34K2 SERIES

GRADE 1 CYLINDRICAL ELECTRONIC LOCK

CODE AND CARD USER MANUAL

Hager Companies
139 Victor Street
St. Louis, MO 63104
(800) 325-9995
(800) 782-0145 (FAX)
www.hagerco.com

Rev 2, 9/17

Table of Contents

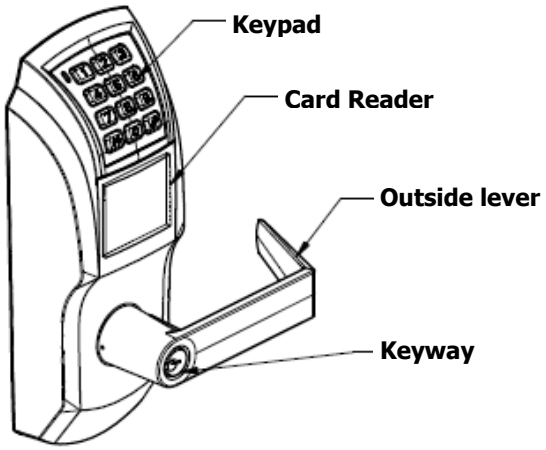
SAVE THIS USER MANUAL FOR FUTURE REFERENCE.

1. OVERVIEW

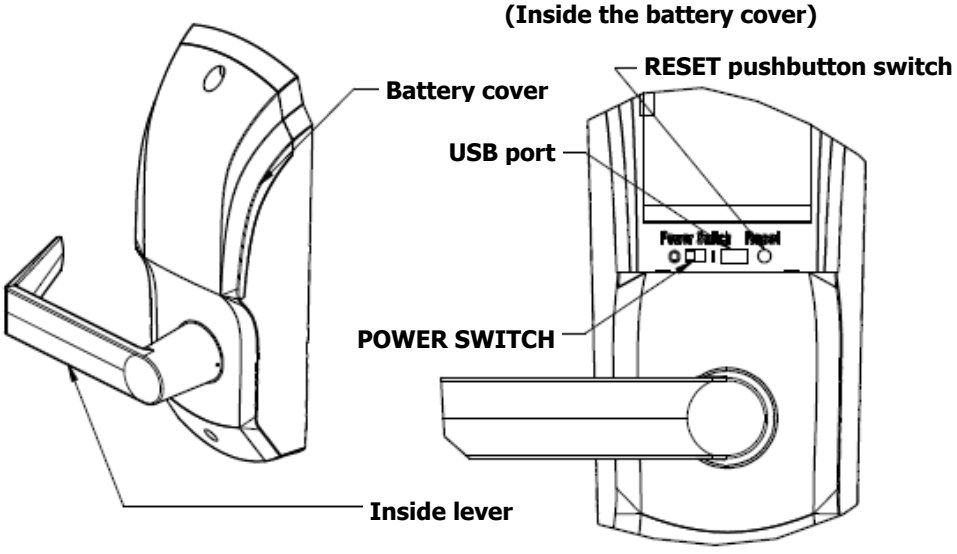
NOTE: This lockset has audit trail capability built in. To utilize this feature, purchase the 34K2 Software Kit, component 2-639-6001. The 34K2 Software Kit comes with a mini-USB cable, software CD, RFID card reader, and an instruction booklet.

READ THIS USER MANUAL BEFORE USING THE LOCK

Exterior Escutcheon



(Inside the battery cover)



2. GETTING STARTED

Please follow these steps when setting up a new lock.

1. Install the lock onto the door. Please refer to Installation Instructions I-LS02110 for more information.
2. Rotate the inside lever. Motion should be smooth and the latch should retract.
3. Insert the key into the keyway and rotate the key. Motion should be smooth and the latch should retract.
4. Install new alkaline batteries and toggle the POWER SWITCH to the **|** position.
5. The lock will be indicated by 3 long beeps with a blinking red light, enter the 12 digit RTC time followed by #. (Refer 7.3)
6. **YOU MUST MODIFY FACTORY MASTER CODE** to your own Master code (always eight digits) before you start to program the lock. (Refer 7.2)
7. Add Access Credentials as desired. (Refer 8.1)

NOTE: To use access codes, enter the number followed by the # button

3. FUNCTIONS DEFINED

STATUS OF THE LOCK:

- **Factory Mode** - Refer unit 7.1. The lock will stay in Factory Mode until the RTC is set and a new Master Code has been entered.
- **Access Mode** - Entry registered user codes to open the lock.
  E.g. If the user code is 1234, you should enter [1234] and [#], the lock will be opened.
- **Programming Mode** - You need Master code to program all the parameters.
  E.g. If the Master code is 12345678, you should enter [∗12345678∗], the lock will enter into Programming Mode and wait for the next part of the command.

Please refer to the default values of the programmable parameters.

PARAMETERS	FACTORY DEFAULT VALUES
Lock State	Locked and Un-programmed
Master Code	12345678
Credentials Status	Activated
Re-lock	Activated
Re-lock time	5 seconds
Passage Mode	De-activated
Lock Tamper Times	1
Alarm Time	30 seconds
Number of Wrong Entries (until suspend)	3
Suspend Time	1 minute
Lockout mode	De-activated
Buzzer Volume Control	High

4. SWITCHES

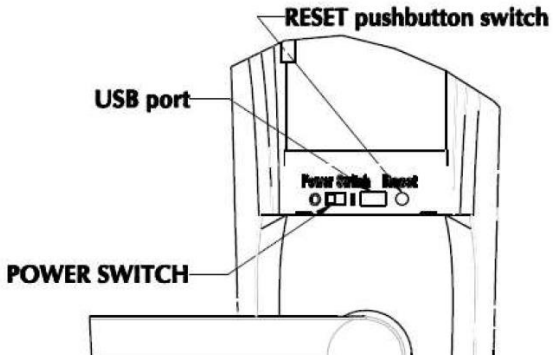
4.1. Power Switch

The Power Switch is located in the battery compartment. It is labeled "POWER SWITCH" on the escutcheon. Sliding the switch to the "I" position turns the power on. Sliding the switch to the "O" position turns the power off.

WARNING:	Turning off the power could require setting the RTC time when power is turned back on. This will be indicated by 3 long beeps with a blinking red light. If 2 beeps with a green light are indicated instead, then no further action is required.

4.2. Reset Switch

The Reset Switch is a recessed pushbutton located in the battery compartment. It is labeled "RESET" on the escutcheon. To press the button, use a thin object, such as a pin tip, to press and hold the button for the reset procedure in 7.4.



5. BATTERIES

You can expect a minimum of 20,000 openings on a set of 4 AA Alkaline batteries. This can be affected by many factors such as lock settings, environment, openings per day, shelf life, battery brand, etc.

LOW BATTERY ALARM:

In a low battery condition, after credentials are entered, the alarm buzzer will beep 10 times with 10 blinks of the red light. Pressing any key will stop the low battery alarm. The batteries must be replaced as soon as possible.

HOW TO REPLACE BATTERIES:

1. Remove the battery cover
2. Remove all 4 old batteries
3. Install 4 new AA alkaline batteries. Make sure the batteries are installed in the correct orientation
4. Reinstall the battery cover

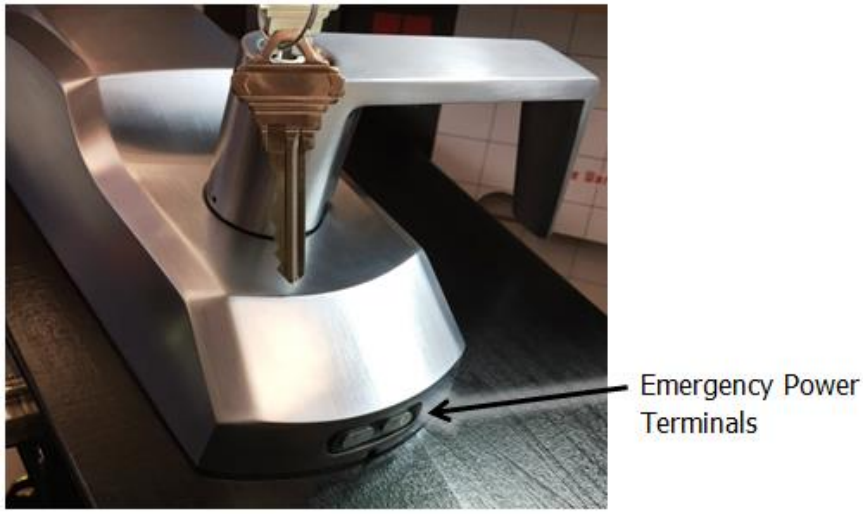
NOTE:

- Only use New AA alkaline batteries
- DO NOT mix old and new batteries! Danger of Explosion if the batteries are incorrectly replaced!
- If three long beeps with a red light are indicated when power is returned, then the RTC will need to be set (Refer 7.3). If 2 beeps with a green light are indicated instead, then no further action is required.

EXTERIOR EMERGENCY POWER:

When the battery power is too low to operate the lock or the POWER SWITCH is turned off, the door can only be accessed using the mechanical key or 9V emergency power to energize the lock. The input terminal of the 9V emergency power is located on the bottom side of the exterior housing. Use a 9V battery by pressing the battery terminals against the lock terminals (polarity is not important). This will give the lock power to unlock the door.

NOTE: To use, press the 9V battery terminals against the emergency power terminals (this will relock the door if unlocked) and enter code to gain entry. This will leave the door unlocked. To relock, remove the battery and reapply to terminals.



6. LED REFERENCE

No.	Condition	Beeps	Lights
1	Turn on Power	2 Short	2 Green
2	Lock or Unlock Door	1 Short	1 Green
3	Suspend Keypad Operation	1 Long	1 Red
4	Tamper Alarm	Rapid Beeps	Red Fast Blinks
5	Enter Programming Mode	1 Middle, 2 Short	3 Green
6	Exit Programming Mode	2 Short, 1 Middle	3 Green
7	Setting Successful	1 Middle	1 Green
8	Wrong Entry or Setting Failed	3 Short	3 Red
9	Enter Connection Mode	1 Long	1 Green
10	Hard Reset Successful	1 Long	1 Green
11	Low Battery	10 Middle	10 Red
12	Set Real Time Clock (RTC)	3 Long	3 Red

7. PROGRAMMING LOCK PARAMETERS

7.1. Factory Mode – The lockset is in Factory Mode until the RTC is set and a new Master Code has been entered.

7.2. Modify Master Code

New locks start with a Default Master code of "12345678", you can use Default Master Code to unlock door before any setting. You must change the Master code before continuing lock setup. A Master code is always 8 digits.

Use the code below to set a new Master Code:

[＊] [original Master code] [＊] [01] [＊] [new Master code] [＊] [new Master code] [＊]

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.3. RTC (Real Time Clock) Setting

After installing the batteries for a new lock, or repowering by on/off switch, you will hear 3 long beeps with a blinking red light, it means the lock time must be entered first. Please complete the following steps:

1. Enter the 12 digit RTC time. It will mean **YY** (year), **MM** (month), **DD** (day), **hh** (hour), **mm** (minute), and **ss** (second) followed by #.
   E.g.: If you want to set the RTC time to 2015-05-27, 15:30 00", you should enter **[**150527153000**]** followed by **[**#**]**.
2. If the setting is successful, the lock will beep once with a green light.
3. An incorrect entry will result in 3 beeps with a blinking red light. Repeat step 1 to correctly enter the RTC time.

NOTE: Once the initial RTC has been set, you can change the RTC time after the lock has been setup. Follow the code sequence below.

[＊] [Master code] [＊] [50] [＊] [YYMMDDhhmmss] [＊]

WARNING! When the RTC is changed, the Passage Mode Active Period and all Service Codes will be reset.

7.4. Reset to Factory Default Settings

Soft Reset- All setting values will return to factory default, except Master Code and event logs.
Use the code below to Reset:

[＊] [Master code] [＊] [00] [＊] [29] [＊]

Hard Reset-All values will return to factory default and the event logs will be deleted.
Follow the steps below to reset the unit:

1. **Remove the battery cover.**
2. **Turn off the POWER SWITCH (refer to section 4.1).**
3. **Press and Hold the RESET button (refer to section 4.2).**
4. **Turn on the POWER SWITCH and wait for 12 seconds.**
5. **After Buzzer beeps once with a green light, release the RESET button.**
   If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
   *The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

NOTE:

- The setting will fail if the RESET button is released during step 4. If this happens, repeat steps 2 through 5.

7.5. Setting Re-lock Delay Time

Use the code below to set the Re-locking Delay Time:

[＊] [Master or Manager code] [＊] [00] [＊] [05] [＊] [SS] [＊]

SS: Re-locking delay time; Range is 00-99 seconds; DEFAULT is 5 seconds

SS=00 will deactivate the re-lock function

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.6. Setting Passage Mode Active Period (Resets when RTC is changed, see Section 7.14 to activate/deactivate)

You can set a time period where the Passage Mode is active. In Passage Mode, the lock requires no credentials to gain entry.

Use the code below to set the Start / End times where Passage Mode is active:

[＊] [Master or Manager code] [＊] [00] [＊] [06] [＊] [hhmmHHMM] [＊]

hh: Starting hour to activate Passage Mode; Range 00-23 (24 hour clock)

mm: Starting minute to activate Passage Mode; Range 00-59

HH: Ending hour to deactivate Passage Mode; Range 00-23

MM: Ending minute to deactivate Passage Mode; Range 00-59

E.g.: To activate Passage Mode from 08:00 am to 05:00 pm, enter the following:

[＊] [Master code] [＊] [00] [＊] [06] [＊] [08001700] [＊]

If you do not require a certain time period for passage mode, enter 00000000 for the time code.

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

NOTE:

- During Passage Mode, ONLY programming functions can be operated. A green light will flash 3 times as a reminder every time another credential is entered.

7.7. Setting Tamper Attempt Limit

This code sets the number of attempts to tamper with the lock before the alarm sounds. Use the code below to set the number of attempts triggering the alarm:

[＊] [Master or Manager code] [＊] [00] [＊] [07] [＊] [TT] [＊]

TT: Tamper Attempts; Range 00-10; Default is 01

TT=00 deactivates the alarm function

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.8. Setting Tamper Alarm Duration

Use the code below to set the duration of the Tamper Alarm in seconds:

[＊] [Master or Manager code] [＊] [00] [＊] [03] [＊] [SS] [＊]

SS: Continuous Alarm Time; Range 10-99 seconds; Default is 30 seconds

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

NOTE:

- You cannot make any operations on the lock during the alarm period
- You can stop the alarm situation by turning off the POWER SWITCH or removing the

7.9. Setting Wrong Entry Attempt Limit

This code sets the limit to the number of credential entry attempts before the lock goes into suspend mode. Keypad and RFID card suspension are both independent and do not affect each other. For example, when the keypad is suspended, the lock can still be unlocked using RFID card. But when the lock is in Double Credential Access Mode, the lock cannot be unlocked if one of the functions is suspended.

Use the code below to set the Entry Attempt Limit:

[＊] [Master or Manager code] [＊] [00] [＊] [08] [＊] [TT] [＊]

TT: Wrong Entry Attempt Limit; Range 00-10; Default is 03

TT=00 deactivates the suspend function

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.10. Setting Suspend Duration

This code sets the time duration (in minutes) for the Suspend Keypad or RFID card reader due to consecutive wrong entry attempts. Use the code below to set the suspend duration:

[＊] [Master or Manager code] [＊] [00] [＊] [04] [＊] [MM] [＊]

MM: Suspend Duration in minutes; Range 01-60 minutes; Default is 01 minute

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

NOTE:

- To return to normal mode during a suspend mode period, turn off the POWER SWITCH and turn on again after 3 seconds.
- In Suspend Mode, all credential entries will not work. Each attempt will be accompanied by a red light blinking 3 times.

7.11. Setting Buzzer Volume

Use the following code to set the Buzzer Volume:

[＊] [Master or Manager code] [＊] [00] [＊] [09] [＊] [BB] [＊]

BB: Buzzer Volume; 00=mute; 01=low volume; 02=high volume; Default is 02

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.12. Setting Keypad Entry Mode

This code toggles the Keypad Entry Mode between **Normal Mode** and **Fuzzy Mode**. Use the following code to toggle the Keypad Entry Mode:

[＊] [Master code] [＊] [00] [＊] [10] [＊]

The Keypad Entry Mode is in **Normal Mode** by default. Once the above code is entered for the first time, it will toggle into **Fuzzy Mode**. Entering it another time will toggle it back to **Normal Mode**, and so forth.

Normal Mode: Allow a user to enter access code at a maximum of 8 digits. If the access code is over 8 digits, the buzzer will beep 3 times with a red light flashing 3 times.

Fuzzy Mode: No limit to the number of digits. This mode allows a user to enter a random string of numbers that includes the user's complete access code. This code will grant access as if the user entered just their given access code.

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.13. Lockout Mode (Activate / Deactivate)

You many need to use Lockout Mode, for example, during a fire or fire drill when you do not want anyone to return to their office. This function will deactivate all Access Credentials that are active, including Manager Credentials, but excluding the Master Code.

Use the code below to activate or deactivate lockout mode:

[＊] [Master code] [＊] [60] [＊] [P] [＊]

P=0: Deactivate Lockout Mode

P=1: Activate Lockout Mode

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

NOTE:

- In Lockout Mode, user access credentials do not work. Only the Master Code will grant access. If a regular access credential is entered, the buzzer will beep three times with a blinking red light.
- Lockout Mode overrides Passage Mode.

7.14. Passage Mode (Activate / Deactivate)

A Passage Mode activation period needs to be programed before this mode can be activated. See **7.6, Setting Passage Mode Active Period** for details. This code activates or deactivates the Passage Mode, so that the lock can operate in free passage for a period of time every day, where no credentials are required to gain entry.

Use the code below to activate or deactivate passage mode:

[＊] [Master or Manager code] [＊] [61] [＊] [P] [＊]

P=0: Deactivate Passage Mode

P=1: Activate Passage Mode

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.15. Double-Credential Access Mode (Activate / Deactivate)

If the lock is to be used at a site requiring higher security, for example confidential archives, you can activate the Double-Credential Access Mode so any user wishing to unlock the door will have to first present the card then input the code to unlock.

Use the code below to activate or deactivate double credential access mode:

[＊] [Master code] [＊] [80] [＊] [P] [＊]

P=0: Deactivate Double Credential Access Mode

P=1: Activate Double Credential Access Mode

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

7.16. Activate Audit Trail Connection Mode

NOTE: Audit trail can be accessed by purchasing 34K2 Software Kit (P/N 2-639-6001).

Connection Mode should be activated if you want to make a connection between the lock and PC software-SecurPass.

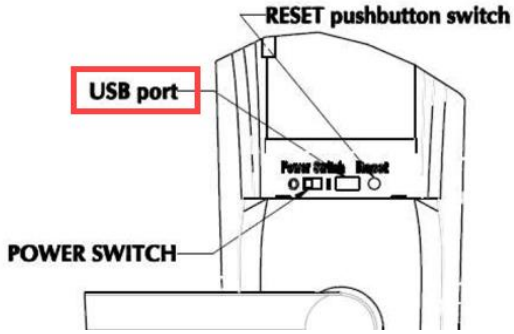
To activate the audit trail connection, complete the steps below:

1. Open the PC software-SecurPass 34K.
2. Connect the lock to the PC via the USB adaptor cable. The USB port on the lock is located under the battery cover.
3. Use the code below to activate the Connection Mode for the lock:

   [＊] [Master code] [＊] [90] [＊] [01] [＊]

   If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

   *The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*
4. After successfully activating the Connection Mode, the red light will turn on. You can start using the PC software to communicate with the lock. For operation and parameter settings, refer to the software instructions that are supplied with the software disc. Connection Mode can be deactivate by either waiting 5 minutes or until the # button is pressed.



8. Programming Access Credentials

Each time you add user access to a door, you must program the lock using the keypad with Access Credentials for this user. The user maybe a Manager user, an Access user, and/or a Service user. The

access credentials can be card only, PIN only, or PIN followed by card for Manager and Regular Access users (Service users must be PIN only). The Master user's access will always be an 8-digit PIN only. Existing user credentials can easily be deleted by the keypad.

The maximum quantity of all Access Credentials is 500 excluding Master Code. Each Access Credential should be unique. Trying to enroll with an existing access credential will fail.
Access Codes must be 4-8 digits long.

HOW to Access the Lock:

- **Credential of the Master User:** PIN code only. Enter the codes followed by # button.
- **Credential of a Manager User or a Regular User:**
  (a) Code only access (4-8 digits). Enter the codes followed by # button.
  (b) Card only access. Present the user's card close to the card reader of lock, the green LED will flash indicating that the card has been read.
  (c) Card & Code access. Present the user's card close to the card reader of lock, the green LED will flash indicating that the card has been read, enter the codes followed by # button.
- **Credential of a Service User:** Code only access (4-8 digits). Enter the codes followed by # button.
  The expiration is either (a) 1 through 24 hours access, or (b) one time entry only.

There are four levels of access users described below:

ITEMS	Authority of the different user levels			
	Master	**Manager User**	**Regular User**	**Service User**
Programming Mode* (Does not include all functions)	Y	Y	N	N
During "Deactivate all access Credentials"	Y	Y	N	N
During Lockout Mode	Y	N	N	N

Y – Allowed to operate lock; **N** – Not allowed to operated lock

You should always maintain an accurate list of User ID and assignments to avoid any confusion in the future should you need to either delete or deactivate these users. A **User ID Log** has been supplied in Appendix A to help organize and keep track of users. A similar data base should be used for proper credential maintenance of all your users in the facility.

*A Manager User can program all lock functions except:

- RTC setting
- Modify master code
- Reset lock to selected default values
- Setting Keypad entry mode
- Adding/Deleting/Activating/Deactivating another Manager user
- Activate/Deactivate Lockout Mode
- Activate/Deactivate Double-Credential Access Mode
- Activate Audit trail Connection Mode

8.1. Add / Modify User Access Credential

This code adds or modifies the credentials of a Regular User using either a Master code or Manager Credential. The Master or Manager can chose either code only or both code and card credential, depending on how the code is entered. When code only is set, that user can only unlock the lock using their code; when card and code is set, that user can unlock the lock using either one of the credentials. When the lock is set in "Double-Credential Access Mode", that user must first present the card, then input the code to unlock.

Use the following code to add or modify user access credentials:
[＊] [Master or Manager code] [＊] [10] [＊] [LLL] [＊] [Present card (optional)] [AAAAAAAA] [＊] [AAAAAAAA] [＊]
LLL: User ID; Range 001-500; Type: Regular Access User
AAAAAAAA: User Access Code from 4 to 8 digits

You can continuously add Access Credentials in this function by repeating the [*] [User ID] [*] [Present card (optional)] [access code] [*] [access code] [*] until finished by hitting [#].
E.g.: If there are 3 user Access Credentials that need to be added (ID#1: 1234; ID#2: 456789; ID#3: 00987654 and a user card), then the complete entry sequence will be as follows:
[＊] [Master or Manager code] [＊] [10] [＊] [1] [＊] [1234] [＊] [1234] [＊] <<beep>> (Press **[#]** to exit immediately or go on to enter the next ID) **[2] [＊] [456789] [＊] [456789] [＊] <<beep>> [3] [＊] [Present card] <<beep>> [00987654] [＊] [00987654] [＊]** and so forth.

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*
If a wrong entry is made during continuous entry, the buzzer will beep three times with a blinking red light. After this, you can continue entering users from the last ID that successfully finished.

8.2. Add / Modify Manager Access Credentials

Use the following code to add or modify manager access credentials:
[＊] [Master code] [＊] [11] [＊] [LLL] [＊] [Present card (optional)] [AAAAAAAA] [＊] [AAAAAAAA] [＊]
LLL: User ID; Range 001-500; Type: Manager
AAAAAAAA: Manager Access Code from 4 to 8 digits
E.g.: For a Manager Access Code of 123456, a user card, and a Manager ID 1, the complete entry will be as follows:
[＊] [Master code] [＊] [11] [＊] [1] [＊] [Present card] [123456] [＊] [123456] [＊]
The Manager User Credentials can be continuously added as shown in 8.1 Add / Modify User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.3. Add / Modify Service User Access Codes

Use the following code to add or modify service user access codes:

[＊] [Master or Manager code] [＊] [12] [＊] [LLL] [＊] [AAAAAAAA]
[＊] [AAAAAAAA] [＊] [EE] [＊]
LLL: User ID; Range 001-500; Type: Service User
AAAAAAAA: Service User Access Code from 4 to 8 digits
EE: Available period of time for Service Access Code; Range 00-24 hours
EE=00 will result in one time use
E.g.: For a Service User Access code of 7777, ID of 3, and available period of time at 4 hours, the complete entry will be as follows:
[＊] [Master or Manager code] [＊] [12] [＊] [3] [＊] [7777] [＊] [7777] [＊] [4] [＊]
The Service User Codes can be continuously added as shown in 8.1 Add / Modify User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.4. Delete User Access Credentials

Use the following code to delete user access credentials:
[＊] [Master or Manager code] [＊] [20] [＊] [LLL] [＊]
LLL: User ID; Range 001-500; Type: Regular Access User
User Access Credentials can be continuously deleted with this function.
E.g.: To delete User ID #1, #5, & #9, use the entry below:
[＊] [Master or Manager code] [＊] [20] [＊] [1] [＊] <<beep>> [5] [＊] <<beep>> [9] [＊], and so forth.

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.5. Delete Manager Access Credentials

Use the following code to delete manager access credentials:
[＊] [Master code] [＊] [21] [＊] [LLL] [＊]
LLL: User ID; Range 001-500; Type: Manager
Manager Access Credentials can be continuously deleted with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.6. Delete Service User Access Codes

Use the following code to delete service user access codes:
[＊] [Master or Manager code] [＊] [22] [＊] [LLL] [＊]
LLL: User ID; Range 001-500; Type: Service User
Service User Access Codes can be continuously deleted with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.
*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.7. Delete All Access Credentials

Use the following code to delete all access credentials except Managers:

[＊] [Master or Manager code] [＊] [23] [＊] [29] [＊]

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.8. Activate User Access Credentials

If a user credential has been deactivated for a period of time, such as during a vacation, it can be reactivated using this function. User credential that will be needed again in the future should be deactivated rather than deleted.

Use the following code to activate user access credentials that have been deactivated:

[＊] [Master or Manager code] [＊] [30] [＊] [LLL] [＊]

LLL: User ID; Range 001-500; Type: Regular Access User

User Access Credentials can be continuously activated with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.9. Activate Manager Access Credentials

If a manager credential has been deactivated for a period of time, such as during a vacation, it can be reactivated using this function. Manager credentials that will be needed again in the future should be deactivated rather than deleted.

Use the following code to activate manager access credentials that have been deactivated:

[＊] [Master code] [＊] [31] [＊] [LLL] [＊]

LLL: User ID; Range 001-500; Type: Manager

Manager Access Credentials can be continuously activated with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.10. Activate Service User Access Codes

If a service user code has been deactivated for a period of time, it can be reactivated using this function. Use the following code to activate service user access codes that have been deactivated:

[＊] [Master or Manager code] [＊] [32] [＊] [LLL] [＊]

LLL: User ID; Range 001-500; Type: Service User

Service User Access Codes can be continuously activated with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.11. Activate All User Access Credentials

All users may need to be activated if a whole group was deactivated for some reason, such as a company trip. Use the code below to reactivate all regular access and service user access codes that are not active.

[＊] [Master or Manager code] [＊] [33] [＊] [29] [＊]

If the setting is successful, then the buzzer will beep once red switching to a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.12. Deactivate User Access Credentials

During events, such as a user's vacation, user access credentials can be deactivated. Additionally, you might want to create a set of user access credentials available to be assigned in the future which are not currently active.

Use the following code to deactivate user access credentials:

[＊] [Master or Manager code] [＊] [40] [＊] [LLL] [＊]

LLL: User ID; Range 001-500; Type: Regular Access User

User Access Credentials can be continuously deactivated with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.13. Deactivate Manager Access Credentials

During events, such as a manager's vacation, manager access credentials can be deactivated. Additionally, you might want to create a set of manager access credentials available to be assigned in the future which are not currently active.

Use the following code to deactivate manager access credentials:

[＊] [Master code] [＊] [41] [＊] [LLL] [＊]

LLL: User ID; Range 001-500; Type: Manager

Manager Access Credentials can be continuously deactivated with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.14. Deactivate Service User Access Codes

If for some reason, a service user's access needs to be suspended for a period of time; their access codes should be deactivated. Additionally, you might want to create a set of service user access codes available to be assigned in the future which are not currently active.

Use the following code to deactivate service user access codes:

[＊] [Master or Manager code] [＊] [42] [＊] [LLL] [＊]

LLL: User ID; Range 001-500; Type: Service User

Service User Access Codes can be continuously deactivated with this function as shown above in 8.4. Delete User Access Credentials until finished by hitting [#].

If the setting is successful, then the buzzer will beep once with a green light. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.15. Deactivate All User Access Credentials

All users may need to be deactivated for some reason, such as a company trip. Use the code below to deactivate all regular and service user access credentials:

[＊] [Master or Manager code] [＊] [43] [＊] [29] [＊]

If the setting is successful, then the buzzer will beep once with a red light switching to green. If the setting fails, then the buzzer will beep three times with a blinking red light.

*The setting sequence will be exited if the idle time is more than 20 seconds, or **[#]** is pressed to exit immediately.*

8.15.1. Programming Code Summary

	FUNCTION NAME	COMMAND STRUCTURE																RANGE
LOCK SETUP SETTINGS	Tamper Alarm Duration	*	Master or Manager Code	*	00	*	03	*	SS	*								SS: 10-99
	Suspend Duration	*	Master or Manager Code	*	00	*	04	*	MM	*								MM: 01-60
	Relock Delay Time	*	Master or Manager Code	*	00	*	05	*	SS	*								SS: 00-99
	Passage Mode Active Period	*	Master or Manager Code	*	00	*	06	*	hhmmHHMM	*								
	Tamper Attempts Limit	*	Master or Manager Code	*	00	*	07	*	TT	*								TT: 00-10
	Wrong Entries Attempt Limit	*	Master or Manager Code	*	00	*	08	*	TT	*								TT: 00-10
	Buzzer Volume	*	Master or Manager Code	*	00	*	09	*	BB	*								BB: 00-02
	Soft Reset to Factory Default	*	Master Code	*	00	*	29	*										
	Set Real Time Clock (RTC)	*	Master Code	*	50	*	YYMMDD hhmmss	*										
	Modify Master Code	*	Master Code	*	01	*	New Master Code	*	New Master Code	*								Code: 8 digits
ADD / DELETE	Add/Modify User Access Credential	*	Master or Manager Code	*	10	*	LLL	*	Present Card	beep	New User Code	*	New User Code	*				LLL: 001-500 code: 4-8 digits
	Add/Modify Manager Access Credential	*	Master Code	*	11	*	LLL	*	Present Card	beep	New Manager Code	*	New Manager Code	*				LLL: 001-500 code: 4-8 digits
	Add/Modify Service User Access Code	*	Master or Manager Code	*	12	*	LLL	*	New Service Code	*	New Service Code	*	EE	*				LLL: 001-500 code: 4-8 digits EE: 00-24
	Delete User Access Credential	*	Master or Manager Code	*	20	*	LLL	*										LLL: 001-500
	Delete Manager Access Credential	*	Master Code	*	21	*	LLL	*										LLL: 001-500
	Delete Service User Access Code	*	Master or Manager Code	*	22	*	LLL	*										LLL: 001-500
	Delete All Access Credentials	*	Master or Manager Code	*	23	*	29	*										
ACTIVATE / DEACTIVATE	Activate User Access Credential	*	Master or Manager Code	*	30	*	LLL	*										LLL: 001-500
	Activate Manager Access Credential	*	Master Code	*	31	*	LLL	*										LLL: 001-500
	Activate Service User Access Code	*	Master or Manager Code	*	32	*	LLL	*										LLL: 001-500
	Activate All Access Credentials	*	Master or Manager Code	*	33	*	29	*										
	Deactivate User Access Credential	*	Master or Manager Code	*	40	*	LLL	*										LLL: 001-500
	Deactivate Manager Access Credential	*	Master Code	*	41	*	LLL	*										LLL: 001-500
	Deactivate Service User Access Code	*	Master or Manager Code	*	42	*	LLL	*										LLL: 001-500
	Deactivate All Access Credentials	*	Master or Manager Code	*	43	*	29	*										
MODES	Lockout Mode (Activate / Deactivate)	*	Master Code	*	60	*	P	*										P=0: Deactivated P=1: Activated
	Passage Mode (Activate / Deactivate)	*	Master or Manager Code	*	61	*	P	*										P=0: Deactivated P=1: Activated
	Double-Credential Access Mode (Activate / Deactivate)	*	Master Code	*	80	*	P	*										P=0: Deactivated P=1: Activated
	Keypad Mode (Normal/Fuzzy)	*	Master Code	*	00	*	10	*										Toggle: Normal/Fuzzy
	Activate Audit Trail Connection	*	Master Code	*	90	*	01	*										

9. TROUBLESHOOTING

Problem	Possible Cause	Solution
Lock does not function when a valid Access Credential is entered or the lock beeper does not sound	The battery cable may not be properly connected. The batteries might be inserted incorrectly. The battery power might be too low to operate the lock. The POWER SWITCH might be turned off. Lock might be in Lock Out Mode or locked out due to attempt limits. If the red light blinks while entering the code, then this is the case.	Check that the battery cable is connected. Check batteries to verify they are inserted correctly. Makes sure the proper terminals are aligned. Replace the batteries. Turn on the POWER SWITCH. Wait until time out period ends and try again (up to 99 seconds for tamper attempt, up to 60 minutes for wrong code attempts). Contact Security Administrator if lock does not recover in a timely manner.
The PC software cannot connect to the lock.	Connection Mode might not be activated on the lock. The USB cable may not be connected properly. The COM port on the PC may be incorrect. The proper drivers for the USB cable may not be loaded on the PC.	Activate Connection Mode on the lock (page 11). Check USB cable to verify proper connection. Verify that the proper COM is selected in the software. Refer to Windows Driver Manual to determine and install proper drivers. (Manual can be found on the software CD)
User Code does not activate the lock	Double Credentials is Active User has been deactivated User has been deleted	Modify the user by adding a card to their credentials (8.1 or 8.2). This will require a new code. Activate the user (8.8 or 8.9) Add the user (8.1 or 8.2)

FCC STATEMENTS

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.

APPENDIX A – USER ID LOG

It is recommended that Managers, Service User, and Regular Access Users be grouped together with like users to ease finding, adding, and managing users. Below is a sample table to aid in grouping users by type.

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

028			Manager	
029			Manager	
030			Manager	
SERVICE USERS				
031			Service User	
032			Service User	
033			Service User	
034			Service User	
035			Service User	
036			Service User	
037			Service User	
038			Service User	
039			Service User	
040			Service User	
041			Service User	
042			Service User	
043			Service User	
044			Service User	
045			Service User	
046			Service User	
047			Service User	
048			Service User	
049			Service User	
050			Service User	
GENERAL ACCESS USERS				
051			General Access User	
052			General Access User	
053			General Access User	
054			General Access User	
055			General Access User	
056			General Access User	
057			General Access User	
058			General Access User	
059			General Access User	

060			General Access User	
061			General Access User	
062			General Access User	
068			General Access User	
069			General Access User	
070			General Access User	
071			General Access User	
072			General Access User	
073			General Access User	
074			General Access User	
075			General Access User	
076			General Access User	
077			General Access User	
078			General Access User	
079			General Access User	
080			General Access User	
081			General Access User	
082			General Access User	
083			General Access User	
084			General Access User	
085			General Access User	
086			General Access User	
087			General Access User	
088			General Access User	
089			General Access User	
090			General Access User	
091			General Access User	
092			General Access User	
093			General Access User	
094			General Access User	
095			General Access User	
↓ ↓ ↓				
500			General Access User	