

# SecurPass34K v1.5.0.0 Software User Guide



**34K1**



**34K2**

## Table of Contents

|  |    |
|--|----|
| System Requirements.....                                   | 1  |
| Application / Installation Functions.....                  | 1  |
| Lock Setup Overview.....                                   | 2  |
| Management System Setup.....                               | 2  |
| Management Functions.....                                  | 3  |
| Login Screen.....  | 3  |
| Main Menu.....   | 4  |
| Programming Users & Lock Configurations                    |    |
| • Buildings.....   | 4  |
| • Locks.....   | 5  |
| • Lock Groups.....   | 6  |
| • Lock Group Assignment.....                               | 6  |
| • User Management.....                                     | 7  |
| Transferring Users & Lock Configuration to Lock            |    |
| • Connect to Lock.....                                     | 9  |
| • Lock Configuration Transfer (Transfer Data to Lock)..... | 9  |
| Utility Functions  |    |
| Audit Trail Retrieval.....                                 | 11 |
| Managing Your Database.....                                | 12 |
| Date Time Sync.....  | 14 |
| Download Configuration.....                                | 14 |
| Changing Software Password.....                            | 14 |

All rights reserved. Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of Hager. Hager reserves the right to change or improve its products and to make changes in the content of this manual without obligation to notify any person or organization of such changes or improvements. Go to [www.hagerco.com](http://www.hagerco.com) for current updates and supplemental information concerning the use of this product.

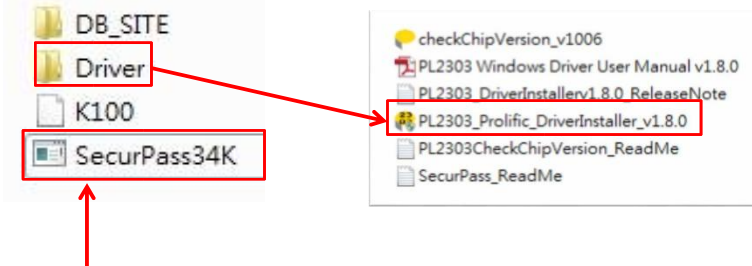
Hager® the Hager logo are trademarks of Hager Companies, Inc., registered in the USA and other countries. These trademarks may not be used without the express permission of Hager.

### System Requirements:

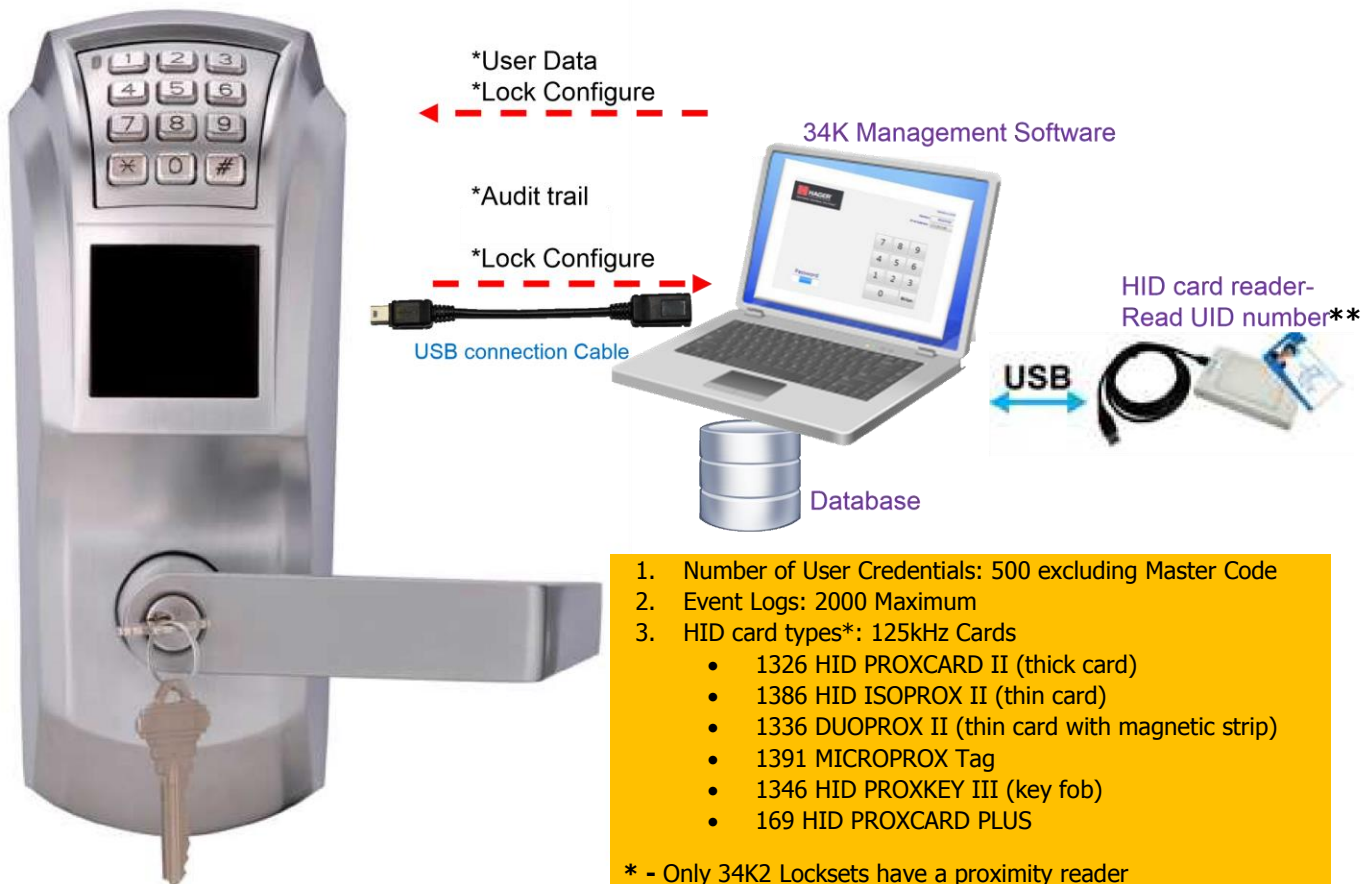
1. Windows XP / Vista / 7 / 8 in 32 or 64 bits.
2. Microsoft® Excel® version 2000 or higher must be installed on your computer.
3. Available USB port on PC or laptop.

### Application / Installation

1. Install Driver PL2303 for USB adaptor.



2. Double Click icon **SecurPass34K** to launch the application software.



1. Number of User Credentials: 500 excluding Master Code
  2. Event Logs: 2000 Maximum
  3. HID card types\*: 125kHz Cards
    - 1326 HID PROXCARD II (thick card)
    - 1386 HID ISOPROX II (thin card)
    - 1336 DUOPROX II (thin card with magnetic strip)
    - 1391 MICROPROX Tag
    - 1346 HID PROXKEY III (key fob)
    - 169 HID PROXCARD PLUS
- \* - Only 34K2 Locksets have a proximity reader  
 \*\* - HID Card Readers are available with the 34K2 Software Kit (2-639-6001)

## Lock Setup Overview

### A QUICK OVERVIEW OF LOCK PROGRAMMING (VIA SOFTWARE)

STEP 1: CREATE BUILDING(S)

STEP 2: ADD LOCK(S) TO EACH BUILDING

STEP 3: CREATE LOCK GROUPS

STEP 4: ASSIGN LOCKS TO LOCK GROUPS

STEP 5: ASSIGN USERS TO A SINGLE LOCK GROUP

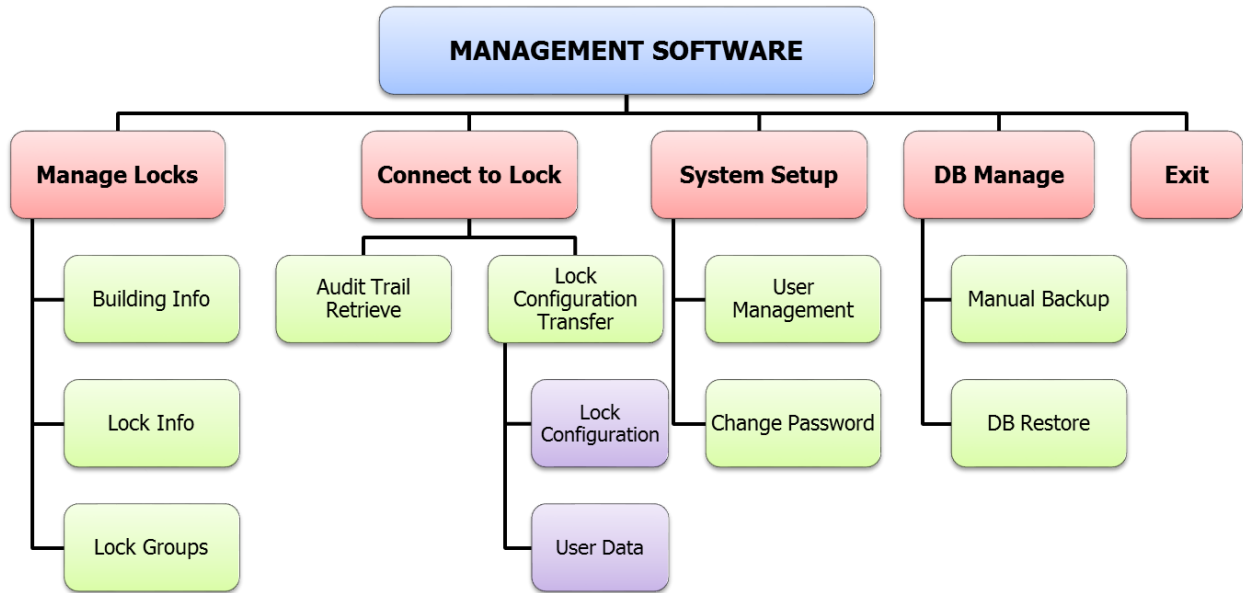
**Note:** Here are a few things to remember while setting up your system:

- Buildings contain locks
- Lock Groups are assigned to many locks which can be in multiple buildings
- Users are assigned to only one Lock Group
- Locks are in a single building but can be referenced by many Lock Groups which contains users
- Locks contain both Configuration and User Data. Each is controlled / transferred separately

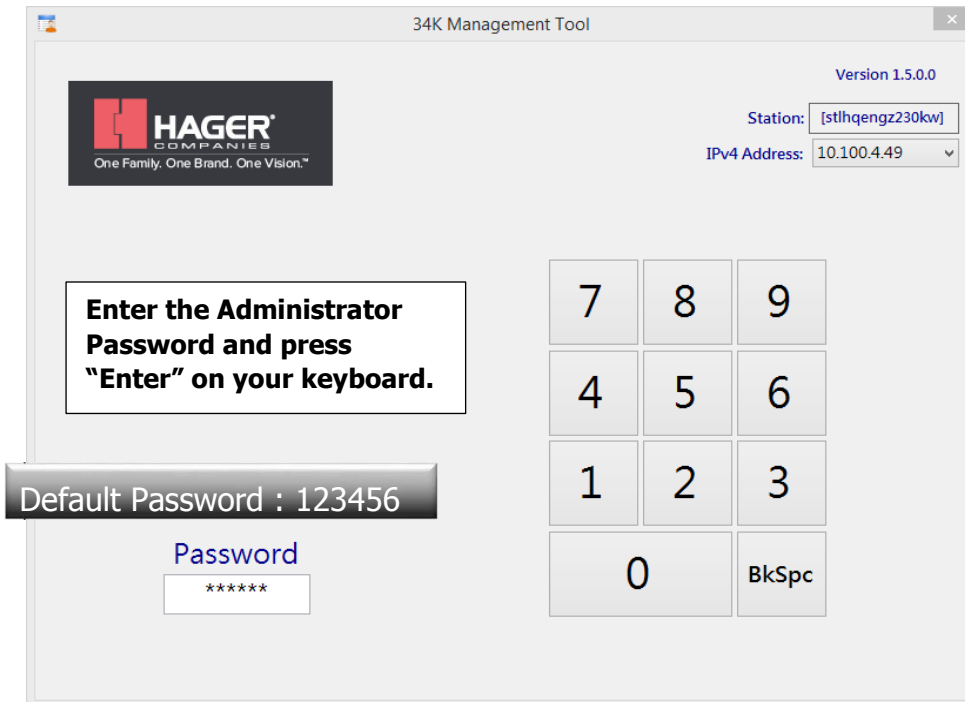
## Management System Setup

- **Programming Users and Lock Configurations**
  1. Buildings  
Manage Locks - Building (Add/Edit/Delete Buildings)
  2. Locks  
Manage Locks - Locks (Add/Edit/Delete Lock Configurations in Buildings)
  3. Lock Groups  
Manage Locks – Lock Groups (Add/Edit/Delete/Assign Lock groups)
  4. Lock Group Assignment  
Manage Locks – Lock Groups – Assign (Assign Locks to Lock groups)
  5. User Management  
System Setup – User Manage (Edit/Delete User Information and Assign to Lock Groups)  
Enable/Activate/Pin Code/Card ID/Assigned Lock Group
- **Transferring Users and Lock Configurations to the Lock**
  1. Connect to Lock through Prolific USB cable
  2. Lock Configuration Transfer
    - a) Lock configuration
    - b) User data
- **Utility Functions**
  1. Audit Trail Retrieval
  2. Managing Your Database
  3. Date Time Sync
  4. Download Configuration
  5. Changing Software Password

## Structure of Management Functions



## Login Screen



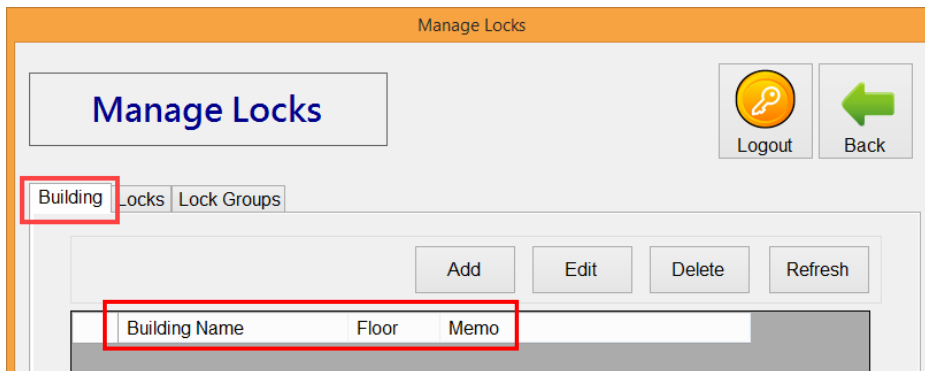
## Main Menu



## Programming Users and Lock Configurations

### 1. Buildings [Manage Locks – Building Info]

From the **Main Menu** select **Manage Locks**, then select the **Building** tab to Add/Edit/Delete/Refresh your Building information

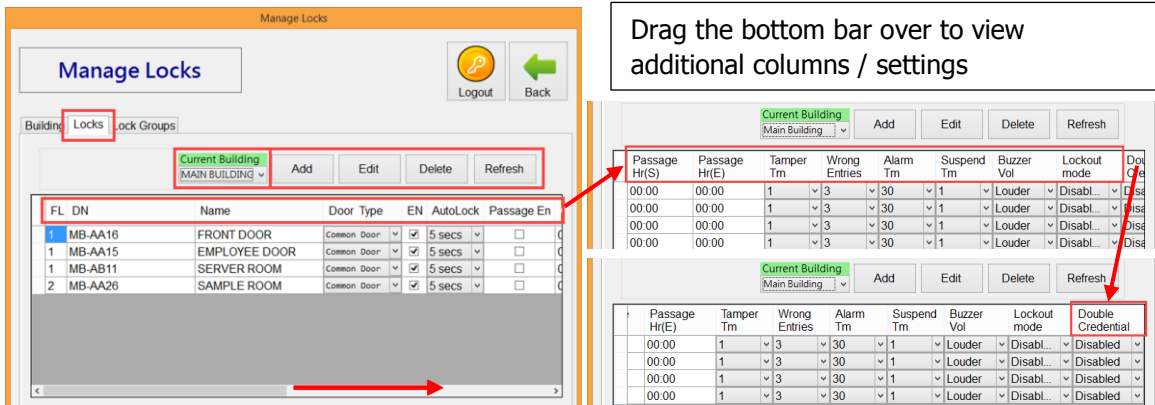


**IMPORTANT!** When Adding / Editing / Deleting, you must check mark the line you are selecting / editing to have it changed when the SAVE button is selected!

|                      |                                  |
|----------------------|----------------------------------|
| <b>Building Name</b> | Building ID or Name              |
| <b>Floor</b>         | Number of floors in the building |
| <b>Memo</b>          | A note about the building        |

## 2. Locks [Manage Locks – Lock Info]

Select the **Locks** tab to Add/Edit/Delete/Refresh your Locks information



Drag the bottom bar over to view additional columns / settings

Use **Current Building** filter to manage lock access in the appropriate building. E.g. if you set **Current Building** to [MAIN BUILDING], it will only show lock information in the MAIN building.

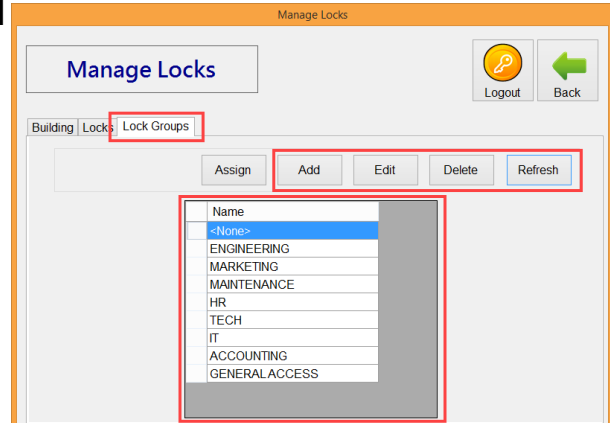
**IMPORTANT!** When Adding / Editing / Deleting, you must check mark the line you are selecting / editing to have it changed when the SAVE button is selected!

|   |  |
|---|--|
| <b>FL</b>   | Identifies Building Floor. Can be edited.  |
| <b>DN</b>   | Door Number. The unique ID number of each lock.  |
| <b>Name</b>   | The name of the lock / opening that the lock is providing access to.   |
| <b>Door Type</b>  | Refers to the lock application for either <u>common lock</u> or <u>access lock</u> .<br><u>Common Lock</u> – Locks that are used to control door in commonly used areas where open access may be needed during business hours. These locks may benefit from using functions like Passage Mode.<br><u>Access Lock</u> – Locks that require access control even during business hours. |
| <b>EN</b>   | When checked, Enables lock to upload data during Transfers and makes the lock available to be Assigned in the Assignment menu.   |
| <b>Auto Lock</b>  | Sets delay timer to relock after credentials are used. The default is 5 seconds.   |
| <b>Passage EN</b>   | Enable Passage Mode if this item is checked.   |
| <b>Passage Hr(S)</b>  | The <b>Start</b> time of the Passage Mode active period, default is 00:00.   |
| <b>Passage Hr(E)</b>  | The <b>End</b> time of the Passage Mode active period, default is 00:00.   |
| * The default value 00:00(S)-00:00(E) means no time limit for Passage Mode activate period.<br><b>Note:</b> This time uses a 24 hour clock. |  |
| <b>Tamper Tm</b>  | Setting Tamper Attempt Limit. The default is 1 attempt.  |
| <b>Wrong Entries</b>  | Setting Wrong Entry Attempt Limit. The default is 3 times.   |
| <b>Alarm Tm</b>   | Setting Tamper Alarm Duration. The default is 30 seconds.  |
| <b>Suspend Tm</b>   | Setting Suspend Duration. The default is 1 minute.   |
| <b>Buzzer Volume</b>  | The default is "Loud" Can be set to "Normal" or "Mute"   |
| <b>Lockout Mode</b>   | Only Master Code can open the lock when "Enabled." The default is "Disabled."  |
| <b>Double Credential</b>  | You must use card and code to open the lock when "Enabled" is selected. The default is "Disabled."   |

### 3. Lock Groups [Manage Locks – Lock Groups]

Select the **Lock Groups** tab to Add / Edit / Delete / Refresh your lock groups

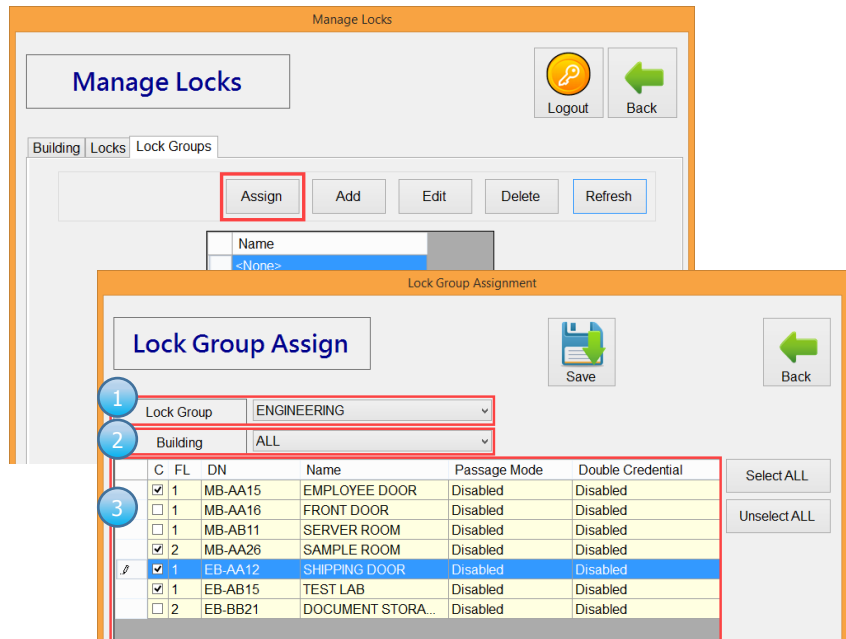
- Name field is manually entered
- Remember to check mark entries to save them



### 4. Lock Group Assignment [Manage Locks – Lock Groups – Lock Group Assignment]

Click **Assign** button to manage the lock assignments to a particular group

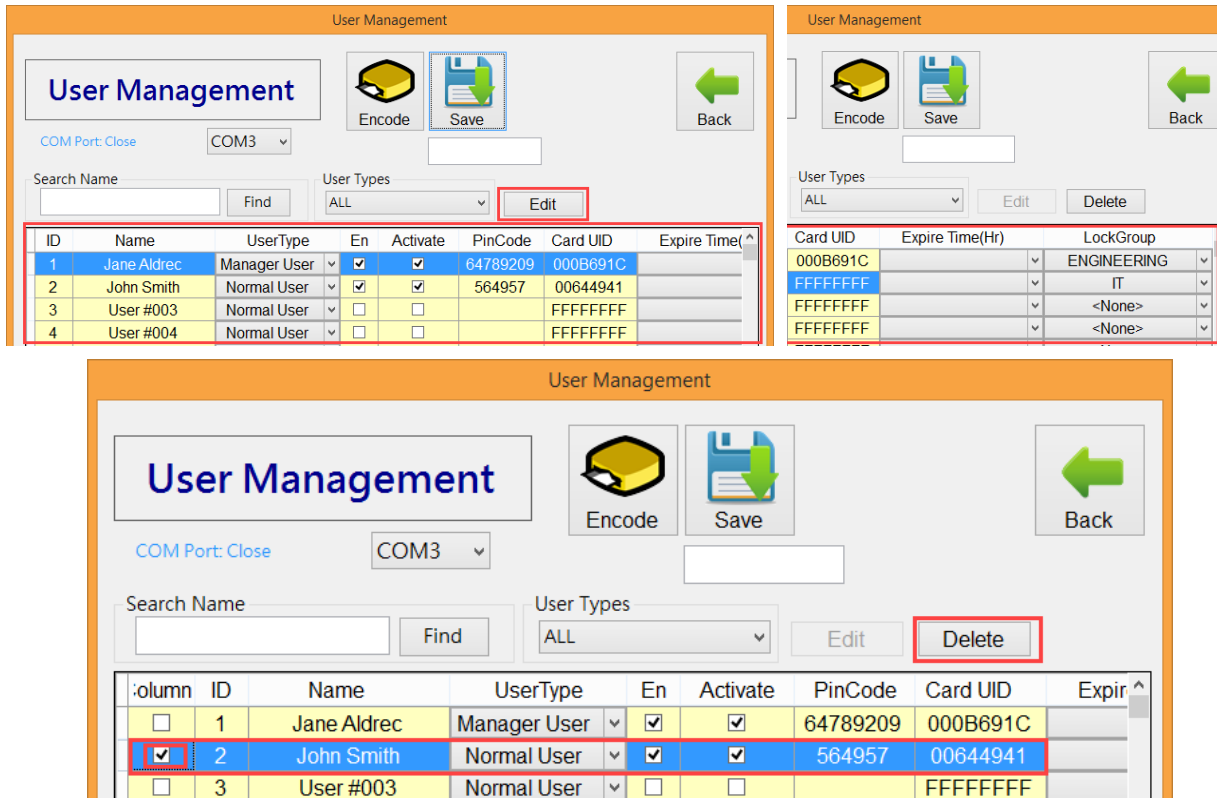
1. Select a Lock Group
2. Select a Building or ALL
3. Select locks you would like to assign to this group
4. Select **Save**
5. Repeat steps 1-3 until all locks are assigned to a building and lock group





## 5. User Management [System Setup – User Manage]

From the **Main Menu**, select **System Setup**, then select **User Manage**.



The screenshots show the 'User Management' interface. The first screenshot shows the 'Edit' button highlighted in red. The second screenshot shows the 'Delete' button highlighted in red. The third screenshot shows a table with user information and checkboxes.

| ID | Name        | UserType     | En                                  | Activate                            | PinCode  | Card UID | Expire Time |
|----|-------------|--------------|-------------------------------------|-------------------------------------|----------|----------|-------------|
| 1  | Jane Aldrec | Manager User | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 64789209 | 000B691C |             |
| 2  | John Smith  | Normal User  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 564957   | 00644941 |             |
| 3  | User #003   | Normal User  | <input type="checkbox"/>            | <input type="checkbox"/>            |          | FFFFFFFF |             |
| 4  | User #004   | Normal User  | <input type="checkbox"/>            | <input type="checkbox"/>            |          | FFFFFFFF |             |

Click **Edit** to add/modify user information or delete user information:

Within the EDIT function, selecting the check box within the column for each user is required to SAVE the information on that line. The DELETE button will immediately clear out all user information on the lines that were checked, exiting the EDIT function, so be sure to use this button before entering any new data you wish to keep.

|                  |   |
|------------------|---|
| <b>Name</b>      | Type in the user's name   |
| <b>User Type</b> | <p>A total of 500 users can be assigned with a variety of access/programming rights.</p> <ul style="list-style-type: none"> <li>• <b>Normal User</b> – standard access (no programming rights)</li> <li>• <b>Manager User</b> – manager access, some programming rights, and access to adding/deleting/modifying users of a particular lock group</li> <li>• <b>Service User</b> – standard access rights to a lockset for a given period of time (0-24 hours) with no programming rights.</li> </ul> |
| <b>En</b>        | <p>Checking this section will allow this user's data to be written to the lock during the <b>Transfer</b> procedure; if not checked, the user's data will be erased from the lock during <b>Transfer</b> procedure.</p> <p><b>Example:</b> If a manager has been transferred out of the facility for an extended period of time, you would uncheck En to remove them from the lock and then recheck it when they return to add them back.</p>   |

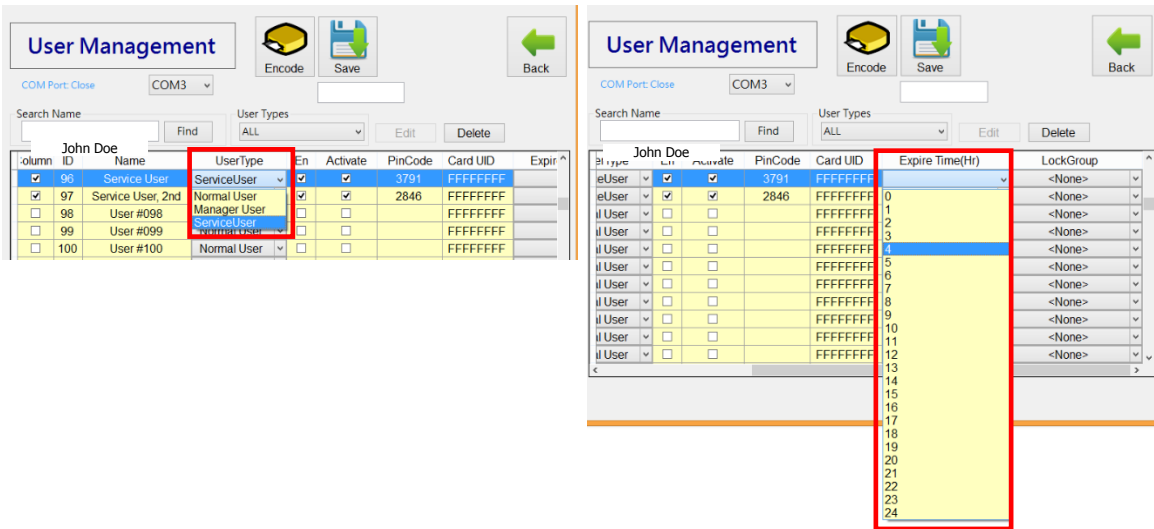
|                 |   |
|-----------------|---|
| <b>Activate</b> | <p>Checking this section will activate the user's credentials during the lock <b>Transfer</b> procedure; if not checked, the user's credential will be deactivated during the <b>Transfer</b> procedure</p> <p><b>NOTE:</b> if the <b>En</b> box is not checked, then the user data will not be activated since it won't be on the lock</p> |
| <b>Pin Code</b> | <p>Create user's Pin code (must be 4-8 digits). Each pin code must be unique, you cannot set the same code for multiple users.</p>  |

34K2 Only!

**Assigning an HID card to a User (34K2 Series Only)** - Connect the HID Card Reader\*\* to the computer first. Select the correct COM port\* (1) of the card reader, click **Encode** (2) and present RFID card close to the reader (3), the card UID will show on the screen (4), you should copy this UID and paste it to the cell of Card UID (5).

- \* - Check on your PC (in the Control Panel/Devices and Printers folder) to find which COM port number the card reader is assigned
- \*\* - Card Readers available in 34K2 Software Kit (2-639-6001)

**Assigning Lock Groups** - Choose a lock group for each user. When complete, make sure each edited user is checked, then hit the **Save** button.



If User Type is **Service User**, then the **Service User Expire Time (Hr)** drop down will need to be used to select a number of hours between 0-24. When complete, make sure each edited user is checked, then hit the **Save** button. Remember, 0 hours is a once and done value.

## Transferring Users and Lock Configurations to the Lock

### 1. Connect to Lock

Be sure the lock has been setup and is out of Factory Mode per Instruction I-LS02111 or I-LS02139

Connect the *Type A* plug of the USB cable provided to the PC/laptop and the *Mini Type B* plug to the lock (located under the battery cover on the lock).

Check on your PC (in the Control Panel / Devices and Printers folder) to find which COM port number the Prolific USB port is located. The example below is COM4.



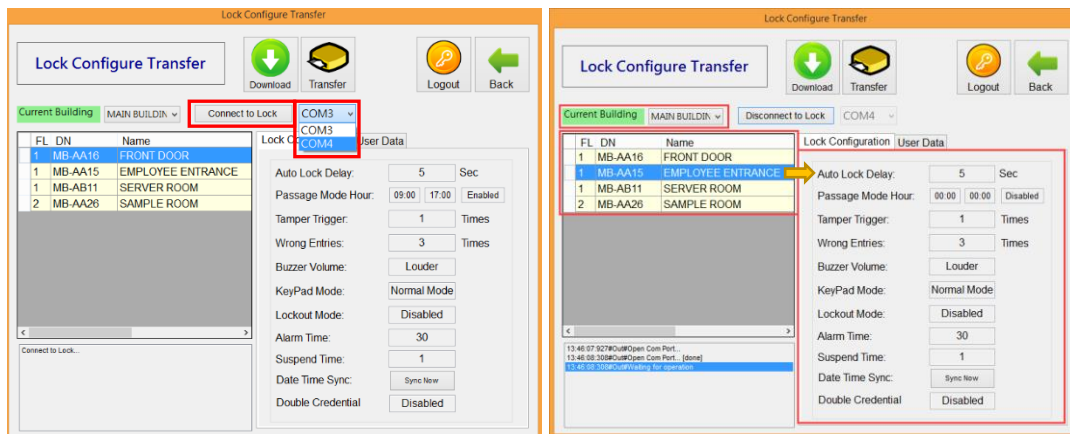
### 2. Configuration Transfer to the Lock

#### a. Lock Configuration

From the **Main Menu**, select the **Connect to Lock** tab and then select **Lock Config Transfer**.

1. Choose the correct COM port\*
2. Click **Connect to Lock**

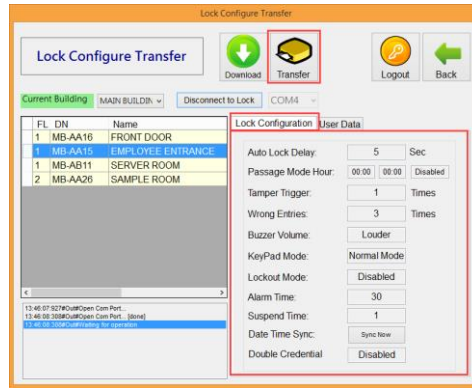
\* - Refer to step 1 on how to find the COM port assigned to the USB cable



Ensure the appropriate building is selected next to **Current Building**.

Choose the appropriate opening on the left side of the screen, the corresponding **Lock Configurations** will show up on the right side of the screen.

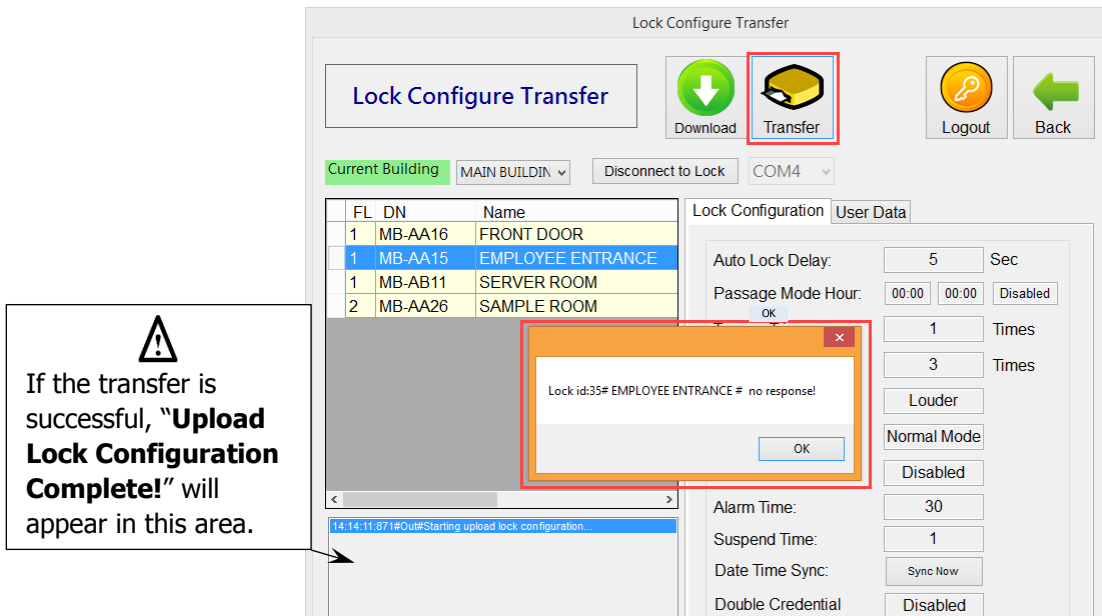
Click **Transfer** to write the **Lock Configurations** to the lock.



The fault prompt will pop-up if the lock is not ready for the information when you clicked **Transfer**. There are three reasons this could happen:

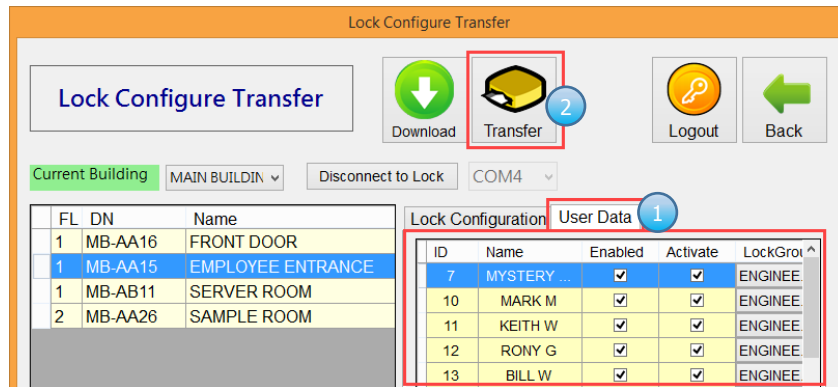
1. Connection Mode was not activated on the lock (see section 3.1.16 in I-LS02111 34K1 Programming Manual or I-LS02139 34K2 Programming Manual).
2. The cable was not connected to the computer and / or lock
3. Wrong COM port selected

Correct the issue, make sure the COM port is selected and try again.




## b. User Data

1. Clicking the **User Data** tab will show which users can unlock this lock.
2. Clicking the **Transfer** icon will complete the delivery of user data to the lock.
3. In order to keep the user data updated, after completing transfer of user data, the original user data will be cleared on the lock.



## Utility Functions

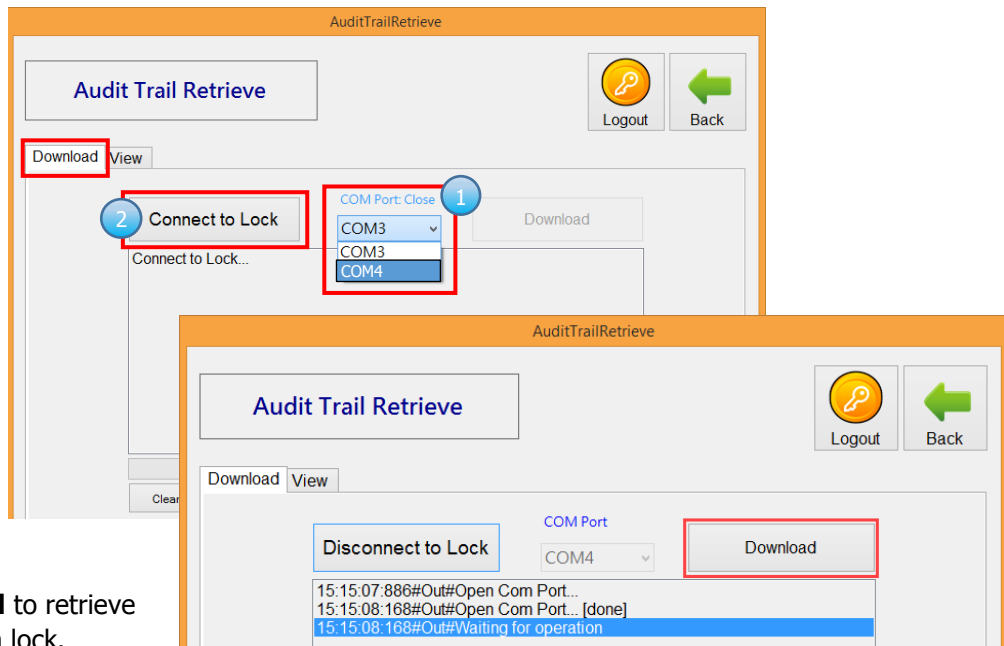
 Ensure Lock is connected to PC with supplied USB cable and make sure the Lock is in Connection Mode. (See step 1 on page 9).

### 1. Audit Trail Retrieval

From the **Main Menu**, select the **Connect to Lock** tab and then select **Audit Trail Retrieve**.

On the **Download** tab,

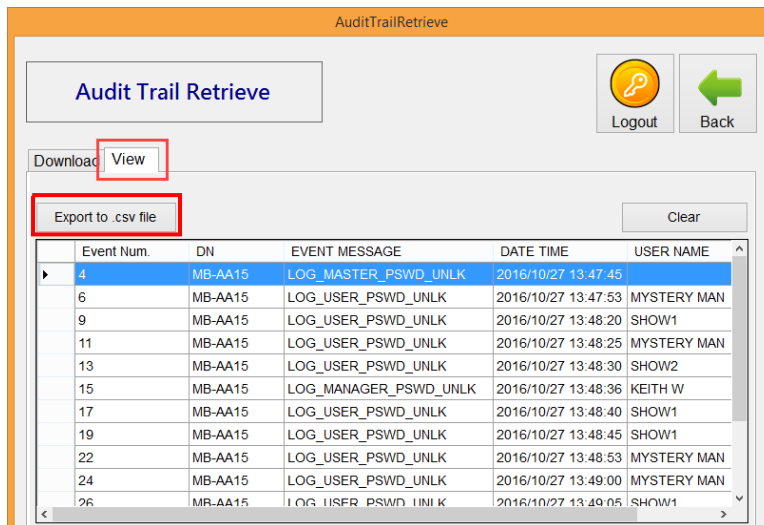
1. Choose the correct COM port (see step 1 from page 9)
2. Click **Connect to Lock**



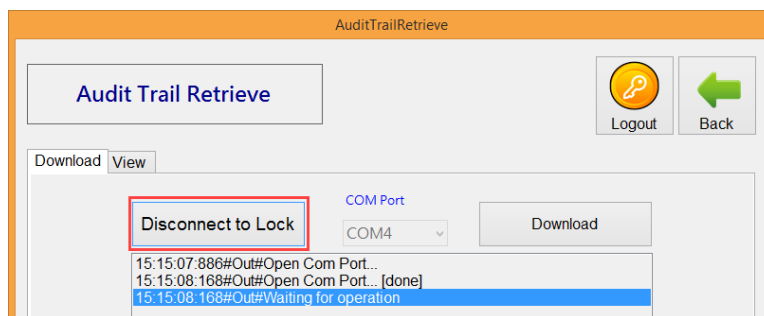
Click **Download** to retrieve Event Logs from lock.

Click **View** tab to show all downloaded audit trails. A few thing to know about the audit trail:

- Each lock stores the most recent 2,000 events. If new events occur over the 2,000 limit on each lock, then the newest events will replace the oldest events in the lock memory.
- When an audit trail is downloaded from a lock, the audit trail is MOVED from the lock to the SecurPass34K software. That means that after download, there are no events left on the lock.
- The audit trail events stored on the locks are only user events such as Master Code unlocked door by password, User #3 Unlocked door by password, etc.
- Each lock is identified by its Door Number (**DN**) and can be sorted by any column, including this one. This means that multiple locks can have their audit trails downloaded and stored in the SecurPass34K software as a single database with the sum total events from all the audit trails downloaded. Sorting can be done by any column, usually Door Number or User Name.
- The full log may be exported as a .csv file if desired and is backed up when the database is backed up. If exported, it can be brought into spreadsheet software that may offer advanced sorting options.
- If for some reason the past audit trails need to be cleared out, pressing the Clear button will erase all past audit trails.



When completed, switch back to **Download** tab and select **Disconnect Lock**.



## 2. Managing Your Database

It is important to back up your database to protect against data corruption, computer failure, or other incidences that could affect the integrity of your data. Keep the backup in a secure location that is backed up as well in another location. You cannot back up only a portion of your data. ALL information will be backed up (including software password) and when restored ALL information will

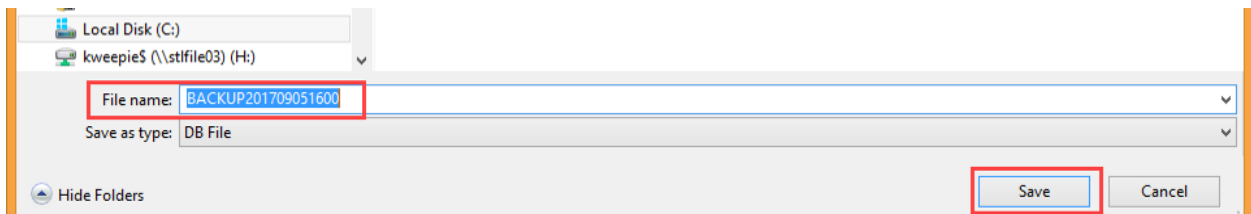
be replaced with the restored database. Restoring a database essentially replaces your current database with a previously saved version of your database. All the items below will be reverted back to the backed up database during a restore:

- **SecurePass34K** password
- Building information
- Locks & their settings
- Lock Groups
- Lock assignments
- User information, credentials, and assignments to Lock Groups
- Downloaded audit trails

## Manual Backup

From the **Main Menu**, select **DB Manage**, select **Manual Backup**

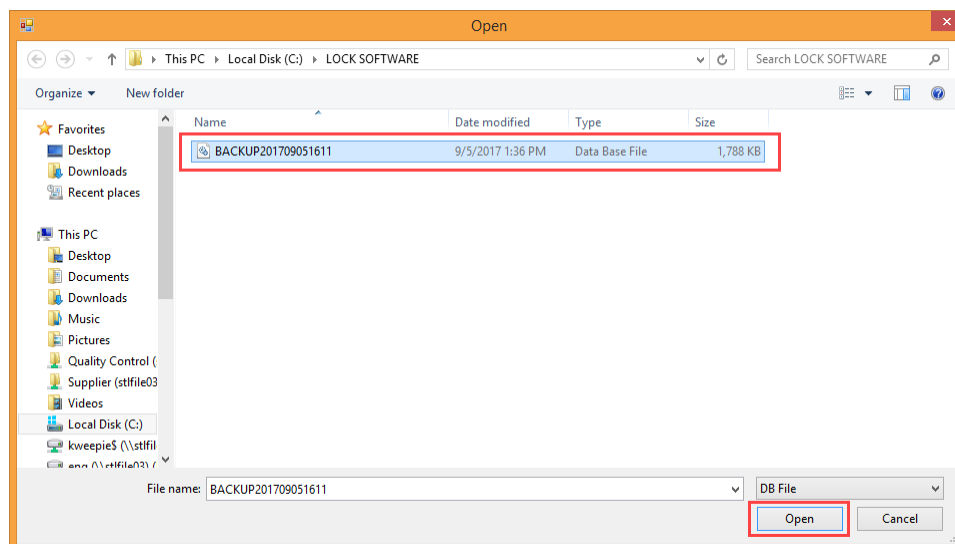
Create a directory in a secure location and save the database. The default name is *BACKUP Year Month Day Hour Min* as shown below. You can enter your own file name if desired.




## Database Restore

If a restoration of the database is required, from the **Main Menu**, select **DB Manage**, select **DB Restore**

Using the pop up menu, go to the file location of the backed up database and select it from the window. Hit **Open** and the database will be replaced with the selected database.



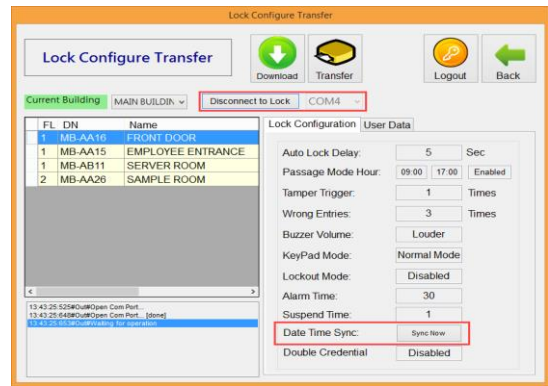
### 3. Date Time Sync

 Ensure Lock is connected to PC with supplied USB cable and make sure the Lock is in Connection Mode. (See step 1 on page 9).


From the **Main Menu**, select the **Connect to Lock** tab and then select **Lock Config Transfer**.

1. Choose the correct COM port
2. Click **Connect to Lock**

Click **Sync Now**, the real time will transfer to the lock. But it will also delete the established parameters of **Passage Mode** and **Service User**. To set the parameters above after a sync, refer to **Lock Management** on pages 4-7.



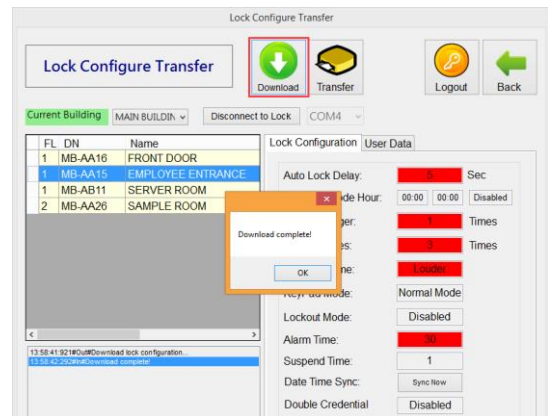
### 4. Download Configuration

 Ensure Lock is connected to PC with supplied USB cable and make sure the Lock is in Connection Mode. (See step 1 on page 9).

From the **Main Menu**, select the **Connect to Lock** tab and then select **Lock Config Transfer**.

1. Choose the correct COM port
2. Click **Connect to Lock**

Click **Download** icon to get the existing configurations from the lock. It will display on the right side of the screen. Any differences from the selected lock and the downloaded configuration will be highlighted in Red.



### 5. Changing Software Password

From the **Main Menu**, select **System Setup**, then select **Change Password**

This page is used for modifying the password of the SecurPass34K software. The password must be 4-8 alpha numeric digits. Once modified, the user must use new password to enter the system the next time they log in. This password is saved when a Manual Backup occurs and brought back to the saved version when a DB Restore is run.

