudit.log and is created in the main directory on the USB so they are easy to find. This file is formatted in tab-separated columns compatible for import by standard spreadsheet software, which can be used to format, sort, analyse or print the audit information. To simply look at or print the file, a regular text editor may also be used.

IMPORTANT: **If another audit transfer is performed on the same USB stick, the new files created will overwrite the previous one. For this reason, it is suggested to immediately copy the audit files onto the PC to save them.**

Use separate directories, or rename audit files once transferred to a PC, to maintain a historical record of audits.

Note that if there is not enough space available on the USB stick, this operation will fail and an error message will be displayed on the screen. The majority of existing USB memory sticks will work with the FDU. If the USB stick is not compatible with the FDU, it will not be detected and the FDU will not display any error message to the user. Another type of USB memory stick should then be used. Additionally, if the USB stick is not formatted, the FDU will detect it but will not be able to access it further and will display an error message. If this occurs, format the USB memory stick on a PC, as per the manufacturer's requirements or contact Kaba Ilco for assistance

If ever there is no USB stick plugged in the FDU, or the FDU does not recognize the USB memory stick plugged in, the following message will be displayed:



7.2 Auditing the FDU

The FDU audit records all keycard encoding as well as the verification of returned Staff keycards using the readback function, and the verification of Guest level keycards that are read back without knowing the room number (either in POS Verifier mode or if the Read Card feature is enabled see section 4.6.14). These are all the functions of the FDU that are important from the standpoint of security or for investigating abuse. When the

audit is viewed or printed, it appears in reverse chronological order (starting with the most recent entry).

Audit Event	Description
03/20/2007 8:15A Firmware version: V0.920 FDU No.: 1 Encoder type: FDU-B Coercivity: Low C HCONF date: 01/01/2001 HCONF version: 0 Filter: All	Information on the FDU, including firmware revision, FDU number, type and date of hotel configuration. Note that the hotel configuration information itself is not shown for security reasons.
03/20/2007 7:49A 1 LOCK AUDIT EVENT Auth 200	Most recent FDU activity showing, the performing of a lock audit.
03/20/2007 7:48A 2 GUEST Encoding Room Number 100 Auth 200 NEW, Seq ID 9705-005 EXPIRY DATE 2007/03/21	Second most recent FDU activity, showing the encoding of a Guest keycard for room 100, by user authorization 200 (GMA authorization level).
03/20/2007 7:46A 3 ELECTRICAL OVERRIDE EVENT Auth 200	Third most recent FDU activity, showing the performing of an electrical override of a lock with the FDU.
03/20/2007 7:45A 4 LOCK PROG EVENT (RESET TIME) Auth 200	Fourth most recent FDU activity, showing the resetting of the time in a lock with the FDU.

Figure 7.2a: *An example of a printed Front Desk Unit audit.*

The Front Desk Unit audit can also be verified on the Front Desk Unit display in abbreviated form.

Figure 7.2b: *An abbreviated version of the audit as seen on the FDU screen.*

Scroll through the audit with the Up and Down arrows on the Front Desk Unit keypad.

7.2.1 Viewing, Printing or Sending the FDU Audit to an USB memory stick

Purpose:

The Front Desk Unit audit can be viewed, printed or sent to an USB memory stick in much the same way as a lock audit. The audit can be filtered according to:

- Sequence of entries (all, previous 100, etc.)
- Authorization number
- Type of keycard
- Room number
- Logged-off Staff cards
- Audited checkouts

Logged-off Staff cards refers to Staff cards read using the readback function *(see Section 4.9.3 – Verifying a Staff Keycard).*

Audited Checkouts refers to Guest cards read using the readback function without room number required *(see Section 4.9.2 – Reading a Guest Keycard and 3.6 part 14 – Guest Keycard Read Back Enable without Room)*. This function, which requires the room number to be entered before information on the keycard can be verified, is not audited *(see Section 3.9.1 – Verifying a Guest Keycard)*.

Minimum keycard required: General Manager Authorization

Steps to view, print or send to a USB memory stick the Front Desk Unit audit entries:

1. Swipe a GMA authorized keycard.

2. Press 9 or use the down <▼> arrow followed by <↵> to reach the "Audit/Report" menu.

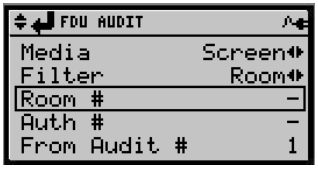
3. Press 2 or use the down <▼> arrow followed by <↵> to reach the “FDU Audit” menu.

4. Select the media on which the audit will be sent. Use the left <◀> or right <▶> arrow to toggle between the LCD (FDU screen), Serial (printer), USB printer, or USB drive(memory stick). For this example, the desired media is LCD but the next steps apply to any media.

   Use the down <▼> arrow to select the Filter option.

   The following options for filtering the Audit entries are available:

Option	Result
All	The entire audit will be displayed in reverse chronological order, from the newest entry to the oldest.
Keycard	When this option is selected, the new option Type is displayed. Only the selected keycard type entries will be displayed.

	 To select the keycard type, select the Type option with the down <▼> arrow and the desired keycard type with the left <◀> or right <▶> arrow.
Room	When this option is selected, the new option Room is displayed.  Use the keypad to enter the room number.
Staff	When this option is selected, the list of the entire log-offs of Staff cards is displayed.  Use the keypad to enter the Authorization number.
Checkout	When this option is selected, the list of all the audited guest check-outs is displayed. 

5. Use the down <▼> arrow to select the “Auth #” option.

Specify the Authorization number. All entries by keycards encoded using the specified Authorization will be displayed.

6. Use the down <▼> arrow to select the “From audit #” option.

Enter the starting entry in the audit. The default value is 1, which is the newest one.

7. Use the down <▼> arrow to select the “Audit quantity” option.

8. Enter the maximum number of entries in the audit that are to be shown up to a maimum of 4000 (if that many are available in memory). Only the most recent entry will be displayed, up to the specified number of entries. If an audit appears more than once, then the last entry is the most recent.

Depending on the media that will receive the result of the audit, the following steps differ. The 3 following sections describes the particularity of the audit sent to the FDU screen, to a line printer or to a USB memory stick.

FDU Audit sent to the FDU screen

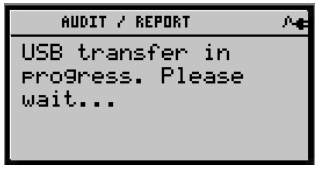
Press <↵> to start the audit report. When viewing the audit on the FDU screen, use the <▲> and <▼> keys to scroll through the list of entries.

FDU Audit sent to the printer

Connect a serial line printer to the FDU serial port, or a USB line printer to the USB port. Press <↵> to start the audit report. The result of the audit is sent to the line printer.

FDU Audit sent to a USB memory stick.

Connect a USB memory stick to the FDU USB port. Press <↵> to start the audit transfer to the USB stick.



When the transfer is completed, a message is displayed to the user.

When the transfer is done, from this moment, the USB stick may be removed and plugged in the PC.

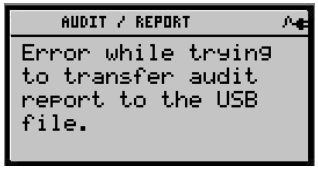
Most modern operating systems will automatically detect the USB stick and show its contents upon detection. The file containing the lock audit is called LockAudit.log and is created in the main directory on the USB so they are easy to find. This file is formatted in tab-separated columns compatible for import by standard spreadsheet software, which can be used to format, sort, analyse or print the audit information. To simply look at or print the file, a regular text editor may also be used.

IMPORTANT: **If another audit transfer is performed on the same USB stick, the new files created will overwrite the previous one. For this reason, it is suggested to immediately copy the audit files onto the PC to save them.**

Use separate directories, or rename audit files once transferred to a PC, to maintain a historical record of audits.

Note that if there is not enough space available on the USB stick, this operation will fail and an error message will be displayed on the screen. The majority of existing USB memory sticks will work with the FDU. If the USB stick is not compatible with the FDU, it will not be detected and the FDU will not display any error message to the user. Another type of USB memory stick should then be used. Additionally, if the USB stick is not formatted, the FDU will detect it but will not be able to access it further and will display an error message. If this occurs, format the USB memory stick on a PC, as per the manufacturer's requirements or contact Kaba Ilco for assistance

If ever there is no USB stick plugged in the FDU, or the FDU does not recognize the USB memory stick plugged in, the following message will be displayed:



Chapter 8: Interfaces

8.1 PMS Interface

In PMS mode, the Property Management System feeds information on the guest's keycard requirements directly to the FDU. For information on configuring the PMS interface, please consult the PMS installer. The PMS should be connected to the FDU using Serial Port A.

Data	Comments
Guest Name	*If supported by the PMS software.* The guest name is especially useful when an FDU is shared by more than one PMS terminal, avoiding any confusion as to which keycard is being encoded.
Room Number	Including all necessary doors for Adjoining Suites or Common Door Suites*, if supported.*
New or Duplicate	
Check out Date and Time	
Guest Common Areas	*If supported by the PMS software and also if enabled in the FDU features.*
Salesman's Lockout	*If supported by the PMS software and also if enabled in the FDU features.*
Folio Number	If supported by the PMS software and also if enabled in the FDU features.
Number of Keycards	
Authorization Number	*If supported by the PMS software.* When available, the Authorization Keycard is not required to encode Guest Keycards.

Table 8.1: *Information provided by the PMS to the FDU for encoding Guest keycards*

The operator first uses the PMS to register the guest. By using the PMS, the operator is assured that the rooms requested are available, and is able to make use of all the functions such as billing and record keeping that are part of the PMS.

When all information is entered in the PMS, the operator simply swipes their Authorization keycard in the FDU, and follows the instructions on the screen to make the

requested number of keycards. There is no data entry on the FDU keypad in PMS mode, which prevents human error and saves time.

Only Guest level keycards can be made in PMS mode. Functions available will vary with the PMS system in use by the property. Options may include checking-in a guest, checking out a guest, and assigning/reading folio numbers. For security reasons, every operation is audited by the FDU, except for reading folio numbers.

NOTE: The FDU will not accept information from the PMS if it does not match the features selected for the FDU. For example, in order to assign a folio number through the PMS, folio numbers must be enabled in the FDU Features Menu.

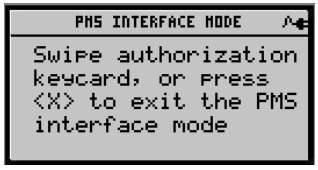
8.1.1 Entering and Exiting the PMS Interface

When the FDU is in Manual Mode, the welcome screen that is displayed when a key is pressed is:

To enter PMS Mode:

1. Swipe a keycard or PIN with a Front Desk Authorization level. If using an FDA keycard or PIN press <⌫> after entering the FDU.

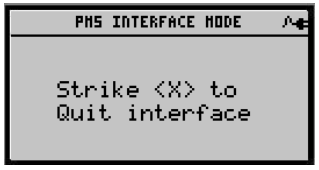
2. Press 3 or use the down <▼> arrow followed by <↵> to reach the “PMS mode” menu.



The FDU is now in PMS mode, and will accept data from the property's PMS software.

Giving an Authorization while in PMS Interface Mode:

Before a keycard can be encoded, a Front Desk Authorization keycard or higher must be swiped or a associated PIN value entered, unless the PMS sends the Authorization Number (the Authorization can be given before or after sending data to the FDU from the PMS, but must be given before blank keycards can be encoded.). ***When an Authorization keycard has been swiped or a valid PIN entered, the welcome screen will change to the following:***



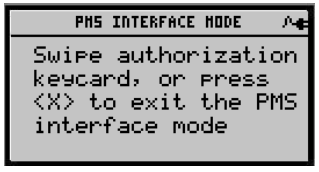
This screen indicates that the last authorization swiped or PIN entered is still valid. The authorization can be cancelled by logging off, or by waiting for the time out period to expire.

NOTE: Do not leave the FDU unattended while the authorization is still valid, as the FDU can be used to make keycards by the next operator logged onto the PMS station. Always logoff and ensure the next operator uses their authorization level to access the system in PMS mode.

Logging off the Current Authorization without Exiting from the PMS Interface:

1. Press <⌫>.

2. Enter 2 to log off the current authorization without exiting the PMS interface.



The FDU is still communicating with the PMS and is waiting for a valid Authorization before keycards can be encoded.

Returning to Manual Mode:

If other operations arte needed to be performed, such as making Reset keycards, or if the PMS link is not functioning, the follow steps are to be followed:

1. Press <⌫>.

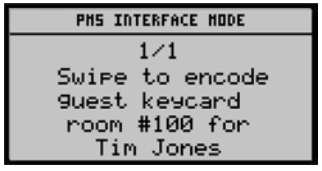
2. Enter 1 to log off and exit the PMS interface.

8.1.2 Making Guest Keycards Using the PMS Interface

Minimum keycard required: Front Desk Authorization

Steps to encode keycards using information from the PMS:

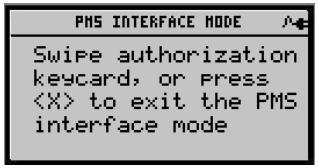
1. Complete the guest's registration using the PMS. The PMS will transmit the data to the FDU for making keycards.



2. Swipe a blank keycard through the encoder.

The FDU will prompt the insertion of blank keycards until the number of keycards requested using the PMS has been encoded.

If a keycard is never swiped, once the PMS delay specified in *Section 3.9 part 9 – FDU Time-outs* has expired, the following message will appear:



To complete the registration, an authorization keycard or valid PIN will have to be used, and the previous steps redone using the PMS in order to create the guest's keycard in PMS mode.

8.2 POS Interface

As described in *Section 2.8 – Interfaces*, the POS interface is a special model of the FDU using a triple track encoder, which writes ABA standard (open-architecture) information on track 2 of the magnetic stripe keycard, and uses the remaining tracks for the encrypted keycard code needed by the system.

The ABA track 2 information is compatible with existing point-of-sale readers. Some properties make use of the folio number to post charges to the guest's account, but any numeric data that can be sent to the FDU by the PMS can be used, or a numeric code can be entered manually. Call Kaba Ilco for assistance to configure the PMS and the FDU to encode the information required by the property on track 2.

Chapter 9: Security Procedures

9.1 Basic Keycard Security

9.1.1 Inform Guests and Staff of How to Handle Keycards

Keycards must be treated as carefully as keys. They should never be lent or left unattended. The loss or theft of a keycard must be reported immediately.

Guests must insert their keycard in all of the doors leading to their room or suite, as soon as they check-in. If multiple identical keycards are issued, only one needs to be inserted in the locks. In case of a removed access to a guest room, the Reset or Lockout keycard must be inserted in all the locks leading to the room or suite.

Keycards can be erased by strong magnetic fields, and should be handled with the same precautions as a credit card.

9.1.2 Do Not Write the Room Number on the Keycard

Like mechanical keys, keycards are often lost or may occasionally be stolen. If a Guest keycard is marked "Room 100" for the convenience of the guest, anyone finding that keycard will know which room it unlocks. ***Guestroom numbers should be recorded on the check-in folder or elsewhere, but NEVER on the keycard. Staff keycards may be marked with a sequence id, as this does not identify the rooms to which the keycards have access.***

9.1.3 Make the Lock and FDU Audit Trail Public Knowledge

The power of the lock audit trail is in its ability to deter inappropriate access to rooms. By informing staff that detailed records exist of every access to any Kaba Ilco lock or RAC, and that all FDU transactions are logged and permit management to track the use of any keycard will maximize the deterrent power of the system.

9.2 Encoding, Issuing and Replacing Keycards

9.2.1 Invalidate Lost Keycards Immediately

With the mechanical key system, staff may have been reluctant to report lost keys because of the expense of re-keying. ***Staff should be encouraged to report any missing keycard*** since re-keying with the system is very inexpensive. As with mechanical keys, not reporting lost keycards could result in unauthorized access and much greater expense.

Any Entry keycard can be invalidated by encoding a new one, or by encoding a Reset keycard and inserting either one in ALL affected locks. Reset keycards do not give access to the room and are intended for use by staff to invalidate a key-card without being able to enter the room. If a Reset keycard is used, it should be made before the new keycard; otherwise, the Reset keycard will advance the lock beyond the new keycard's creation time, and the new keycard will not function.

Guests should be made aware that lost keycards must be immediately reported. Guests may occasionally report lost keycards as they leave to go to the theatre or to important meetings. The re-keying of the guestroom should not wait for the guest's return. Either the guest with their new keycard or a staff member with a Reset keycard should go to the room as soon as possible and update the lock with the new keycard.

The same security consideration should be given to lost Authorization keycards. The lost Authorization keycard must be invalidated on all Front Desk Units. Simply make a new Authorization keycard of the same number (1-200) and pass it through the reader of each of the FDUs on the property. The old Authorization keycard of the same number is then invalidated without affecting the other Authorizations.

9.2.2 Log the Encoding and Issuing of Every Staff Keycard

The lock and FDU audit trail feature of the system is only useful if keycards issued to staff (Authorization, Sub-Master, Master, Emergency, Passage and Restricted Area) are properly accounted for. It is of no value to know that a Section 6 keycard with ID # 101561 entered Room 601 at 3:41 if there is no record of who legitimately carries that keycard.

Whenever a staff keycard is issued (signed out to an employee) it must be logged with the sequence id with which it was encoded, the name of the person accepting the keycard, their signature, and the date and time of its acceptance. (The sequence id is obtained from the encoding transaction.) When the keycard is returned, the log sheet should be signed again and the time of return entered. A Staff Keycard Issuing Log is provided in Appendix C for this purpose.

It should be made clear to all staff members that each person's keycard is their responsibility between the issue and return of the keycard. When a Sub-master (Section, Floor, Group, Zone or Area) keycard is returned, it should also be verified on the Front Desk Unit using the readback function to provide an audit of the time at which the card was returned. Auditing the card on the Front Desk Unit does not invalidate the keycard. By following all of these instructions, if anyone makes unauthorized use of their keycard, loses it and does not report it, or fails to return it, they can be held accountable.

NOTE: The printed record of keycard encoding and the Keycard Issuing Log (form provided in Appendix C) have been designed specifically to help maintain a secure and reliable system. It is strongly encouraged to be vigilant in their use.

9.2.3 Safe Storage of Staff Keycards (when not in use)

For the highest possible security, it is common practice to ensure that valid Staff keycards do not leave the premises. This can be accomplished either by encoding new Sub-master keycards each day, with an expiry time of one night, or by storing the keycards between shifts.

Storing valid keycards is perfectly acceptable as long as the returned keycards are properly secured when not in use. For reissuing the same keycard each day, it is helpful to make keycards identifiable. Keycards with embossed sequence ids are available from Kaba Ilco. This sequence id also provides the ability to check that the key-card issued is the same as the one being returned, without using the readback function.

9.2.4 Keycards that are Used Infrequently

All keycards that are used infrequently should be accounted for regularly. In general, it is good security policy to issue keycards only to those who have a need for them. It is a common error to issue high level Master Entry keycards or Authorization keycards to senior staff members that they rarely use. Keycards rarely used are rarely accounted for. Consequently, a keycard may be missing for some time before its loss is noticed.

Keycards should be issued on the basis of their projected use. All valid keycards should be kept in a secure location when not in use.

9.2.5 Access to Keycards

Keycards should be restricted to those who require them, and each person should be issued the lowest level keycard that they require. However, the system offers enough security to allow even relatively junior staff a high level key-card. For example, if a valet has duties which require entry into rooms in three different groups, it makes much more sense to issue an Area or Zone keycard, or even a Bellman's Master, than it does to issue several Group keycards.

9.2.6 Access to Emergency Keycards

In general, the Emergency keycard should be available but not in circulation. With the exception of its ability to override the deadbolt/privacy lock, and the other lockouts, its functions are the same as those of the Grand Master keycard.

Some properties do prefer that their security officers carry the Emergency keycard in the event that they must urgently enter a double-locked room. However, security officers carrying the Emergency keycard should be careful when opening doors routinely. They should check the indicator light that shows a guest does not want to be disturbed.

9.2.7 Choose the Appropriate Time-outs for the FDUs

This is the time after each transaction during which the FDU remains authorized to make more keycards. A time-out from zero to twenty minutes may be selected.

Front Desk Units that are shared by several operators should have a time-out of zero. Otherwise, the FDU remains open for long intervals during which time several individuals are making keycards, but all keycards carry the Authorization number of one person. A zero time-out should also be set if operators must leave their stations frequently during the check-in process.

The FDU time-out is a convenience and it should not be allowed to diminish the security of the system. If operators are leaving Front Desk Units unattended in the authorized state, the time-outs should be set to zero. If it becomes necessary to encode a large number of keycards in succession, the time-out can be temporarily increased using a General Manager Authorization, and then reset to zero for normal operation.

NOTE: A user can return the FDU to the unauthorized state by pressing <⌫> repeatedly, until the FDU display reads "KABA".

Don't forget to set the timeout for PMS Interface Mode, in addition to the "Between Keycards" and "Between Keystrokes" timeouts *(see section 3.6 part 9 – FDU Time-outs)*.

9.2.8 Handle Returned Keycards Appropriately

If a guest returns one copy of a keycard for which they still hold other valid copies, re-encode the keycard as a Battery Test keycard in order to erase the information it contains. Returned Staff keycards should be signed in and kept in a secure location. By reading the Staff Keycard an audit record of returned Staff keycards can be generated.

Destroy keycards that are discarded due to wear and tear by cutting them into pieces. Damaged or worn keycards may still work intermittently in the lock until they expire or are cancelled by a more recent New keycard or a Reset keycard. Destroying the worn keycard prevents illicit use, and even prevents unauthorized persons from posing as guests or staff in possession of a keycard.

9.3 General Safety and Security

9.3.1 General Manager Authorization and Emergency Keycard Availability

Have a valid General Manager Authorization and a valid Emergency keycard available at all times.

The Emergency keycard is the fastest means to open a deadbolted room and any other door in an emergency, with another option being the mechanical override. An Emergency keycard should always be available to authorized personnel.

A Master Authorization keycard is sufficient to make an Emergency Reset keycard to invalidate a lost or stolen Emergency keycard. However, since only the General Manager Authorization (GMA) keycard can replace an Emergency keycard, there must always be a GMA keycard available to authorized personnel.

The GMA keycard is also the only keycard that can invalidate a lost or stolen GMA keycard, by encoding a new GMA keycard with the same number as the missing keycard, and swiping it in all FDUs on the property.

Two spare GMA keycards with different Authorization numbers from any other GMA on the property should be kept in a safe for use in emergencies, such as the need to perform a Hotel Restart, to audit the FDU, or to set FDU features.

9.3.2 The Mechanical Override Option

Some people view a key override as a poor feature for a keycard access control system. Why should the system allow a mechanical key to override the need for a keycard? Some users prefer an override option in the event of damaged or failed electronics.

Locks have an optional high-security removable-core cylinder override for the following reasons:

- Access is assured even if the electronics do not work.
- The override is virtually pickproof.
- Access can be tightly restricted (key blanks are factory restricted).
- Even the use of the override key is audited in the lock.
- In the unlikely event of a lost key, cylinders can be removed and re-pinned.

Some security and safety precautions should be taken with the mechanical override:

- The override key should not circulate. It should always be available, with a signature, to an authorized person on each shift for use in an emergency. After use, the override key must be secured again.
- All override keys, the cylinder change key, and the cylinders should be strictly controlled. Kaba Ilco keeps a small stock of spare keys and cylinders so it is not necessary for the property to keep any spares which could be stolen or misused. The cylinder of a defective lock removed from a door should be removed and installed immediately in the replacement lock. Any spare cylinder should be well secured.
- Report any loss of keys or cylinders to Kaba Ilco.
- Do not install any lock without the cylinder in place.

9.3.3 The Front Desk Unit Audit

The Front Desk Unit audit capacity is a complement to the audit trail of the lock. The Front Desk Unit audit trail is not necessary for revealing who made a specific keycard; this information is in the lock and the Staff Keycard Issuing Log. The Front Desk Unit audit provides an additional check on abuse of the system. For example, if unauthorized entry to a room is detected, the individual who encoded the offending keycard can be identified, and the FDU audit can be used to determine if other inappropriate use was made of the FDU.

NOTE: It is important to keep the Staff Keycard Issuing Log up to date (form provided in Appendix C).

Chapter 10: Emergency Procedures

This chapter describes situations that require prompt action by staff to ensure the safety and/or security of guests. A good understanding of the System is necessary to ensure a proper response, and all staff should know which managers to contact in an emergency to deal with access control matters. The Emergency keycard, spare batteries, override keys for locks equipped with a mechanical override, the tools necessary to uncover the override, and spare replacement locks should be kept in a secure location that is nonetheless instantly accessible to authorized persons in an emergency. For properties with the E-760, 770, and 710-II locks, the lock to FDU communication cable is needed to activate the electronic override *(see Section 5.7.2 – The Electronic Override)*.

This chapter also deals with certain situations that are not emergencies, in order to avoid unnecessary concern, and to give the correct response to the situation.

10.1 If a lock will not open

If the batteries are dead, the red and green LED indicators will flash together when a Battery Test or Staff sub-master (Section, Floor, Group, Zone or Area) keycard is inserted in the lock. The lock batteries must be replaced, and the lock time reset using the FDU. If the batteries are on the inside of the door, the electrical or mechanical override must be used first to enter the room *(see Section 5.7 – The Emergency Override)*. On a Generation E-760 series or 770 series lock, replace the batteries on the outside of the door, reset the lock time, and then open the door normally with any valid keycard (Guest or Staff). Battery replacement procedures are described in *Section 11.4 – Replacing a Battery*.

If the deadbolt is thrown, or if the door has been locked out with the Hotel Lockout keycard, Room Lockout keycard, or the Salesman's Lockout feature, consult management before opening the door. Use the Emergency keycard for authorized emergency access, which will be recorded in the lock audit.

If there is an electrical or mechanical failure, activate the override *(see Section 5.7 – The Emergency Override)*. Override use is recorded in the audit. Call for service on the defective lock from the local Kaba Ilco dealer**. DO NOT provide guests with the mechanical override key.** Remove the mechanical override cylinder before shipping a lock for repair. Once a new or repaired lock is installed, reset the addresses from a nearby lock *(see Section 5.4 – Resetting Lock Addresses)*.

10.2 If a guest has lost his keycard on property

Issue a NEW keycard (NOT a duplicate) to the guest, and instruct them to immediately insert it in all the guest room locks to which they have access, including all doors of a

Common Door Suite, Adjoining Suite, or Convention Suite. If a guest or their party had more than one copy of the lost keycard, all of the keycards must be replaced with duplicates of the new keycard, which can all be made together, or as each guest returns their cancelled keycard, by using the duplicate keycard option. The guest need not insert their new keycard in common area doors such as entrances, pool, etc.

10.3 If a guest has lost their keycard and is absent from the property

The room must be protected from unauthorized entry until the guest returns. A new Guest keycard should therefore NOT be issued right away. Instead, ***a Group Lockout or Guest Reset keycard should be inserted in the lock to cancel any circulating guest keycard.*** A new keycard can be issued to the guest when they return.

10.4 If a Pre-registered keycard is lost or stolen before the guest arrives

Make a Pre-registered Reset keycard and insert it in the affected locks to prevent the missing keycard from becoming valid. Make a new Pre-registered keycard or wait for the guest to arrive, and issue them a new Guest level keycard.

If a Pre-registered keycard is no longer needed and was never given to a guest, simply re-encode it to serve as another guest's keycard.

10.5 If a Staff level Entry keycard is lost or stolen

These keycards include all Sub-Master (Section, Floor, Group, Zone, Area), Master (Bellman's Master, Grand Master), Emergency and Passage keycards. ***Cancel the missing keycard by issuing the appropriate Reset keycard or a new keycard (for Sub-Master levels only), and inserting it immediately in all affected locks.*** Re-encode the keycards of other employees affected by this change as duplicates of the new card, or issue them duplicate keycards and collect the cancelled keycards. Remember to print the FDU transactions when issuing staff keycards and record the changes in the Keycard Issuing Log for the analysis of any future lock audit.

NOTE: The Bellman's Master, Grand Master and Emergency keycards are always duplicates, so a new Reset keycard must be used in all locks on the property to cancel any of these three keycards.

10.6 If an Authorization keycard is lost or stolen

Issue a new Authorization keycard for the same authorization number, and swipe it immediately in ALL the FDUs in the property, including the FDU used to encode it. If the Authorization keycard had a PIN assigned, the PIN access will be revoked.

10.7 If an employee leaves or is fired

All authorizations, access keycards and PINs for the employee must be revoked. If their keycards have been returned, they can be signed out to a new employee. If the employee had a PIN assigned, this PIN must be revoked. If the keycards were not returned or have been copied, follow the procedures described above for lost or stolen Staff keycards and Authorization keycards.

10.8 If the hotel Code becomes known (i.e. security is compromised).

The property must be restarted with a new Hotel Code. Follow the instructions in S*ection 3.5.9 – Hotel Restart* of this manual, or contact Kaba Ilco for assistance. All locks, RACs and FDUs must be reprogrammed with the new Hotel Code using a Hotel Restart keycard.

10.9 If an FDU is stolen

Immediately make an FDU Cancel keycard for the missing FDU, then swipe it through all the other FDUs in the property AND through every lock in the property. This procedure will prevent any keycard made by the missing FDU from opening a door or from authorizing the use of another FDU to make keycards or change settings. Issue new keycards to guests and staff whose keycards were issued by the missing FDU, to restore their access privileges and authorizations.

When a replacement FDU is obtained, transfer the settings from another FDU to the new FDU. See section 3.5.4 – Transferring Data to Another FDU.

As soon as possible, within 24 hours of FDU Cancel, perform a Hotel Restart with a new Hotel Code, for complete security (see Section 3.5.9 – Hotel Restart). Contact Kaba Ilco for assistance.

10.10 If a crime occurs in a room

Immediately lock out the room using a Room Lockout or Hotel Lockout keycard. Download and print the audit trail from the lock and the FDU used to encode any suspect keycard, to provide evidence for any investigation.

10.11 If an override key is lost or stolen

Replace the cylinders of all the mechanical overrides that open with the lost key immediately.

Chapter 11: Maintenance and Troubleshooting

It is common for new users to have trouble in the first days after installation associated with misunderstanding some aspect of the system. Whatever the problem, Kaba Ilco is anxious to help. To make the implementation of the Kaba Ilco Lodging Access Control System as complete and trouble-free as possible, Kaba provides on-site installation supervision, staff training, and a 24-hour telephone line for any questions (see Chapter 12 – Service).

11.1 Preventative Maintenance

11.1.1 Battery Testing and Replacement

Regular testing of the batteries in all locks is probably the most important regular maintenance task, since replacing a battery before it fails avoids the need to use the override to open the door. Have staff check the indicator lights routinely when they insert their sub-master (Section, Floor, Group, Zone, Area) keycard or routinely use a Battery Test keycard *(see Section 4.10 part D.1. – Battery Test)*. If the red and green indicators flash together, the battery is low and should be replaced promptly. Instructions for battery replacement are in *Section 11.4 – Replacing a Battery*.

Note that when doing a lock audit *(see Section 7.1 – Auditing a Lock)* of a Generation E-760 or 770 lock the battery level will also be indicated at the start of the audit.

Battery Level Features:

The batteries in a lock have varying levels of operation to ensure that there is sufficient warning before preventing complete access. In fail mode (one short flash of red led every 4 seconds), only the Emergency keycard can be used to unlock the door. At this point it is critical that the batteries are changed.

Level of Batteries	
Normal operating voltage:	4.0V - 6.2V
Low Batteries:	4V
Fail mode (inhibit):	3.6V
Halt Mode:	Between 3.0 and 3.5V

11.1.2 Kaba Ilco Electronic Locks

Kaba Ilco locks require very little preventative maintenance. Each lock should be cleaned once a month by simply inserting and withdrawing a cleaning card several times in each lock. If the locks are exposed to high levels of dust or salt, they should be cleaned more often. The reader is vertically mounted and is designed with an open track for the specific purpose of being dirt resistant. Cleaning cards are commercially available or may be purchased from www.keycard.com.

The lock housing should be cleaned and polished every two months with a clean dry rag in normal environments. Harsh environments may require weekly cleaning. Do not use harsh cleaners or abrasives, as they will damage the finish.

Locks mounted on exterior doors should be treated, and then maintained regularly, with a wax based product to prevent corrosion from the elements. Some of our customers have used LPS3 Heavy Duty Rust Inhibitor, manufactured by LPS Laboratories Inc., Tucker, Georgia, 1-800-241-8334. Another effective protectant is Satin Chrome Turtle Wax. Please contact a local cleaning products supplier for other appropriate products to use.

11.1.3 The Locking Mechanism

The locking mechanism (mortise or cylindrical) may require occasional maintenance. These devices are similar to those used in standard key locks and require the same periodic attention.

Mortise locks should be inspected occasionally to ensure that the retraction is still adequate (the latch can be drawn into the door completely) from both the inside and outside. The mortise should also be checked to ensure that the deadbolt can be easily thrown and retracted, and to ensure that the dead latch is functioning (the latch is deadlocked when the auxiliary latch is depressed.

It is also important that the doors themselves be inspected to ensure that the door-to-frame alignment is correct and is allowing the latch bolt to engage in the strike. At the same time, the gap between the door and the frame should be small enough to allow the strike to depress the auxiliary latch.

A leading cause of mortise lock failure is the habit of using the deadbolt to keep the door ajar. Often the door is allowed to slam against the deadbolt which damages the mortise and the frame.

Make sure that the cylindrical lock functions properly. Check the dead latching, the privacy lockout, and the fit of the door.

11.1.4 The Override Cylinder

All override cylinders should be tested every month, especially in humid environments, to ensure emergency access is possible when required.

11.1.5 The Front Desk Unit

The read and write heads of the FDU magnetic stripe encoder must be kept clean to ensure reliable reading and encoding of keycards. The encoder(s) should be cleaned once a week for small hotels and once a day for higher volume hotels using the same type of cleaning cards used to clean the locks.

There are no moving parts to be serviced in the FDU and it should never be disassembled or opened.

After several years, the FDU battery pack may no longer be able to accept a charge and the battery pack will have to be replaced. Contact Kaba Ilco for part number and replacement instructions.

11.1.6 Synchronizing the Front Desk Units

Because the FDU is a stand-alone system, each FDU maintains its own internal time, feature settings and valid authorization information. All the FDUs in the property should be synchronized twice a year, by selecting any FDU, and using it to transfer data to each of the other FDUs. This procedure, described in *Section 3.5.4 – Transferring Data to Another FDU*, will ensure that all keycards encoded by any FDU on the property function well together, and that all FDUs accept the same Authorization keycards and have the same default expiries, etc.

11.2 Troubleshooting

Having read the sections of this manual relating to the information encoded on the keycard, how keycards are cancelled, how the levels and addresses work, when keycards expire, etc., a good knowledge is gained of the logical processes occurring inside the locks and the FDU. This knowledge allows the user to understand any reported problems with the system and determine the cause and solution.

11.2.1 Synchronizing the Front Desk Units

When troubleshooting, first determine whether the problem is caused by the equipment, or by the way it is being used. If a lock does not recognize a specific keycard, but it recognizes other keycards, the problem is probably in the keycard or its encoding. If no keycard is acceptable, then it is probably a lock problem, such as a dead battery or improper programming.

11.2.2 Operating Problems

1

Problem:

1) The lock does not respond to the keycard.

Possible causes:

- Keycard is not properly encoded.
- Keycard is encoded for the wrong room/section/group, etc.
- Keycard has been cancelled by a newer keycard or has expired.
- Keycard has been cancelled by the Group Lockout.
- Keycard has been cancelled by a Reset keycard.
- Keycard valid for different time zone.

Solutions:

- It is quite common to make errors in encoding, such as assigning the wrong room number. It may also be possible that the keycards have not been properly encoded but the operator has not noticed the warning from the FDU. In most cases, a new keycard will work in the lock.
- If the problem persists, the addresses in the lock should be verified using the Reset Addresses function.
- In the days following installation, it is common to have problems with staff keycards. If the staff keycards appear to be denied access to certain rooms for no reason, new keycards may have been issued instead of duplicates or original copies of the New keycard made in a single transaction of the FDU. In this case, each new keycard cancels the existing keycards in all the locks in which it is used, creating what appears to be a random pattern of malfunctions. The solution is to reset the rooms in that address (Section/Group/etc.) and issue a new keycard. Subsequent keycards to other individuals should be encoded as duplicates.

2

Problem:

2) The lock displays a red light in response to the keycard.

Possible causes:

- The deadbolt has been thrown from the inside.
- The Hotel, Room or Salesman's Lockout has been used.

Solutions:

- Before removing a Room or Hotel Lockout, it is advisable to check with security to see what the purpose of the lockout was. The room may have been locked out

to secure valuables or to protect evidence of a crime. In any case, a General Manager Authorization keycard is required to make the Unlock keycard to remove the lockout. An Emergency keycard can override the deadbolt without removing the lockout.

3

Problem:

3) The keycard works intermittently in the same lock.

Possible causes:

- The reader head needs to be cleaned.
- The FDU encoder head needs to be cleaned.

Solutions:

- Clean the reader head using a standard head-cleaning card.

4

Problem:

4) The keycard works intermittently in different locks.

Possible causes:

- The keycard is worn out, defective or improperly encoded.

Solutions:

- Re-encode the keycard. If this does not solve the problem, discard the keycard and use a new one.

5

Problem:

5) Keycards expire before the guest checkout date.

Possible causes:

- The Group lockout is being used on occupied rooms.
- The Guest expiry date is being improperly set.

Solutions:

- Check with Housekeeping to see that users of the Group Lockout understand its function.
- Check the expiry default; it may be set for a short expiry that the front desk staff is selecting automatically.
- Issue a new keycard to the guest.

6

Problem:

6) The lock flashes both a red and a green light when a staff keycard is used.

Possible causes:

- The batteries are getting low.

Solutions:

- Change the batteries. Follow the instructions in *Section 11.4 – Replacing a Bettery*.

7

Problem:

7) The lock cannot communicate with the Front Desk Unit.

Possible causes:

- A Programming keycard has not been inserted into the lock prior to the insertion of the infrared communication adapter.
- 30 seconds have elapsed since the Programming keycard was inserted in the lock.

Solutions:

- In the case of a battery change, insert the Initialization keycard, then the Programming keycard, followed by the infrared communication adapter.
- The FDU/lock communication must be started within 30 seconds of inserting the Programming keycard in the lock.

8

Problem:

8) The Front Desk Unit does not accept an Authorization keycard.

Possible causes:

- If no Authorization keycards are accepted, the magnetic heads of the FDU may be dirty.
- The Authorization keycard may have been cancelled.

Solutions:

- Use a cleaning card to clean the heads of the FDU. Issue a new Authorization keycard of the same number as the cancelled one. Ensure that this Authorization keycard is passed through each FDU so that the previous one is cancelled.

9

Problem:

9) The Front Desk Unit is not encoding well; it takes more than one pass to encode the keycard.

Possible causes:

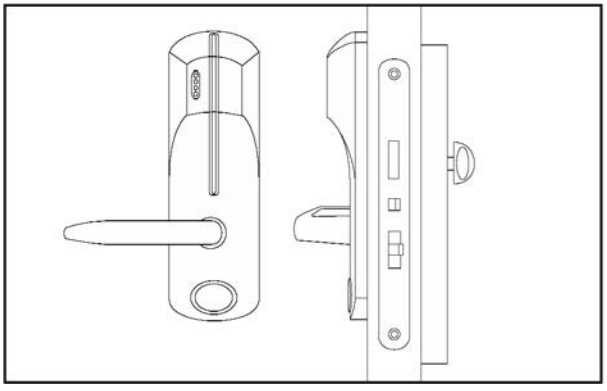
- The heads of the FDU encoder are dirty.

Solutions:

- Use a cleaning card to clean the heads.

11.2.3 Malfunction Problems

If none of the above operational solutions are effective, the lock may have failed mechanically. If a lock requires replacement, have an authorized person remove the security override cylinder (if the lock has the mechanical key override option), and replace it in the new lock. An override cylinder removed from a lock should be carefully secured until it is replaced. A replacement lock or a lock from which the battery has been temporarily disconnected will need to be connected to the FDU in order to set the lock time and/or the lock addresses. To avoid shipping damage, please ensure that defective locks are properly packaged for return.



1

Problem:

1) After responding to keycards (flashing green light), the latch does not retract from the outside.

Possible causes:

- The mortise is malfunctioning.

Solutions:

- Open the door using the mechanical override and try to provoke the malfunction while the door is open. While the door is open, verify the movement of the latch by rotating the inside lever. If the latch is binding while rotating the inside lever, change the mortise.
- Open the door from the inside and verify that the latch is moving freely. If the malfunction does not persist when the door is open, and the latch moves freely, change the lock.
- If the malfunction does not persist when the door is open, then the strike needs to be filed. File the strike on the side of the latch that is rubbing. Refer to the installation instructions shipped with the lock for more details.

2

Problem:

2) Lock allows entry without reading cards.

Possible causes:

- The lock is in passage mode.
- The door and the frame are misaligned.
- The actuator is defective.

Solutions:

- Take the lock out of passage mode.
- Try opening the door without a keycard and without rotating the lever. Verify the latch and strike alignments. Make sure that the latch is entering the strike.
- If the latch does not enter the strike, check if the door bumper pad insulation or the door closers are impeding the full closing of the door; if not, it may be necessary to file the strike. Always file the strike plates the minimum amount required.
- If the latch does enter the strike properly and the door can still be opened without keycards, then change the lock.

3

Problem:

3) The latch is binding and not returning to the rest position.

Possible causes:

- The mortise face plate and the latch are misaligned.
- The mortise is improperly installed.

- The mortise is malfunctioning.

Solutions:

- Make sure that the latch is not rubbing against the mortise faceplate. Remove the plate and verify the latch movement.
- Verify the mortise bevel angle (see the lock installation instructions). If the latch moves freely when the plate is removed, replace the mortise face plate by using the thrown deadbolt as a guide. If the latch binds when the front plate is removed, try to readjust the mortise's bevel angle. If the mortise still binds, remove it from the door. If the latch binds when it is removed from the door, replace the mortise. If the latch does not bind while it is removed, then use a wood chisel to enlarge the cutout.

Problem:

4) The latch does not move freely.

Possible causes:

- The lock's anti-friction mechanism is broken.

Solutions:

- Depress the auxiliary latch (lowest of the three bolts or latches on the mortise). The latch bolt, including the anti-friction, should be dead latched. If not, the mechanism is broken. Change the mortise.

Problem:

5) There is an incomplete retraction of the latch bolt.

Possible causes:

- The mortise is malfunctioning.
- The stop plate is malfunctioning.

Solutions:

- Turn the inside and outside levers to test the retraction. The latch must not protrude from the mortise front plate. If the latch does not fully retract it may start to bind on the strike. Replace the mortise.
- If the retraction is still not full, replace the lock.

6

Problem:

6) Both the red and green indicators flash, then the red one flashes.

Possible causes:

- The lock battery is low.

Solutions:

- Use the mechanical override key to open the door. (On Generation E¬760 & 770 locks, the batteries are easily accessible on the outside of the door.) Change the batteries and reset the lock time, see *Section 11.4 – Replacing a Battery*.
- Avoid dead batteries by testing all locks periodically using the Battery Test keycard or a Staff Sub-master keycard.
- Disconnect the battery for 2 minutes, reconnect and reprogram the lock.

11.3 Frequently asked Questions

Over the last fifteen years, Kaba Ilco has been asked many questions by users. The most frequently asked questions and their responses are listed in this section. If the responses suggested here don't help, please see the rest of this section on Troubleshooting.

When replacing the batteries, do I have to reprogram the lock?
No, all that is required is to reset the time. See *Section 5.6 – Resetting Lock Time*.

How do I reset the time on a lock?
After inserting the initialization and programming keycards, attach the communication cable to the FDU and the lock. Reset the time from the programming menu using the Reset Lock Time function. See *Section 5.6 – Resetting Lock Time*.

How do I set Daylight Saving Time?
DO NOT change the internal time of the FDU after the installation of the FDU system. The internal time is used to keep the FDUs and the locks in time with each other, and is not related to the local time. The local time is the time displayed on the FDU screen when making keycards, choosing expiries, etc. In response to the change of seasons, simply change the local time forward 1 hour for Daylight Saving Time, or back one hour for Standard Time. The time displayed by the FDU when communicating with the user will thus be the correct local time. This requires a GMA keycard. See *Section 3.6 part 10 – Current Time*.

How do I synchronize two or more Front Desk Units?
Use the "Program another Front Desk Unit" function in the programming menu on the FDU. See *Section 3.5.4 – Transferring Data to Another FDU*.

Why isn't my lock responding to any keycards?
The keycard was not properly encoded, was not encoded for that lock, has been cancelled by a newer keycard, has expired or has been canceled by a Group Lockout or a Reset keycard. Alternatively, the lock time may not have been reset following a battery replacement *(see Section 5.6 – Resetting Lock Time)*, or the lock may be malfunctioning. See the foregoing section on Troubleshooting.

What are the time zones for?
The time zone feature allows keycards to be valid only during certain hours of the day. See *Sections 4.6.7.1 – Fixed Time Zones, 4.6.7.2 – Flexible Time Zones, and 5.5 – Remote Access Controller (RAC) Models 3.5, 4 & 4XT Flexible Time Zones*. Note that there are two types of time zones, Fixed time zones which apply to locks only, and Flexible time zones that apply only to RAC models 3.5, 4 & 4XT.

How do I transfer the addresses from the old lock or a lock on a nearby door, to a replacement lock that has just been installed?
After setting the lock time, use the "Reset Addresses" function in the programming menu on the FDU.

How do I invalidate a lost GMA keycard?
Make a new GMA keycard with the same authorization number and swipe it through all the Front Desk Units on the property, including the FDU used to encode the new keycard.

Why is the Front Desk Unit screen blank?
The contrast may be too low. See *Section 3.5.1 – Adjusting the Contrast and Volume*.

How long will the Front Desk Unit hold its charge in case of a power outage?
The battery pack will provide power for about 8 hours on 50% operating duty or 4 hours of constant use.

Why don't the keycards made by one of my Front Desk Units work in the locks, even though keycards made on another FDU work properly?
Try synchronizing the malfunctioning FDU with another FDU that is working properly. Transfer the settings from the working FDU to the malfunctioning FDU. See *Section 3.5.4 – Transferring Date to Another FDU*.

I just received a new FDU. How do I set it up to work with my existing system?
Charge the FDU overnight, and then transfer the settings from another FDU *(see Section 3.5.4 – Transferring Date to Another FDU)*. Use the GMA keycard attached to the new FDU to set it to receive data.

11.4 Replacing a Battery

The expected life of the battery pack depends on the use of the lock. Common Area locks, for instance, may require more frequent battery replacements than regular guestrooms. In any case, the same procedure is followed.

Only the time needs to be reset when the batteries are changed. The lock does NOT need to be reprogrammed. Any lock taken off battery power for more than a few seconds stops counting time and ceases to function even when the batteries are replaced. This is a precaution that forces maintenance staff to reset the time using the FDU to keep the two synchronized. The addresses do not have to be reprogrammed, since the Room, Sub-Master, and Master addresses remain saved in the lock.

Use a Master Authorization keycard to make Initialization and Programming key-cards. Replace the batteries. Insert the Initialization keycard and then the Programming keycard into the lock, and then connect the communication cable to the lock and the FDU. Reset the lock time as per section 5.6. The battery replacement is now complete.

NOTE: The Initialization keycard must be inserted prior to the Programming keycard.

11.5 Replacing a Lock

If it has been determined that the malfunction is caused by a defect in the lock, then the lock should be changed. During the installation of the system, a Kaba Ilco representative is available to train the maintenance staff in the proper procedures for removing and replacing locks. Keep the installation instructions shipped with the locks available for future reference.

If the locks have the mechanical override option, it is very important that the high-security cylinder be removed from the defective lock and placed in the new lock. (Replacement locks are not supplied with cylinders.)

Once the lock is changed it must be programmed to accept the valid keycards already in circulation for that room, using the Reset Addresses function. As discussed in section 5.4, the addresses can be taken from the defective lock or from one of the neighboring locks with the same addresses (except room number).

NOTE: When a new lock (i.e. a lock that has never been programmed for the property) is installed, the Initialization keycard must be inserted prior to the Programming keycard.

11.6 Replacing a Front Desk Unit

Since the keycard encoder has no moving parts, there is very little which can go wrong with a Front Desk Unit. In some cases, where a defect exists, it will be diagnosed by the FDU itself and reported on the display.

If an FDU is defective, it should be returned as soon as possible to Kaba Ilco, or to one of our representatives. Before returning the unit, perform a FDU audit on a printer or a USB drive. Refer to *Section 7.2 – Auditing the FDU* for details on FDU audit. No Authorization keycards should be returned with the machine.

Once a new Front Desk Unit arrives at the property, it can be connected to any of the other FDUs in the property in order to download the time, feature settings, and a list of currently valid Authorizations. Refer to *Section 3.5.4 – Transfering Data to Another FDU* for step-by-step instructions on data transfer between two FDUs.

NOTE: If the property has only a single FDU, inform Kaba Ilco when the unit is returned, so that the Authorization information can be transferred to the new FDU at the factory. Due to the possibility that an FDU may require occasional servicing, at least two FDUs are recommended.

The Backup Keycard Kit (Part # BK7911) is strongly recommended for hotels of up to 100 rooms with only 1 or 2 FDUs.

11.7 Warranty

The Kaba Ilco Lodging Access Control System is covered by a two-year replacement warranty. Please read the warranty documentation for coverage specifics. The warranty can be extended beyond the two years if desired. Under the warranty, defective equipment should be returned to Kaba Ilco for repair or replacement. In order to be repaired under warranty, the equipment must be returned with a completed RMA card which explains the reason for the return. The reason should be more specific than “not working”; as this will assist Kaba in finding the defect quickly and to return the equipment as fast as possible.

The warranty does not cover product deterioration and failure resulting from improper maintenance.

Chapter 12: Service

12.1 Technical Support Contact

Kaba Ilco maintains a 24-hour hotline with qualified technicians to assist with the operation of the system. If a problem cannot be resolved following the instructions in this manual, call one of the following numbers:

Toll-free: (800) 906-4526
Local calls: (514) 340-9025

12.2 Returning a Unit for Repair

Step 1: Obtain an RMA Number and Prepare an RMA Card.

A FDU or lock cannot be returned for repair unless an RMA (Return Materials Authorization) number is obtained from Kaba Ilco.

1. Call Kaba Ilco at (800) 906-4526 (toll free) or (514) 340-9025 (Montreal area local calls), and explain the problem to the service technician. If the service technician is unable to assist in resolving the problem and the unit must be returned to Kaba the technician will issue an RMA number.
2. Write the RMA number in the appropriate box on the RMA card.
3. Fill in the problem section on the RMA card with the assistance of the service technician.
4. Remove the protective backing from the RMA card and stick the card to the top of the box.
5. Fill in the return address on the RMA card.

Step 2: Pack the Unit Properly

1. Pack the unit in a factory-supplied box.
2. Pack only one unit per box.
3. Pack the unit so that it does not move around in the box during transit.
4. If a lock with the mechanical override option is being returned, make sure to remove the override cylinder so that it can be used in the replacement lock. Replacement locks ship without override cylinders.

Step 3: Ship the Unit to the Correct Address

There is a shipping address on the RMA card. Confirm that the unit is shipped to the right address.

If shipping from outside Canada, the declaration on the shipping documents must include:

- Quantity
- Full description
- Unit price
- Total value
- The statement "Canadian Returned Goods."

Shipping from Canada:
Ship to:

Kaba Ilco Inc.
7301 Decarie Blvd.
Montreal, Quebec
H4P 2G7

Shipping from the USA:
Ship to:

Precision Telecom & Security (PTS)
6805 Crosstimbers Dr.
Corpus Christi, TX
78431

OR

Kaba Ilco Inc.
c/o Fritz Starber Inc. 25 Railroad Ave.
Highway 114 East Norton, VT
05907

Returning by air or by sea from anywhere outside the USA or Canada:
Ship to:

Kaba Ilco Inc.
7301 Decarie Blvd.
Montreal, Quebec
H4P 2G7

OR, for repairs to model 700 locks only,

Precision Telecom & Security (PTS)
6805 Crosstimbers Dr.
Corpus Christi, TX
78431

Appendices

Appendix A: Keycard Quick Reference Guide

		Reset Keycard Available	Maximum Addresses	Minimum Authorization Required	Selectable Expiry	Factory Default Expiry	Variable Expiry	Guest Common Areas	Salesman's Lockout	Staff Common Areas	Time Zone On Keycard	Menus Navigation & Options
Guest Level Access												
1	Guest	Yes	16,000	FDA	1 hr to 2730 nights	1 night	Yes	8	Yes	-		FDA/1/1/Room#...
2	One-Shot	Yes	16,000	FDA	1 hr to 4 hrs	1 hr	No	-	No	-		FDA/1/2/Room#... For Guest Rooms only
3	Adjoining Suite	Yes	16,000	FDA	1 hr to 2730 nights	1 night	Yes	8	Yes	-		FDA/1/3/Starting Room#...
4	Common Door Suite	Yes	1,000	FDA	1 hr to 2730 nights	1 night	Yes	8	Yes	-		FDA/1/4/Suite#...
5	Convention Suite	Yes	1,000	FDA	1 hr to 2730 nights	1 night	Yes	8	Yes	-		FDA/1/5/Convention Suite#...
6	Pre-registered	Yes	16,000	FDA	1 hr to 2730 nights	1 night	Yes	8	Yes	-		FDA/1/6/Guest or Adj. or Comm. Door...
Rest. Area Level Access												
7	Restricted Area	Yes	200	GMA	1 night to 2730 nights	1 night	No	-	No	-		GMA/1/7/#...
Sub-Master Level Access												
8	Section	Yes	255	MA	1 night to 2730 nights	365 nights	-	***	**	16	6	MA/1/8/Section#...
9	Floor	Yes	255	MA	1 night to 2730 nights	365 nights	-	***	**	16	6	MA/1/9/Floor#...
10	Group	Yes	255	MA	1 night to 2730 nights	365 nights	-	***	**	16	6	MA/1/10/Group#...
11	Zone	Yes	255	MA	1 night to 2730 nights	365 nights	-	***	**	16	6	MA/1/1 1/Zone# ...
12	Area	Yes	255	MA	1 night to 2730 nights	365 nights	-	***	**	16	6	MA/1/12/Area#...
Master Level Access												
13	Bellman's Master	Yes	1	BA/GMA	1 hr to 24 hrs	24 hrs	-	None	**	None	All	BA or GMA/1/13
14	Grand Master	Yes	1	GMA	1 night to 2730 nights	365 nights	-	All	**	All	All	GMA/1/14
15	Emergency	Yes	1	GMA	1 night to 2730 nights	365 nights	-	All	†	All	All	GMA/1/15
Authorization												
16	Front Desk (FDA)	No	100	MA	None	-	-	-	-	-	-	MA/1/16
17	Bellman's (BA)	No	40	GMA	None	-	-	-	-	-	-	GMA/1/17
18	Programming (PA)	No	20	GMA	None	-	-	-	-	-	-	GMA/1/18/2
18	Master (MA)	No	20	GMA	None	-	-	-	-	-	-	GMA/1/18/1
19	Grand Master (GMA)	No	20	GMA	None	-	-	-	-	-	-	GMA/1/19
30	POS	Yes	200	MA	None	-	-	-	-	-	-	MA/1/30
Lockout / Unlock												
*	Salesman's	-	-	FDA	-	-	-	-	-	-	-	Not a keycard*
20	Hotel	No	1	GMA	1 hr to 2730 nights	24 hrs	-	-	-	-	-	GMA/1/20
21	Room	No	16,000	GMA	1 hr to 24 hrs	24 hrs	-	-	-	-	-	GMA/1/21
22	Group	No	255	MA	1 night to 2730 nights	365 nights	-	-	-	-	-	MA/1/22 for locking out guests who have checked out.
Special Purpose												
23	Battery Test	No	All	FDA	None	-	-	-	-	-	-	FDA/1/23
24	Programmiing	No	All	PA	1 night to 2730 nights	2730 nights	-	-	-	-	-	PA/1/24
25	Passage	Yes	16,000	MA	1 night to 2730 nights	1 night	-	-	-	-	-	MA/1/25
26	Hotel Restart	No	1	GMA	1 hr to 24 hrs	24 hrs		**CALL KABA ILCO SERVICE LINE FOR ASSISTANCE**				
27	FDU Cancel	No	1	GMA	1 hr to 24 hrs	24 hrs						
28	Installation											
(1)	Test	No	1	PA	None	-	-	-	-	-	-	PA/1/28/1 Expiry 2730 nights recommended
(2)	Initialization	No	1	PA	None	-	-	-	-	-	-	PA/1/28/2
31	Audit Lock	No	1	PA	None	-	-	-	-	-	-	PA/1/31 SolitaireSMART only

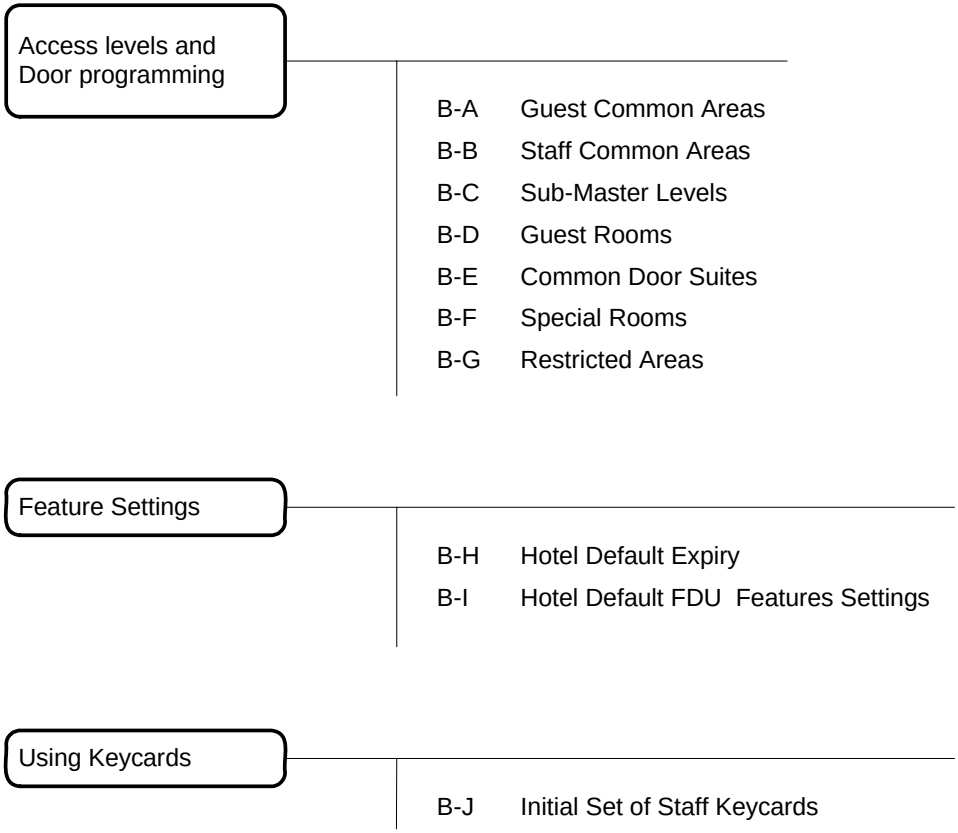
* The Salesman's Lockout is not a keycard but rather an option on the Guest or Suite keycard (consult the manual).

** Will not override the Salesman's Lockout, Room or Hotel Lockout, or deadbolt.

*** The FDU features can be set to encode access to either all 8, or none of the Guest Common Areas on Sub-Master level (Staff) Keycards.

† Will override the Salesman's Lockout, Room or Hotel Lockout, or deadbolt.

Appendix B: System Planning Forms



B-A Guest Common Areas

1. Definitions and Options

	Description	Given To	Default	Linked Rooms
1			Yes/No/Auto	
2			Yes/No/Auto	
3			Yes/No/Auto	
4			Yes/No/Auto	
5			Yes/No/Auto	
6			Yes/No/Auto	
7			Yes/No/Auto	
8			Yes/No/Auto	

Notes:

(i) Default Type of Access
Yes = Per pay (e.g. parking, spa, pool); decide when encoding Guest keycard
No = Unused, OR available only if renting a linked room (set at the factory
Auto = All guests

(ii) To save some Guest Common Area numbers, all doors which will always be encoded on all Guest keycards can be given the same Guest Common Area number (and that Guest Common Area should be set to Auto)

(iii) Common Areas with linked rooms or unused Common Areas must be set to NO

Example:

	Description	Given To	Default	Linked Rooms
1	Elevator and side entrances	All guests	Yes/No/(Auto)	
2	Pool and tennis	All guests	Yes/No/(Auto)	
3	Parking gate	Paying guests	(Yes)/No/Auto	
4	Penthouse elevator access	Penthouse	Yes/(No)/Auto	2201 - 2204
5-8	Unused		Yes/(No)/Auto	

In the above example, the card reader in the elevator control panel is installed so that one relay gives access to the penthouse floor (GCA 4), while another relay gives access to all other floors accessible to guests (GCA 1).

B-A Guest Common Areas (Continued)

2. Guest Common Area Doors

GCA	Door [iii]	Lock / Reader Model	(RAC 3.5 / 4) [i] Time Zone (1-8) [ii] Guest	Staff [iv]	Passage

Example [v]:

2	Pool(main door)	(Reader) RAC	1	2	1
2	Pool (side door)	710-II [vi]	n/a	n/a	n/a
2	Sauna	(Reader) RAC	1	2	1
2	Tennis court	(Reader) RAC	3	2	3

Notes:

(i) When programming the Model 3 or 4 card reader, one of the eight flexible time zones as defined in the FDU features can be selected to restrict each of: Guest access, Staff access and the hours that the reader will be unlocked when in Passage mode.

If no Time Zone or Time Zone 0 is programmed, there are no restrictions.

(ii) Common Area locks can have more than one GCA address and the selected Time Zones will apply to all of them.

(iii) Common Area doors all have the Passage Mode option, meaning that the lock or card reader can be put in Passage Mode with a valid Passage Mode keycard.

(iv) Staff may be given automatic access to all Guest Common Areas (option 2 in the FDU Features Menu).

(v) In this example, the pool and tennis areas have different hours for guest access (Time Zones #1 and #3), but staff who supervise and maintain the sports facilities have the same Time Zone (Time Zone #2). The amenities in the example can only be in Passage mode during normal guest access hours.

(vi) Lock model 760, 740, 710-II, 710 and 700-II do not support the Flexible Time Zone feature for GCA's.

B-B Staff Common Areas

1. Definitions and Options

	Description [(i)]	Default [(ii)]
1		Yes/No/Auto
2		Yes/No/Auto
3		Yes/No/Auto
4		Yes/No/Auto
5		Yes/No/Auto
6		Yes/No/Auto
7		Yes/No/Auto
8		Yes/No/Auto
9		Yes/No/Auto
10		Yes/No/Auto
11		Yes/No/Auto
12		Yes/No/Auto
13		Yes/No/Auto
14		Yes/No/Auto
15		Yes/No/Auto
16		Yes/No/Auto

Notes:

(i) To save some Staff Common Area numbers, all doors which will always be encoded on all Staff keycards can be given the same Staff Common Area number (and that Staff Common Area should be set to Auto)

(ii) Default Type of Access

Yes = Some staff (decide when encoding Section/Floor/Group/Zone/Area keycards)
No = Unused
Auto = All staff

Example:

1	Staff cafeteria, locker room and washrooms (Women)
2	Staff cafeteria, locker room and washrooms (Men)
3	Service entrances and service elevator
4 - 16	Unused

B-B Staff Common Areas (Continued)

2. Staff Common Area Doors

SCA	Door [iii]	Lock / RAC Reader Model	(RAC 3.5 / 4) [i] Time Zone (1-8) Staff	Passage

Example:

1, 2 [ii]	Cafeteria	RAC	4	5
1	Women's washroom	710-II [iv]	n/a	n/a
1	Women's lockers	RAC		5
2	Men's washroom	710-II	n/a	n/a
2	Men's lockers	RAC		5
1, 2 [ii]	Smoking room	RAC	4	5

Notes:

(i) When programming the Model 3 card reader, one of the eight flexible time zones as defined in the FDU features can be selected to restrict each of: Staff access and the hours that the reader will be unlocked when in Passage mode. If no Time Zone or Time Zone 0 is programmed, there are no restrictions. (The Guest level Time Zone does not apply to Staff Common Area card readers.)

(ii) A Common Area lock can have more than one SCA address. In this example, all women staff are given access to SCA 1, and all men staff are given access to SCA2. The cafeteria and smoking room are open to both sexes. Note that the selected Time Zones apply to all SCA addresses programmed in a given lock.

(iii) Common Area doors all have the Passage Mode option, meaning that the lock or card reader can be put in Passage Mode with a valid Passage Mode keycard.

(iv) Lock model 760, 740, 710-II, 710 and 700-II do not support the Flexible Time Zone feature for SCA's.

B-C Sub-Master Levels

	Description
Section	
Floor	
Group*	
Zone	
Area**	

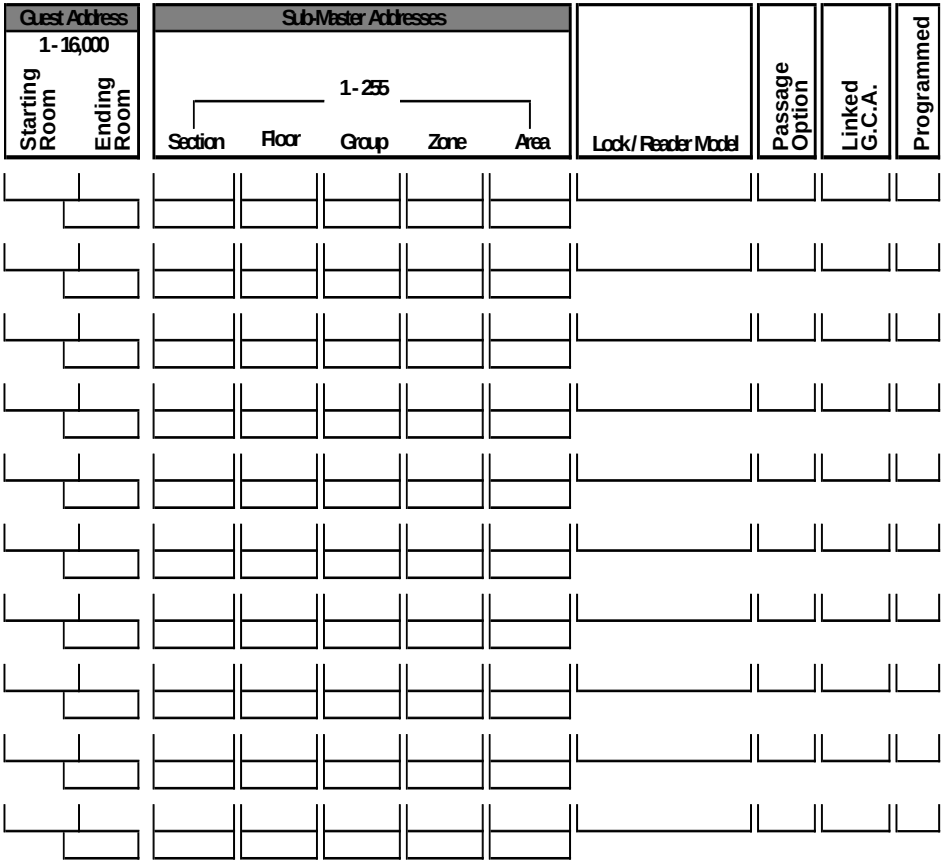
Notes: * The Group Lockout function allows the housekeeper manager to invalidate the last guest's keycard when the room is ready. The Group address should be assigned according to the duties of housekeepers and the housekeeper manager.

** In order to use the Back-Up Keycard Kit, properties with two or fewer FDUs should set all locks to Group 1 and assign a different Area number to each guest room.

Example:

Section	Rooms serviced by one housekeeper.
Floor	Corresponds to the actual floor.
Group*	Rooms which are the responsibility of one housekeeper manager
Zone	Divide rooms according to the duties of minibar servicing personnel.
Area**	Different number for each room, for giving staff access to a specific room only.
	(Because employees should never carry a Guest keycard)

B-D Guest Rooms



* Passage mode is not normally available as an option for Guest Room doors.

B-E Common Door Suites

Guest Address 1 - 1,000		Sub-Master Addresses 1 - 255							
Common Door	Inner Doors	Section	Floor	Group	Zone	Area	Lock / Reader Model	Linked G.C.A.	Programmed
	1								
	2								
	3								
	4								
	5								
	6								
	7								
	8								
	1								
	2								
	3								
	4								
	5								
	6								
	7								
	8								
	1								
	2								
	3								
	4								
	5								
	6								
	7								
	8								

B-F Special Rooms

Guest Address	Sub-Master Addresses								
1 - 16,000	1 - 255								
Door	Section	Floor	Group	Zone	Area	Lock / Reader Model	Passage Option	Linked G.C.A.	Programmed
Description:									
Description:									
Description:									
Description:									
Description:									
Description:									
Description:									
Description:									
Description:									

* Passage mode is available if requested for preprogramming into the FDU at the factory.
The passage Option must be requested for each lock individually.

B-G Restricted Access

Door Identification		Restricted Area Access			
Door	Description	1 - 200 Restricted Area	Lock / Reader Model	Passage Option	Programmed
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	
				YES	

*Passage mode is always available for Restricted Area doors, using a valid Passage keycard.

B-H Hotel Default Expiry

		Selectable Expiry	Factory Default	Hotel Default Setting	Reason
Guest Level Access					
1	Guest	1 hr to 2730 nights	1 night		
2	One-Shot	1 hr to 4 hrs	1 hr		
3	Adjoining Suite	1 hr to 2730 nights	1 night		
4	Common Door Suite	1 hr to 2730 nights	1 night		
5	Convention Suite	1 hr to 2730 nights	1 night		
6	Pre-registered	1 hr to 2730 nights	1 night		
Rest. Area Level Access					
7	Restricted Area	1 night to 2730 nights	1 night		
Sub-Master Level Acess					
8	Section	1 night to 2730 nights	365 nights		
9	Floor	1 night to 2730 nights	365 nights		
10	Group	1 night to 2730 nights	365 nights		
11	Zone	1 night to 2730 nights	365 nights		
12	Area	1 night to 2730 nights	365 nights		
Master Level Access					
13	Bellman's Master	1 hr to 24 hrs	24 hrs		
14	Grand Master	1 night to 2730 nights	365 nights		
15	Emergency	1 night to 2730 nights	365 nights		
Lockout / Unlock					
20	Hotel	1 hr to 2730 nights	24 hrs		
21	Room	1 hr to 24 hrs	24 hrs		
22	Group	1 night to 2730 nights	365 nights		

Special Purpose					
23	Battery Test	None	-		
24	Programming	1 night to 2730 nights	2730 nights		
25	Passage	1 night to 2730 nights	1 night		
26	Hotel Restart	1 hr to 24 hrs	24 hrs		
27	FDU Cancel	1 hr to 24 hrs	24 hrs		
28	Installation	None	-		

Example:

1	Guest	1 hr to 2730 nights	1 night	1 night	Short stay facility

B-I Hotel Default FDU Feature Settings

Features		Comment	Factory Default	Hotel Set Default	Reason
	Language	Multi-language availability	English		
	Variable Expiry	YES or NO	YES		
	Guest Common Areas	YES/NO/AUTO	NO		
		See Appendix C-A.1 for planned use of each Guest Common Area			
	Salesman's Lockout	YES/NO/AUTO	NO		
	Staff Access all Guest Common Areas	YES/NO/AUTO	AUTO		
	Staff Common Areas	YES/NO/AUTO	NO		
		See Appendix C-B.1 for planned use of each Staff Common Area			
	Fixed Time Zones (locks)	YES or NO	NO		
	Zone 0 (00:00 to 04:00)	YES/NO/AUTO	NO		
	Zone 4 (04:00 to 08:00)	YES/NO/AUTO	NO		
	Zone 8 (08:00 to 12:00)	YES/NO/AUTO	NO		
	Zone 12 (12:00 to 16:00)	YES/NO/AUTO	NO		

	Zone 16 (16:00 to 20:00)	YES/NO/AUTO	NO		
	Zone 20 (20:00 to 24:00)	YES/NO/AUTO	NO		
	Flexible Time Zones (RAC)	Customize the intervals in each zone			
	Checkout Time	00:00 to 23:00 in hours	12:00		
	Timeout Between Keycards	Immediate to 20 minutes	2 minutes		
	Timeout Between Keystrokes	1 to 20 minutes	2 minutes		
	Timeout in PMS mode	1 to 60 minutes	2 minutes		
	Current Date and Time	Local time, 24 hr. clock	n/a		
	Adjust DST	YES or NO	NO		
	Time Display	12H or 24H	24H		
	Folio Number	YES or NO	NO		
	PMS Interface Options	For use by technician only			
	Programming Authorization	YES or NO	NO		
	Media Type	LCD, USB, or Serial	LCD		
	Guest Keycard Read Back	WITH VALIDATION or WITHOUT VALIDATION	WITH VALIDATION		
	Hide Init. Prompt	YES or NO	NO (show prompts)		

	Enable POS	YES or NO	NO		
	Disability	YES (15 sec.) or NO (4 sec.)	NO		
	Privacy Override (for common door suite)*	YES* or NO	NO		
	Change privacy Override	YES or NO	NO		
	Global Privacy Override**	YES** or NO	NO		
	Accept PIN	YES or NO	NO		
	Create PIN	YES or NO	NO		

* YES = allow valid inner door keycard to override privacy function enabled by the thumbturn of the common door of a Common Door Suite.
** YES = allow valid keycard to override the privacy function enabled by the door thumbturn.

Example:

2	Variable Expiry	YES or NO	YES	NO	GSAs do not adjust Guest expiry

B-J Initial Set of Staff Keycards

All copies should be encoded as identical NEW keycards in one transaction of the FDU

Keycards	Used by	Copies

Appendix C: Staff Issuing Log

Employee **MUST** sign for Restricted Area, Sub-Master and Master level entry keycards and all Authorization keycards*									
ID Code	**Keycard**	**Sequence ID**	**Employee Name**	**Date**	**Time OUT**	**Signature**	**Date**	**Time IN**	**Signature**

* Authorization Keycards: Only one Authorization keycard with a given Authorization number can be valid at any time. The most recently encoded Authorization keycard will cancel the previous keycard with the same Authorization number.

FDU Menu Chart

	Authorization levels				
	Bellman's Master	Front Desk	Programming	Master	General Manager
1- Guest Keycard		x	x	x	x
1- Guest		x	x	x	x
2- Adjoining Suite		x	x	x	x
3- Common Door Suite		x	x	x	x
4- Guest One Shot		x	x	x	x
5- Convention Suite		x	x	x	x
6- Preregistered Guest		x	x	x	x
7- Preregistered Adjoining Suite		x	x	x	x
8- Preregistered Common Door Suite		x	x	x	x
2- Read/Verify		x	x	x	x
3- PMS mode		x	x	x	x
4- Lock Action Keycard		x	x	x	x
1- Battery Test		x	x	x	x
2- Programming			x	x	x
3- Installation				x	x
4- Passage				x	x
Guest Room				x	x
Guest Common Area				x	x
Staff Common Area					x
Restricted Area					x
5- Lockout				x	x
Group				x	x
Room					x
Hotel					x
6- Hotel Restart					x
7- FDU Cancel					x

	Bellman's Master	Front Desk	Programming	Master	General Manager
5- Reset Keycard		x	x	x	x
1- Reset Guest		x	x	x	x
1- Reset Guest		x	x	x	x
2- Reset Adjoining Suite		x	x	x	x
3- Reset Com Door Suite		x	x	x	x
4- Reset One Shot		x	x	x	x
5- Reset Convention				x	x
6- Reset Preregistered				x	x
2- Reset Passage		x	x	x	x
Guest		x	x	x	x
Guest Common Area		x	x	x	x
Staff Common Area		x	x	x	x
Restricted Area		x	x	x	x
3- Reset Staff				x	x
1- Reset Submaster				x	x
Section				x	x
Floor				x	x
Group				x	x
Zone				x	x
Area				x	x
2- Reset Restricted Area				x	x
3- Reset Bellman				x	x
4- Reset Grand Master				x	x
5- Reset Emergency				x	x

	Bellman's Master	Front Desk	Programming	Master	General Manager
6- Staff Keycard				x	x
1- Submaster				x	x
Section				x	x
Floor				x	x
Group				x	x
Zone				x	x
Area				x	x
2- FDU Authorization				x	x
Front Desk				x	x
POS					x
Bellman's					x
Programming				x	x
Master					x
General Master					x
3- Restricted Area					x
4- Bellman's Master	x				x
5- Grand Master					x
6- Emergency					x

	Bellman's Master	Front Desk	Programming	Master	General Manager
7- FDU Setup				x	x
1- Keycard Expiry				x	x
1- Guest Keycards				x	x
2- Lock Action Keycards				x	x
3- Reset Keycards				x	x
4- Staff Keycards				x	x
5- Load Factory Default				x	x
2- FDU Features					x
1- Look and feel					x
Language					x
Read Back (with or without entering room number)					x
Time Display					x
Hide Initial Setup Prompt Menu					x
2- Keycards Encoding					x
1- Guest					x
1- Options					x
Folio					x
Variable Exp.					x
Checkout Time					x
Salesman Lockout					x
Disability Option					x
2- Common Areas					x
2- Staff					x
1- Staff Com Areas					x
2- Guest Com. Areas					x
3- Fixed Timezones					x

	Bellman's Master	Front Desk	Programming	Master	General Manager
3- FDU Configuration					x
1- Adjust DST					x
2- Timeouts					x
Keycards					x
Keystroke					x
PMS					x
3- PMS Options					x
Baud Rate					x
LRC seed					x
SOF					x
4 Misc Options					x
Programming Authorization Level Enable					x
Enable POS					x
Accept PIN					x
4- Lock Options					x
Common Door Privacy Override					x
Change Privacy Override					x
Global Privacy Override					x
5- Flexible Timezones					x
6- Load Factory Default					x
3- PIN management					x
4- Volume					x
5- Contrast					x

	Bellman's Master	Front Desk	Programming	Master	General Manager
8- Programming			x	x	x
1- Lock			x	x	x
1- Program Addresses			x	x	x
2- Reset Addresses			x	x	x
3- Program Common Door Suites			x	x	x
4- Program Common Areas			x	x	x
5- Program Restricted Areas			x	x	x
6- Reset Time			x	x	x
7- Electrical Override			x	x	x
2- Another FDU				x	x
1- Receive Configuration				x	x
2- Send Configuration				x	x
9- Audit/Report			x	x	x
1- Lock Audit			x	x	x
1- Audit Lock			x	x	x
2- Clear Lock Audit			x	x	x
3- Lock Report			x	x	x
2- FDU Audit					x
FDU Audit Search					x

Kaba Lodging Systems
7301 Boul. Décarie Montréal (QC) H4P 2G7

Technical Support:
1.800.906.4526
Customer Service:
T: 1.877.468.3555
F: 514.735.6589

General Information:
www.kabalodging.com

Online Consumable Orders:
www.keycard.com

To access all of our easy steps, please visit our Support Website:
http://connect.kabalodging.com

PK3514_06_07 Printed in Canada