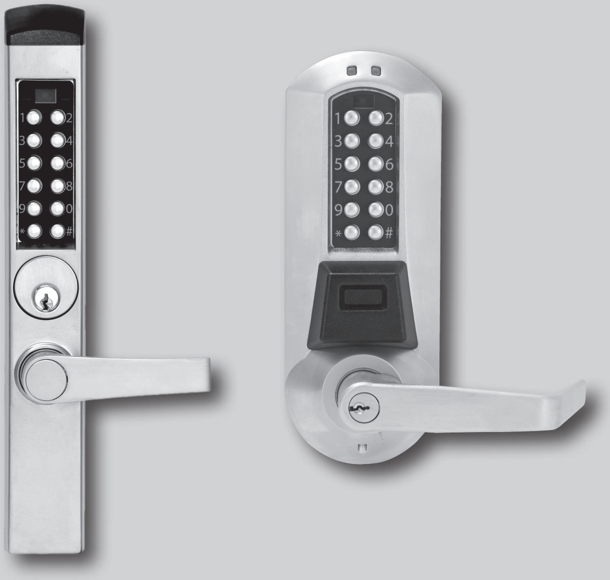

BEYOND SECURITY

KABA®

E-PLEX® CARD BASED 36xx/37xx/56xx/57xx LOCK SERIES

Operations Manual

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

A publication of
Kaba Access & Data Systems Americas
2941 Indiana Avenue
Winston-Salem, NC 27105. USA
Tel: (800) 849-8324 or (336) 725-1331
Fax: (800) 346-9640 or (336) 725-3269
www.kaba-adsamericas.com

The information contained in this publication is accurate to the best of Kaba Access Control's knowledge.

Specifications are subject to change without notice.

Legend
- "E-Plex Lock" refers to E-Plex 57xx; 56xx and E-Plex 37xx; 36xx locks.
- "E-Plex 5xxx" refers to the E-Plex 57xx and 56xx series locks only.
- "E-Plex 3xxx" refers to the E-Plex 37xx and 36xx series locks only.

Definition of the Term "LearnLok™ "

The term "LearnLok" with Kaba designed card based E-Plex Series lock refers to being able to enroll users' ID cards and PINs directly at the lock's keypad without uploading any software data to the lock from a handheld PDA unit. Here you make the lock "learn" the credential enrolling process simply by programming the lock at its keypad with your finger tip. The following E-Plex card based locks will work in "LearnLok" mode: E3600 and 5600; credentials supported are Mifare, DESFire and iClass, operates under 13.56 MHz frequency (ISO 14443 compliant). E3700 and 5700; credential supported is Prox, operating under 125 kHz.

States of the E-Plex Lock

Factory Mode

The factory mode is one of three primary states of the E-Plex Lock. The main characteristics of this state are:

- The E-Plex Lock opens only when the 8-digit master combination (1-2-3-4-5-6-7-8) is keyed in.
- The visual indication for 'access granted' is green LED flashing once. A high-pitched tone is also generated while the green LED is on.
- Important: The Master User must change the factory default Master combination to be able to exit the factory mode and switch to the access mode for normal use of the lock.

Access Mode (up to 300 users per lock in LearnLok™ mode)

This mode refers to a lock that is operational for user access, and not in factory or Programming Mode.

"LearnLok™" Pushbutton Programming Mode

The E-Plex lock enters the Pushbutton Programming Mode when the user enters the master combination or one of the manager combinations, preceded and followed by the character '#' (ex: #87654321#). Once the E-Plex Lock is in the Pushbutton Programming Mode, the Master / Manager can enter one or more command sequences. Each command sequence ends with a '#' character that acts like an <**enter**> character. At the very end of all sequences of programming commands, enter one more # to remove the lock from the Pushbutton Programming Mode to return to normal access mode.

Sequence of Operations for Start-Up Programming

What is the recommended sequence of operations?

Ensure that the E-Plex Lock is in Factory Mode:

- Program the Access PIN Length (default length is four digits). *The access PIN field length can only be changed when the lock is not yet activated (ie, when it is still in the factory mode).*
- Change factory Master to your own Master PIN (always eight digits) to place lock in access mode, for example, changing it from the default 12345678 to say 87654321.

Put lock in Pushbutton Programming (LearnLok™) Mode.

Note: "LearnLok™" (LL) means the Master or the Manager users' can make the lock "learn" to enroll and/or to remove credentials in the lock by simply programming these functions at the lock keypad itself WITHOUT any software - up to 300 users. But later on if you use the software and program the lock with a Maintenance Unit (M-Unit_ handheld, the lock will exit the LearnLok™ keypad programming mode. In other words, from now on you must use the software and the M-Unit PDA to manage all lock operations including adding and/or deleting user credentials (up to 3.000) in the lock. Important: When you perform a "hard reset" of the lock with the mechanical override key, the lock will revert back to the factory default LearnLok™ keypad programming mode

- Set the Date / Time (optional; useful only if you use the lock with software in future)
- Program the Unlock time period

- Program the Lock for the Duration of Passage Mode (if desired)
- Program the Lock for Tamper Time Settings
- Program the Lock for Buzzer Volume
- Add Access Credentials as desired

Note: A credential can be either Card only access or PIN followed by Card access for regular Access users and Manager users. Or, it can be PIN only access for Service users. In LearnLok™ mode only, the Master credential is always PIN only mode and it is always 8 digits in length.

Default values of the E-Plex® Lock programmable parameters

Parameters	Factory Default Values
Date (MM/DD/YY)	01/01/00
Time (HH:MM)	00:00
Lock state	Unprogrammed
Passage mode open time limit	9 hours
Passage mode	De-activated/Disabled
Lockout mode	Disabled
Unlock time	2 seconds
Buzzer volume control	Low (=1)
Tamper shutdown time	30 seconds
Tamper attempt count	4 attempts
Access code length	4 digits
Latch Holdback Mode	Disabled (E-3xxx only)
Swingbolt Privilege	Disabled (E-3xxx only)
Privacy Privilege	Disabled (E-5xxx only)
BHMA Lock Function	Entry (E5xxx); Latch (E3xxx)
Master combination	12345678 (8 digits)
Access credential	None
Credential status	Activated
M-Unit user's combination	None (*used with software only)
M-Unit user's status	Disabled (*used with software only)

Configuring the Lock

General Procedure for Pushbutton Programming

1. The pages that follow provide step-by-step instructions for programming the E-Plex Lock.
2. The general procedure for all programming functions is as follows:
   a. Put the lock in Programming Mode by pressing # Master Credential #
   b. Use the Summary of Commands Table in the appendix section of this guide to enter the three digit command sequence (Command Code + Function Code), followed by #.
   c. Enter the appropriate numbers as required.
   d. Press # to end Programming Mode.
   e. Once the lock is in programming mode, multiple command sequences can be entered without having to repeat the # master credential #. However, if there is no activity for 15 seconds at the keypad, the lock will automatically exit from programming mode.

For example

- If the Master (or Manager) enters her/his credential of **87654321**, the door will open.
- If he enters **#87654321#**, the lock will enter into the LearnLok™ Programming Mode and wait for the next part of the command.
- If he enters the # sign twice at the end of the last programming command sequence, for example **#87654321##**, the lock will go out of Programming Mode and return to its normal access grant/deny mode.

> **Note:** The # pound sign acts like the Enter key on a PC keyboard in your communications with the lock. The # tells the lock that one part of the entry is finished. The # serves another purpose - to distinguish a programming type command from a simple Access PIN to open the door. A Master or Manager User can use the same credential to open the door or to put the lock in Programming Mode, the only difference being that he uses the # sign in front to signal that he is about to enter a programming command. For increased security, it is recommended that the master user PIN not be used for everyday access. This can be accomplished by creating a non expiry Service user PIN for the master user.

Reset Procedures

There are three different "Reset" levels available in the E-Plex Lock.

Command Code 099# will reset the lock to the factory default settings, except for the access credential length (Master and Manager User credentials and Time / Date are retained if already programmed)

Command Code 299# will delete all access and service user credentials (Master, Manager and M-Unit * (see below) users are retained.

Hard Reset will return the lock to full factory default mode including deleting all credentials, putting the lock back to factory default configuration values (4 digit access credential lengths) and making the master PIN to again 1-2-3-4-5-6-7-8. A hard reset is performed as follows.

Hard reset sequence for the E-Plex E5xxx Series:

A) User knows the Master code:

1. Insert mechanical override key, turn counterclockwise and hold so that lock is in open position (cylindrical latch is retracted). Within 5 seconds, press # and release the key (latch).
2. You have up to 5 seconds to push '#' and release the override key. If 5-second timeout is reached without pressing '#', the lock continues its normal operation. As soon as the '#' is pressed, the lock exits the current state. If timeout is reached or if any other key is pressed after the '#' was pressed, the lock exits the sequence and stays in access state. If '#' is pushed and reset button is released within 5-second period, the lock goes in Reset Sequence State and the lock displays the 'Reset Sequence In Progress' message by flashing Green and Red LED alternatively once every second.
3. In this state, users have a 20-second period to enter the Master Code to per form a hard reset. If a bad Master Code is keyed-in, the lock exits the Reset Sequence State and goes back in access state. If the correct Master Code is entered within 20 seconds, the lock performs a hard reset and goes back in unprogrammed state. When an incorrect Master Code is entered, the Tamper Count decrements. After 4 unsuccessful attempts to Reset the lock with a bad Master code, the lock goes in the Tamper Shutdown state for 30 seconds. It will resume normal operations after this delay. If no master code is entered during the 20 seconds delay, the lock will enter a 15 minute wait period assuming the Master Code is unknown.

B) User does not know the Master code:

1. Insert mechanical override key, turn counterclockwise and hold so that lock is in open position (cylindrical latch is retracted). Within 5 seconds, press # and release the key (latch).
2. You have up to 5 seconds to push '#' and release the override key. If 5-second timeout is reached without pressing '#', the lock continues its normal operation. As soon as the '#' is pressed, the lock exits the current state. If timeout is reached or if any other access state. If '#' is pushed and reset button is release within 5-second period, the lock goes in Reset Sequence State and the lock dis plays the 'Reset Sequence In Progress message by flashing Green and Red LED alternatively once every second.
3. In this state, users have a 20-second period to enter the Master Code to per form a hard reset. When the user does not know the master code, the user must not enter anything during that 20 seconds delay. The Reset sequence in progress message will be displayed on the LEDs.
4. When the 20 seconds delay will be exhausted, a 15 minutes wait period will begin. During that state, any operation on the lock will be ignored (green LED will not blink when pressing keys) and the Green and Red LED will blink once a minute.
5. After the 15 minutes delay has exhausted, the Reset sequence in progress message will be displayed on the LEDs again for 20 seconds. During this period, the user must enter the 1-2-3-4-5-6-7-8-# sequence and the lock will reset. If the user fails to do so, the sequence will abort and the lock will resume normal operation.

Hard reset sequence for E-Plex 3xxx Series:

A) User knows the Master code:

1. Insert mechanical override key, turn to 3 o'clock position, press # and then turn key back to 12 o'clock position within 5 seconds.
2. You have up to 5 seconds to push '#' and then turn key back to 12 o'clock position. If 5-second timeout is reached without pressing '#', the lock continues its normal operation. As soon as the '#' is pressed, the lock exits the current state. If timeout is reached or if any other key is pressed after the '#' was pressed, the lock exits the sequence and stays in access state. If '#' is pushed and reset button is released within 5-second period, the lock goes in Reset Sequence State and the lock displays the 'Reset Sequence In Progress' message by flashing Green and Red LED alternatively once every second.
3. In this state, users have a 20-second period to enter the Master Code to per form a hard reset. If a bad Master Code is keyed-in, the lock exits the Reset Sequence State and goes back in access state. If the correct Master Code is entered within 20 seconds, the lock performs a hard reset and goes back in unprogrammed state. When an incorrect Master Code is entered, the Tamper Count decrements. After 4 unsuccessful attempts to Reset the lock with a bad Master code, the lock goes in the Tamper Shutdown state for 30 seconds. It will resume normal operations after this delay. If no master code is entered during the 20 seconds delay, the lock will enter a 15 minute wait period assuming the Master Code is unknown.

B) User does not know the Master code:

1. Insert mechanical override key, turn to 3 o'clock position, press # and then turn key back to 12 o'clock position within 5 seconds.
2. You have up to 5 seconds to push '#' and then turn key back to 12 o'clock position. If 5-second timeout is reached without pressing '#', the lock continues its normal operation. As soon as the '#' is pressed, the lock exits the current state. If timeout is reached or if any other key is pressed after the '#' was pressed, the lock exits the sequence and stays in access state. If '#' is pushed and reset button is release within 5-second period, the lock goes in Reset Sequence State and the lock displays the 'Reset Sequence In Progress message by flashing Green and Red LED alternatively once every second.
3. In this state, users have a 20-second period to enter the Master Code to per form a hard reset. When the user does not know the master code, the user must not enter anything during that 20 seconds delay. The Reset sequence in progress message will be displayed on the LEDs.
4. When the 20 seconds delay will be exhausted, a 15 minutes wait period will begin. During that state, any operation on the lock will be ignored (green LED will not blink when pressing keys) and the Green and Red LED will blink once a minute.
5. After the 15 minutes delay has exhausted, the Reset sequence in progress message will be displayed on the LEDs again for 20 seconds. During this period, the user must enter the 1-2-3-4-5-6-7-8-# sequence and the lock will reset. If the user fails to do so, the sequence will abort and the lock will resume normal operation.

PROCEDURE 1A - PROGRAM THE (GLOBAL) ACCESS PIN LENGTH

PINs are required for Access users and Manager users in PIN & Card access mode and also for all Service users since they have only PIN access. Setting the length of Access PIN must be the first lock programmable function you perform, because all of your other access PINs (except for the Master) must have the same length. If a user enters a PIN of a different length, the lock will not accept it. Longer length Access PINs permit a greater number of PIN combination possibilities, and thus higher security. The Master credential PIN length must always be 8 digits which cannot be changed.

Required User Level: Master

1. To configure the E-Plex Lock, it must be still in Factory mode before doing any programming functions at the lock keypad.

Important: This global user PIN length setup and the BHMA Lock Function setup operations are the only two programmable functions that can be done during the factory mode using the factory default Master PIN. Changing the factory default Master PIN to a new Master PIN has to be done here also. For the BHMA Lock Function setup instructions, please refer to the applicable "E-PLEX Lock Function Setup Guide" that came with this lock.

2. Put the lock in pushbutton programming mode using the factory Master PIN (**#12345678#**). The lock responds with a flashing green light. If for some reason 1-2-3-4-5-6-7-8 does not seem to work, please follow the steps for a **Hard Reset** by following the procedure on page 6.
3. Enter the command sequence **009 #LL #**, where **LL** represents the length (number of digits in a PIN). The range is from 04 to 08 digits. You can leave the factory default Access PIN length (4 digits) if you wish by not changing the length.
4. Example of Complete Entry: **009#05#** to change the code length to 5 digits.
5. Key in another **#** to indicate the end of programming.
6. From now on, all the user Access PINs you create will have 5 digits length as setup in step 4 above.

PROCEDURE 2A - MODIFY THE MASTER USER ACCESS PIN

Required User Level: Master

1. To change the factory default Master PIN, follow the next three steps:
2. Put lock into Pushbutton Programming Mode.
3. Use the command, **000,** to change the Master PIN, followed by the new Master PIN itself.
4. You must use 8 digits between **00000000** and **99999999** as follows: **000#MMMMMMMM#**, we'll use **000#87654321#** as an example.
5. Enter the Master PIN again **87654321#** for confirmation.
6. Example of Complete Entry: **000#87654321#87654321#**.
7. Key in another **#** to indicate the end of programming.
8. After that, you will always use your own Master PIN. Please write this PIN down and keep in a safe place. From now on the factory default Master PIN is no longer valid.

Note: In the E-Plex LearnLok™ keypad programming and usage mode, the master's credential is PIN only and no card can be assigned to the Master.

PROCEDURE 3A - SET THE DATE / TIME

Note: Not required if software is not used since you will not be able to audit lock without the software.

You must enter the current date and time in each lock to enable accurate programming and auditing. Always enter Standard Time; the software package (if and when used) will make the adjustment for Daylight Savings Time and from then on will switch the 1 hour spring/fall time automatically when the DST switch occurs every spring and fall. Enter **001** for date settings and **002** for time settings. Date / time settings are maintained even after a battery change unless you remove the batteries for more than two minutes. If this happens, the time will be reset to 00:00:00 and the date to 01/01/2000 and you must rest the lock to the current date & time.

Required User Level: Master

1. Put lock into pushbutton programming mode.
2. Enter the date as follows: **001#MMDDYY#** (Month, Day, Year, where **MM** = 01 to 12; **DD** = 01 to 31; **YY** = 00 to 99. For example, Nov. 22, 2007 would be entered as 112207).
3. Enter the date again to confirm **MMDDYY#**. Example of Complete Entry: **001#112207#112207#**.
4. For the time, enter as follows: **002#HHMM#,** where HH = 00 to 23 hours; MM = 00 to 59 minutes. Use military time - for example eight-thirty in the morning would be 0830, while in the evening it would be 2030).
5. Enter the code again **HHMM#,** for example **0830**.
6. Example of Complete Entry: **002#0830#0830#**.
7. Enter another **#** to indicate the end of programming.
8. The current date and time are now programmed into the lock.

PROCEDURE 4A - PROGRAM THE UNLOCK TIME

Unlock time is the length of time the door will remain unlocked when a correct user credential is used before the lock automatically re-locks itself.

Required User Level: Master, Manager

1. Put the lock into Pushbutton Programming Mode.
7. To establish Unlock Time, enter the following code: **004#TT#**, where **TT** is the time in seconds, (**TT**=02 to 20 seconds, for example 5 seconds).
8. Example of Complete Entry: **004#05#**.
9. Enter another **#** to indicate the end of programming.
10. You have now programmed the lock an Unlock Time of 5 seconds for the door.

PROCEDURE 5A - PROGRAM THE DURATION OF THE (MANUAL) PASSAGE MODE PERIOD

You might want to program locks for public areas, such as cafeterias, to have free access (Passage Mode) during certain periods of the day, and revert to required credential access outside of these regular hours.

The length of time that the lock remains in Passage Mode is programmable.

The factory default length of time for manual keypad Passage Mode is 9 hours - you may leave the default. Though the free passage hours are already set in the lock, the lock's passage mode is de-activated by default and you must activate it at the lock's keypad whenever you want it.

When the lock is activated at the lock keypad to go into Passage Mode, it will automatically relock after the designated duration expires - after 9 hours in this case.

Required User Level: Master, Manager

1. Put the lock into Pushbutton Programming Mode.
2. Enter command code **005#**.
3. Then **TT#**, where **TT= 01 to 24** hours.
4. A TT entry of 00 means there is no time limit - the door remains unlocked permanently which is not secure
5. Enter **005 #TT#**; for example, **005#06#** for six hours free passage.
6. Example of Complete Entry: **005#06#**.
7. Enter another **#** to indicate the end of programming.
8. In this example, the lock will remain unlocked for six hours, starting from the time you activate it in Passage Mode.
9. Important: You have now configured the duration of the Passage Mode for that lock. This does **NOT** initiate the Passage Mode until you activate it manually at the lock keypad - See Procedure 12 on "How to activate/de-activate the Passage Mode."
10. Within the Passage mode duration (6 hours in this example), you can activate and de-activate the free passage mode any number of times.

Note: There are two more Passage mode options available when software is used - the Auto Passage mode and the First Privileged user Passage mode.

PROCEDURE 6A - PROGRAM THE LOCK FOR TAMPER TIME PARAMETERS

You can set the Tamper Time Wrong Tries parameter referring to the number of times the wrong credential can be tried to access before the lock goes into a Tamper Shutdown Mode. For example, if you program the lock to accept three wrong tries, the lock will tolerate three wrong entries, staying locked but providing visual feedback (see visual message chart in rear section). After that, it will go into a Tamper Shutdown Mode and remain locked until the end of the Tamper Shutdown Time period - the length of that period is configured in Step 4 of this procedure below. During this shutdown period, only the Master PIN or the mechanical key will unlock the lock.

Required User Level: Master, Manager

1. Set the tamper time for the period of time during which the keypad will remain inaccessible after the specified number of wrong Access Credentials are entered
2. Put the lock into Pushbutton Programming Mode.
3. Enter the command sequence as follows - **006#TT#** (**TT** is seconds - **00 to 90** seconds).
4. Example of Complete Entry: **006#60#**. (for 60 seconds tamper shutdown)

Note: If a value of 00 second is entered here, the lock will **never** go into tamper shutdown mode even after the number of illegal attempts specified (step 6 below).

5. Enter the code as follows: **007 #TT#** (**TT** is number of wrong entries - **03** to **09**), let's use **05** for example.
6. Example of Complete Entry: **007#05#**.
7. Enter another **#** to indicate the end of programming.
8. The lock will stay locked after three wrong entries for the length of time you select in the steps below, **even if a valid code (including the Master or a Manager Code) is entered after the three wrong codes. Only the mechanical key override will open the lock during the tamper shut down Period.**
9. Enter another **#** to indicate the end of programming.

PROCEDURE 7A - PROGRAMMING THE LOCK FOR KEYPAD BUZZER VOLUME

You may want to adjust the volume of the Keypad Buzzer depending on where the lock is located - a noisy or quiet area.

Required User Level: Master, Manager

1. Put the lock into Pushbutton Programming Mode.
2. Enter the command sequence **008#VV#** (where VV is a scale of volume from 00 to 03; 00 = off; 01 = Low; 02 = Normal; 03 = High).
3. Example of Complete Entry: **008#02#**.
4. Enter another **#** to indicate the end of programming.
5. The lock will now sound the buzzer at the desired volume Normal/Medium, until you change it.

USER - GENERAL INFORMATION

1. Master and Manager Credentials can do two different things:
   - Open the door by entering the Access Credential without # signs.
   - Put the lock into LearnLok™ Pushbutton Programming Mode by entering # before and after their Access Credential.
2. Each user - the Manager user, the Access user or the Access user occupies one of the available 300 locations in the user table of the lock's memory, from 001 through 300.
3. By default, the Master user occupies user table location 000 which is reserved for the Master.
4. The Master and Manager users have a 15-second period to enter the entire programming key sequence, and 5 seconds between pressing each pushbutton number. If they pause longer than 5 seconds between pressing each pushbutton number. If they pause longer than 5 seconds between each pushbutton pressed, or exceed the 15-second period to enter the total programming sequence, the lock:
   - aborts the current programming sequence
   - automatically exits the programming state
   - sends the user a 'Keypad Timeout' feedback message (LEDs and buzzer)

Note: Correct errors during a command sequence. If an invalid entry occurs, recover from the mistake by entering the (*) key, which will clear all entries made from the beginning of the current command sequence, and will reset the 15-second time limit for entering the code. In this case, you still have 15 seconds from the first number entered to enter the whole command code sequence.

USER LEVELS

Five different classifications of users can perform various operations at the lock.

Master User - The Master User is the top-level manager who performs the initial lock setup activities, can program all lock functions and has complete access to the locks anytime without any restrictions.

Manager - A Manager can open the lock and can also program all lock functions except:

- defining the Access User Code length
- modifying master user PIN
- changing date and time
- resetting lock to selected default values
- activating/de-activating global lockout mode
- adding / deleting / enabling / disabling another Manager User. The number of Managers is limited only by available user table space - 300 maximum.

Access User - A regular Access User has the ability to only open the lock. The number of Access Users is limited only by the available user table - 300 maximum.

Service User - A Service user can open the lock either one time only, or from 1 through 96 hours, or can access the lock with no expiry, depending on how s/he is enrolled in the lock. When in non expiry mode, the period of Service's user's access time starts on the first user of his PIN. Each Service User PIN is automatically deleted from the lock's memory after its period of time expires. The number of service users is limited only by the available user table space - 300 maximum.

M-Unit User - There can be also M-Unit (Maintenance Unit) users and Guest users in the lock, available only if the E-Plex Enterprise software is used - sold separately.

Note: The total number of users enrolled into the lock at any given time cannot exceed 300, plus the Master user. You can enroll a user mix of Access, Manager and Service users but the total aggregate of users cannot exceed 300 users.

USER CREDENTIALS

Each time you add a user to give access to a door, you must program the lock at the keypad with an Access Credential for this user who may be a Manager user and/or an Access user and/or a Service user. This user access credential can be either card only, or PIN followed by card for Manager and regular Access users; and can be PIN only the Service users. The global Master user's access will always be an 8-digit PIN only. You can also easily delete the access credential for an existing user right at the lock keypad.

Credential to Access the Lock:

Credential of the Master User: (i) PIN only access - no expiry

Credential of a Manager User: (i) Card only access; or,
(ii) PIN & card access -> no expiry

Credential of an Access User: (i) Card only access; or,
(ii) PIN & card access -> no expiry

Credential of a Service User: (i) PIN only access -> with either (a) no expiry, or (b) 1 through 96 hours access, or (c) one time entry only ("one shot")

Credential to Program the Lock:

Programming Sequence of Master User: #Master PIN# complete command code sequence ##

Programming Sequence of Manager User:

In Card only mode: # present card (green LED flashes) complete command code sequence ##

In PIN & Card mode: # PIN # present card (green LED flashes) complete command code sequence ##

Important: User PINs that will be used in PIN & card access mode must not have the exact same digits in the same position as the Master PIN.

The Master Code **00004992** is used as an example in the table below.

USER ACCESS CODES (PINS) - EXAMPLES

Master Code	**User Code Length**	**Sample User Codes**	
		Acceptable	**Unacceptable**
00004992	4 digits	1000	0000
		0005	
		1206	
		0001	
00004992	5 digits	32000	00004
		00006	
		00100	
		00044	
00004992	6 digits	001041	000049
		000046	
		400492	
		000048	
00004992	7 digits	0005521	0000499
		2000499	
		9900872	
		1000892	
00004992	8 digits	80009765	00004992
		12006654	
		00004993	
		40004992	

PROCEDURE 1B - ADD / MODIFY AN ACCESS USER CREDENTIAL

- A User ID location -> which can be for a regular Access user or for a Manager user or for a Service user is a 3-digit number assigned by the Master or a Manager. You should have the list of User ID Location ready with you when programming locks to enroll (add) users in the lock.
- You should always maintain an accurate and correct list of User ID locations and users assigned to those ID locations to avoid any confusion in future if you need to either delete or de-activate these users. Please make use of the User ID List Sample Table on page 32 for proper credential maintenance of all your users in the facility.

Required User Level: Master, Manager

1. Put the lock into LearnLok™ Pushbutton Programming Mode. -> **# Master PIN (or Manager credential) #**
2. Enter command **100#** to add / modify a User Access Credential.
3. Enter the User ID location NNN followed by # - **NNN#**, we use **023#** for example (Range = 001 to 300).

4a. Card Only Mode: After 100# 023# entry, **present this user's card** close to the (black) card reader of lock; the **green LED flashes** indicating that the card has been enrolled (added); enter **#** which confirms that this user is not assigned a PIN. You can add more cards by entering the next user's ID location (NNN#) followed by presenting this next user's card and then #; add up to 300 cards, if desired.

Enter a last # to indicate the end of the programming.

Example of Complete Entry for user ID=023:

100#023# Present card # #.

4b. PIN & Card Mode: Procedure is similar to step 4a above, but after enrolling the card you must not enter the # but continue with assigning the user's PIN (4 to 8 digits as configured initially).

Example of Complete Entry for user ID=023 and PIN=1234:

100#023# Present card (no # entry here) 1234# 1234# (to re-confirm) #.

In the first example above, this user's card will open the lock with PIN assigned (card only mode), or in the second example above, the lock will open on entering the PIN first (1234) followed by presenting the associated card (PIN & card mode).

PROCEDURE 2B - ADD / MODIFY A MANAGER USER CREDENTIAL

The procedure to add a Manager user is exactly the same as adding a regular Access user except for the different 3-digit command code **101** (instead of 100) usage. Also, only the Master can add, delete, etc, of the Manager users.

Required User Level: Master

1. Put the lock into "LearnLok™" Pushbutton Programming Mode.
2. Enter command **101#** to add / modify a Manager User's Access Credential
3. Enter the User ID location NNN followed by #: **NNN#;** we will use 015# for example (Range = 001 to 300)

4a. Card Only Mode: After 101# 015# entry, **present this Managers card** close to the (black) card reader of the lock; the **green LED flashes** indicating that the card has been enrolled (added); enter # which confirms that this manager user is not assigned a PIN. You can add more cards by entering the next user's ID location (NNN#) followed by presenting this next manager user's card and then #; add up to 300 cards, if desired.

Enter a last # to indicate the end of programming.

Example of Complete Entry for manager user ID=015

101# 015# Present card # #.

4b. Pin & Card Mode: Procedure is similar to step 4a above, but after enrolling the card you must not enter the # but continue with assigning the user's PIN (4 to 8 digits as configured initially).

Example of Complete Entry for Manager user ID=015 and PIN=9876:

101# 015# Present card (no # entry here) 9876# 9876# (to re-confirm) #.

In the above examples, this Manager user's card will open the lock if no PIN was assigned (card only mode), or the lock will open on entering the PIN first (9876) followed by presenting the associated card (PIN & Card mode).

5. The Manager User can also **program the lock at the lock keypad** like the Master user by putting the lock in "LearnLok™" pushbutton programming mode as shown below.

Card only Manager:

# Present Manager's card (no # key entry after) 3-digit command code #

Continue with other desire program input sequence

End with the last # key to exit programming mode.

PIN & Card Manager:

# Manager's PIN # Present Manager's card (no # entry after) 3-digit command code #

Continue with other desire program input sequence

End with the last # key to exit programming mode.

PROCEDURE 3B - ADD / MODIFY A SERVICE USER CREDENTIAL

A Service User is any person who needs access to the lock for a limited time period in order to perform a service, such as painting or repairs to the room or area. A Service User's access credential is always PIN only. Typically a Service user's PIN can be valid for either, one time use only ("one shot" entry), or from 1 through 96 hours expiry use. Additionally, you can assign "super" Service users whose PINs will never expire until you delete them from the lock.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **#**
   Master PIN (or Manager credential) #
2. Enter Command **102#** to add / modify a Service User Access PIN.
3. Enter the Service User ID location NNN followed by #, **NNN#**; we will use 125# for example (Range = 001 to 300).
4. (PIN only mode): After 102# 125# entry, enter the Service user's PIN (we will use 7777 in this example) twice, the second time is for re-confirmation and finally enter the expiry time -> either one shot (00), or 1 through 96 hours (01 through 96), or no expiry (99).

   Example of Complete Entry for Service user ID=125 with one shot expiry:

   102# 125# 7777# 7777# 00# #.

   Example of Complete Entry for Service user ID=125 with expiry of 12 hours:

   102# 125# 7777# 7777# 12# #.

   Example of Complete Entry for Service user ID=125 with no expiry:

   102# 125# 7777# 7777# 99# #.

Note: In all the above examples, the Service User's Access PIN will work in that door for the programmed period of the time the Service user enters her/his PIN the first time.

PROCEDURE 4B - DELETE ACCESS USER CREDENTIALS

Access User credentials should be deleted from the lock if no longer needed since there is no expiry. This frees this ID location to the assigned to another user. Credentials that may be needed sometime in the future should be just de-activated rather than deleted (see Procedure 13).

Required User Level: Master, Manager

1. Put the lock into "LearnLok™"Pushbutton Programming Mode.
2. Enter Command **200#** to delete an Access User Credential whether it is card only credential or PIN & card credential; you do not need this person's card and/or the PIN to delete.
3. Enter the Access User ID location **NNN#**, where **NNN** is the specific User ID location from 001 to 300.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=023

   200# 023# #.

   Now this user's credential will not work in the lock anymore. This allows you to assign another user to this deleted User ID location if you wish.

PROCEDURE 5B - DELETE MANAGER USER CREDENTIALS

Manager User credentials should be deleted from the lock if no longer needed since there is no expiry. This frees this ID location to be assigned to another user. Credentials that may be needed again sometime in the future should be just de-activated rather than deleted (see Procedure 13).

Required User Level: Master

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN #**
2. Enter Command **201#** to delete a Manager User Credential whether it is card only credential or PIN & card credential; you do not need this person's card and/or the PIN to delete.
3. Enter the ID location **NNN#**, where **NNN** is the specific User ID location from 001 to 300; we will use the ID location 015 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=015:

   201#015# #.

   Now this user's credential will not work in the lock anymore. This allows you to assign another user to this deleted User ID location if you wish.

PROCEDURE 6B - DELETE SERVICE USER CREDENTIALS

A Service user's Access Credential (PIN) is automatically deleted from the lock at the end of its specified expiry time -> one time entry or from 1 through 96 hours. However, you must use this procedure if you want to delete the Service user's PIN earlier than the specified expiry time. For the "super" Service user(s), you must delete the PIN if need be since it does not expire. The "one shot" Service user's access PIN will expire automatically after it is used once.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **202#** to delete a Service User PIN if it has not expired already; you do not need this person's PIN to delete.
3. Enter the Service User ID location **NNN#**, where **NNN** is the specific User ID location from 001 to 300; we will use the ID location 125 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=125:

   202#125# #.

   Now this user's credential will not work in the lock anymore. This allows you to assign another user to this deleted User ID location if you wish.

KABA SIMPLEX®/E-PLEX® 5x00/3x00 SERIES LIMITED WARRANTY

Kaba Access Control warrants this product to be free from defects in material and workmanship under normal use and service for a period of three (3) years. Kaba Access Control will repair or replace, at our discretion, E-Plex 5x00 and 3x00 Series Locks found by Kaba Access Control analysis to be defective during this period. Our only liability, whether in tort or in contract, under this warranty is to repair or replace products that are returned to Kaba Access Control within the three (3) year warranty period.

This warranty is in lieu of and not in addition to any other warranty or condition, express or implied, including without limitation merchantability, fitness for purpose or absence of latent defects.

ATTENTION: This warranty does not cover problems arising out of improper installation, neglect or misuse. All warranties implied or written will be null and void if the lock is not installed properly and / or if any supplied component part is substituted with a foreign part. If the lock is used with a wall bumper, the warranty is null and void. If a doorstop is required, we recommend the use of a floor secured stop.

The environment and conditions of use determine the life of finishes on Kaba Access Control products. Finishes on Kaba Access Control products are subject to change due to wear and environmental corrosion. Kaba Access Control cannot be held responsible for the deterioration of finishes.

Authorization to Return Goods

Returned merchandise will not be accepted without prior approval. Approvals and Returned Goods Authorization Numbers (RGA Numbers) for the E-Plex 5x00 and 3x00 Series are available through our Customer Service department in Winston-Salem, NC (800) 849-8324. **The serial number of a lock is required to obtain this RGA Number**. The issuance of an RGA does not imply that a credit or replacement will be issued.

The RGA number must be included on the address label when material is returned to the factory. All component parts including latches and strikes (even if not inoperative) must be included in the package with return. All merchandise must be returned prepaid and properly packaged to the address indicated.

* E-Plex 5x00/3x00 Series locks are warranted three (3) years from date of activation.

PLACE
STAMP
HERE

KABA ACCESS & DATA SYSTEMS AMERICAS
2941 INDIANA AVE
WINSTON-SALEM, NC 27199-3770

Register your Kaba lock online at www.kaba-adsamericas.com/register

or fill in this product registration card and return to Kaba Access & Data Systems Americas (postage required to mail).

Name ____________________

Title ____________________

Company ____________________

Address ____________________

City ____________________

State ____________ Zip ____________ Country ____________

Phone ____________________

Email ____________________

Name of Dealer Purchased From ____________________

Date of Purchase ____________________

Lock Model Number ____________________

Serial Number ____________________

UMAN

This lock will be used in what type of facility?

- ❑ Airport
- ❑ Commercial Building
- ❑ Daycare/Childcare
- ❑ Education – ❑ K-12 Facility, ❑ College/University
- ❑ Financial/Bank
- ❑ Government
- ❑ Hospital/Healthcare
- ❑ Industrial/Manufacturing
- ❑ Military/DOD Operations
- ❑ Public Safety
- ❑ Residential
- ❑ Retail
- ❑ Telecommunications/Utilities
- ❑ Other ____________________

This Kaba Lock is:

- ❑ A new installation
- ❑ Replacing a conventional keyed lock
- ❑ Replacing an electronic lock (specify brand) ____________________
- ❑ Replacing a mechanical lock (specify brand) ____________________

What area is being secured with this lock?
(e.g., front/back door, cabinet, common door, office)

____

- ❑ Check here to be advised of important product and software updates

How did you learn about Kaba Locks?

- ❑ Advertisement
- ❑ Contract Hardware Dealer
- ❑ Direct Mail
- ❑ Internet
- ❑ Kaba Sales Representative
- ❑ Locksmith
- ❑ Maintenance
- ❑ Previous Use
- ❑ Security Hardware Distributor
- ❑ Systems Integrator
- ❑ Trade Show
- ❑ Training Class
- ❑ Word of Mouth
- ❑ Other ____________________

What was your reason for buying this lock?

____

Who installed your lock?

- ❑ Contractor
- ❑ Locksmith
- ❑ Maintenance
- ❑ Security Company
- ❑ Self
- ❑ Systems Integrator
- ❑ Other ____________________

PROCEDURE 7B - DELETE ALL USER CREDENTIALS EXCEPT MASTER & MANAGER(S)

All credentials may be deleted together if you are changing everything because of, for example, suspected theft of credentials. ***Warning*:** be sure that you want to do this, because manually re-enrolling hundreds of credentials for all the users again will be time consuming at the lock keypad.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **299#** to delete all users except the Master and the Managers.

   Enter a last **#** to indicate the end of programming.

   Example of Complete Entry:

   299# #.

   You have now deleted all regular Access and Service user credentials, allowing you to re-assign those deleted credentials to the same or new users.

PROCEDURE 8B - ACTIVATE ACCESS USER CREDENTIALS

A User credential should be re-activated if it had been de-activated earlier - for instance during a users' vacation. Any user's credential that was inactive but is needed to be back in service again can be easily re-activated as described in **Procedure 13B**.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN #**
2. Enter Command **300#** to re-activate an Access user's credential; you do not need this person's PIN and/or card to do this.
3. Enter this user's ID location (001 through 300); we will use the ID location 023 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=023:

   300#023# #.

   You have now activated this Access user's credential which was temporarily de-activated.

PROCEDURE 9B - ACTIVATE MANAGER USER CREDENTIAL

A Manager user's credential should be re-activated if it had been de-activated earlier - the procedure is very similar to the above procedure of activating an Access user.

Required User Level: Master

1. Put the lock into "LearnLok™" Pushbutton Programming Mode.
2. Enter Command **301#** to re-activate a Manager user's credential; you do not need this person's PIN and/or card to do this.
3. Enter this user's ID location (001 through 300); we will use the ID location 015 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=015:

   301#015# #.

   You have now activated this Manager user's credential which was temporarily de-activated.

PROCEDURE 10B - ACTIVATE SERVICE USER CREDENTIAL

A Service user's credential (PIN) should be re-activated if it had been de-activated earlier - the procedure is very similar to the above procedure of activating an Manager or Access user.

Required User Level: Master

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **302#** to re-activate a Service user's credential; you do not need this person's PIN and/or card to do this.
3. Enter this user's ID location (001 through 300); we will use the ID location 125 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=125:

   302#125# #.

   You have now activated this Service user's credential which was temporarily de-activated.

PROCEDURE 11B - ACTIVATE ALL USER CREDENTIALS

You will need to re-activate all regular Access and Service users if you had de-activated them earlier as described in **Procedure 16B** temporarily - after a lockout or a strike, for example. After this procedure is executed, all these users will have access to the lock again.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**

2. Enter Command **398#** to re-activate all Access and Service users.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry:

   398# #.

PROCEDURE 12B - ACTIVATE / DE-ACTIVATE PASSAGE MODE

Let's assume that you had already programmed a default duration for a door to remain in Passage Mode as per **Procedure 5A, Program the Duration of the Passage Mode Period**, on page 9. This procedure 12B shows you how to activate the Passage Mode so that the lock is in free passage and no credential is required to gain entry during the duration set in **Procedure 5A**.

If your set passage duration is 6 hours for example, and you activate the Passage Mode at 1:00, it will automatically relock at 7:00. The lock can be taken in and out of Passage Mode multiple times during the six hour period but it will still automatically re-lock after six hours from the original starting period. This ensures that a lock will never remain in free Passage Mode beyond the programmed time period of 1 to 24 hours.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **399#** to re-activate all Access and Service users.
3. Enter **1#** to activate Passage Mode (or, **0#** to de-activate Passage Mode).
4. Example of Complete Entry to activate Passage Mode

   399#1# #.
5. Example of Complete Entry to de-activate Passage Mode if free passage was still active: **399#0# #**.

PROCEDURE 13B - DE-ACTIVATE ACCESS USER CREDENTIALS

An Access user's credential can be de-activated (rather than deleted) if required, for example during her/his vacation temporarily; or return, can then be easily re-activated as described in **Procedure 8B**.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **400#** to de-activate an Access user's credential; you do not need this person's PIN and/or card to do this.
3. Enter this user's ID location (001 through 300); we will use the ID location 023 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=023:

   400#023# #.

   You have now temporarily de-activated this Access user's credential.

PROCEDURE 14B - DE-ACTIVATE MANAGER USER CREDENTIALS

A Manager user's credential can be de-activated (rather than deleted) if required, for example during her/his vacation temporarily; on return, can then be easily reactivated as described in **Procedure 9B**.

Required User Level: Master

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN #**
2. Enter Command **401#** to de-activate a Manager user's credential; you do not need this person's PIN and/or card to do this.
3. Enter this user's ID location (001 through 300); we will use the ID location 015 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=015:

   401#015# #.

   You have now temporarily de-activated this Access user's credential.

PROCEDURE 15B - DE-ACTIVATE SERVICE USER CREDENTIALS

A Service user's credential if it had not expired, can be de-activated (rather than deleted) if required, for example during her/his vacation temporarily; on return, can then be easily reactivated as described in **Procedure 10B**.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **402#** to de-activate a Manager user's credential; you do not need this person's PIN and/or card to do this.
3. Enter this user's ID location (001 through 300); we will use the ID location 125 in this example.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry for user ID=125:

   402#125# #.

   You have now temporarily de-activated this Service user's credential (PIN).

PROCEDURE 16B - DE-ACTIVATE ALL USER CREDENTIALS EXCEPT MASTER AND MANAGER(S)

You may want to de-activate all regular Access and Service users temporarily rather than deleting them permanently - after a lockout or a strike, for example. After this procedure is executed, all these users will have no access to the lock until they are re-activated as described in **Procedure 11B**.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **498#** to de-activate all Access and Service users.

   Enter a last # to indicate the end of programming.

   Example of Complete Entry:

   498# #.

PROCEDURE 17B - ACTIVATE/DE-ACTIVATE LOCKOUT MODE

The Master user (and only the Master) can perform a global lockout if required, for example during a strike or fire, etc. At times like this you do not want anyone to return to work and so you should perform a global lockout temporarily. The following procedure can either de-activate & re-activate all user credentials including the managers (but not the Master user) temporarily.

Required User Level: Master

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN #**
2. Enter Command **499#** to de-activate all users.
3. Enter **1#** to activate the Global Lockout Mode (or, **0#** to de-activate Lockout Mode).
4. Example of Complete Entry to activate Lockout Mode:

   499#1# #.
5. Example of Complete Entry to de-activate Lockout Mode if Lockout was still in effect:

   499#0# #.

PROCEDURE 18B - PERFORM MANUAL DIAGNOSTICS

Use the Diagnostic command code to perform manual diagnostics of the lock to verify proper operations of the lock's electronic circuit including the green LED, red LED, buzzer and the twelve keypad/pushbuttons - 0 through 9, * and # keys.

Required User Level: Master, Manager

1. Put the lock into "LearnLok™" Pushbutton Programming Mode -> **# Master PIN (or Manager credential) #**
2. Enter Command **500#** for Diagnostics.
3. You will see a green LED and hear a high beep, followed by a red LED and a low beep to indicate that the LEDs and the buzzer's circuits are working properly.
4. Enter **1234567890*#**, in that order exactly, to test each pushbutton's electronic circuit. If every pushbutton's electronics is working correctly, you will see a green LED and hear a normal beep for each pushbutton that is pressed; this indicates successful test.
5. Example of Complete Entry:

   500#1234567890*#.

7. If you see a red LED at any time you are pressing a pushbutton, in Step 5 above, or at the end of the sequence, there could be a problem with the pushbutton electronics.
8. Try the Diagnostics again as show in Step 5 above.

Important: If you still see the red LED and/or hear the low beep, the lock has a problem. Contact Kaba's technical support at 800-849-TECH(8324) Option 5 to help diagnose and fix the problem.

***Note:* The following proceedure applies to the E-Plex 37xx locks only:**

PROCEDURE 19B - SWINGBOLT OPERATION

This operation is fairly similar to the Privacy function of a conventional lock with a physical deadbolt, but not quite! In the Swingbolt operation, any valid user can disengage, ie., override the "privacy" by entering a valid Credential and then turning the thumbturn which will retract the swingbolt down. Now the lock will behave as though it is in a "latch holdback" mode since the swingbolt is completely retracted and stays retracted, thus allowing free access without any credentials. You perform the same sequence of operations to engage, ie., re-lock by bringing the swingbolt back to its "Home" (horizontal locked) position.

- Important: the swingbolt engage (project it) and disengage (retract it) actions are strictly manual and are accomplished by flipping the thumbturn on the lock front housing. This function is neither programmable nor automatic and so you must be sure to manually re-lock if it was left in a retracted/open position.
- any user with a valid Credential can perform this function – ie., engage or disengage the swingbolt anytime.
- when the swingbolt is disengaged (retracted), it will physically stay retracted down when the door closes so that users carrying packages etc. do not have the incovenience of having to turn the thumbturn again to open the door, but simply push the door to enter without a credential.
- from the interior side of the door, any person (valid user or not) can manually disengage (retract) or engage (project) the swingbolt to unlock or lock the door.

Required User Level: Master, Manager, Access user & Service user

1. **To Disengage (retract swingbolt)**: Enter/present a valid Credential to open and the lock will flash the green LED indicating that you are a valid user and you are allowed to disengage the swingbolt to unlock. Turn the thumbturn on the lock front housing clockwise and hold. The swingbolt will fully retract down and will stay retracted, allowing you to enter the door. Let go of the thumbturn so that it will revert back to its normal horizontal (home) position but the swingbolt will stay retracted and disengaged.

2. You can **also** disengage the swingbolt using the **mechanical override key** by performing the following operation: insert the mechanical key in the lock override cylinder's vertical slit and turn it clockwise to the horizontal position. **With the key still in this horizontal position**, turn the thumbturn clockwise to disengage the swingbolt which will fully retract down and will stay retracted. Let go off the thumbturn so that it will revert back to its normal horizontal (home) position. Turn the key back to its vertical position and remove it from the lock cylinder.

Warning: Ensure that you relock the door (engage the swingbolt) when not needed; otherwise the lock will stay unlocked permanently compromising security.

3. **To Engage (project swingbolt):** This procedure is almost the same as in Step 1 above. Enter/present a valid Credential and the lock will flash the green LED indicating that you are a valid user and you are allowed to engage the swingbolt to lock back. Turn the thumbturn on the lock front housing clockwise and hold. The swingbolt will revert back up to its locked, horizontal (home) position. Let go off the thumbturn so that it will also revert back to its normal horizontal (home) position.

4. You can **also** engage the swingbolt using the **mechanical override key** by performing the following operation and the procedure is almost the same as in Step 2. above. Insert the mechanical key in the lock override cylinder's vertical slit and turn it clockwise to the horizontal position. With the key still in this horizontal position, turn the thumbturn clockwise to engage the swingbolt which will revert back up to its locked, horizontal (home) position. Let go off the thumbturn so that it will also revert back to its normal horizontal (home) position. Turn the key back to its vertical position and remove it from the lock cylinder.

Warning: Ensure that you relock the door (engage the swingbolt) when not needed; otherwise the lock will stay unlocked permanently compromising security.

BATTERY LIFE AND REPLACEMENT

The E-Plex Lock uses 4 "AA" alkaline (only) batteries. A variety of factors such as the shelf life, number of lock openings per day, if the users have been accessing the lock in card only mode or PIN and card mode, the environment, battery brand, lock settings, etc., will determine how long your lock will operate on a set of batteries. In average conditions, a set of 4AA alkaline batteries can last up to 150,000 openings.

A Low Battery condition is identified by a flash of both red and green LEDs when a valid access credential is entered/presented and the lock will still give access. During the low battery state, the lock can continue operating another 500+ openings. However, it is strongly recommended that all four alkaline batteries in the pack should be replaced as soon as possible. This is especially true in winter when the temperatures go down very low and the battery low duration is considerably shortened.

Summary of LearnLok™ Pushbutton Programming Commands

Name	Command	Description of Command	Authorization
Configure	000 # MMMMMMMM# MMMMMMMM#	'Modify Master User Access Credential (lock's activation)' (Always 8 digits)	Master
	001 # MMDDYY# MMDDYY#	'Date setup' (MM = 01 to 12; DD = 01 to 31; YY = 00 to 99)	Master
	002 # HHMM# HHMM#	'Time setup' (HH = 00 to 23; MM = 00 to 59)	Master
	004 # TT#	'Unlock time setup' (TT = 02 to 20 seconds)	Master, Mgr
	005 # TT#	'Passage Mode Timeout setup' (TT = 01 to 24 hours - duration time in hours; 00 = no time limit)	Master, Mgr
	006 # TT#	'Tamper time setup' (TT = 00 to 90 seconds)	Master, Mgr
	007 # TT#	'Tamper wrong try setup' (TT = 03 to 09)	Master, Mgr
	008 # VV#	'Buzzer volume control' (VV = 00 to 03; 00 = off; 01 = Low; 02 = Normal; 03 = High)	Master, Mgr
	009 # LL#	'Modify access length' (LL = 04 to 08 digits)	Master
	099 #	'Reset to factory default values', except access PIN length. (Master, Managers, all other users and time/date are retained if already programmed; Users are not reset.)	Master

Summary of LearnLok™ Pushbutton Programming Commands

Name	Command	Description of Command	Authorization
Add/Modify Users	100 # NNN # Card only: Present Card & then # PIN & Card: Present Card (no # after) UUUU (UUUU) # UUUU(UUUU) #	'Add/Modify User Access Credential' NNN=specific User ID location (001 to 300) UUUU(UUUU) = PIN length which can be 4 to 8 digits, depending on global PIN length setting.	Master, Mgr
	101 # NNN # Card only: Present Card & then # PIN & Card: Present Card (no # after) UUUU (UUUU) # UUUU(UUUU) #	'Add/Modify Manager Access Credential' NNN=specific User ID location (001 to 300) UUUU(UUUU) = PIN length which can be 4 to 8 digits.	Master
	102 # NNN # PIN only: UUUU (UUUU) # UUUU(UUUU) # HH #	'Add/Modify Service User Access Credential' NNN=specific User ID location (001 to 300); HH = 01 to 96 hours - duration time in hours; 00=one-time entry; 99=no expiry; UUUU(UUUU)=PIN length which can be 4 to 8 digits	Master, Mgr
Delete Users	200 # NNN#	'Delete User Access Credential'	Master, Mgr
	201 # NNN#	'Delete Manager Access Credential'	Master
	202 # NNN#	'Delete Service User Access Credential'	Master, Mgr
	299 #	'Delete All User Access Credential (except Master and Manager Users)	Master, Mgr

Summary of LearnLok™ Pushbutton Programming Commands

Name	**Command**	**Description of Command**	**Authorization**
Activate Users	300 # NNN#	'Activate User Access Credential' NNN = specific User ID location (001 to 300)	Master, Mgr
	301 # NNN#	'Activate Manager Access Credential' NNN = specific User ID location (001 to 300)	Master
	302 # NNN#	'Activate Service User Access Credential' NNN = specific User ID location (001 to 300	Master, Mgr
Delete Users	398 #	'Activate all User Credentials' (except Master, and Manager Users)	Master, Mgr
	399 # P#	'Activate / De-Activate Passage Mode' (P = 0 or 1; 0 = disable Passage Mode; 1 = enable Passage Mode)	Master, Mgr
De-activate Users	400 # NNN#	'De-Activate User Access Credential' NNN = specific User ID location (001 to 300)	Master, Mgr
	401 # NNN#	'De-Activate Manager Access Credential' NNN = specific User ID location (001 to 300)	Master
	402 # NNN#	'De-Activate Service User Access Credential' NNN = specific User ID location (001 to 300)	Master, Mgr
	498 #	'De-Activate all User Credential' (except Master, and Manager Users)	Master, Mgr
	499 # L#	'Activate / De-Activate Lockout Mode' (only Master can have access during Lockout) L = 0 or 1; 0 = disable Lockout Mode; 1 = enable Lockout Mode)	Master
Diagnostic	500 # 1234567890*#	'Manual diagnostic'	Master, Mgr
	501#	Identify if the lock is E-Plex 57xx/37xx; 56xx/36xx; LearnLok (LL) or Full Featured (FF) with software; E57xx/37xx: LL mode = 7 flashes, 1 second pause and 1 flash FF mode = 7 flashes E56xx/36xx: LL mode = 6 flashes, 1 second pause and flash FF mode = 6 flashes	Master, Mgr
Communication Startup (when used with software only)	900 #	'Communications startup'	Master, Mgr

Visual Feedback Message Definitions

Condition	**Parameters**			
	Green LED	**Red LED**	**Duration**	**Rate**
Valid pushbutton pressed	ON	OFF	1/10 sec	Once
Timeout expired	OFF	ON	1 sec	Once
Valid access credential entered/presented	ON	OFF	1 sec	Once
Access granted	ON	OFF	1/10 sec	Once
Access granted (battery low condition	ON	ON	1/10 sec	1 sec
Access denied	OFF	ON	1 sec	1 sec
Valid programming entry	ON	OFF	1 sec	Once
Invalid programming entry (including duplicate access credential)	OFF	ON	1 sec	Once
Tamper shutdown beginning	OFF	ON	2 sec	Once
Tamper shutdown state	OFF	ON	1 sec	10 sec
Tamper shutdown ending	ON	OFF	2 sec	Once
*Communication starting	ON	OFF	1 sec	Once
*Communication ending	ON	OFF	1 sec	Once
*Communication aborted	OFF	ON	1 sec	Once
*Communication in progress	ON (Alternate)	ON (Alternate)	1/10 sec	1 sec
Deadbolt/Thumbturn Privacy Activated	OFF	ON	1 sec	Once
Deadbolt/Thumbturn Privacy de-activated	ON	OFF	1 sec	Once
Hard Reset sequence progress	ON (Alternate)	ON (Alternate)	1/2 sec	Continuously
Hard Reset sequence ended successfully	ON	OFF	2 sec	Once
Hard Reset sequence failed	OFF	ON	2 sec	Once

**When used with the E-Plex Maintenance Unit (M-Unit) handheld and software only*

User ID List Sample Table

User ID #	**Access Credential** (PIN and/or Card #)	**User Name**	**User Type** (A=Access, S=Service, M=Manager)
001			
002			
003			
004			
005			
006			
007			
008			
009			
010			
011			
012			
013			
014			
015			
016			
017			
018			
019			
020			
021			
022			
023			
024			
025			
026			
027			

User ID List Sample Table

User ID #	**Access Credential** (PIN and/or Card #)	**User Name**	**User Type** (A=Access, S=Service, M=Manager)
028			
029			
030			
031			
032			
033			
034			
035			
036			
037			
038			
039			
040			
041			
042			
043			
044			
045			
046			
047			
048			
049			
050			
051			
052			
053			
054			

User ID List Sample Table

User ID #	**Access Credential** (PIN and/or Card #)	**User Name**	**User Type** (A=Access, S=Service, M=Manager)
055			
056			
057			
058			
059			
060			
061			
062			
063			
064			
065			
066			
067			
068			
069			
070			
071			
072			
073			
074			
075			
076			
077			
078			
079			
080			
081			

User ID List Sample Table

User ID #	**Access Credential** (PIN and/or Card #)	**User Name**	**User Type** (A=Access, S=Service, M=Manager)
082			
083			
084			
085			
086			
087			
088			
089			
090			
091			
092			
093			
094			
095			
096			
097			
098			
099			
100			
↓↓↓			
300			

Note: You can upgrade from the "LearnLok™" keypad programming functions to a less labor intensive way of programming and managing the locks & users by using Kaba's optional PC based software kit: the "E-Plex Enterprise" software.

For more information, please go to Kaba Access Control's website at www.kaba-adsamericas.com

Notes

Notes

KABA®

BEYOND SECURITY

Kaba Acess & Data Systems Americas
2941 Indiana Avenue
Winston-Salem, NC 27105 USA
Tel: (800) 849-8324 (336) 725-1331
Fax: (800) 346-9640 (336) 725-3269

www.kaba-adsamericas.com