LockView 5/5Pro

CompX LockView

Software Instruction Manual

CompX SECURITY PRODUCTS

TABLE OF CONTENTS

CompX LockView Software Instruction Manual

Introduction **4**
Operation **5**
LockView Login 5
Screen Information 6
Operator Editor **7**
Lock/User Editor
User Editor 9
Lock Editor 14
Access Rights 20
Group Editor 24
Read/Write Lock
Connection 26
Read Slots 28
Audit Trail 30
Notes Entry 34
Lock Settings 36
Temperature Options **38**
Notifier **42**
Add Responder 43
Edit Responder 44
Delete Responder 44
Global Lock Settings 45
Technical Setup 46
eReports 48
Compliance Dashboard 50
Wizards **53**
Programming Example **56**
Settings **66**
Create ODBC Connection for an Existing Access Database **68**
Create ODBC Connection for New Access Database **70**
Calibration Instructions (temperature monitoring required) **72**

NOTE:

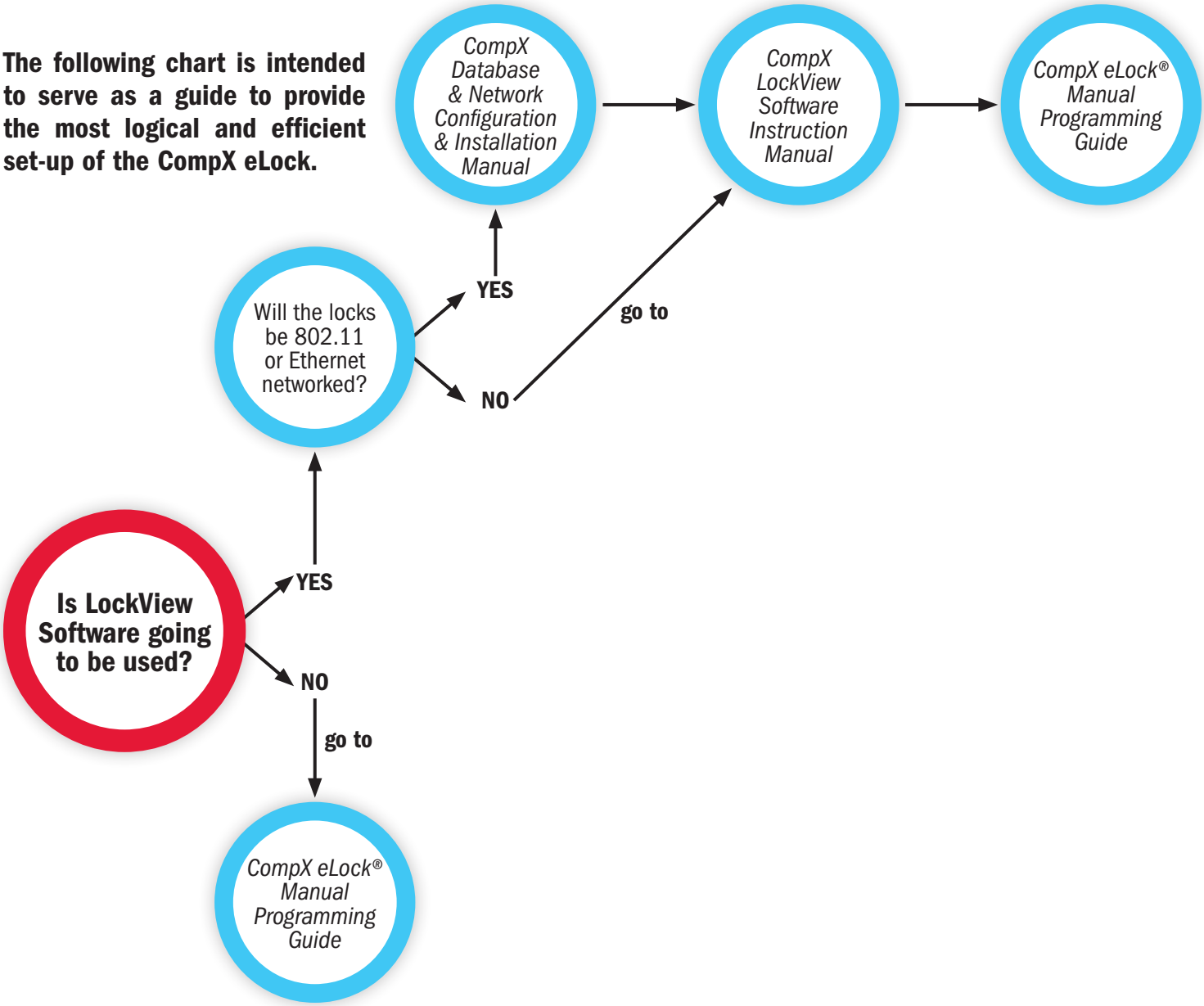
The Table of Contents contains live links. Click on any section, and the corresponding page will load.

TABLE OF CONTENTS continued

Other manuals available as separate pdfs:

- ***CompX eLock Manual Programming Guide***
- ***CompX Database & Network Configuration & Installation Manual***

The following chart is intended to serve as a guide to provide the most logical and efficient set-up of the CompX eLock.



INTRODUCTION

An authorized Operator of LockView® can create a database of users and locks on a local or networked computer. Each user in this computer's database is assigned to a slot in each lock to which they have access. A lock's internal memory is divided into 3000 slots that store user information thereby giving each lock a maximum of 3000 users. That is, 3000 individuals are capable of opening the eLock.

The computer with LockView® loaded onto it has the ability to connect to locks (directly, through a USB cable or through a computer network, using Ethernet or 802.11g Wi-Fi) and update the lock's memory to correspond with its own database. It is able to gather and manipulate a lock's audit trail, or past operation log. Audit trail information contains, among other things, the lock's name, the name of the user attempting to gain access, the credential used, if access was granted or denied, and the date and time of each interaction.

LockView 5/5Pro works with LockServ to communicate with locks. LockServ has the ability to communicate with multiple locks simultaneously over a computer network, eliminating the need for the Operator to visit each lock to update the lock's database, or download audit trails.

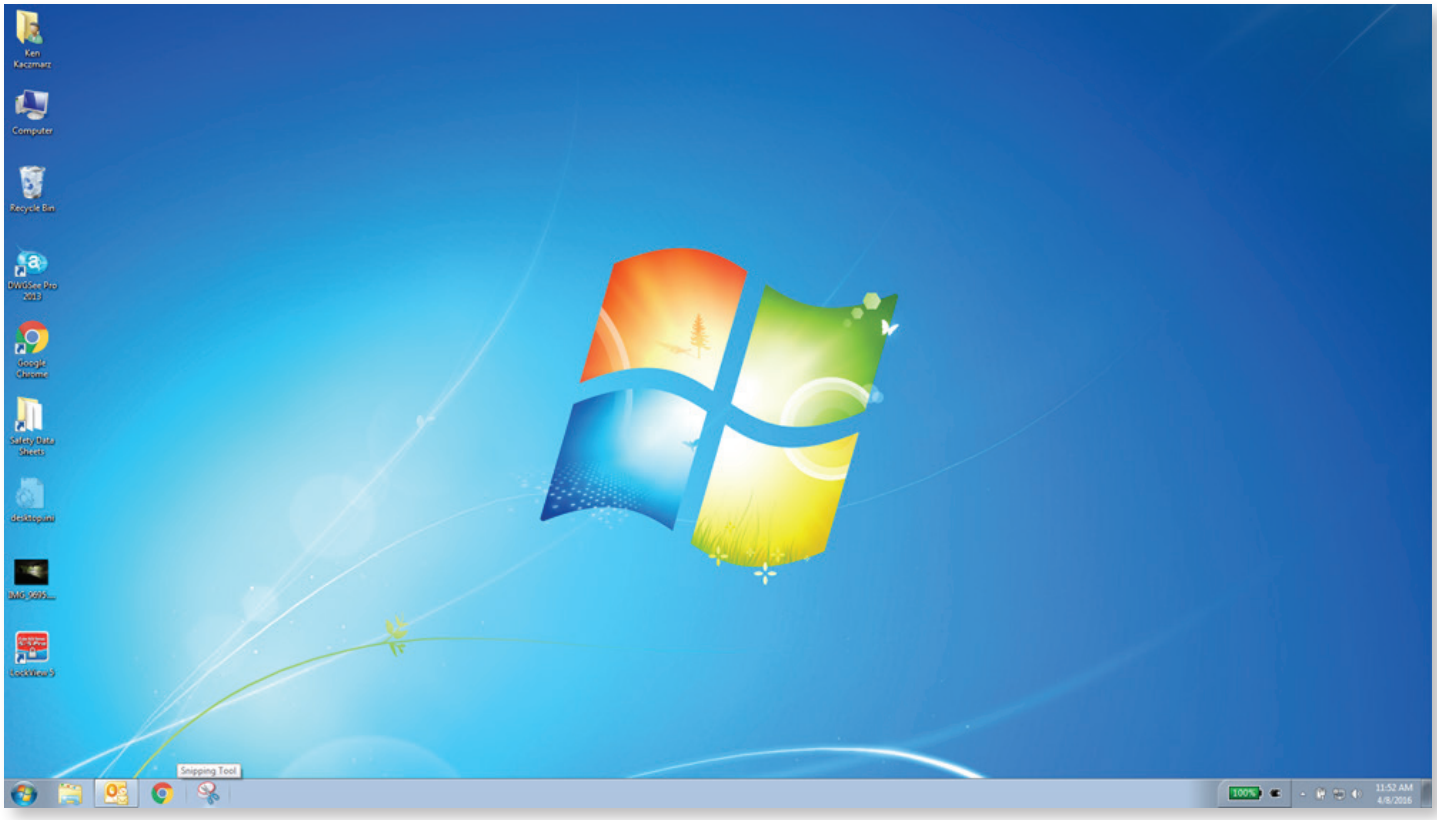
Alternately, LockServ can communicate with locks using a USB cable if network hardware is not available.

On units equipped with temperature monitoring, LockView® 5/5Pro allows, among other things, viewing of temperature logs, graphs and allows manipulation of temperature range settings.

On units equipped with an internet connected network, LockView 5/5Pro has the ability to email responders when an eLock's battery is low, is in temperature alarm mode, has a door switch alarm, or is past-due for a network connection. Alternately, LockView 5/5Pro can connect to an SMS provider and send text messages, faxes or voice phone calls.

OPERATION

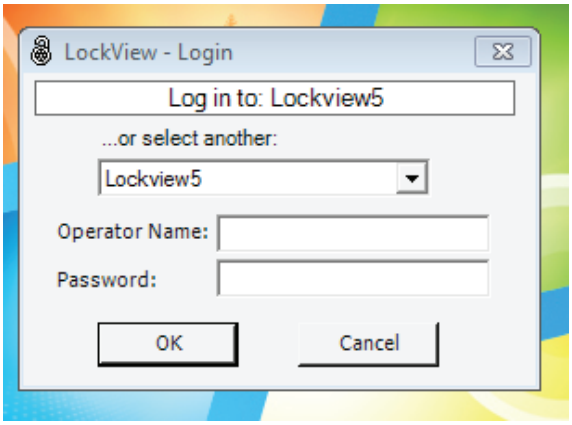
Double click the LockView® icon on the desktop to open and run the LockView program.



NOTE: *If the LockView® ODBC entry was not created properly, it will need to be created manually. Refer to* **DATABASE FILE LOCATION ON PAGE 68.**

LOCKVIEW® LOGIN

Double click the **LockView** icon on the desktop. The below window will appear:



For first time Login, enter "**admin**" under both Operator Name and Password. Click **OK**. Note: Password is case sensitive.

➔ After an Operator has been added to LockView, use of personalized **Operator Name** and **Password** should be used for Login.

See *Database & Network Configuration & Install Manual* for more information.

OPERATION continued

NOTE: *There is NO security while logged in under "admin." The "admin" user should be deleted after a new Operator Name and Password have been completed to ensure database security.*

SCREEN INFORMATION

FILE DROP DOWN MENU – Used to EXIT program.
VIEW DROP DOWN MENU – Used to display or eliminate the shortcut and/or status bars on the program screen; display or eliminate the background image; select another background image from a saved file; or return program to default settings.
WINDOW DROP DOWN MENU – An alternate way to access the following programming menus:

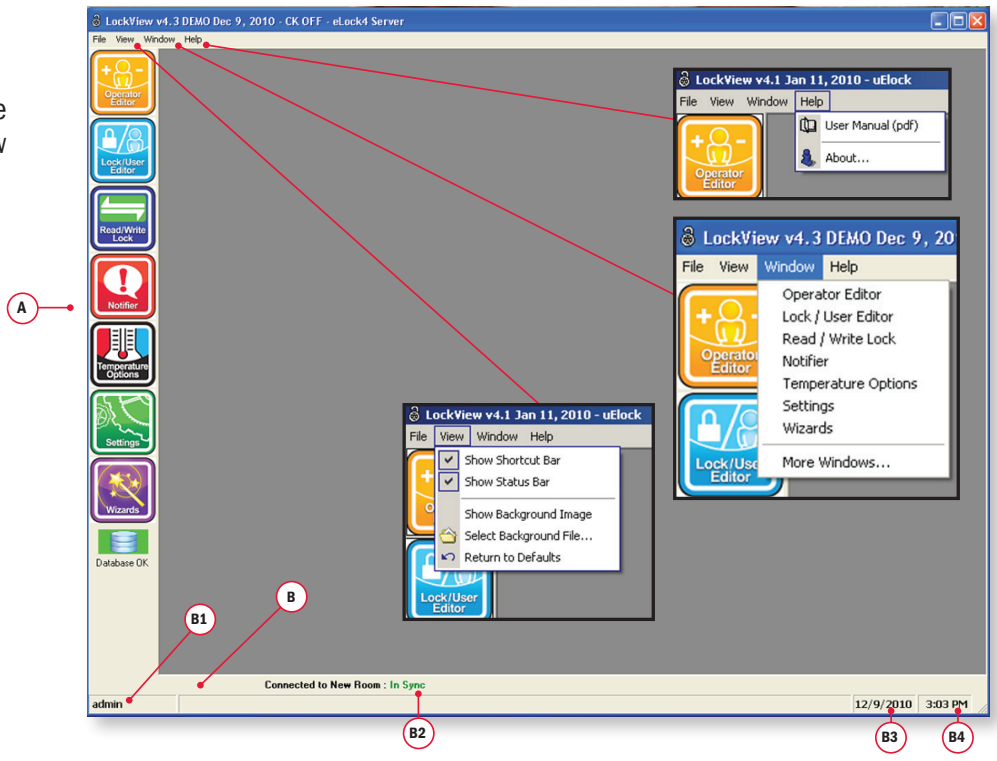
- Operator Editor
- Lock/User Editor
- Read/Write Lock
- Notifier (network required)
- Temperature Options (temperature monitoring required)
- Settings
- Wizard
- More Windows

HELP DROP DOWN MENU – pdfs of eLock / LockView manuals.

A SHORTCUT BAR - Quick start buttons for the **Operator Editor, Lock/User Editor, Read/Write Lock, Notifier** (network required), **Temperature Options** (temperature monitoring required), **Settings**, **Wizard** menus. The shortcut bar can be displayed or hidden, refer to the **VIEW** drop down menu.

B STATUS BAR - Displays the following LockView program status information:
B1 – Name of Operator that is currently logged into software.
B2 – "Connected to" lock status. Displays the lock to which LockView is currently connected as well as the connection status: **In Sync** or **Change is Pending.**
B3 – Current local computer date.
B4 – Current local computer time.

NOTE: The status bar can be displayed or hidden, refer to the View drop down menu.



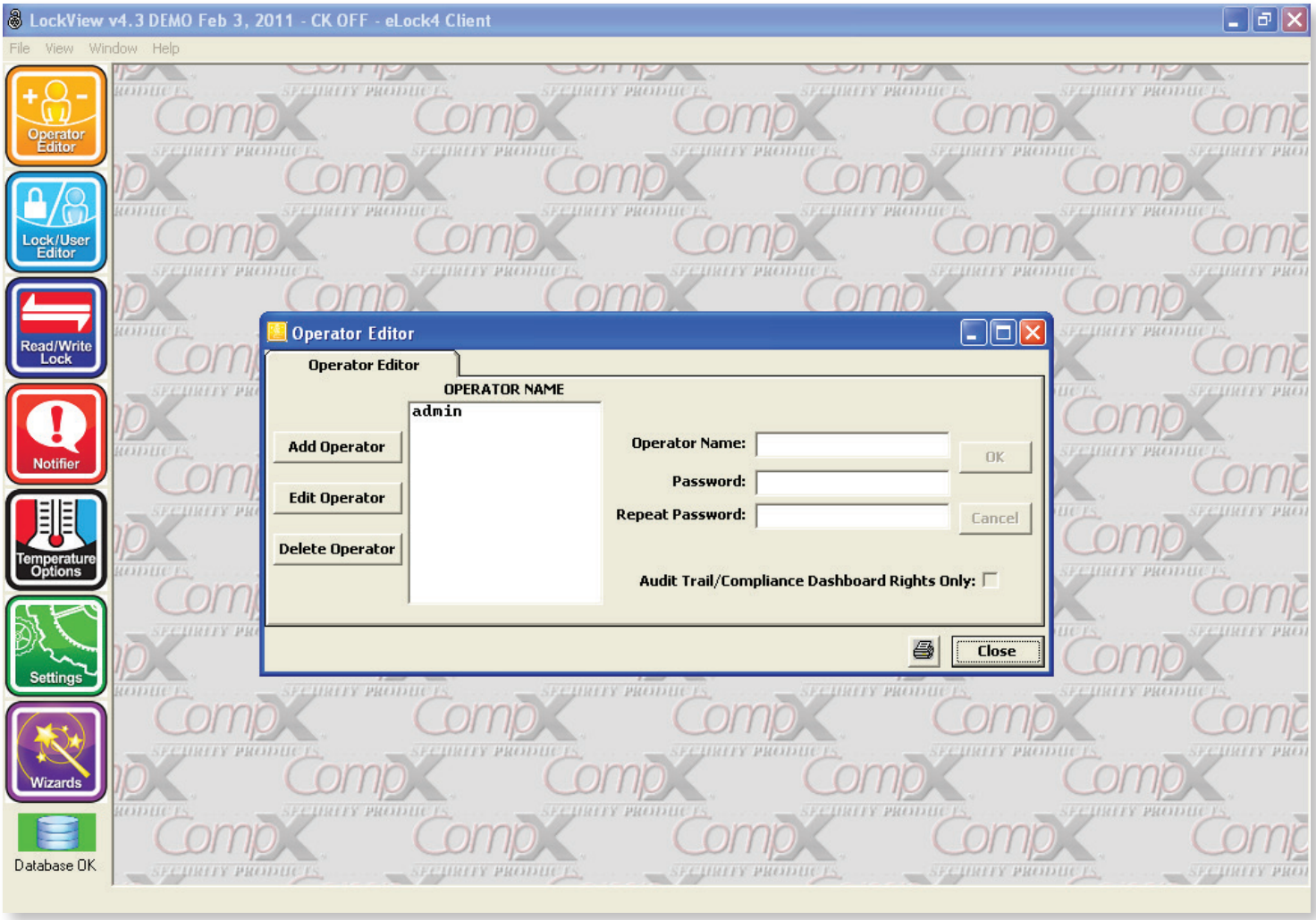
OPERATOR EDITOR

An Operator is someone who is responsible for building and maintaining a database of users and locks. An Operator does NOT have to be a user of locks. The **Operator Editor** window allows the Operator to create new Operators. New Operators can be given full access in LockView or Audit Trail Rights Only.

➔ The deletion of the logged-in Operator is prohibited.

NOTE: *After the first new Operator is added, exit LockView and login as the new Operator. Delete the "admin" Operator.*

NOTE: *First Operator added to LockView® should be given full access rights.*



TO ADD A NEW OPERATOR

1. Select the **Operator Editor**.
2. Select **Add Operator** to create a new Operator.
3. Enter the new Operator Name and Password.
   ➔ If **Audit Trail / Compliance Dashboard Rights Only** is chosen, the Operator will only be able to retrieve and view audit trails and compliance dashboard information.

OPERATOR EDITOR continued

NOTE: *Passwords are case sensitive and must be a minimum of 4 characters.*

4. Select **OK** when done.
5. Select **Close** to close the Operator Editor tab.

TO EDIT AN OPERATOR

1. Select **Operator Editor**.
2. Select **Operator Name** and then select **Edit Operator** to edit an Operator's information.
3. Select **OK** when done.
4. Select **Close** to close the **Operator Editor** tab.

TO DELETE AN OPERATOR

1. Select the **Operator Editor**.
2. Select **Operator Name** and then select **Delete Operator** to delete an existing Operator.

NOTE: *Deletion of the currently logged in Operator is prohibited.*

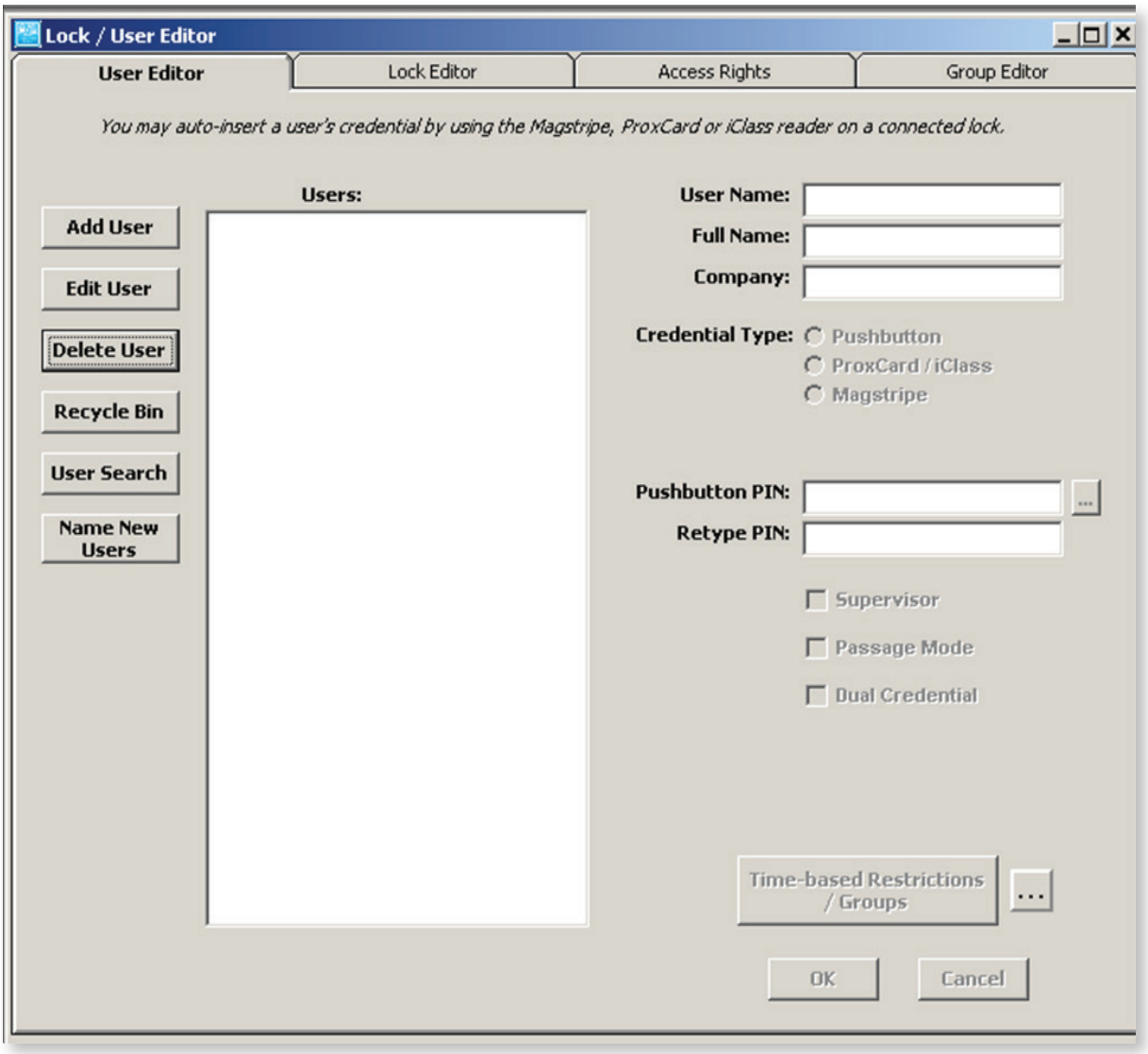
3. Select **Close** to close the **Operator Editor** tab.

LOCK / USER EDITOR

The **Lock/User Editor** window allows the Operator to modify the user and lock databases.

USER EDITOR

The **User Editor** tab is used to add, edit or delete users from the computer database.



TO ADD A NEW USER

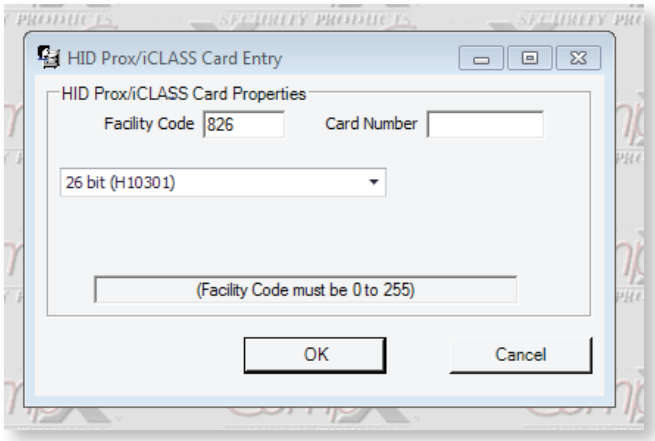
1. Select the **Lock/User Editor**.
2. Select **Add User** to create a new user in the database.
3. Enter the new user's information.
   User Name must be a minimum of 4 and a maximum of 14 characters.
   The user's **Full Name** and **Company** are optional. **User Name** is required and will appear in other places and reports in LockView.
4. Enter the new user's credential information.
   - ➔ If the user is to have a PIN (pushbutton) credential, press the more info button [...] next to the pushbutton PIN field to generate a random PIN.
   - ➔ If a lock is connected via USB cable, and is equipped with a magstripe card reader, HID Prox reader, or HID iCLASS reader, select the appropriate **Credential Type** and present or swipe the card to the card reader to enroll the information automatically into the database.

LOCK / USER EDITOR *continued*

➔ To manually input an HID credential (Prox or iCLASS), select **ProxCard/iCLASS** and click the more info button [...]. The HID **Facility Code, Card Number,** and **bit Format** are needed in order to enroll a proximity card manually. This information can be obtained from the purchaser of the HID cards.

NOTE: *Use of the more info button [...] is optional and not required to generate a PIN or HID prox credential.*

➔ Using the pull down menu, choose the HID Format (26, 33(RS2), 34, 35, 36, 37 bit, 37 bit with facility code, or 42 bit)

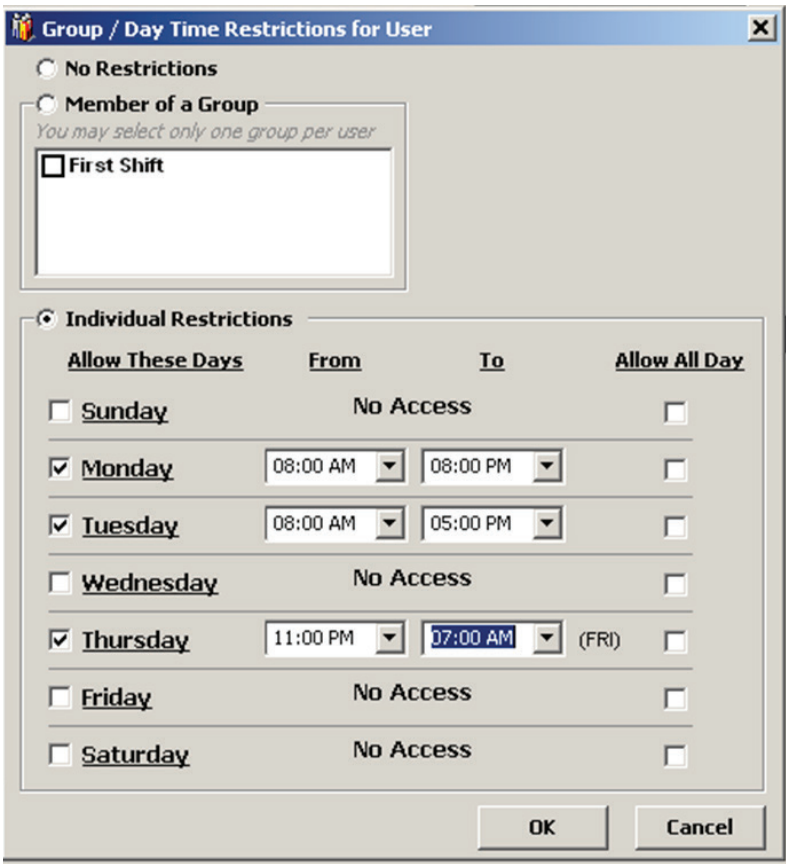


➔ Enter the **Facility Code** (if that format has a facility code)
➔ Enter the **Card Number**
➔ The hexadecimal number corresponding to that **Format**, **Facility Code**, and **Card Number** will appear in the box. Clicking **OK** will automatically transfer that number into the **User Editor**.
➔ A user can have one "primary" credential (PIN, prox card, mag stripe or barcode) as well as a secondary PIN credential if they have dual credential rights.

NOTE: *Two users cannot have the same PIN or card credential. This includes users in the Recycle Bin. If a credential is "recycled," the user who was previously using the credential must be completely removed from the database. (Including from the Recycle Bin.)* *See page 12 for more details.*

5. If the new user has **supervisor** rights, check the **Supervisor** box. Supervisor rights are especially useful for programming locks without the LockView software.
6. If the new user has **Passage Mode** rights, check the **Passage Mode** box. **Passage Mode** allows the user to change the lock's state (lock/unlock) by pressing "ENTER" (at the lock) after the PIN or card has been accepted and the unit is unlocked. Note: when in passage mode, the lock open time is disabled.
7. If the new user has **Dual Credential** rights, check the **Dual Credential** box and enter the dual credential PIN
   ➔ Dual credential users are users that are required to present two credentials in order to gain access.
   ➔ Dual credential users must use a PIN after the primary credential.
   ➔ If the user has a PIN/PIN dual credential, the PIN numbers must be different. (**Note**: Primary and secondary PINs are NOT interchangeable.)
   ➔ If **Force Unique Dual Pin** is selected in **Settings**, each dual credential PIN must be different..
8. If the new user will have day and time access restrictions, select **Time-Based Restrictions/Groups**.
9. If the new user will be a group member, check the button adjacent to **Member of a Group**, then click the group name. For more information on groups, go to page 24.

LOCK / USER EDITOR continued



10. Fill in the time slots the user is allowed access, or check **No Restrictions** if the user has 24 hour access. When filling in time slots, LockView will automatically wrap a day. (Example: 11 p.m. Monday - 7 a.m. Tuesday.)
11. Select **OK** when done.

LOCK / USER EDITOR continued

TO EDIT A USER

1. Select **Lock/User Editor**. Select **User Editor**.
2. Highlight **User Name** and select **Edit User**.
3. Select **OK** when done. Any changes made to a user must be uploaded to the locks to which the user has access. (See Read/Write Lock.)
4. Select **Close** when done.

TO DELETE A USER

1. Select **Lock/User Editor**. Select **User Editor**.

NOTE: *Before deleting a user, it is recommended the user's access rights be removed from all locks. This ensures the user is deleted and will not be accidentally reinstated into the computer database.*

2. Highlight **User Name** and select **Delete User**.

NOTE: *It is possible to delete multiple users by holding control and shift while selecting users. To select every user between two users simply click on the first user, press and hold shift, then click on the second user. All users between the two users will then be highlighted and can be deleted. To select individual multiple users click on the first user, press and hold control, then click on every user that will be deleted.*

3. Select **Close** when done**.**

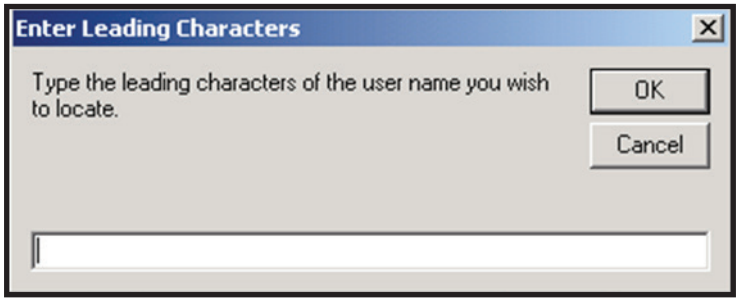
RECYCLE BIN

When a user is deleted from the LockView database, the user is moved into the **Recycle Bin**. Once in the **Recycle Bin**, the user can either be restored to the database or completely deleted from the database.

NOTE (VERY IMPORTANT): *Two users cannot have the same PIN or card credential. This includes users in the recycle bin. If a credential is to be passed to a different user, the person who previously had the credential must be removed from the* ***Recycle Bin.***

TO FIND A USER

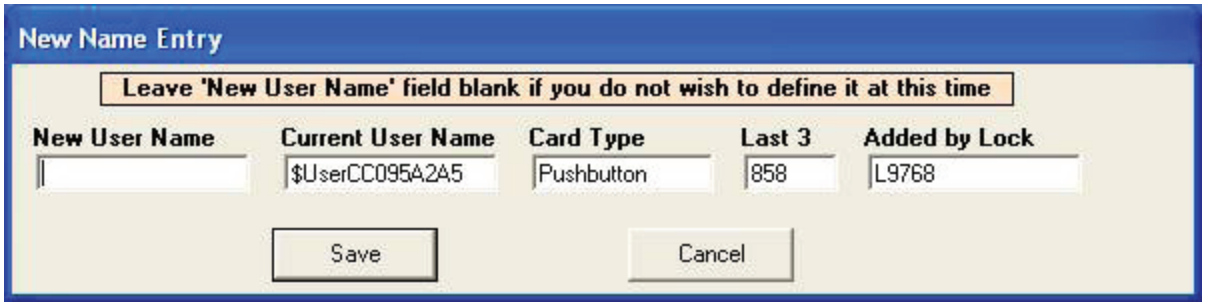
If a user cannot be found in the **User Editor,** *click* **User Search.** *Enter the first few characters of the user's name and click* **OK.**



LOCK / USER EDITOR continued

TO NAME A NEW USER

Manually entered users entered at the lock will appear as $xxxxxxx. Click **Name New Users** *and a window will be opened that will prompt the naming of these users.*



Enter the desired **New User Name** *and click* **Save.**

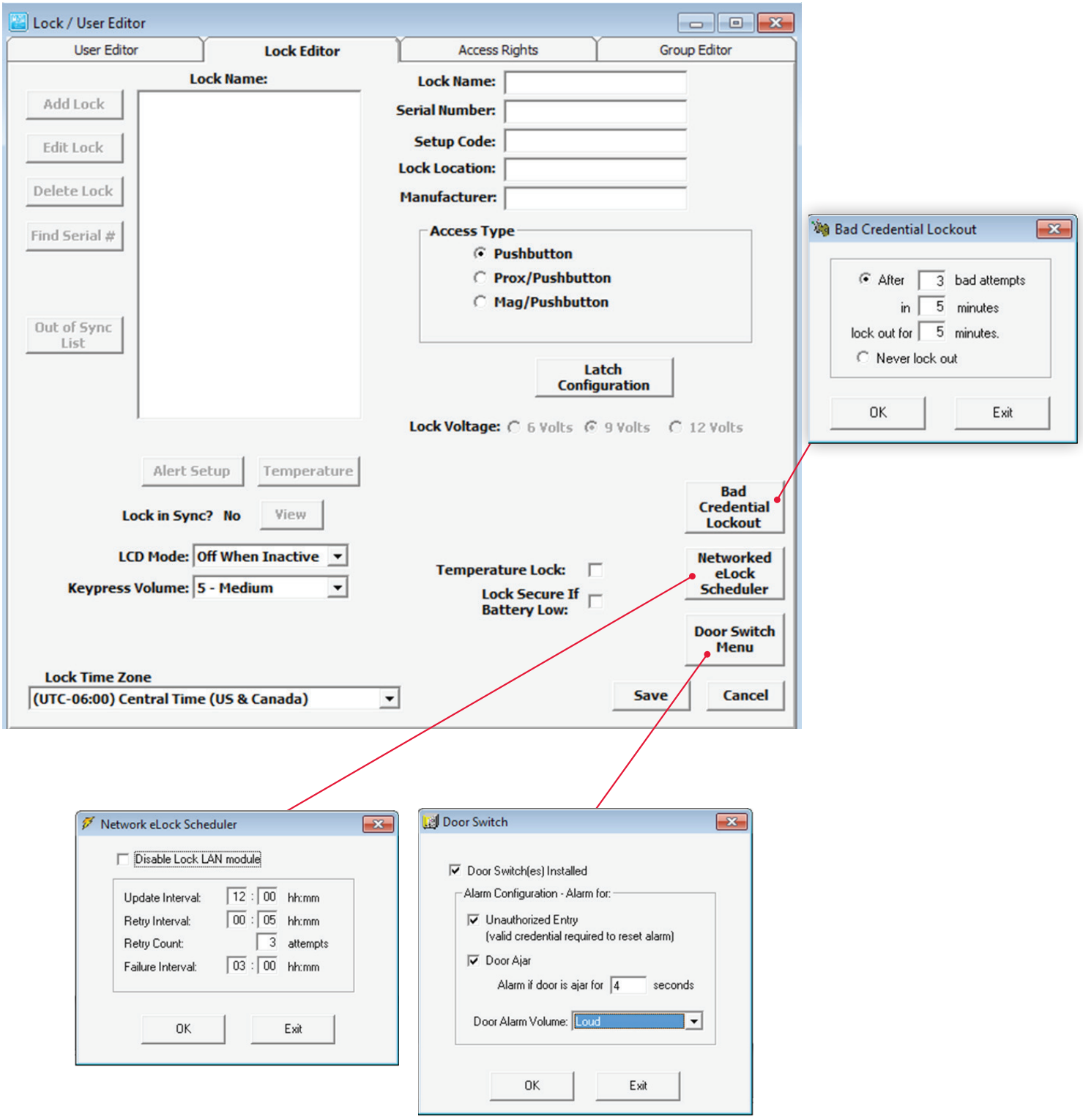
LOCK / USER EDITOR continued

LOCK EDITOR

The **Lock Editor** tab is used to add, edit, or delete locks from the database.

TO ADD A NEW LOCK MANUALLY

1. Select **Lock/User Editor**. Select **Lock Editor**.
2. Select **Add Lock** to create a new lock in the database.



LOCK / USER EDITOR *continued*

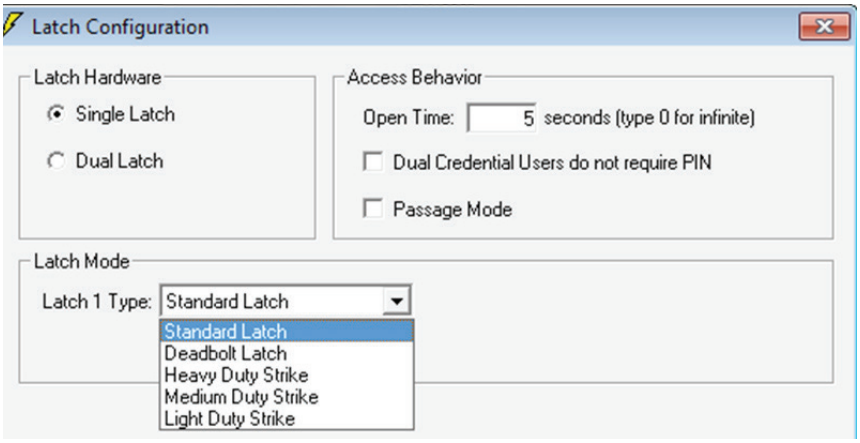
3. Enter a name for the new lock being created. **Lock Name** must be between 4 and 14 characters in length including spaces.
4. Enter the **Lock Serial** and **Setup Code** numbers.
   ➔ **The lock's serial and setup code numbers are on a sticker included with the lock.**
5. If the application (cart, cabinet, enclosure, etc) on which the eLock is installed comes with special LockView instructions, enter the name of the manufacturer of the application into the box next to Manufacturer. Entering this manufacturer name will open up additional settings for the application. NOTE: If the hub system attached to a CompX 200/300 series cabinet lock is being set up, enter **CompxCab**.
6. Choose the **Pushbutton, Prox/Pushbutton, Mag/Pushbutton** (under access type) if the lock being entered is provided with one of these card readers. **Note**: It is not possible to edit a lock's access type. If the lock's access type needs to be changed, the lock must be ***deleted*** and ***recreated*** with the appropriate card reader selected. **Prox/Pushbutton** corresponds to HID Prox/keypad and HID iCLASS/keypad.
7. Select the **Lock Voltage** box for the appropriate voltage for the eLock. The lock voltage selection will determine the low battery indicator threshold. If it is set incorrectly, the low battery indicator will not operate properly.
8. If the eLock is equipped with temperature monitoring, check the box adjacent to **Temperature Lock**. Temperature will appear after clicking OK and allow access to additional temperature monitoring settings.
9. Select **Lock Secure If Battery Low** to prevent access to an eLock if the battery is low. If this box is checked, the eLock will NOT open if the battery is low. Replacing the battery will allow normal use.
10. To conserve battery, the LCD screen on the eLock can be set to turn "off" when not in use. **LCD Mode**; **Off When Inactive** is the default. Select **Always On** if the LCD is to remain on at all times.
12. The volume of the beeps that are heard when the buttons are pressed at the eLock is adjustable under **Keypress Volume**. Choose **0** to **9**: 0 is **Off** and 9 is **Loud**.
13. The local time zone on which the eLock is installed can be selected in **Lock Time Zone**. Provided the eLock is networked and in the event that the server resides in a different time zone, this feature ensures the correct time is recorded in the LockView audit trail
14. **Bad Credential Lockout** allows the operator to restrict access to a lock if multiple invalid attempts are made; default is **Never Lockout**. Click bad credential lockout to adjust.
    There are three adjustments:
    a) **After __ bad attempts**
    b) **In __ minutes**
    c) **Lockout for __ minutes**
    For example, after 5 bad attempts in 5 minutes, lockout for 5 minutes.
15. If the lock is provided with an Ethernet or 802.11 module, choose how often the lock will check for updates to the database buy clicking **Networked eLock Scheduler**. This will pop up a window. NOTE: If the lock does not have a LAN module, choose **Disable Lock LAN Module.**
    a. **Update Interval**- How often the lock will turn on the LAN module and check the network database for updates (enter in HH:MM format). **Default is 12 hours**.
    b. **Retry Interval**- If the networked lock was unable to connect to the database through the network, enter the amount of time before it retries. (enter in HH:MM format). **Default is five minutes**.
    c. **Retry Count**- If the networked lock fails to connect to the database upon retry, the lock will continue to retry the number of times in the "retry count." **Default is five attempts**.
    d. **Failure Interval**: If every attempt to connect to the database under the **Retry Count** is unsuccessful, **Failure Interval** is the amount of time the lock will wait before starting the **Retry Interval** again. (Enter in HH:MM format.) **Default is one hour**.

    Note*: Each time the lock turns on the LAN module to check the database for updates, a significant amount of energy is drained from the battery, reducing battery life.*

16. If a door switch is installed, click **Door Switch Menu** to open the door switch submenu. The eLock can be set to alarm if the door switch opens without a valid credential (**Unauthorized Entry**) and/or it can be set to alarm if the door has been left open for a programmable amount of time (**Door Ajar**). The alarm volume can also be set to **Off**/**Soft**/**Medium**/**Loud**.

LOCK / USER EDITOR continued

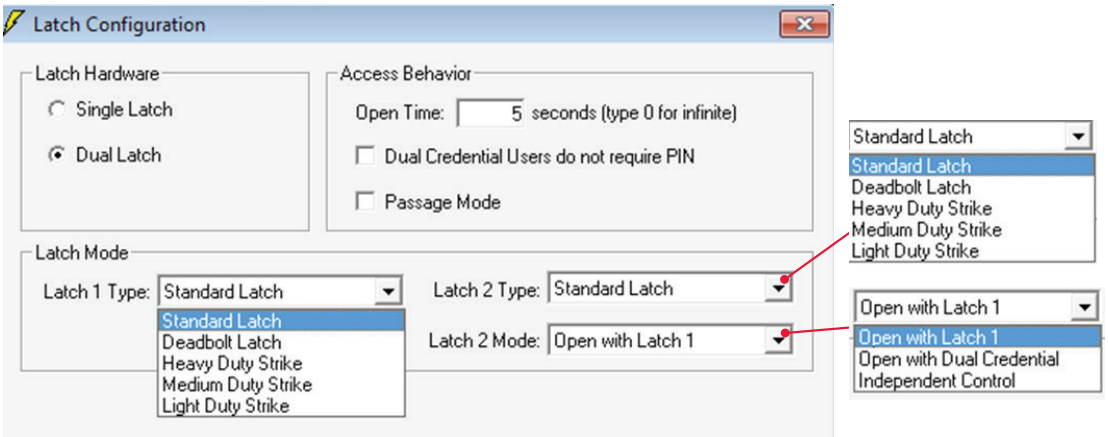
17. Click **Latch Configuration** to set up the latch behavior attributes.
    a. Under **Access behavior** the following can be chosen
        - ➔ The latch **Open Time** in seconds. (NOTE: entering 0 will keep the latch(es) open indefinitely.)
        - ➔ Select **Dual Credential Users do not Require PIN** for this eLock in order to allow all dual credential users access with only their primary credential. Note: This will result in a reduction of security, as dual credential users will no longer be required to present both of their credentials.
        - ➔ **Passage Mode** – this mode allows the eLatch to change its state (lock/unlock) after a valid credential is presented To enter passage mode, press "ENTER" (at the eLock) after presenting a valid credential. Once the eLock is held open in passage mode, closing the eLock requires the acceptance of a valid credential
    b. Under **Latch Hardware** choose the type of Latch hardware that is being setup: single latch, dual latch or Multiple Latch with the HUB system.



Single latch – if the CompX eLock only has one latch connected, choose "single latch." Then, under **Latch Mode**, choose the type of latch connected.

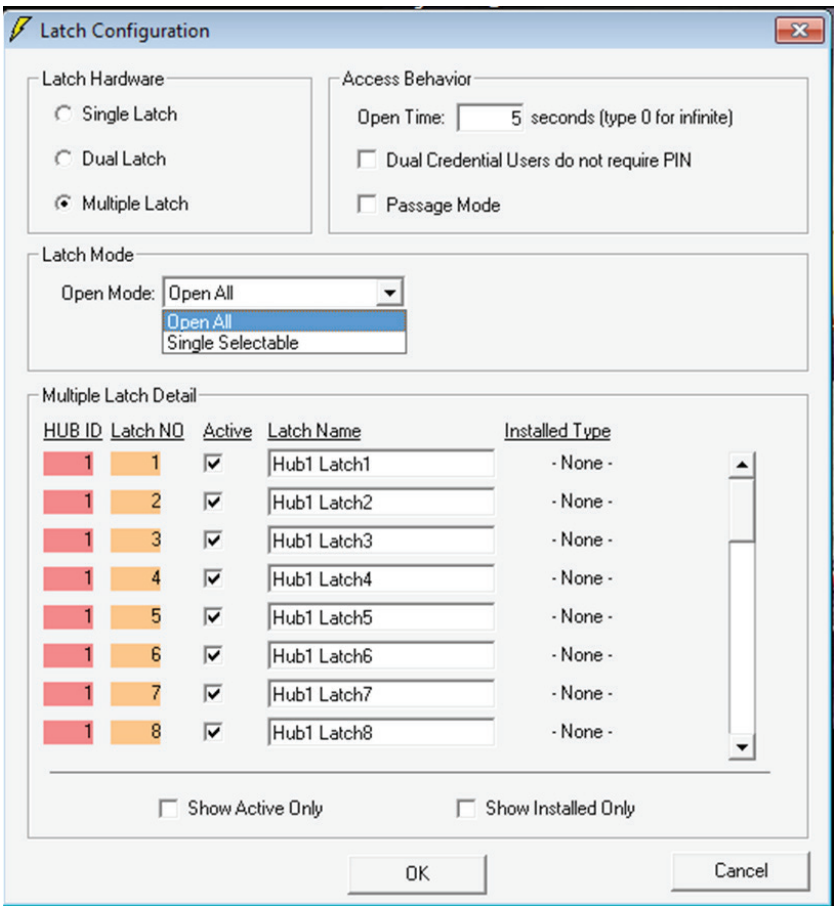
- ➔ Standard Latch is the standard die cast CompX eLatch that is typically installed in the retrofit eLock product.
- ➔ Deadbolt Latch is a specially equipped CompX eLatch that has been constructed to push the bolt out upon locking. There is no spring return.
- ➔ If a 12V door strike is connected, select the smallest size strike (Heavy Duty, Medium Duty or Light Duty) that will keep the internal solenoid pulled in after it opens. This will conserve battery life.
- ➔ If a 12V door strike is connected the Lock Voltage setting must be 12V.

LOCK / USER EDITOR continued



Dual latch – if the CompX elock only has two latches connected, choose "dual latch." Then, under **Latch mode**, choose the types of latches connected under **Latch 1 Type** and **Latch 2 Type**: they can be set to any of the styles available for Latch 1 Type noted above. Finally, choose the **Latch 2 Mode**. There are three settings for **Latch 2 Mode**: Open with Latch1, Open with Dual Credential, and Independent Control.

If Open with Latch1 is selected, latch 2 will open simultaneously with latch 1. If Open with Dual Credential is selected, latch 1 will open with the first credential of a dual credential user and latch 2 will open with the second credential of that dual credential user. Note: All second credentials must be a 4 to 14 digit PIN. If Independent control is chosen, then this lock will have ability to grant access to its latches independently. In the access rights screen (see page 20) the operator will be able to press "+" which will then list the latches that the lock has. Access can then be granted in a latch-by-latch basis.



Multiple latch – if the CompX eLock only has the CompX Hub system attached choose "Multiple latch." The hub system will automatically determine the number and types of latches connected. Under **Open Mode** choose how the latches will open. If Open All is selected, all latches that a user has access to will open simultaneously upon presentation of a valid credential. If Single Selectable is chosen, the user will choose which latch they desire to open upon presentation of a valid credential. In the access rights screen (see page 21) the operator will be able to press "+" which will then list the latches that the lock has. Access can then be granted in a latch-by-latch basis.

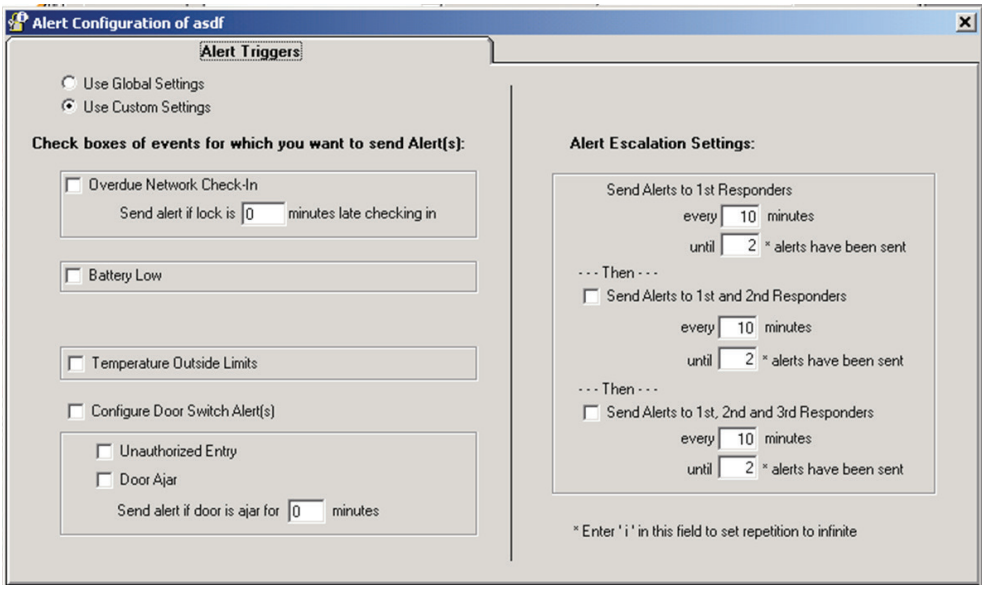
➔ **Multiple Latch Detail** If Multiple Latch is chosen under **Latch Hardware**, additional options will appear in the **Multiple Latch Detail** area. It is possible to assign each latch connected to the Hub a **Latch Name**. This latch name will appear in the access rights screen, the audit trail and on the LCD screen of the lock itself. To modify a latch name simply click on the default latch name (e.g. Hub 1 latch 3) and replace it with the desired name. When the Hub recognizes that a latch is connected,

LOCK / USER EDITOR continued

the type of latch will appear under **Installed Type**. It is possible to make latches active or inactive under the **Active** column. If a latch is not active, it will not appear in the access rights screen and therefore access cannot be granted to it. Finally, there are check boxes on the bottom identified as **Show Active Only** and **Show Installed Only**. If these are chosen, the non-active and/or non-installed laches will not appear on the LockView **Multiple Latch Detail** screen.

18. **GLOBAL LOCK SETTINGS**

If the new eLock will be part of the Notifier system (See **Notifier** page 42) click **Alert Setup** to enter the proper settings.



19. **SETUP THE ALERT TRIGGERS**

Click **Use Global Settings** or **Use Custom Settings** to select how this lock's alerting will be set up. **Use Global Settings** will allow this eLock to follow the **Global Settings** that are programmed under **Notifier**; **Global Lock Settings**. **Global Settings** allows the LockView Operator to manage multiple similar eLocks simultaneously without having to adjust each one individually. See page 46 for instructions on **Global Lock Settings**. Click **Use Custom Settings** if this eLock will have different alarming settings from those that follow global settings.

If **Use Custom Settings** is selected:

a. Choose the eLock alert events for which notification is desired.

- ➔ Select **Overdue Network Check-In** to send an alert(s) if an eLock has missed the scheduled network update (see **Lock/User Editor; Lock Editor Network eLock Scheduler** on page 15) for which the amount of time past due is programmable.
- ➔ Select **Battery Low** to send an alert(s) if the battery power drops too low.
- ➔ If the eLock is a temperature monitoring eLock, **Temperature Outside of Limits** selection will appear. This setting will send an alert(s) if the eLock has 1) temperature alarming enabled, 2) the current temperature is outside of the high/low limits and 3) the temperature has been outside of the specified limits for a time exceeding the **Alarm Delay** time. See page 39 for more information on temperature alarming.
- ➔ If **Door Switch Installed** was selected in the **Lock Editor**; **Door Switch** menu, the **Configure Door Switch Alerts** selection will appear. This alert can be sent for two types of **Door Switch Alerts**. **Unauthorized Entry** will send an alert(s) if the door switch opens at a time not immediately following the presentation of a valid credential. **Door Ajar** will send an alert(s) if the door has been open for a programmable amount of time; past the standard eLock open time (see **Lock Editor-Door Switch Menu** on page 15).

LOCK / USER EDITOR continued

b. **Alert Escalation Settings** allows the LockView Operator to set up a schedule for how often and how many alert(s) will be sent to the Responder(s).
   - ➔ Enter how often and how many alert(s) will be sent to the 1st Responder(s) before escalating to the 2nd Responder(s).
   - ➔ Enter how often and how many alert(s) will be sent to the 2nd Responder(s) before escalating to the 3rd Responder(s).
   - ➔ Enter how often and how many alert(s) will be sent to the 3rd Responder(s).

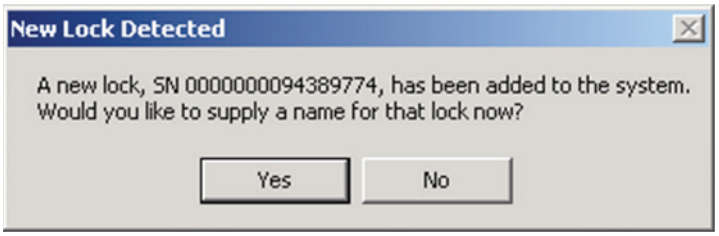
   NOTE: *Entering an "i" in the number of alerts field will force an infinite number of alerts.*

c. Click **Save** when done.

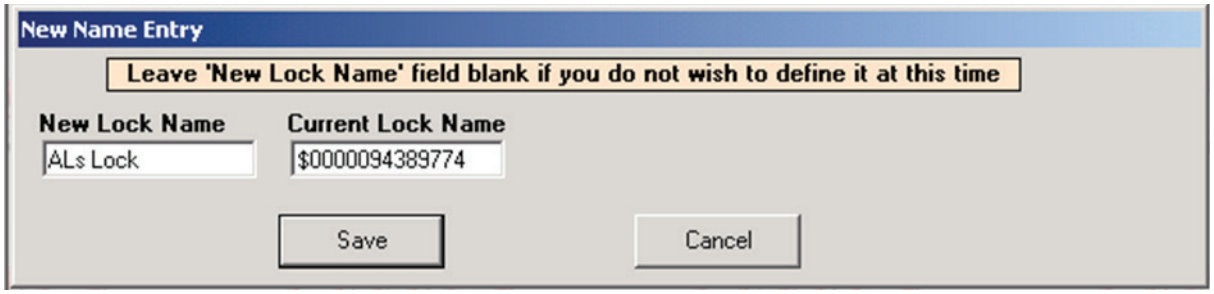
   Note: *The lock's internal memory must match the database for every setting noted above. The status of the lock setting VS database setting is shown adjacent to* ***Lock in Sync? Yes/No****. If the lock and the database are NOT in sync, the* ***VIEW*** *button will appear. This button will open the* ***Lock Settings*** *tab in* ***Read/Write Lock****.*

TO ADD A NEW LOCK AUTOMATICALLY

1. Press and hold "CLEAR" on the keypad. "**ENTER SETUP CODE**" will appear.
2. Enter the setup code that was provided on the sticker set with the lock into the keypad.
3. Connect a USB cable from the computer to the lock. If a network module (802.11 or Ethernet) is being used and it is setup and properly configured, press the "NETWORK" button on the keypad to initiate a manual update.
4. Within a few seconds, the following window will appear in LockView. SNXXXX is the serial number of the lock being added.



5. Click **Yes.**
6. Enter the **New Lock Name**. The lock and all of the settings will be loaded into the database.



TO EDIT AN EXISTING LOCK

1. Select **Lock/User Editor**. Select **Lock Editor**.
2. Highlight **Lock Name** and select **Edit Lock**. Note: lock **Access Type** cannot be edited.
3. Select **OK** when done.

NOTE: *The lock's internal memory must match the database for:* ***Access Type, Open Time, Passage Mode, Dual Credential Users do not Require PIN, Keypress Volume, Bad Credential Lockout, LCD Mode, Lock Secure If Battery Low, Lock Voltage, Door Switch Menu, latch number and type.*** *To compare the lock settings information and database information, go to the* ***Lock Settings*** *tab under* ***Read/Write Lock*** *and update as necessary.*

LOCK / USER EDITOR continued

4. Select **Close**.

TO DELETE A LOCK

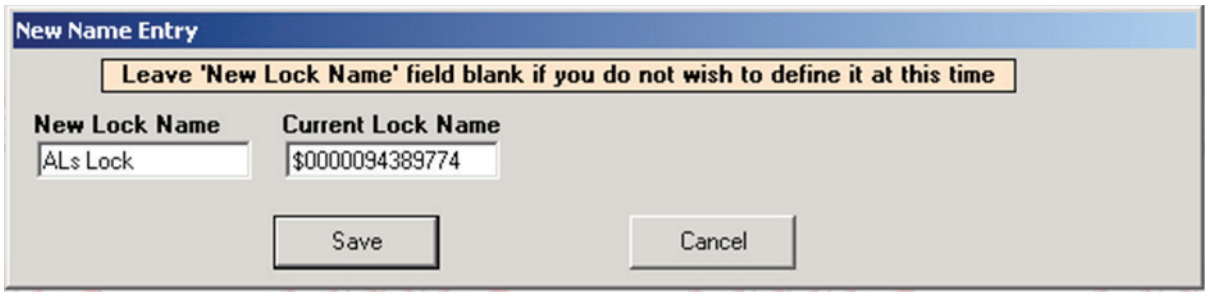
1. Select **Lock/User Editor**. Select **Lock Editor**.

NOTE: *Before deleting a lock, it is recommended to remove all access rights to the lock from all users. This ensures the lock is deleted and will not be accidentally reinstated.*

2. Highlight lock name and select **Delete Lock**.
3. Select **Close** to close **Lock Editor**.

TO NAME A NEW LOCK

If a lock was automatically entered into the database and has not been given a proper name; the lock name will appear as $xxxxxxx in the list of locks in the **Lock Editor**, "xxxxxxx" represents the serial number of the lock. To give the locks a proper name, click **Name New Locks.**



OUT OF SYNC LIST

Clicking the **Out of Sync** button will open a window that shows the list of locks that are not "in sync" with the database (lock settings or current users)

ACCESS RIGHTS

Access Rights is used to choose which locks users can have access to in the database. Each lock is limited to a total of 3000 users.

1. Select **Access Rights** from the **Lock/User Editor** window.

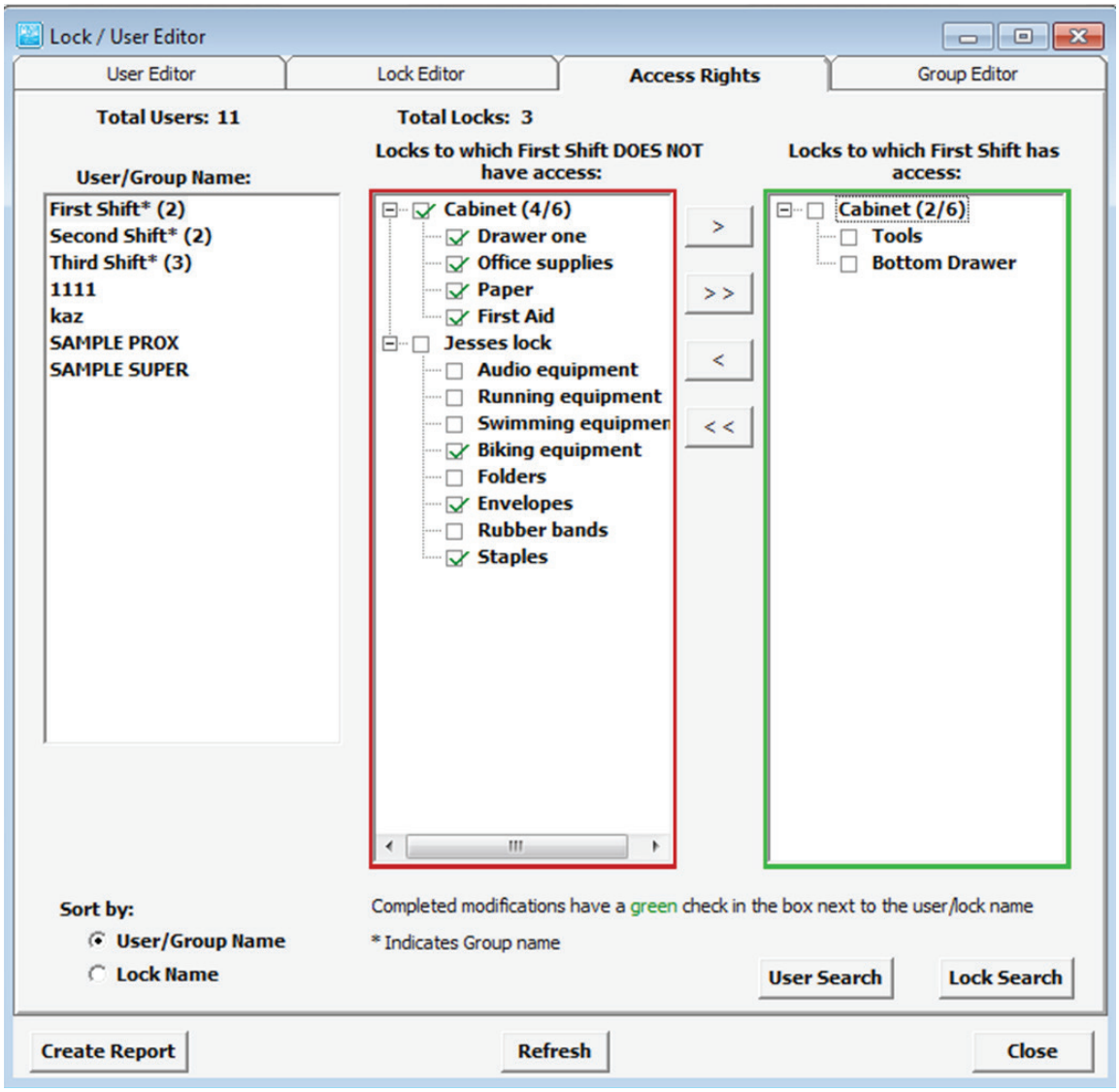
NOTE: *Select **User/Group Name** or **Lock Name** in the bottom left corner under **Sort by** to view access rights organized by user/group name or lock name. In steps 2-4, the window is set for Sort by: User/Group Name.*

2. Select the user/group whose access rights will be modified.
   - ➔ All locks in the middle column (red box) are locks to which the selected user/group does not have access.
   - ➔ All locks in the right column (green box) are locks to which the selected user/group has access.

NOTE: *An unchecked box in the adjacent entry represents information that has not yet been uploaded into the lock.*

LOCK / USER EDITOR continued

3. To change access rights for a single lock, select lock from the list and:



- ➔ Press the appropriate single arrow button between the two columns, or
- ➔ Double click on the lock name.

4. To change access rights for all the listed locks:
   - ➔ Switch one lock at a time (refer to step 3), or
   - ➔ Press the appropriate double arrow button between the two columns.

NOTE: *Changing a position in **Access Rights** only changes the LockView database. The contents of the lock do not automatically change. See **READ/WRITE LOCK** for instructions on updating the lock database.*

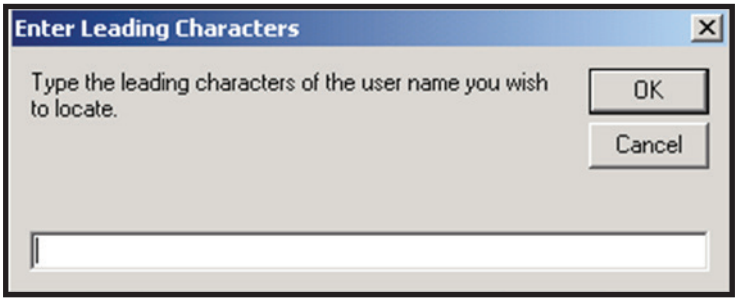
NOTE: *If a user's attributes have changed (in the User Editor) and that user has access to a given lock(s), the check in the the box next to their name will be red, thereby indicating the lock(s) need to be updated.*

NOTE: *Once the locks memory matches that of the LockView database, the color will return to green.*

LOCK / USER EDITOR continued

5. When viewing users/groups, the group name will be followed by an asterisk (*) along with the number of members of the group in parentheses, for example **(4)** indicates four members. When adding groups, each group member will use one memory slot in the lock.
   ➔ Access rights can also be sorted according to the lock name. If organized by lock name, refer to steps 2-4 but substitute lock access rights for users access rights.

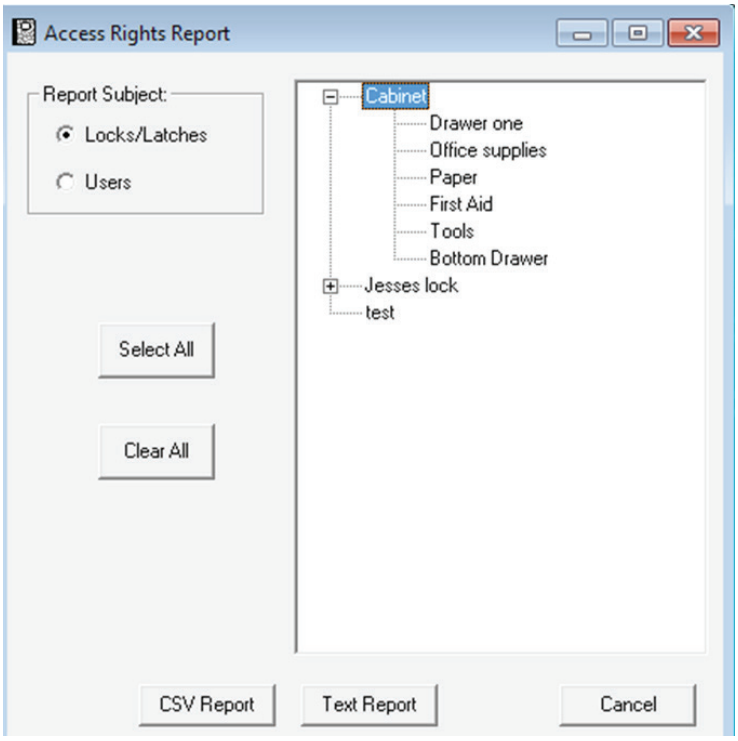
6. If a user/group/lock cannot be found, click **User Search** or **Lock Search**. Click **OK** after the leading characters of the lock name user/group/lock have been entered.



7. If a report of users that can access a lock/latch or a report of locks/latches that a user can access is desired, click "**Create Report.**" This will open a window allowing the operator to choose.

   Report Subject – choose the report type: 1) which users can access which locks/latches or 2) which locks/latches a can be accessed by which users

   After the **Report Subject** is chosen, select which users (or locks) the report will be detailing. Multiple users (or locks) can be chosen by holding control (pick specific) or shift (pick a range). **Select all** and **clear all** can also be chosen. Once the selections have been made, pick **CSV Report** or **Text Report** depending on the type of report desired.



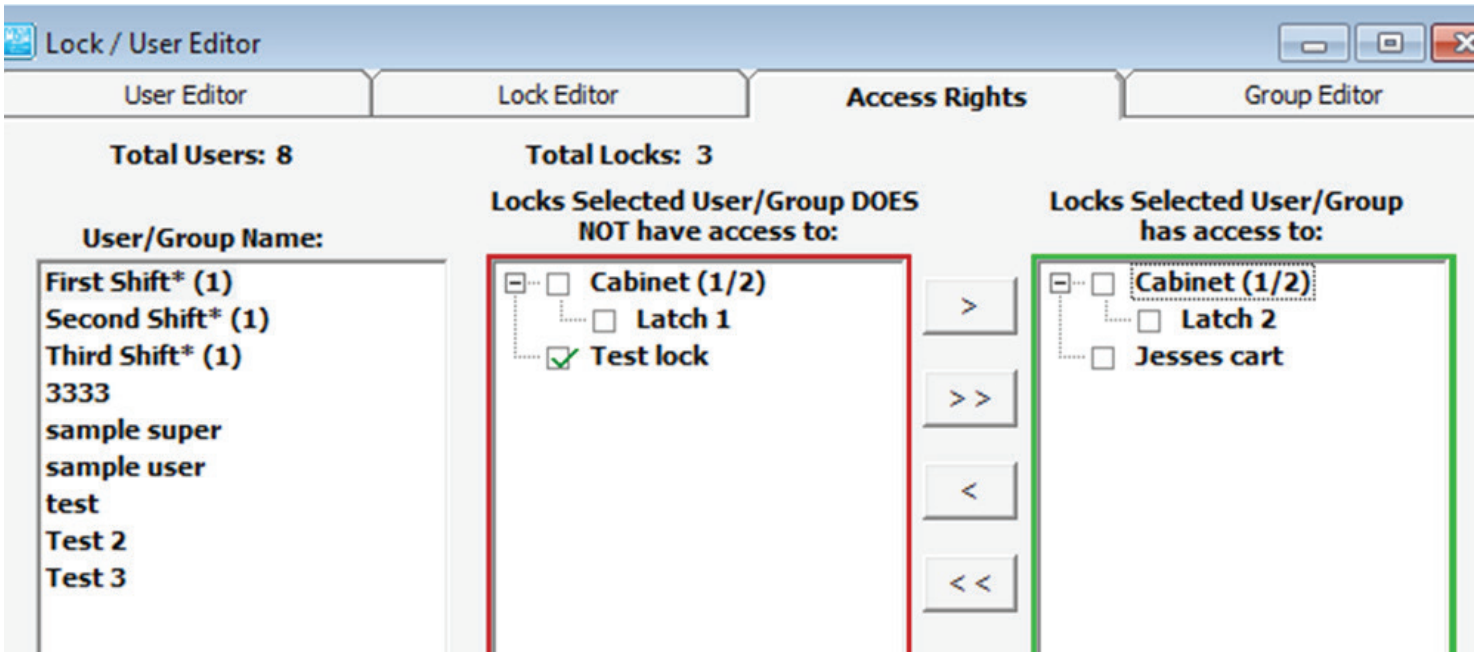
LOCK / USER EDITOR continued

MULTI LATCH ACCESS RIGHTS

If one (or more) of the locks in the system were set up for Dual latch-Independent Control or Multiple Latch (see **Lock Editor** page 17) there will be a couple of differences in the Access Rights screen. If the screen is set to sort by Users, there will be a "+" or "-" next to each lock with independent or multiple latch control. Clicking "+" will expand the lock so that each latch is visible within the lock, as show below.

Granting access to a latch within a lock is done in exactly the same fashion as granting access to the entire lock; click on the latch that the user will have (will not have) access to and press one of the arrow buttons to grant/remove access for the selected user.

It is possible for a user to have access to one latch and not have access to another within a lock. In this case, following the user name there will appear a parenthesis showing how many latches the user has access to (does not have access to), followed by the total number of latches. This is illustrated in the example shown below.



In this case the user has access to **Latch 2** in **Cabinet** and does not have access to **Latch 1**.

LOCK / USER EDITOR continued

GROUP EDITOR

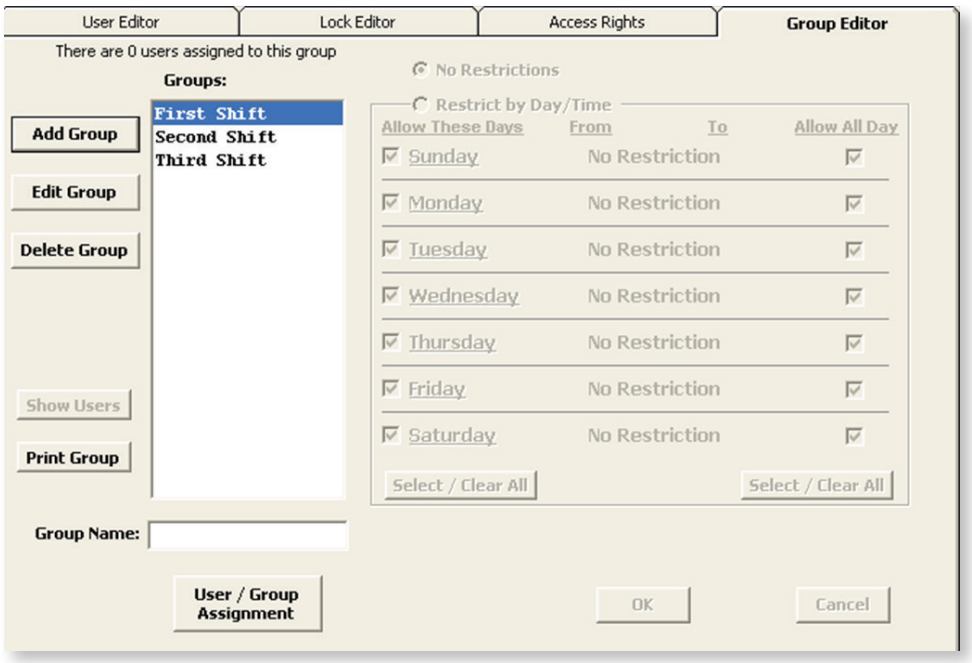
The **Group Editor** tab is used to add, edit, or delete groups from the computer database. This option makes it easier to add or delete groups of users from a lock. Users in a group will all have the same time-based access to locks, as well as common access rights.

TO ADD A NEW GROUP

1. Select the **Lock/User Editor** window. Select the **Group Editor** tab.
2. Select **Add Group** to create a new group in the computer database.
3. Enter the new group's name.
4. If the new group has no restrictions, check the **No Restrictions** box.
5. If the new group has restricted access to locks, check the days the group is not restricted.
6. Fill in the time slots the new group can access the locks, or check the **All Day** box if the group has 24 hour access. When filling in time slots, LockView® will automatically wrap a day. (Example: 11 p.m. Monday - 7 a.m. Tuesday.)
7. Select **OK** when done.
8. Select **Close** to close the **Group Editor** tab.

TO EDIT A NEW GROUP

1. Select the **Lock/User Editor** window. Select the **Group Editor** tab.
2. Select group name and then select **Edit Group** to edit the group's restriction information.
3. Select **OK** when done.
4. Select **Close** to close the **Group Editor** tab.



TO DELETE A GROUP

1. Select the **Lock/User Editor** window.

NOTE: *If you delete a restriction group, all users assigned to it will be set to "No Access."*

2. Select group name and then select **Delete Group** to delete an existing user from the local computer database.
3. Select OK to close the **Group Editor** tab.

PRINT GROUP

To print the names of the members of a group(s) AND the locks to which they have access, click the **Print Group** tab.

MORE INFORMATION BUTTON

Clicking the More Information button ... will pop up a list of all users currently assigned to a highlighted group.

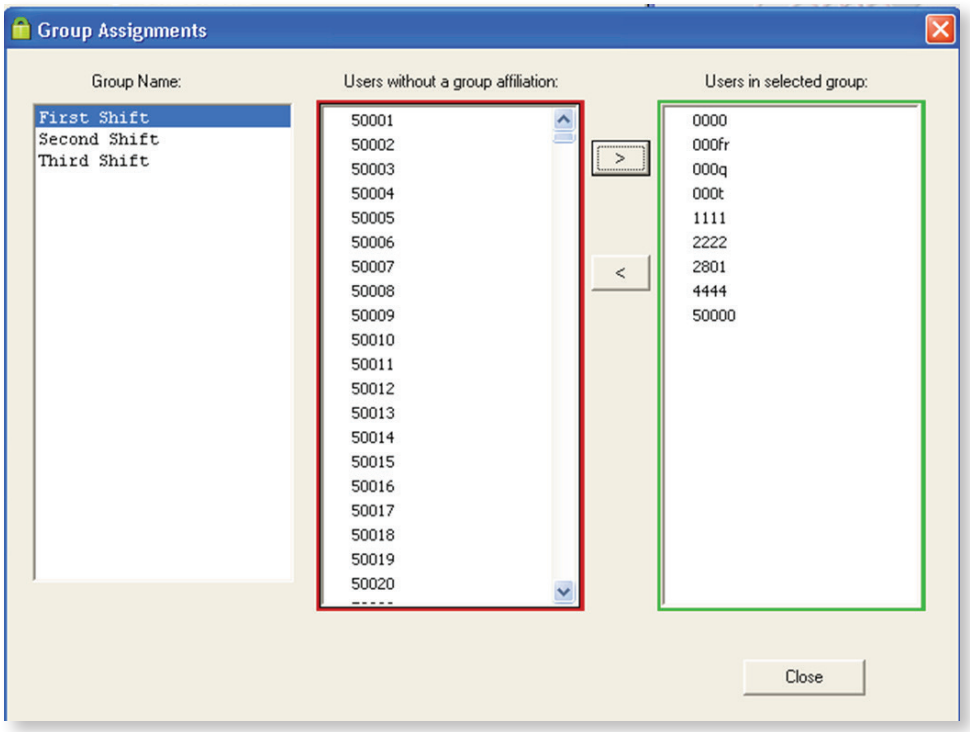
LOCK / USER EDITOR continued

USER/GROUP ASSIGNMENT

1. Select **User / Group Assignment** to open up the **Group Assignments** window. The name of the group(s) appear in the left column.
2. Click to highlight the name of the group of interest.
3. The middle column (outlined in red) lists all users who do not have an affiliation to the selected group. The right column (outlined in green) lists all users who are affiliated with the selected group.
4. Click to highlight the user(s) to be manipulated and click the **<** or **>** button to shift the user(s) into the desired columns.

   NOTE: *Ctrl + click or Shift + click can be used to highlight multiple users.*

5. Click **Close** button when done.



READ / WRITE LOCK

Read/Write Lock contains four (4) tabs that allow the Operator to view the database of a lock and download the audit trail from a lock.

CONNECTION

Connection allows the Operator to view a lock's memory content — either virtually (with a networked connection) or in real time with a USB cable connection.

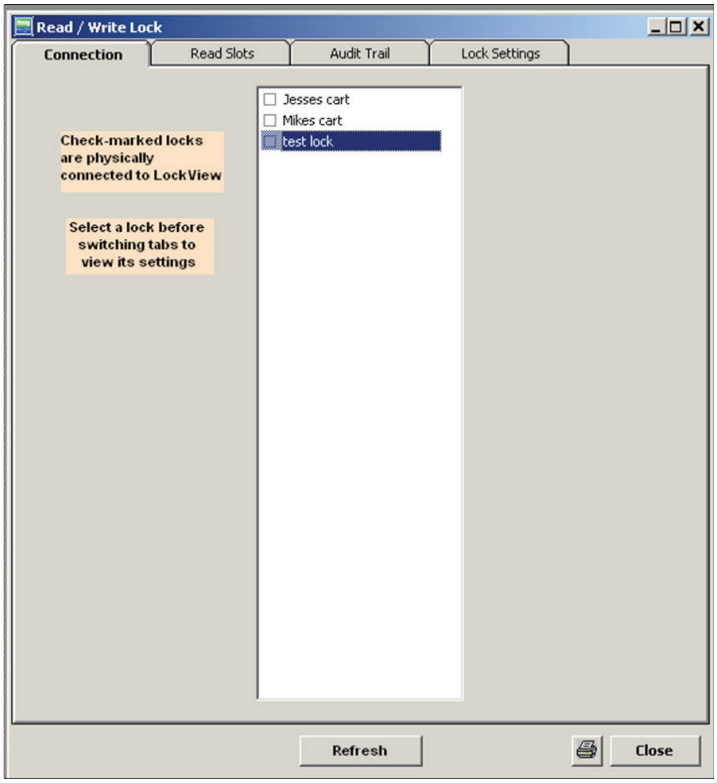
TO CONNECT TO A LOCK:

1. Select **Read/Write Lock**. Select the **Connection** tab.
2. Connect the USB cable from the lock to the computer if real time slot reading or update is desired.
3. The **Read/Write Lock** icon should show a **RED** background.

When the lock is properly connected and LockView is properly communicating with the lock, the **Read/Write Lock** icon should show a **GREEN** background.

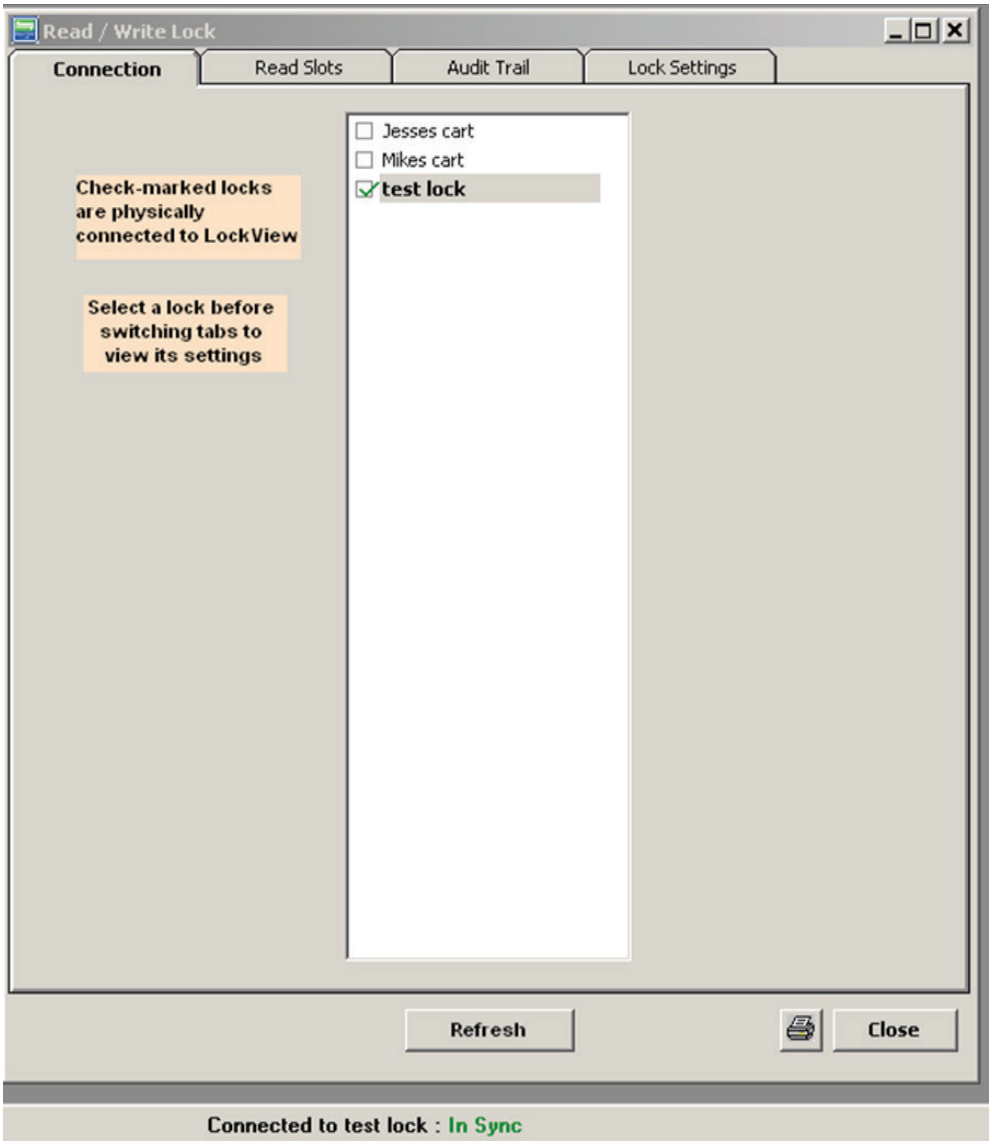
If the icon background does not change to green, the USB drivers are not properly loaded. Visit **compx.com** to download new USB drivers or contact technical support.

4. The **Read/Write Lock** screen is shown below.



READ / WRITE LOCK continued

5. Insert the USB cable into the lock. After a few seconds, the screen should look similar to the figure below, with the lock name to which the USB cable is connected being highlighted with a check appearing the box next to it. Further, the status bar will now say **Connected to: "*lock name*"** where lock name is the name of the connected lock.



READ / WRITE LOCK continued

READ SLOTS

Read Slots allows the Operator to view the slots assigned to users in the database along with the actual contents of the slots in the lock. If the computer database and the lock contents for a numbered slot do not match, the information in the corresponding slots will be displayed in different colors.

1. Highlight the lock to view in the **Connection** tab of the **Read/Write Lock** menu.
2. Select **Read Slots**.

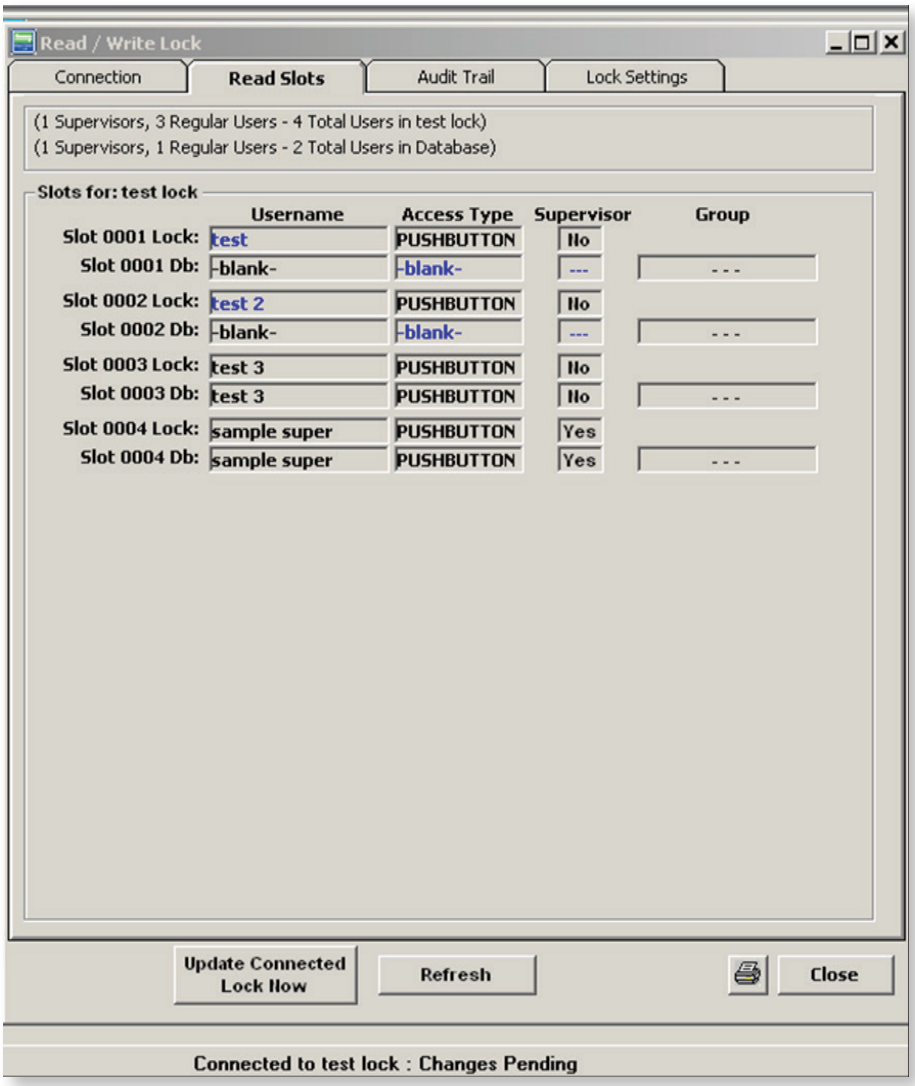
LOCK DATABASE INFORMATION "LOCK"

- User name
- Access type
- Slot number
- Supervisor status
- Group membership

COMPUTER DATABASE INFORMATION "DB"

- User name
- Access type
- Slot number
- Supervisor status
- Group membership

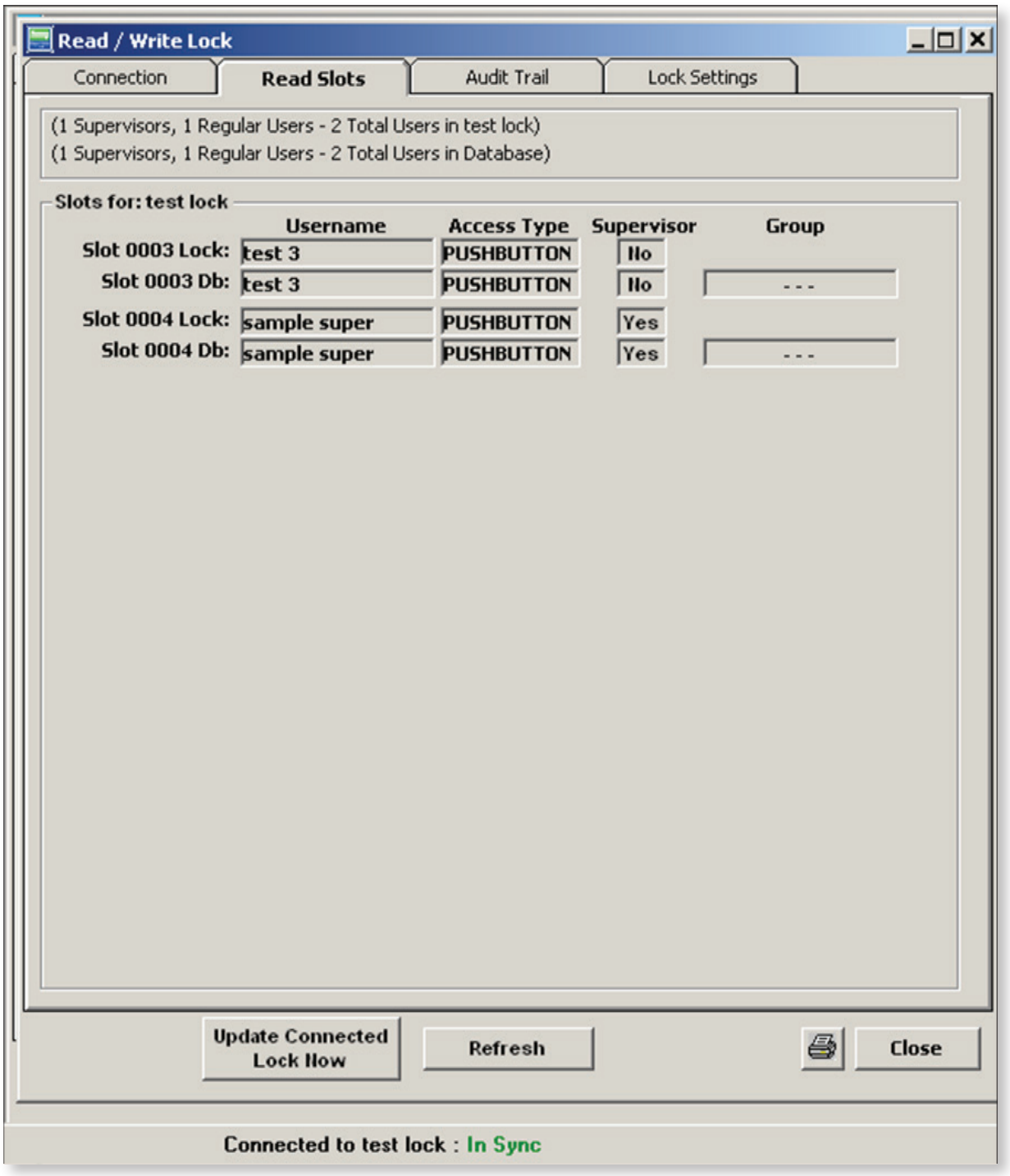
This report also shows if information in the slot database of the lock differs from the slot in the computer database. This is illustrated with blue text, and black text. If the entry in the computer database is in orange, the users information (supervisor status, passage mode status, dual credential status, time based access status) in the database has been modified and will need to be updated within the lock's database.



READ / WRITE LOCK *continued*

The **Read Slots** screen on the previous page shows:

- Four slot assignments for the computer database and a lock titled "Test Lock"
- Slots 0001 and 0002 of the computer database do not match the lock's database.



The **Update Connected Lock Now** button was pressed. The computer database and lock database now match.

Note: *The Update Connected Lock Now button does not appear in a network connection. The databases will automatically sync upon a network connection.*

READ / WRITE LOCK continued

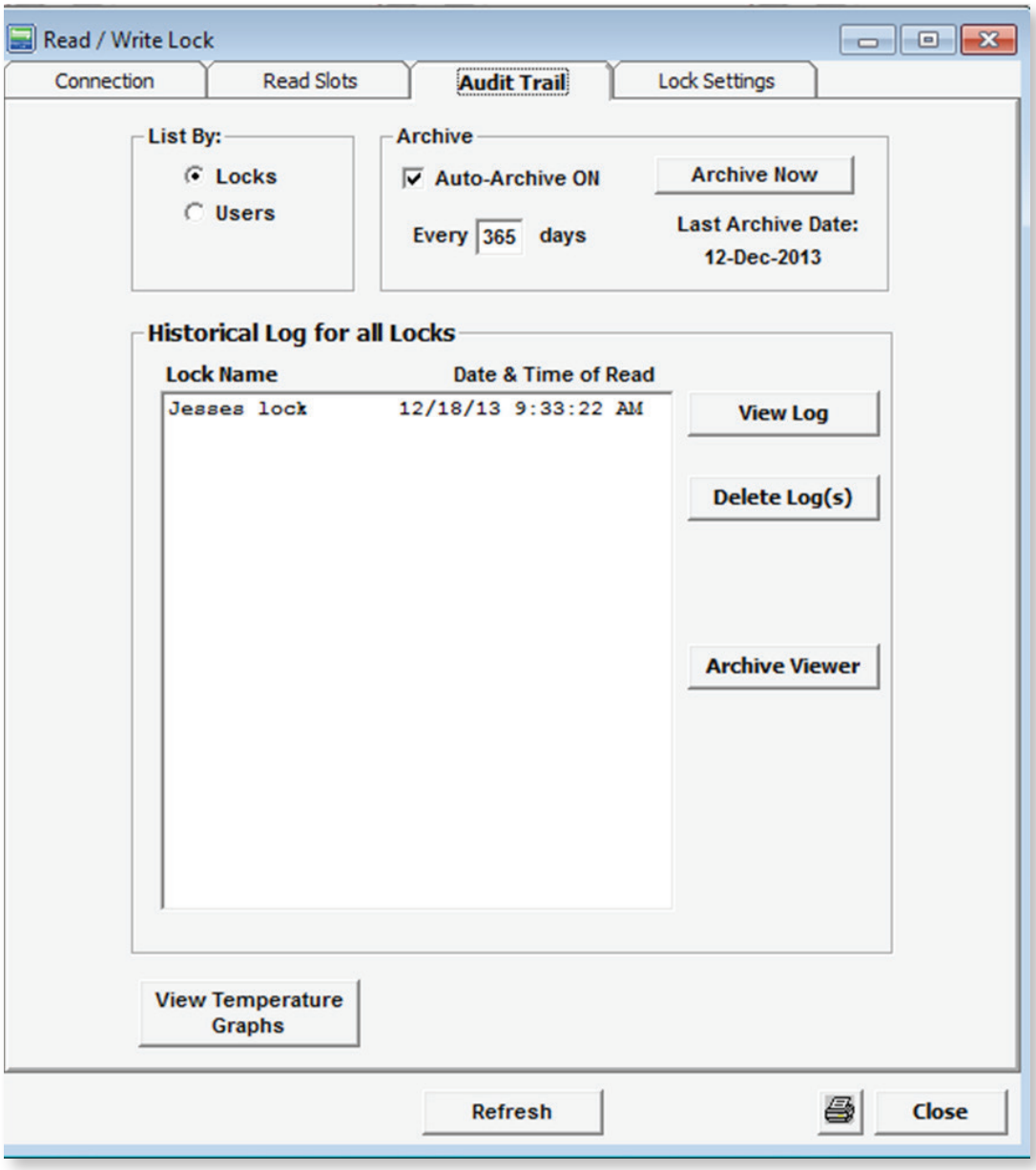
AUDIT TRAIL

Audit Trail allows the Operator to view the audit trail of a lock or a user. A "lock" audit trail is a log of a lock's past operation. These logs include the name of a user attempting to gain access, name of the lock being accessed, what type of credential is being used, and the date and time of attempted access. A "user" audit trail is a log of a users's past operation. These logs include the name of a user , name of the locks being accessed by the user, what type of credential is being used, and the date and time of attempted access.

The size of the cumulative audit trail data can become quite large over time. In order to minimize the load on the database, choose **Auto-Archive On** and enter the number of days between the automatic archiving. The last archive date will be noted under **Last Archive Date**. Once selected, LockView will automatically archive data that is older than half of the auto archive interval (e.g: LockView will archive 183 days worth of audit events if set to archive every 365days)

Choose which type of audit trail is desired by pressing the **locks** or **users** button under **List by**.

1. Select **Audit Trail** from **Read / Write Lock** window.
2. Select the lock whose audit trail is to be viewed.
3. Select **View Log**.



LOG INFORMATION INCLUDES:

- Name of the lock
- Name of the user that attempted access to the lock (if the database has a record for that credential)
- The credential type that was used by the user
- Date and time of attempted access
- Activity detail, noted under "Status"

READ / WRITE LOCK continued

FULL STATUS LIST:

ACCESS

Latch 1 closed:
Latch bolt extended

Latch 2 closed:
Latch 2 bolt extended

(HUB Latch Name) Opened
If the eLock has the HUB system attached, the name of the latch that is opened will appear in the audit trail.

(HUB Latch Name) Closed
If the eLock has the HUB system attached, the name of the latch that is closed will appear in the audit trail.

Access granted:
Credential was authorized to open lock

Access Denied- No rights:
Credential was not authorized to open lock

Access Denied - Lock was in lockout mode:
Credential was not accepted due to lockout mode

Access Denied- Time restriction:
Credential was not accepted due to programmed time based access restrictions

Access Denied- 2nd PIN mismatch:
Incorrect second PIN credential was entered for dual credential user/supervisor

Unauthorized entry alarm cleared:
A valid credential was presented at the lock in order to clear the local alarm (door switch required)

Ajar alarm cleared:
Door switch closed (door switch required)

Access Pending- Await 2nd PIN:
The first credential of a dual credential user/supervisor has been accepted; lock waiting for second PIN in order to grant access

Access granted on 2nd PIN:
The second credential of a dual credential user/supervisor has been accepted; access is granted

Door alarm: Unauthorized Entry:
Unauthorized entry alarm at the lock has been triggered (door switch required)

Door alarm: Ajar:
Ajar alarm at the lock has been triggered (door switch required)

Door opened:
The position of the door switch changed from closed to open (door switch required)

Access Pending: Await 2nd PIN:
Identifies the primary credential of a dual credential has been accepted. Access has not yet been granted.

Door closed:
The position of the door switch changed from open to closed (door switch required).

XXXX added user ABC to slot:
Identifies the supervisor (XXXX) that manually added a new user (ABC) in slot number X

XXXX added supervisor ABC to slot:
Identifies the supervisor (XXXX) that manually added a new supervisor (ABC) in slot number X

XXXX deleted user ABC in slot:
Identifies the supervisor (XXXX) that manually deleted a user (ABC) in slot number X

XXXX deleted supervisor ABC in slot:
Identifies the supervisor (XXXX) that manually deleted a supervisor (ABC) in slot number X

NOTIFIER

Networked (802.11g or Ethernet) eLock is required

LockView Alert TERMINATED:
Confirmation the remote notification alert has been squelched in LockView

LockView Alert Temperature Outside of Limits SENT:
Confirmation the remote notification alert has been started

LockView Alert Door Ajar SENT:
Confirmation the remote notification alert has been started (door switch required)

READ / WRITE LOCK *continued*

LockView Alert Unauthorized Entry SENT:
Confirmation the remote notification alert has been started (door switch required)

LockView Alert Battery State SENT:
Confirmation the remote notification alert has been started

LockView Alert Lock Overdue for Check-In SENT:
Confirmation the remote notification alert has been started

LockView Alert: Lock Overdue for Check-In completed:
Confirmation the remote notification schedule for missed network check-in has been completed

TEMPERATURE

Temperature monitoring eLock is required

Temperature alarm cleared:
Temperature alarm was muted or reset in order to clear the local alarm

Temperature alarm disabled:
Temperature alarm has been turned OFF

Temperature alarm enabled:
Temperature alarm has been turned ON

Temperature warning:
Temperature has gone outside of the acceptable programmed range

Temperature warning cleared:
Temperature has returned to the acceptable programmed range

New Log Freq In: XX:
The temperature logging frequency when in-range has been changed to XX

New Log Freq Out: XX:
The temperature logging frequency when out-of-range has been changed to XX

Alarm: Temperature:
The recorded temperature has been outside of the acceptable range beyond the alarm delay time, thereby activating the temperature alarm

New Low Limit: XX °F (or °C):
Temperature limit changed

New High Limit: XX °F (or °C):
Temperature limit changed

MISCELLANEOUS

Menu access granted:
Supervisor credential was used to gain access to the eLock manual programming menu

Battery state alarm cleared:
Battery charge has been restored. Low battery status has ended.

Time synchronized: Prior to change:
Time to which the lock was set when the time was changed

Time synchronized: After change:
Time to which the was set

Exit passage mode:
A valid credential was presented at the lock whose state was passage mode

Passage mode entered:
A valid credential was presented at the lock whose state was not passage mode

Reboot FW version XX:
The microprocessor has restarted the firmware; firmware version is noted (XX)

Timezone offset changed from -X to -Y:
Time zone to which the lock was set has been manually changed from GMT (X) to GMT (Y).

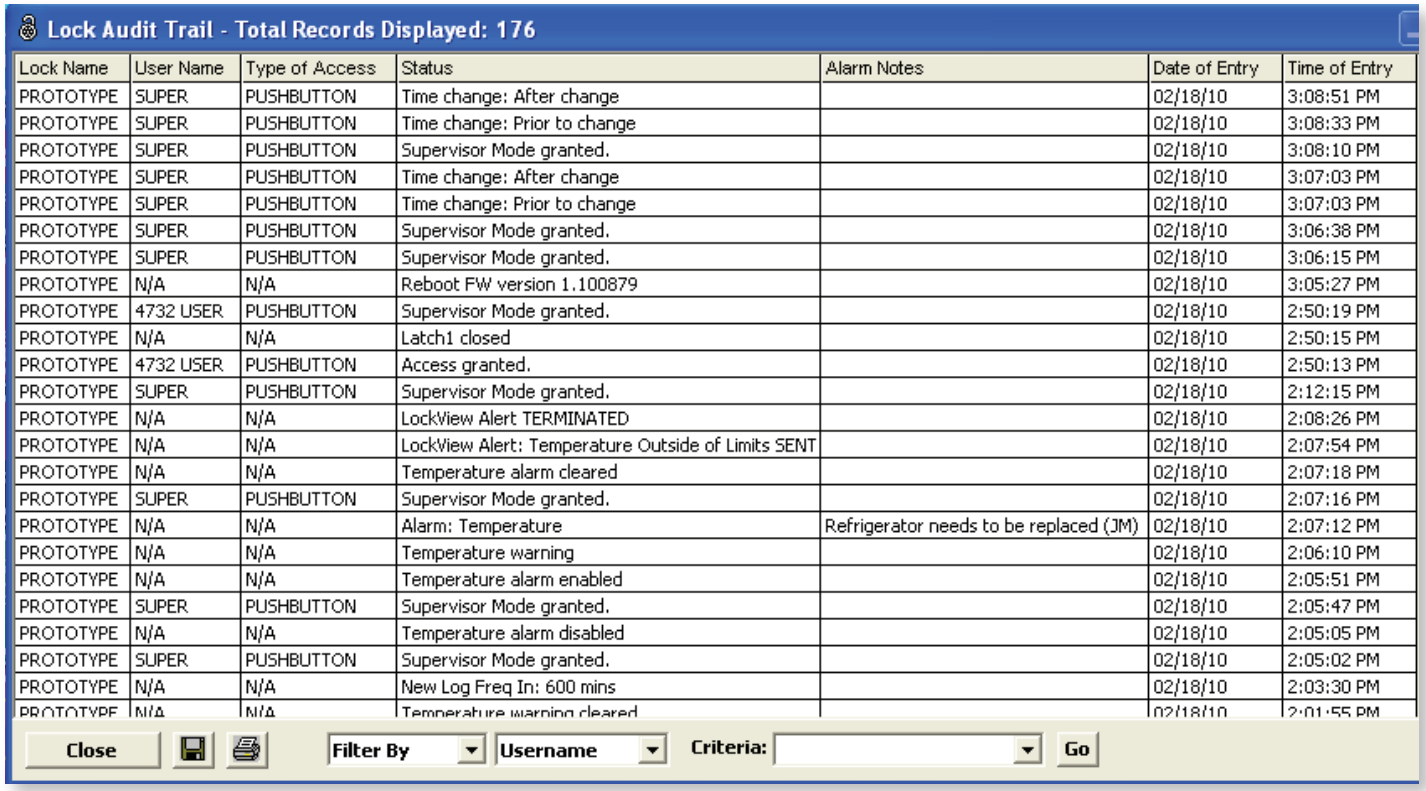
DST ends; Timezone offset changed from -X to -Y:
Time to which the lock was set has automatically changed from GMT (X) to GMT (Y).

Audit trail reviewed by LockView Operator *date/time:*
LockView Operator opened the file that contains the audit trail for the eLock

READ / WRITE LOCK continued

To view an older audit trail entry, select a historical audit trail log file and press the **View Log** button.

4. The tool bar at the bottom of the audit trail display allows the Operator to **Close, Print or Save** to an external text file or csv file, filter or sort the audit trail log information.



Lock Audit Trail - Total Records Displayed: 176

Lock Name	User Name	Type of Access	Status	Alarm Notes	Date of Entry	Time of Entry
PROTOTYPE	SUPER	PUSHBUTTON	Time change: After change		02/18/10	3:08:51 PM
PROTOTYPE	SUPER	PUSHBUTTON	Time change: Prior to change		02/18/10	3:08:33 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	3:08:10 PM
PROTOTYPE	SUPER	PUSHBUTTON	Time change: After change		02/18/10	3:07:03 PM
PROTOTYPE	SUPER	PUSHBUTTON	Time change: Prior to change		02/18/10	3:07:03 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	3:06:38 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	3:06:15 PM
PROTOTYPE	N/A	N/A	Reboot FW version 1.100879		02/18/10	3:05:27 PM
PROTOTYPE	4732 USER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	2:50:19 PM
PROTOTYPE	N/A	N/A	Latch1 closed		02/18/10	2:50:15 PM
PROTOTYPE	4732 USER	PUSHBUTTON	Access granted.		02/18/10	2:50:13 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	2:12:15 PM
PROTOTYPE	N/A	N/A	LockView Alert TERMINATED		02/18/10	2:08:26 PM
PROTOTYPE	N/A	N/A	LockView Alert: Temperature Outside of Limits SENT		02/18/10	2:07:54 PM
PROTOTYPE	N/A	N/A	Temperature alarm cleared		02/18/10	2:07:18 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	2:07:16 PM
PROTOTYPE	N/A	N/A	Alarm: Temperature	Refrigerator needs to be replaced (JM)	02/18/10	2:07:12 PM
PROTOTYPE	N/A	N/A	Temperature warning		02/18/10	2:06:10 PM
PROTOTYPE	N/A	N/A	Temperature alarm enabled		02/18/10	2:05:51 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	2:05:47 PM
PROTOTYPE	N/A	N/A	Temperature alarm disabled		02/18/10	2:05:05 PM
PROTOTYPE	SUPER	PUSHBUTTON	Supervisor Mode granted.		02/18/10	2:05:02 PM
PROTOTYPE	N/A	N/A	New Log Freq In: 600 mins		02/18/10	2:03:30 PM
PROTOTYPE	N/A	N/A	Temperature warning cleared		02/18/10	2:01:55 PM

Close | Filter By | Username | Criteria: | Go

THE AUDIT TRAIL LOG CAN BE FILTERED ACCORDING TO:

- User Name
- Type of Access
- Status: Access Requests only and Hide latch actions. These selections will significantly reduce the size of the audit trail by removing ancillary lock actions and latch actions by HUB connected locks.

THE AUDIT TRAIL LOG CAN BE SORTED ACCORDING TO:

- User Name
- Type of Access
- Status
- Date and Time
- Chronological

5. Audit trails can be viewed, deleted and archived by selecting the appropriate button.

READ / WRITE LOCK continued

NOTES ENTRY

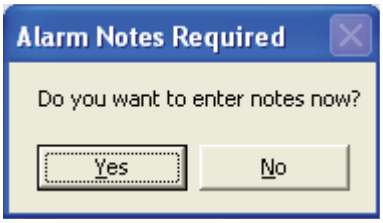
The Operator of LockView will be automatically prompted to enter a note if an eLock records

1) a temperature alarm* (requires temp eLock)
2) an unauthorized entry alarm (requires door switch) and/or
3) a door ajar alarm (requires door switch).

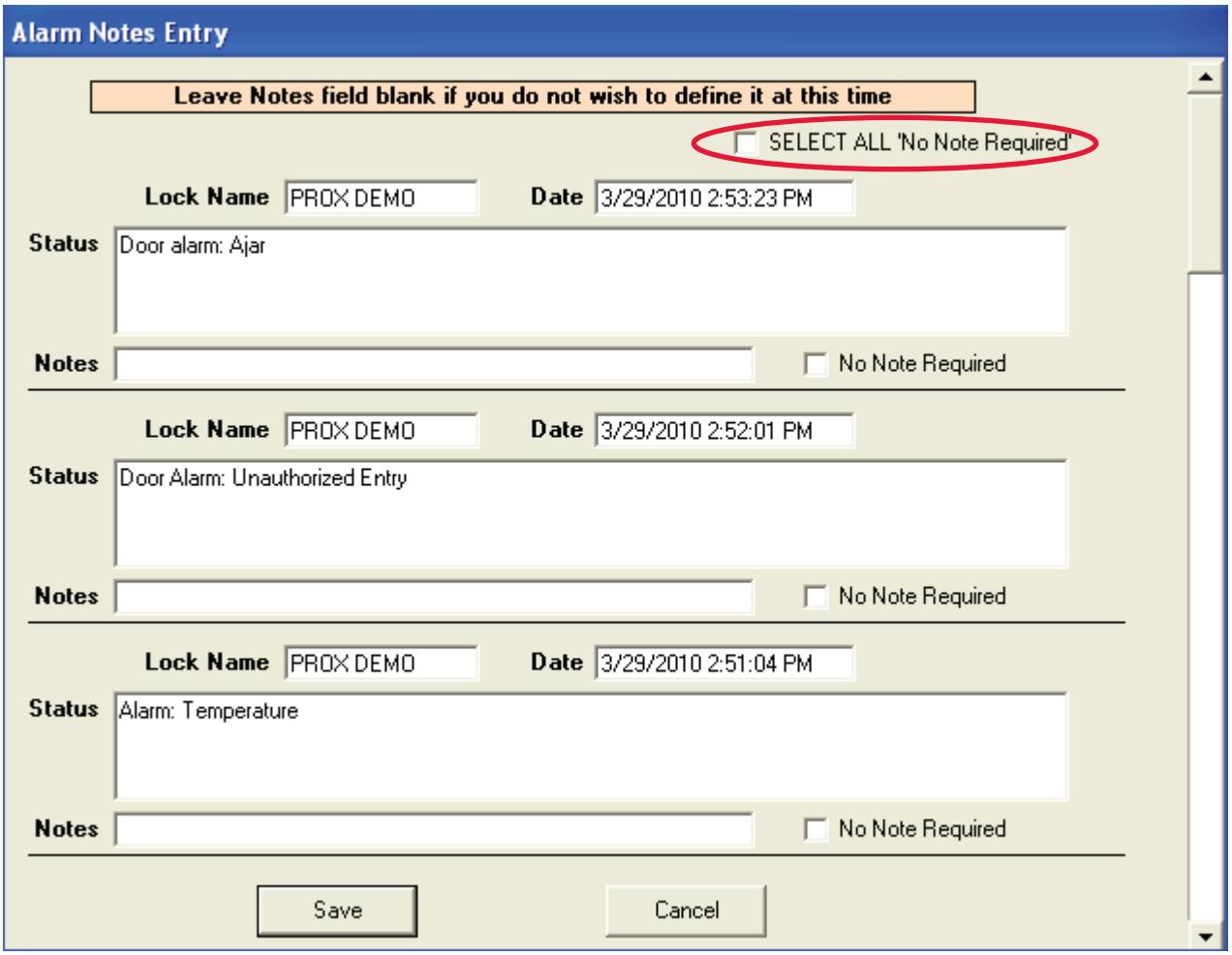
Using the Notes Entry feature, the action that was taken as a result of the alarm can be documented. This note will then become part of the access audit trail.

* *Notes entered for a temperature alarm will also become part of the temperature log.*

The below will automatically appear if a temperature, unauthorized entry, and/or a door ajar alert is recorded by an eLock. (Temperature monitoring requires temperature monitoring eLock. Unauthorized entry and door ajar requires door switch to be installed (door switch not included).

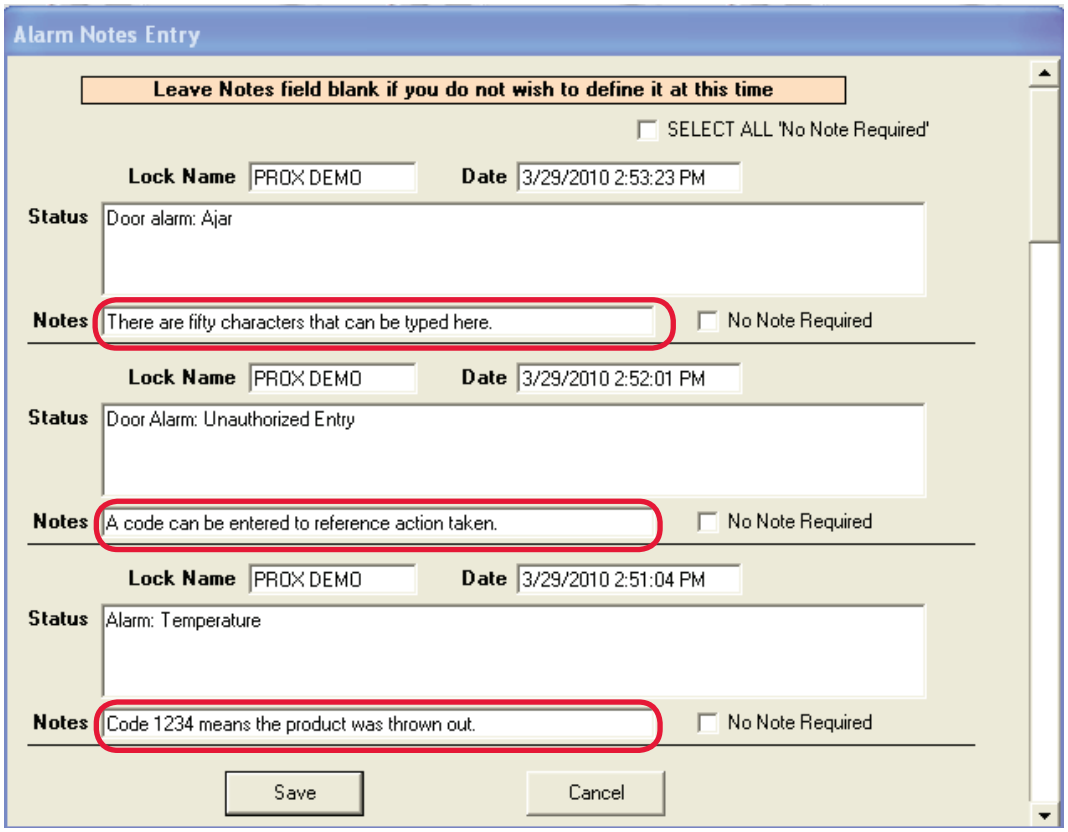


In the event that notes are not required for multiple alerts, check the SELECT ALL 'No Note Required' option.

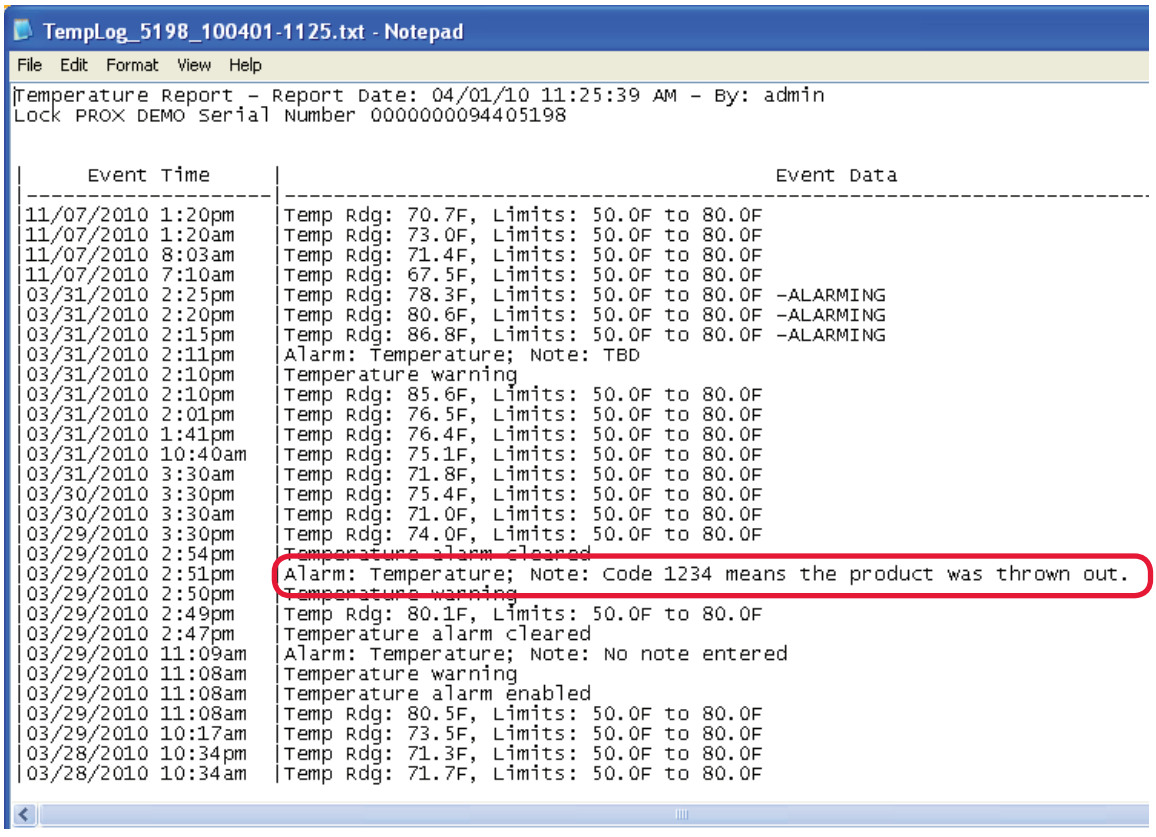


READ / WRITE LOCK continued

Click in the **Notes** field to document what action was taken as a result of the recorded alert.



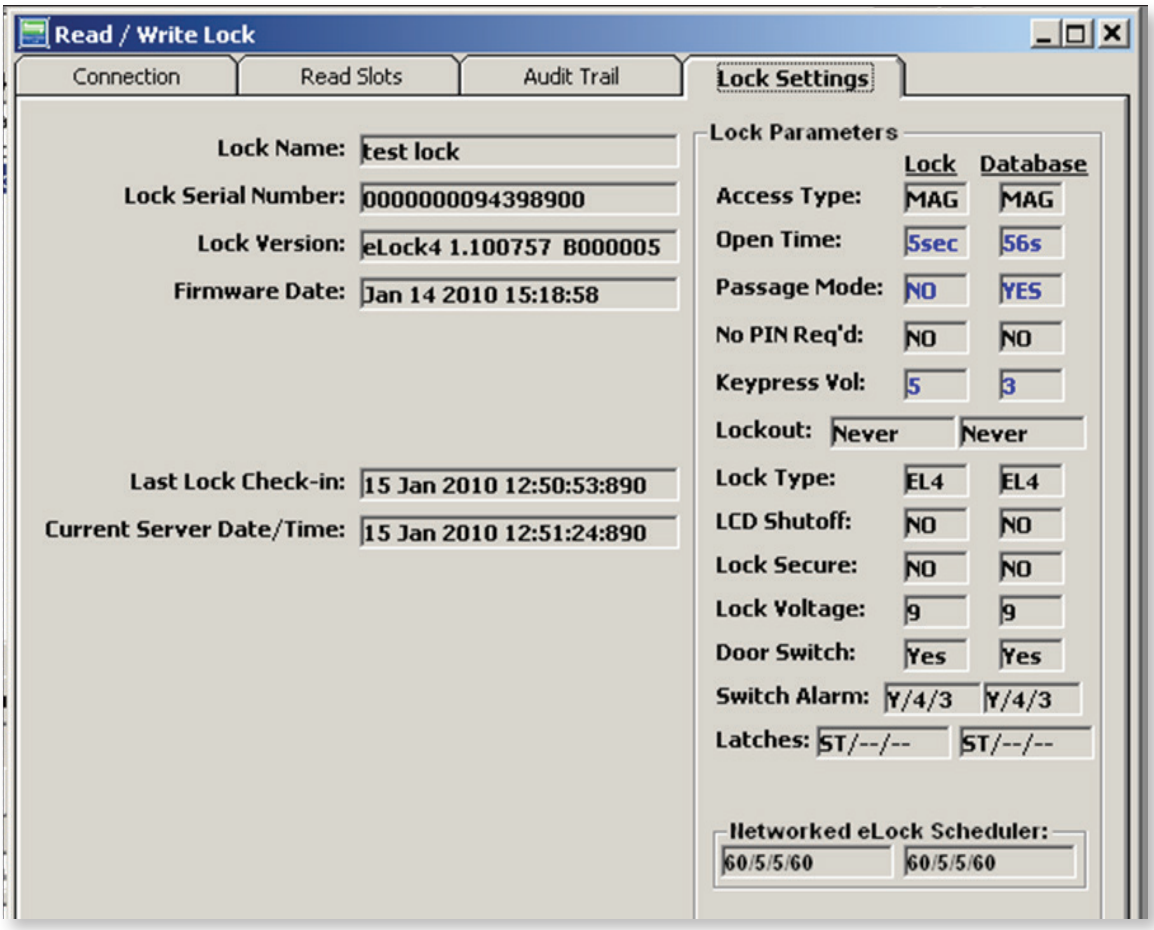
The note for a temperature alarm will also become a part of the temperature audit trail.



READ / WRITE LOCK continued

LOCK SETTINGS

1. Choose desired lock to view under **Connection** tab.
2. Select **Lock Settings** from **Read/Write Lock**.
3. The lock and computer database characteristics and parameters are displayed.



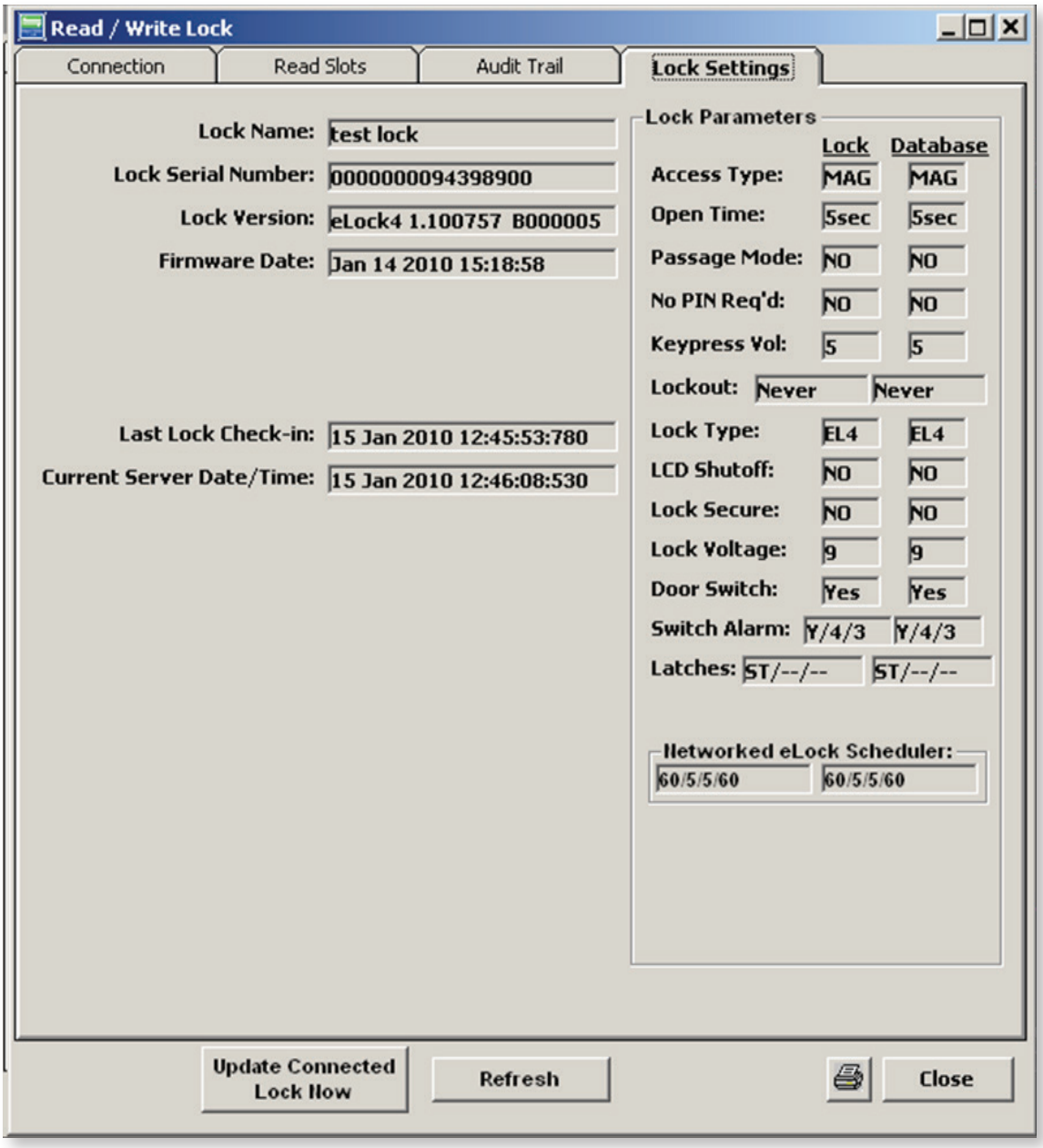
This screen shows:

- Lock Access Type
- Open time
- Passage Mode
- No PIN Req'd (dual credential users do not require PIN)
- Keypress volume
- Lockout
- Lock type
- LCD shutoff
- Lock secure
- Lock voltage
- Door switch
- Switch Alarm
- Latches
- LAN times (network required)

READ / WRITE LOCK continued

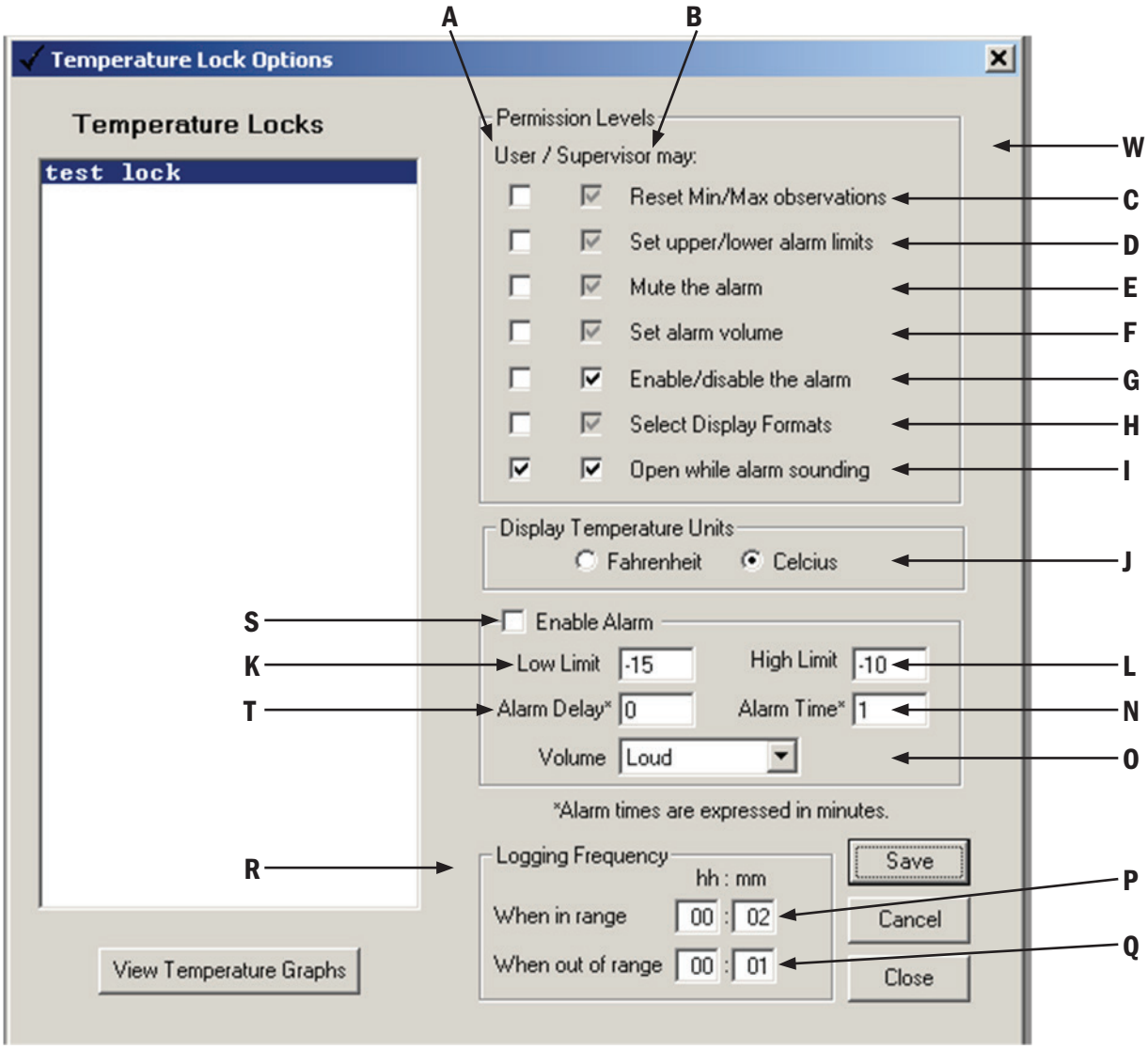
This report also shows if information in the lock database differs from the information in the computer database. This is illustrated with blue text and black text. The Lock Parameter information can be found and/or edited by opening **Lock Editor**.

4. Click the **Refresh** button to compare lock data to computer database data.
5. **Update Connected Lock Now** permits a direct manipulation of the lock database. Click the **Update Connected Lock Now** button to match up the lock with the computer database.



TEMPERATURE OPTIONS

Clicking the **Temperature Lock** icon allows changes to be made to locks provided with temperature monitoring capabilities. Viewing of temperature output graphs and data output is also provided.



To change a temperature lock's settings or view output reports or graphs, first choose the desired lock in the column on the left. Note: the "temperature lock" column is a list of all locks that are checked as being "temperature lock" in the lock editor. See page 14.

The upper section **(W) (Permission Levels)** is used to select which manual programming temperature monitoring options can be accessed by Supervisors and Users at the lock. The first column of check boxes **(A)** shows which options are available to Users; the second column **(B)** shows which options are available to Supervisors. The presence of a check mark denotes if Supervisors or Users can use the corresponding option.

The following options are available:

Reset min/max observations (C)
This option allows Supervisors/Users to access the (reset) option within the temperature menu at the lock. The temperature monitoring CompX eLock® has the ability to show the maximum and minimum temperatures that the electronics observed since the last time the screens were reset. These observations can be viewed by pressing the "up" and "down" buttons on the upper keypad at the lock. If it is desired to reset these observations to the currently observed temperature, Users and Supervisors can

TEMPERATURE OPTIONS continued

access the **TEMPERATURE MENU/RESET OBS. TEMPS**. This setting mode allows the Operator to control if Users (in addition to Supervisors) have the ability to reset these observations. It is not possible to remove the ability for Supervisors to reset these observations.

Set upper / lower alarm limits (D) This option allows Supervisors/Users to set the high temperature and low temperature alarming points within the manual temperature programming screens at the lock. The temperature monitoring CompX eLock® has the ability to sound an alarm if the temperature that the electronics observes goes over the maximum temperature set point or under the minimum temperature set point. This setting mode allows the Operator to control if Users (in addition to Supervisors) have the ability to modify these set points. It is not possible to remove the ability for Supervisors to change these set points.

Mute the alarm (E) This option allows Supervisors/Users to mute an alarm that is sounding for XX minutes.

Set alarm volume (F) This option allows Supervisors/Users to set the alarm volume within the manual temperature programming screens **TEMPERATURE MENU/ALARM SETTINGS**. If the temperature that the electronics observes exceeds the maximum set point or is under the minimum temperature set point, the alarm will sound after the programmed alarm delay expires. This alarm can have one of four different volume levels: **LOUD, MEDIUM, SOFT,** or **OFF**. If the volume needs to be changed this can be done with the manual temperature programming screens **TEMPERATURE MENU/ALARM SETTINGS**. This setting mode allows the Operator to control if Users (in addition to Supervisors) have the ability to change the alarm volume. It is not possible to remove the ability for Supervisors to change the alarm volume.

Enable/disable the alarm (G) This option allows Supervisors/Users to turn on the high temperature and low temperature alarm within the manual temperature programming screens **TEMPERATURE MENU/TURN ON ALARM**. The temperature monitoring CompX eLock® has the ability to sound an alarm if the temperature that the electronics observes goes over the maximum temperature set point or under the minimum temperature set point after the programmed alarm delay expires. This alarm feature can be enabled or disabled within the manual temperature programming screens **TEMPERATURE MENU/TURN ON ALARM**. This setting mode allows the Operator to control if Supervisors/Users have the ability to enable or disable the alarm. If neither Supervisors nor Users have the authority to enable or disable the alarm, the only way to do so is through LockView®.

Select Display Formats (H) This option allows Supervisors/Users to choose the unit of measure that the CompX eLock® will display within the **DISPLAY FORMATS** menu. This setting mode allows the Operator to control if Users (in addition to Supervisors) have the ability to change the units of measure. It is not possible to remove the ability for Supervisors to change the units of measure.

Open while alarm sounding (I) This option allows Supervisors/Users to access (open) the CompX eLock® when the alarm is sounding. If the box is checked, Users/Supervisors will have the ability to unlock the lock when the CompX eLock® is alarming. If the Supervisor button is not checked, Supervisors will have to mute or turn off the alarm before accessing the lock, thereby preventing inadvertent use of a product that has been exposed to temperatures outside of the programmed alarm temperatures ranges.

(J) is the display temperature units section of the menu. Choose which temperature units are displayed; degrees Fahrenheit or degrees Celsius.

(V) (Enable Alarm) is used to enable and set the temperature alarm. Checking the **Alarm Enabled** check box **(S)** enables the temperature alarm. It will have a High Limit **(L)**, a Low Limit **(K)**, and the volume of the alarm **(O)** will correspond to the volume selected.

Alarm Delay (T) allows the Operator to choose how much time (in minutes) the electronics will observe a temperature above the high limit or below the low limit before sounding the alarm.

TEMPERATURE OPTIONS continued

Alarm Time (N) allows the Operator to choose how long the alarm will sound (in minutes) after the alarm is triggered. Once the programmed amount of time has passed, the CompX eLock® will periodically sound until alarm has been disabled or muted.

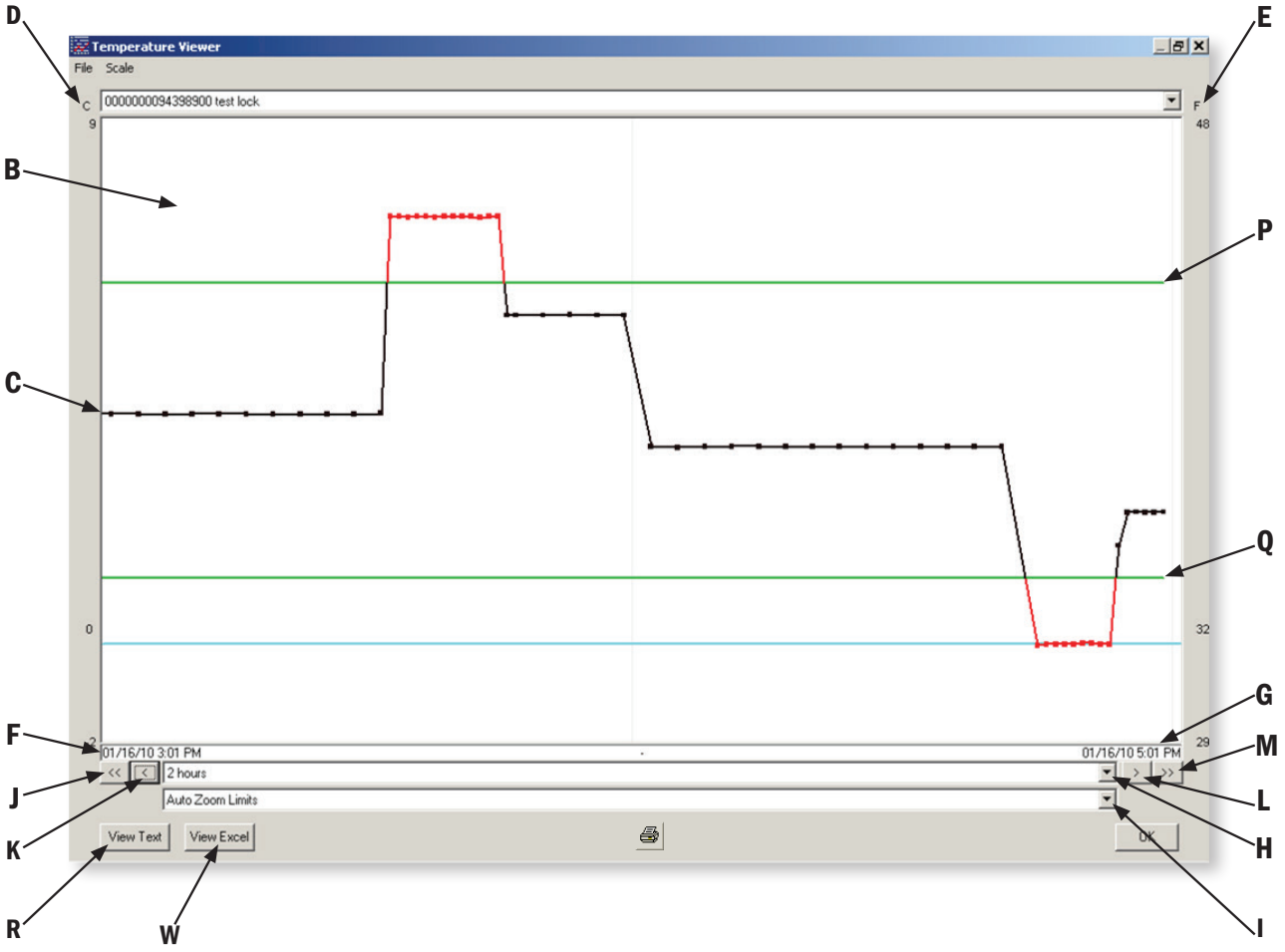
The lower section **(R) Logging Frequency** is used to set how often the CompX eLock® will log the temperature. If the temperature the CompX eLock® observes is above the low limit setting and below the high limit setting, the temperature will be logged at the rate (noted as Hours::Minutes) that is in the **When in range (P)** entry area. If the temperature the CompX eLock® observes is below the low limit setting or above the high limit setting, the temperature will be logged at the rate (noted as Hours::Minutes) that is in the **When out of range (Q)** entry area.

Clicking **Save** will save the settings.

VIEW TEMPERATURE GRAPHS

If **View Temperature Graphs** is chosen, the eLock's temperature logs will be displayed (see below). The pull down shown at point **A** allows the operator to choose which temperature monitoring eLock's temperature log will be viewed.

After a lock is chosen, the temperature graph is shown in graph area **B**. The corresponding X axis values in the accompanying illustration are shown at point **F** (illustrating the far left time value 1/16/10 3:01 p.m.) and **G** (illustrating the far right time value 1/16/10 5:01 p.m.). The Y axis on this accompanying graph is temperature. The temperature values in Celsius are shown on the left side at **D** and on the right side in Fahrenheit at **E**. The actual graph of temperature vs time is shown at **C**. The time axis can be moved right (earlier in time) or left (later in time) by control buttons **J, K, L and M**. The size (in time) of the overall window can be changed by pull down **H**. The Y axis size can be selected by pull down **I**; there are three options for the y-scale: Auto Zoom Limits, Auto Zoom Full, and Lock Vertical Scale. Auto Zoom Limits creates a y-axis that is 5˚F higher and lower than the highest and lowest alarm limits. Auto Zoom Full creates a y-axis that is 5˚F higher and lower than the highest and lowest data points and alarm limits, whichever is greater.



TEMPERATURE OPTIONS *continued*

The green lines (**P** and **Q**) display the high and low temperature limits.

Finally, the Operator can view the actual temperature and time data in text format by pressing button **R** (previous page).

NOTIFIER

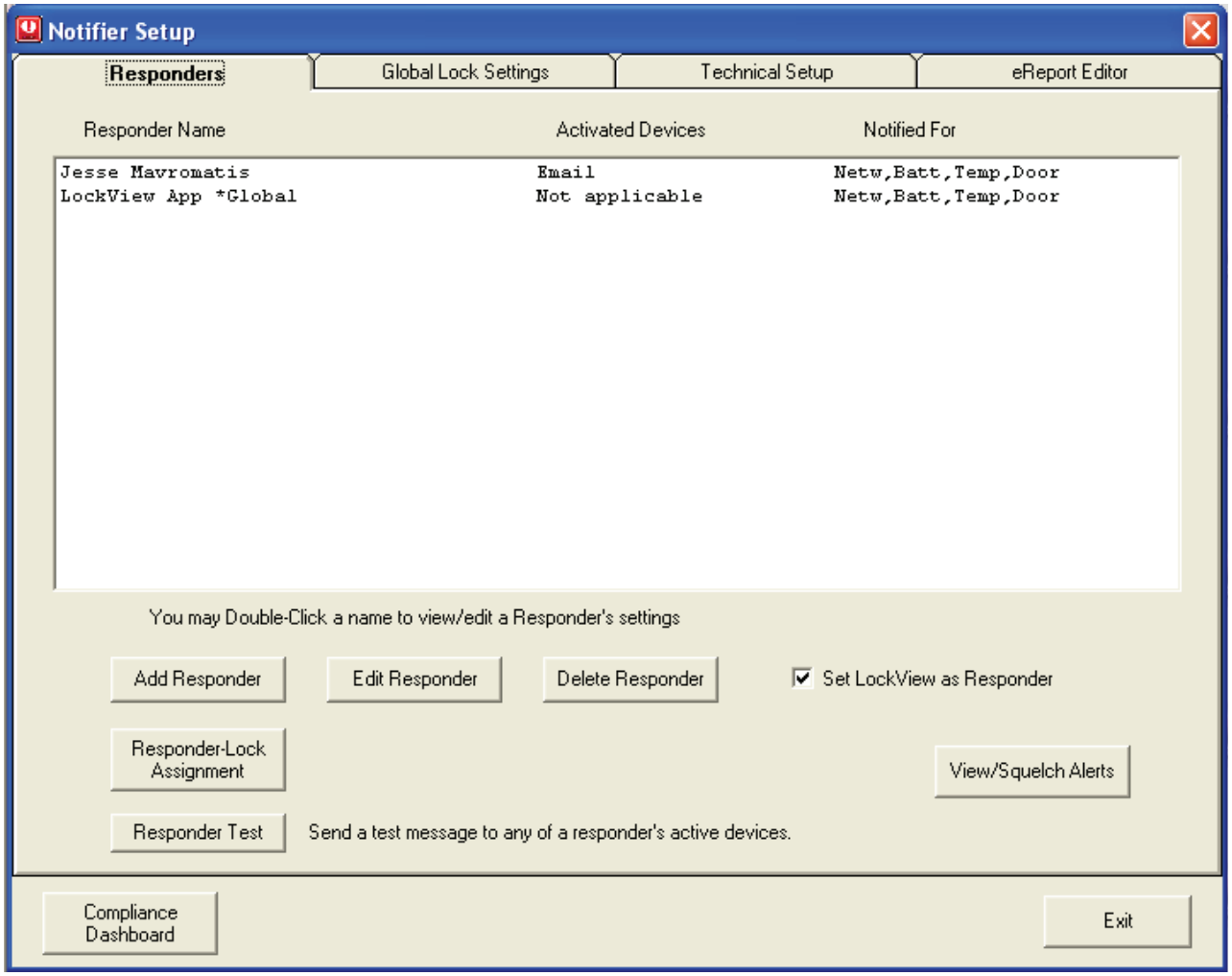
Notifier allows the LockView Operator to set up 3 different systems of notifications; Remote Notification, eReports and Compliance Dashboard. Remote Notification can be configured to send emails, text messages, phone calls, and/or faxes to a list of responders if an eLock(s) has entered a distressed mode. These modes include **Overdue Network Check-in**, **Battery Low**, **Temperature Outside Limits** and **Door Switch Alert(s)**. eReports can create and send (through email) audit trail and temperature data reports from eLocks to a list of recipients on a programmable interval. eReports can also save these reports to a local hard drive. Compliance Dashboard allows the Operator to quickly see the status of each eLock on their system in one simple window.

The "Notifier" requires an internet connected network as well as a MSSQL database.
There are four tabs in the **Notifier** menu: **Responders, Global Lock Settings, Technical Setup** and **eReports Editor**.

There are three levels of responders; 1st Responder(s), 2nd Responder(s) and 3rd Responder(s). The LockView Operator can setup a system whereby if a distressed condition(s) at the eLock(s) persists, the level of responder will escalate, from 1st Responder(s) to 2nd Responder(s) and 3rd Responder(s).

Select **Set LockView as Responder** to allow the Notifier to create and send "pop up" alert(s) that will appear on a computer that has LockView running.

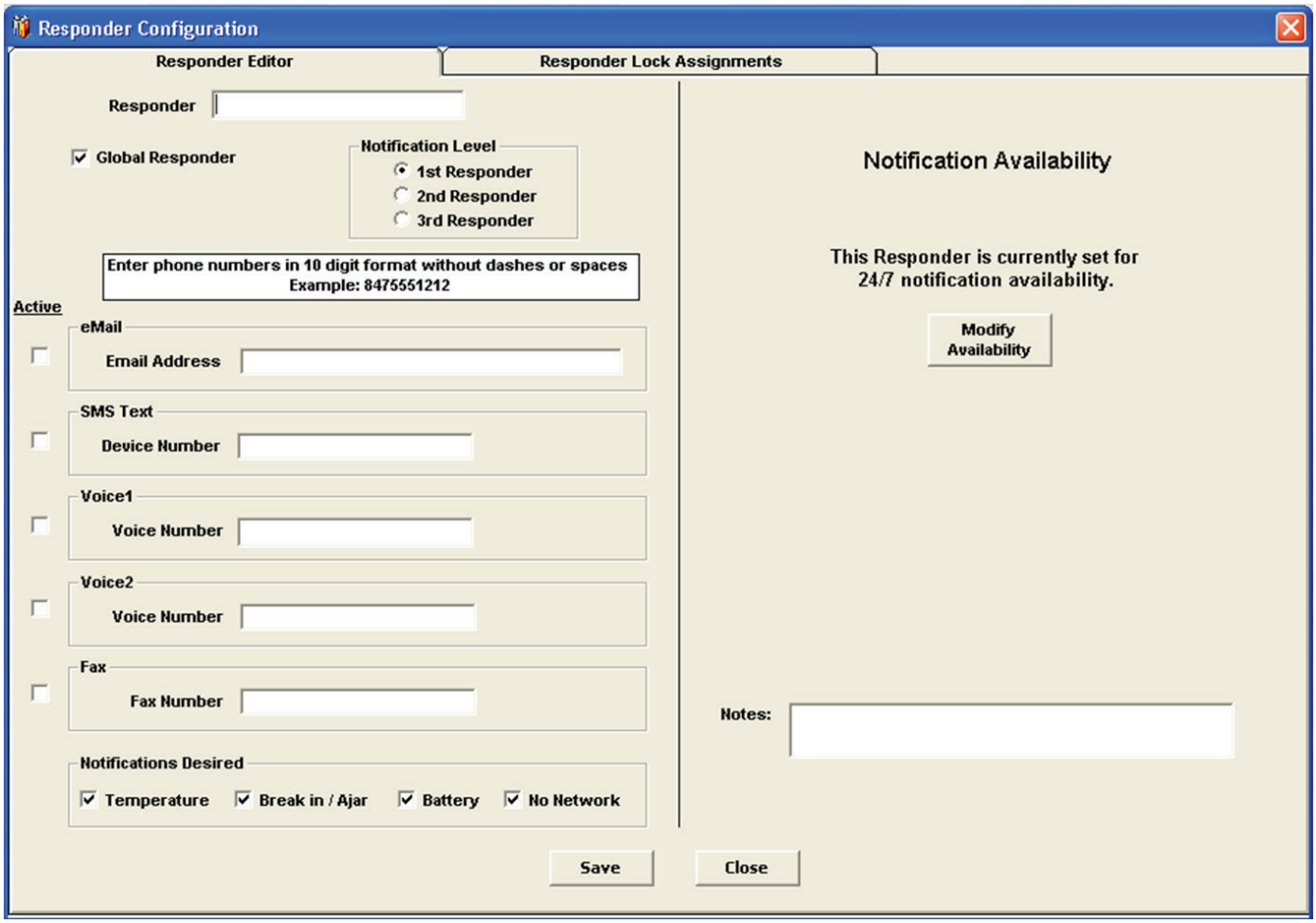
The remote notification can be an email sent through SMTP, or an SMS sent via TeleMessage. TeleMessage provides text messages, fax, voice message and email. The services TeleMessage provides are not included. See **http://www.telemessage.com/download/signUpForm.jsp?loc=enUS&prodid=34** for details.



NOTIFIER continued

ADD A RESPONDER

1. Click the **Add Responder** button in the **Responders** tab of the **Notifier** icon.
2. Enter the Responder's name in the **Responder** field.
3. Select **Global Responder** if the Responder should be notified for ALL eLocks that may enter a distressed condition.
4. Select the **Notification Level**. If an eLock enters a distressed condition, 1st Responder(s) are notified first, followed by 2nd Responder(s) and lastly 3rd Responder(s). The escalation of notification to Responders is programmable as noted on page 46.
5. Choose which method(s) of alert(s) the Responder will receive by clicking the **Active** button next to each method of notification. If an alert method is active, the destination of that notification must be entered. For example, email notification requires an email address; a text message requires a phone number equipped to receive text messages.
6. Choose which type(s) of notification(s) the Responder will receive by selecting the Notifications desired. (Temperature, Break-in, Ajar, Battery, and/or No Network)
7. If the Responder will not be available 24 hours a day/7 day a week, choose the availability by clicking **Modify Availability**. Choose the days of the week and the time of day that the responder will be available to receive messages regarding distressed eLocks.
8. Additional information regarding the Responder can be entered in the **Notes** field.
9. Click **Save** when done.



NOTIFIER continued

EDIT A RESPONDER

1. In the **Responders** tab, highlight the responder to be edited.
2. Click the **Edit Responder** button.
3. Edit the desired fields.
4. Click **Save** to save the changes

DELETE A RESPONDER

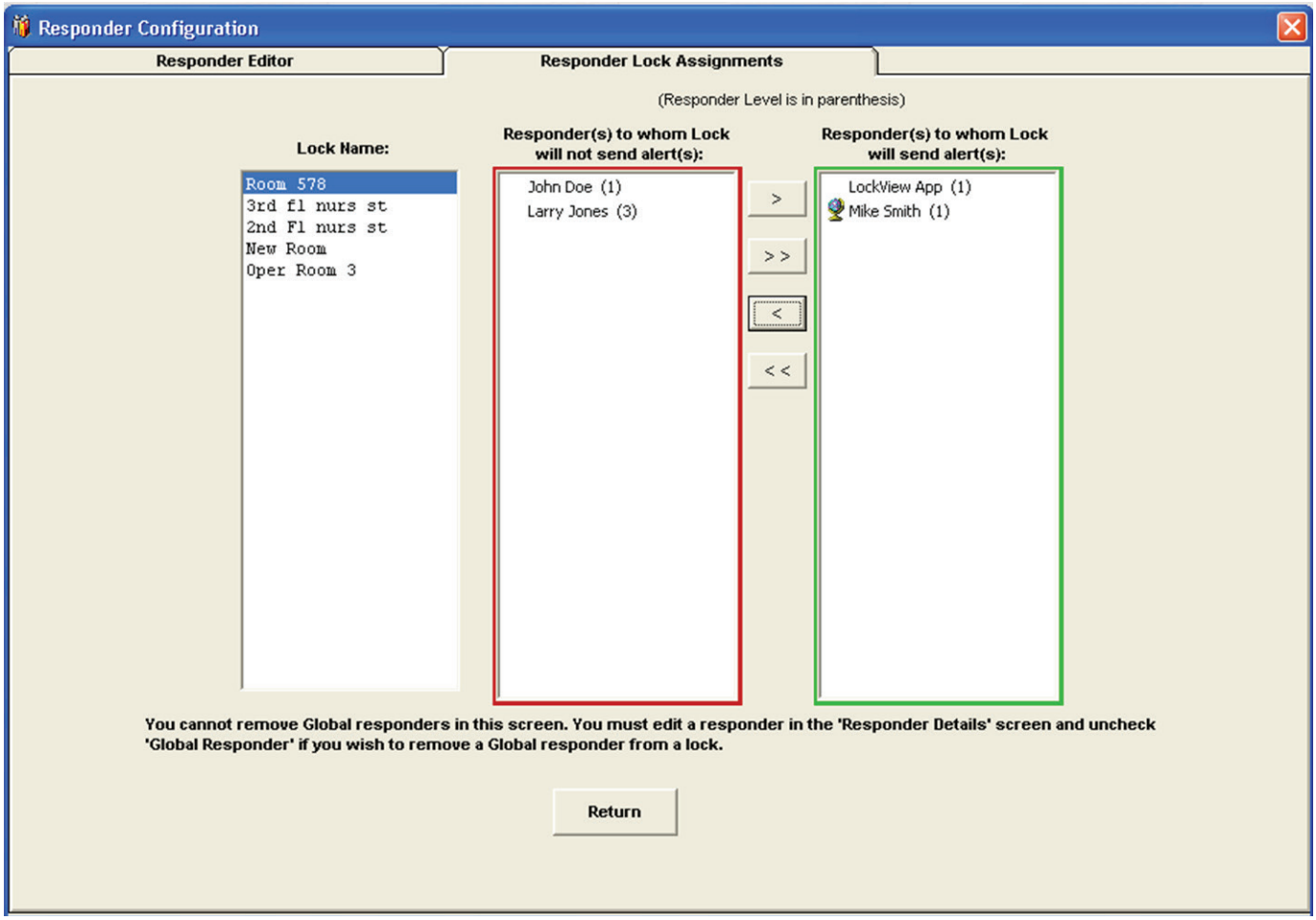
1. In the **Responders** tab, highlight the Responder to be deleted.
2. Click the **Delete Responder** button.
3. Verify then click **OK**

TEST IF A RESPONDER IS PROPERLY SET UP

1. In the **Responders** tab, highlight the Responder that is going to be tested.
2. Clicking **Responder Test** will send a test message to all of the Responder's active devices.

ASSIGN LOCKS TO RESPONDERS

Unless a Responder is global, the distressed eLock(s) to which a Responder will be notified must be selected. To assign eLock(s) to Responders, click **Responder Lock Assignments**.



NOTIFIER continued

1. Choose the eLock to which the Responder(s) is/are assigned by highlighting the **Lock Name**. This will bring up the list of Responders in the next two columns.
   - The Responder(s) in the red box are **Responder(s) to whom the lock will not send alert(s)**.
   - The Responder(s) in the green box are **Responder(s) to whom the lock will send alert(s)**.
   - If Show Instant Notifications is selected, a pop-up will appear on the computer screen. If/when an eLock(s) goes into an alarming mode (LockView program must be running in order to see the pop-up alert)

   NOTE*: The number in the parenthesis following the Responder name corresponds to their notification level.*

   - A globe icon next to the Responder name identifies that they are a Global Responder.

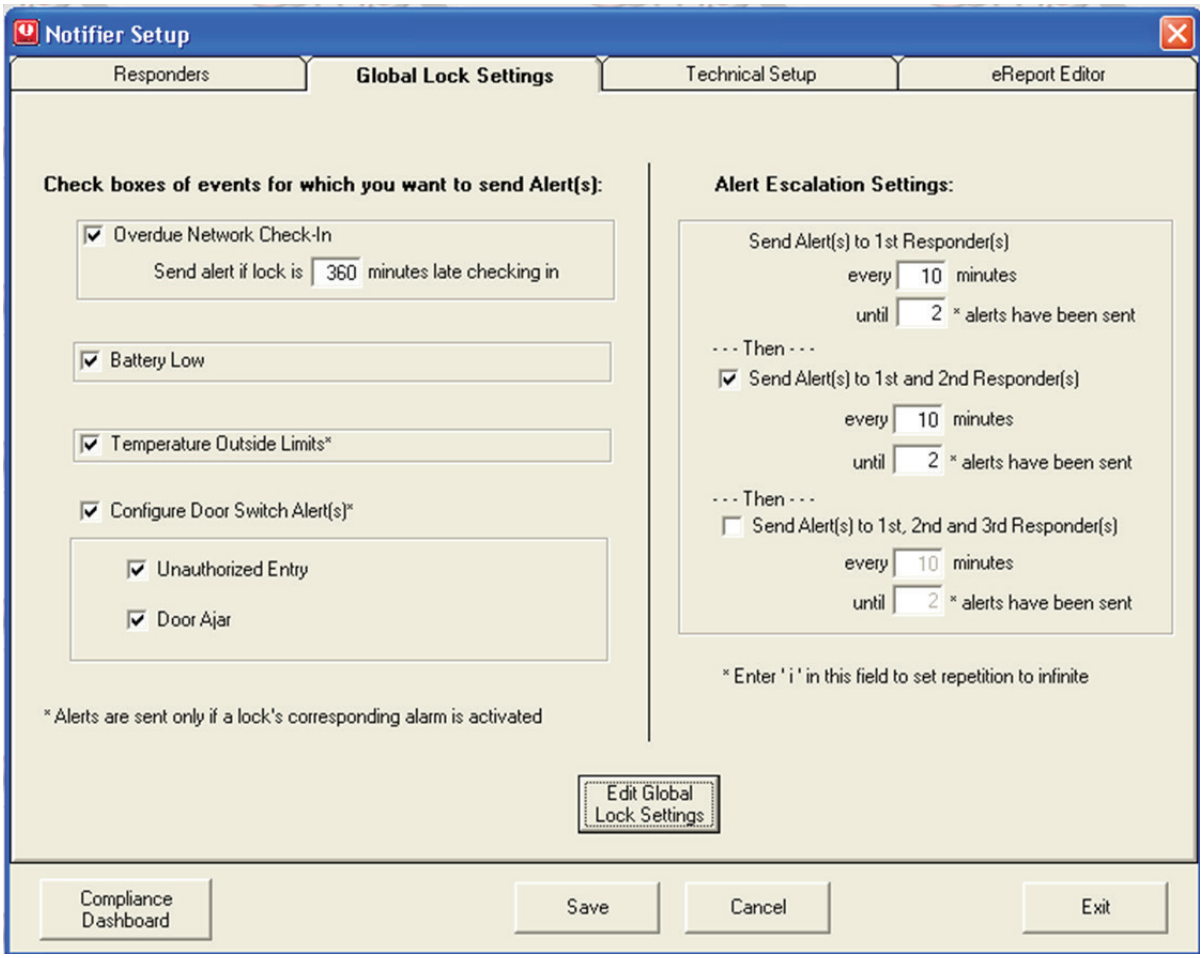
2. To change which Responders will be notified, select the Responder and click the appropriate single arrow; moving the Responder from the red box to the green, or vice versa. Note: Global Responders reside in the green box and cannot be moved to the red box.

3. To change ALL Responders status for the eLock, click the appropriate double arrow; moving ALL Responders from the red box to the green, or vice versa.

GLOBAL LOCK SETTINGS

All eLocks in the Notifier system will have global settings or individual settings. Global settings allow the LockView Operator to manage multiple similar eLocks simultaneously; without having to adjust each one individually.

Click the **Global Lock Settings** tab to adjust the global lock settings.



NOTIFIER continued

PROGRAMMING GLOBAL LOCK SETTINGS

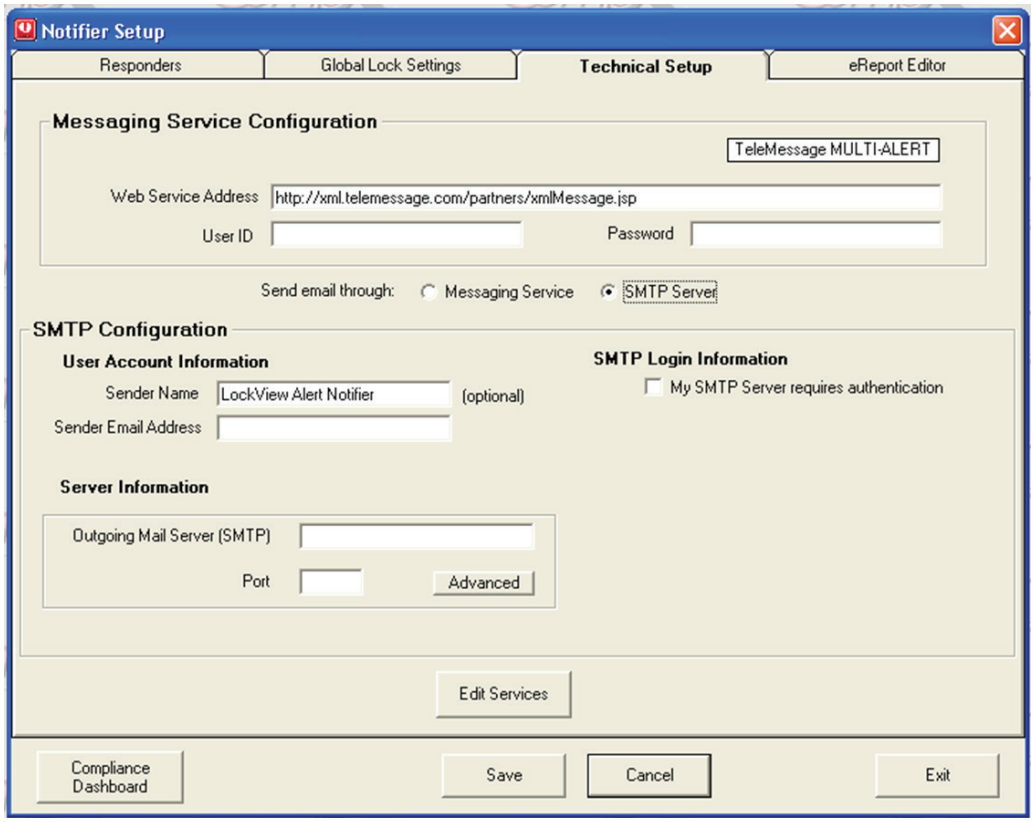
1. Clock **Edit Global Lock Settings** box.
2. Choose the eLock distress events for which notification is globally desired.
   - Selecting **Overdue Network Check-In** will send a notification if an eLock has missed the programmed scheduled network update (see **Lock Editor-Networked eLock Scheduler** on page 15).
   - Selecting **Battery Low** will send a notification if the battery power drops to "LOW."
   - Selecting **Temperature Outside Limits/Probe Failure** will send a notification if the eLock has 1) temperature alarming enabled, 2) the current temperature is outside of the high/low limits and 3) the temperature has been outside of the specified limits for a time exceeding the **Alarm Delay**. See page 39 for more information on temperature alarming. Note: This notification only applies to eLocks equipped with temperature monitoring.
   - Notification can be sent for the two types of **Door Switch Alerts**. Selecting **Unauthorized Entry** will send notification if the door switch opens at any time not immediately following the presentation of a valid credential. Selecting **Door Ajar** will send notification if the door has been open for a programmable amount of time past the standard eLock open time (see **Lock Editor-Door Switch Menu** on page 15). Note: This notification only applies to eLocks with door switch hardware.
3. **Alert Escalation Settings** allows the LockView Operator to set up a schedule for how often and how many alert(s) will be sent to the Responder(s).
   - Enter how often and how many alert(s) will be sent to the 1st Responder(s) before escalating to the 2nd Responder(s).
   - Enter how often and how many alert(s) will be sent to the 2nd Responder(s) before escalating to the 3rd Responder(s).
   - Enter how often and how many alert(s) will be sent to the 3rd Responder(s)

   NOTE: *Entering an "i" in the number of alerts field will force an infinite number of alerts.*

4. Click **Save** when done.

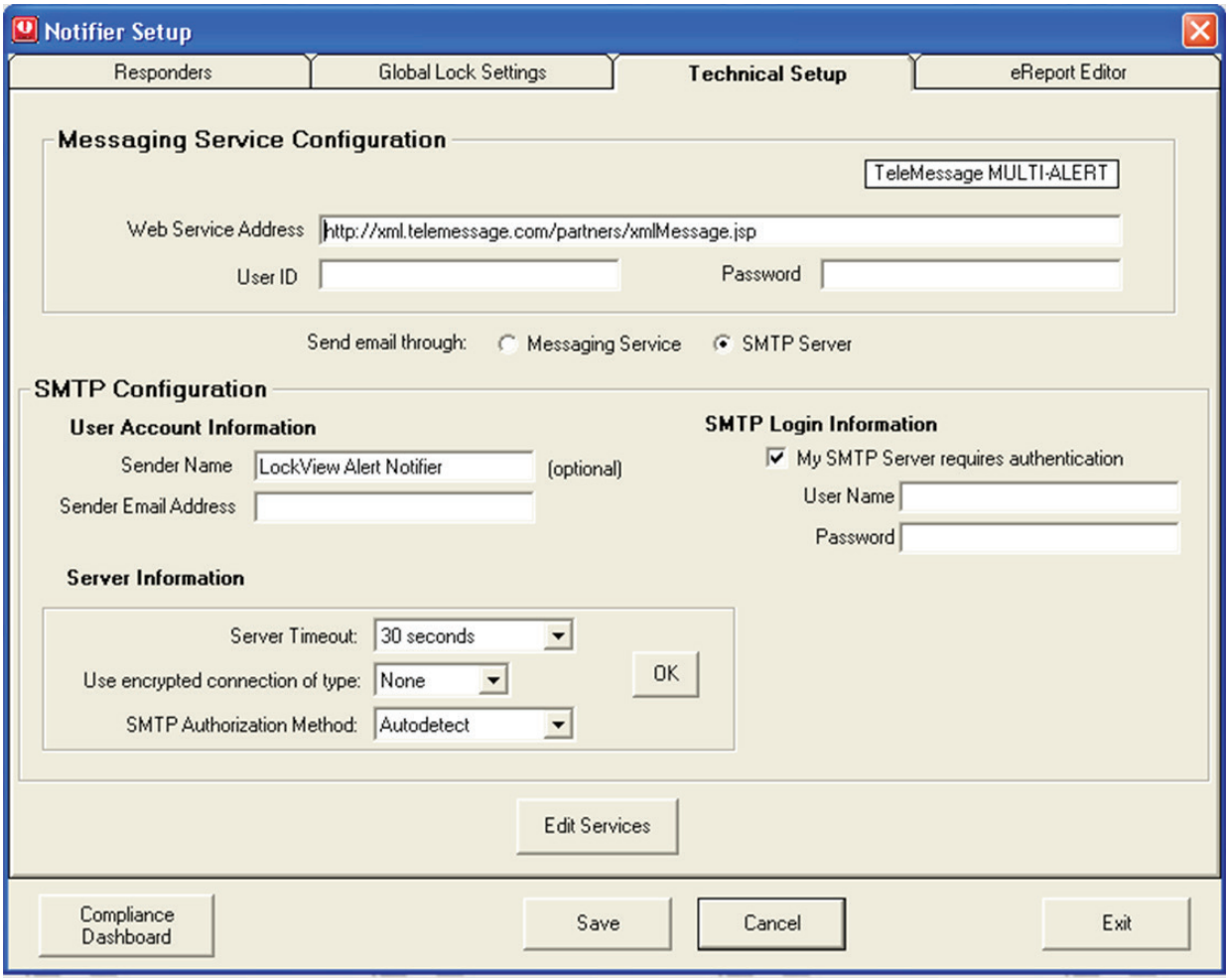
TECHNICAL SETUP

The Notifier sends alerts through SMTP or through the third party SMS provider TeleMessage. Setting up SMTP and TeleMessage is done in **Technical Setup**.



NOTIFIER continued

1. To set up the SMS system, it is first required that a TeleMessage account is set up. Visit www.telemessge.com for details. A User ID and Password is required.
2. In the **Messaging Service Configuration** portion of the **Technical Setup** tab, enter the TeleMessage User ID and Password. The Web Service Address is already filled in, but can be edited if necessary.
3. Choose how an email notification will be sent; either by the messaging service (TeleMessage) or through SMTP by clicking the proper button in the middle of the **Technical Setup** window, adjacent to **Send email through**:
4. If SMTP is selected, enter the **Sender Name** and **Sender Email Address** in the **User Account Information** Section. Enter the **Outgoing Mail Server** and **Port information** in the **Server Information** area.
5. Selecting **Advanced** will open up the following options:



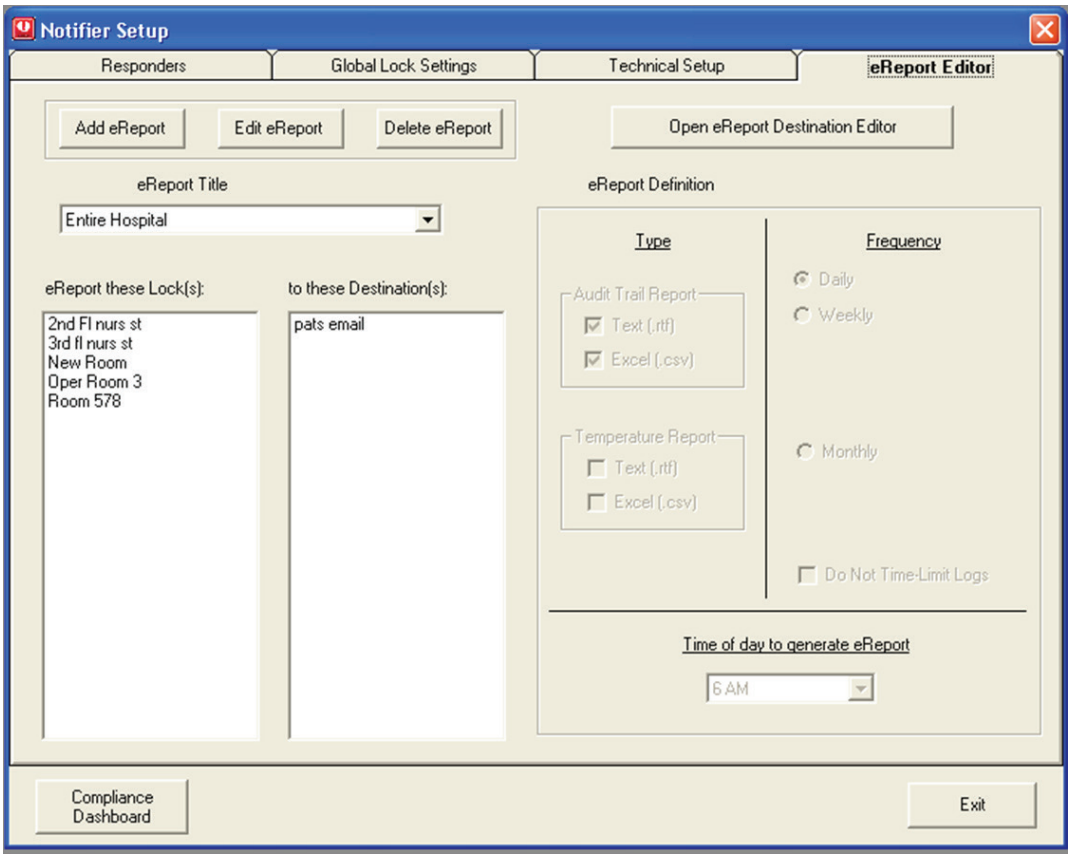
The additional information will allow **Server Timeout**, **Encrypted Connection** (SSL or TLS), and **SMTP Authorization Method** (auto detect, PAIN, LOGIN, or CAM-MD5) to be entered.

6. If the SMTP server requires authentication, user name and password can be entered in the bottom right corner of the Technical Setup tab, by clicking the box next to **My SMTP Server requires authentication**.

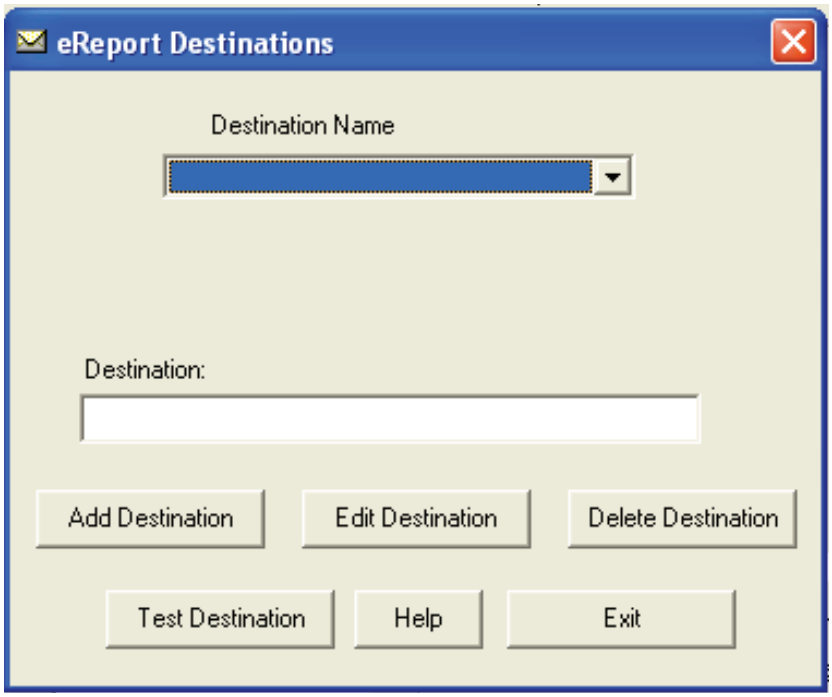
NOTIFIER continued

eREPORTS

eReports can automatically create and send access audit trail and temperature data reports from eLocks to a list of recipient's email addresses known as **Destinations** on a programmable interval. These reports can also be saved to a local hard drive. Click the **eReports** tab of the **Notifier** to set up **eReports**



To Add/Edit/Delete **Destinations**, click the **Open eReport Destination Editor** button



NOTIFIER continued

ADD DESTINATION

1. Click the **Add Destination** button in the **eReport Destinations** window of the eReport editor tab.
2. Enter the **Destination Name** and type of destination (email address or network folder)
3. If the type of destination is an email address, enter the email address.
4. If the type of destination is an network folder, click the more information button (...) and navigate to the desired network folder.
5. Click **Save**
6. Click **Exit**

EDIT DESTINATION

1. Choose the Destination be edited in the **Destination Name** pull down menu of the **eReport Destinations Editor**.
2. Click the **Edit Destination** button
3. Edit the type of destination (email address or network folder) and the details regarding the destination.
4. Click **Save**
5. Click **Exit**

DELETE DESTINATION

1. Choose the Destination to be deleted in the **Destination Name** pull down menu of the **eReport Destinations Editor**.
2. Click the **Delete Destination** button
3. Verify the deletion by clicking **OK**
4. Click **Exit**

Once destinations have been created, eReports can be created.

ADD eREPORT

1. Click the **Add eReport** button in the **eReport Editor**.
2. Enter a title for the eReport in the eReport Title entry box.
3. Choose which eLock(s) to report in the **eReport these Lock(s)** selection box.
4. Choose which destination(s) will receive the eReports in the **to these Destination(s)**: selection box.

NOTE: Multiple eReports can be sent to multiple destinations by holding Ctrl on the keyboard while clicking the destination and/or name.

5. Choose the type of report in the **eReport Definition** section. There are two report types (access audit trail and temperature) and two formats (Text and Excel)
6. Choose how often the report will be sent in the **eReport Definition** section. There are three options available: **Daily**, **Weekly** and **Monthly**. If **Weekly** is chosen, the day of the week must be selected. If **Monthly** is chosen, the day of the month must be selected.
7. Selecting **Do Not Time-Limit Logs** will cause a full report to be sent each time. That is, all data available for that eLock will be sent every time a report is generated. If **Do Not Time-Limit Logs** is not chosen, only data accumulated since the last report was created will be sent. For example, if **Daily** is chosen, only the past day's events will be in the report.
8. Choose the time of day the report will be created and sent under **Time of day to generate eReport**.
9. Click **Save** when complete.

EDIT AN eREPORT

1. Choose the eReport to be edited in the **eReport Title** drop down menu of the **eReport Editor**.
2. Click the **Edit eReport** button.
3. Edit the desired eLock, destination, eReport type and frequency
4. Click **Save** when complete.

NOTIFIER continued

DELETE AN eREPORT

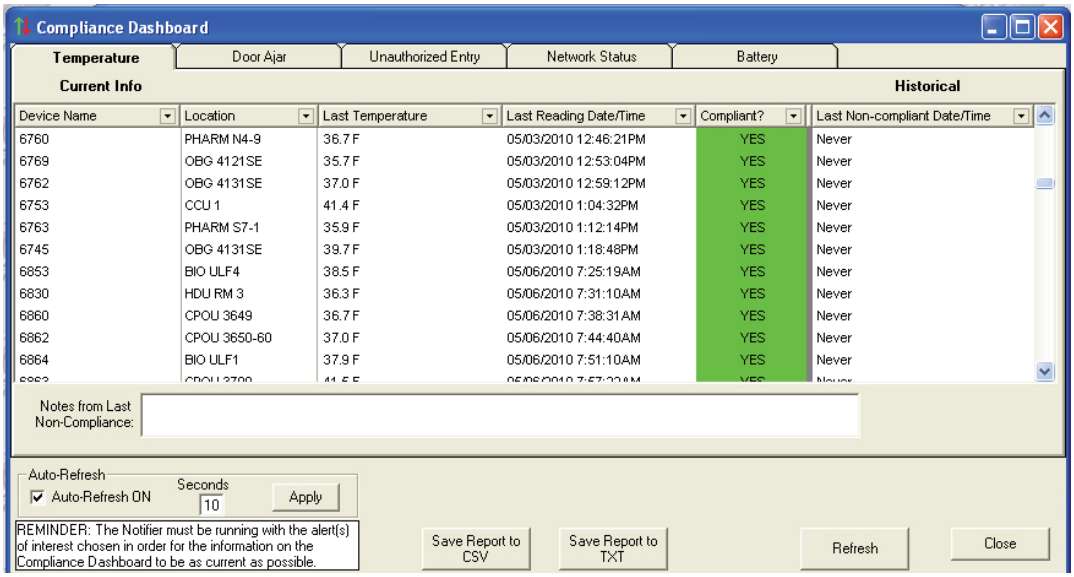
1. Choose the eReport to be deleted in the **eReport Title** drop down menu of the **eReport Editor**.
2. Click the **Delete eReport** button.
3. Verify the deletion by clicking **OK**

COMPLIANCE DASHBOARD

At the bottom of the **Notifer** is the **Compliance Dashboard** button. The **Compliance Dashboard** provides the Operator a current and historical quick look at Temperature (if equipped) door position: Ajar & Unauthorized Entry (if equipped), Network Status (if equipped), and Battery Level of all eLocks in the database.

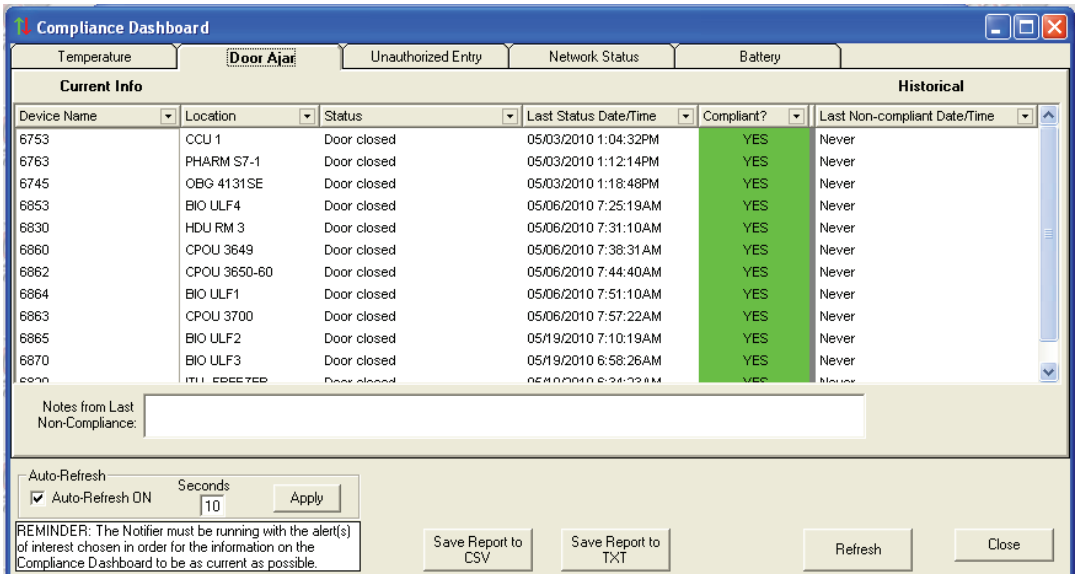
TEMPERATURE DASHBOARD

Select the **Temperature** tab to view the Location, Last Temperature, Last Reading Date/Time, Compliance status, and Last Non-compliant date/time for each eLock with a temperature monitoring system.



DOOR AJAR DASHBOARD

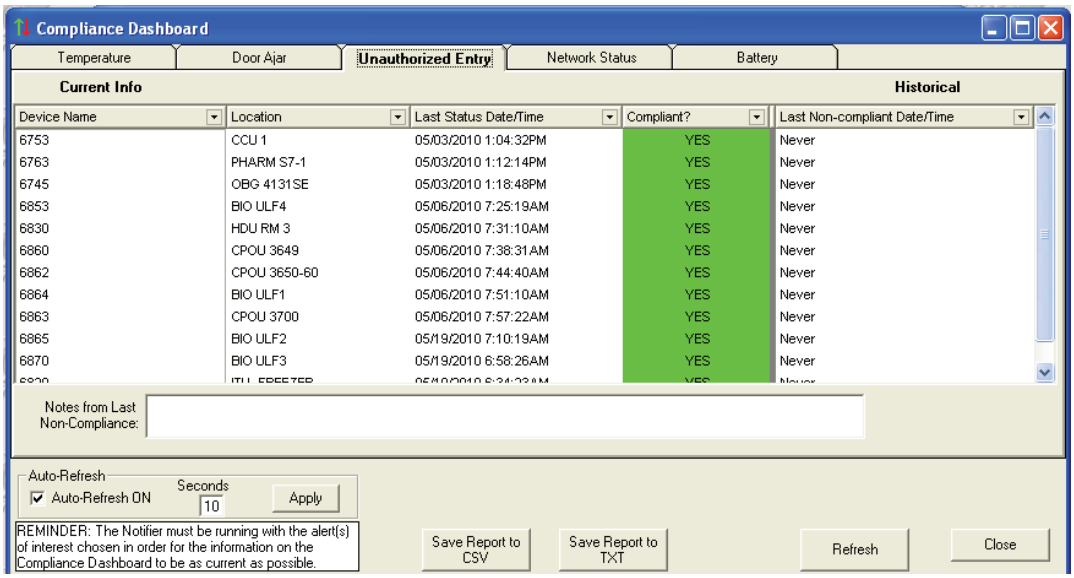
Select the **Door Ajar** tab to view the Location, door ajar Status, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each eLock with door switch installed.



NOTIFIER continued

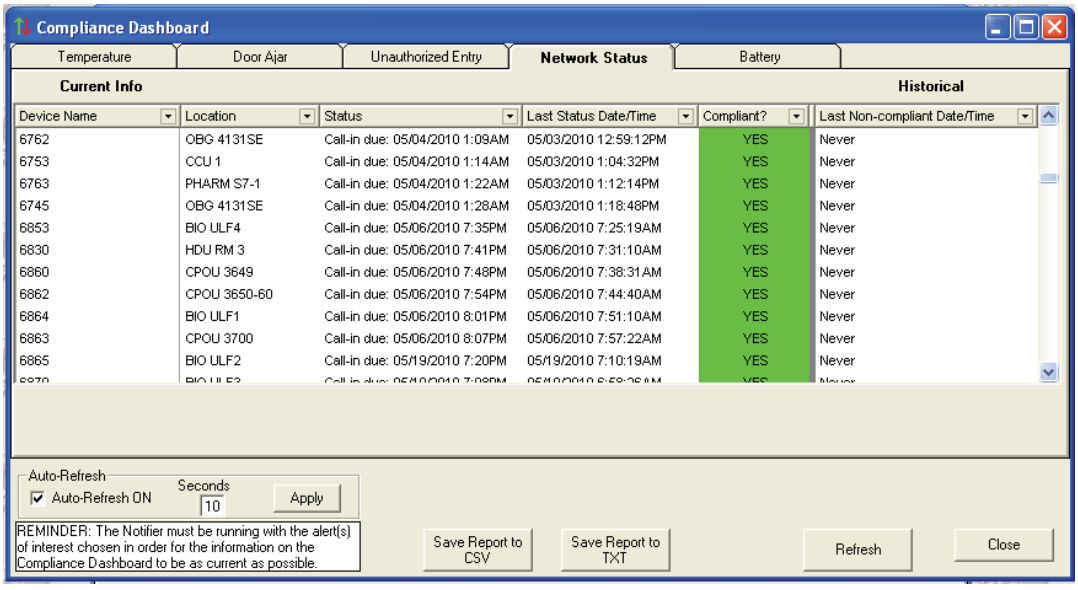
UNAUTHORIZED ENTRY DASHBOARD

Select the **Unauthorized Entry** tab to view the Location, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each eLock with door switch installed.



NETWORK STATUS DASHBOARD

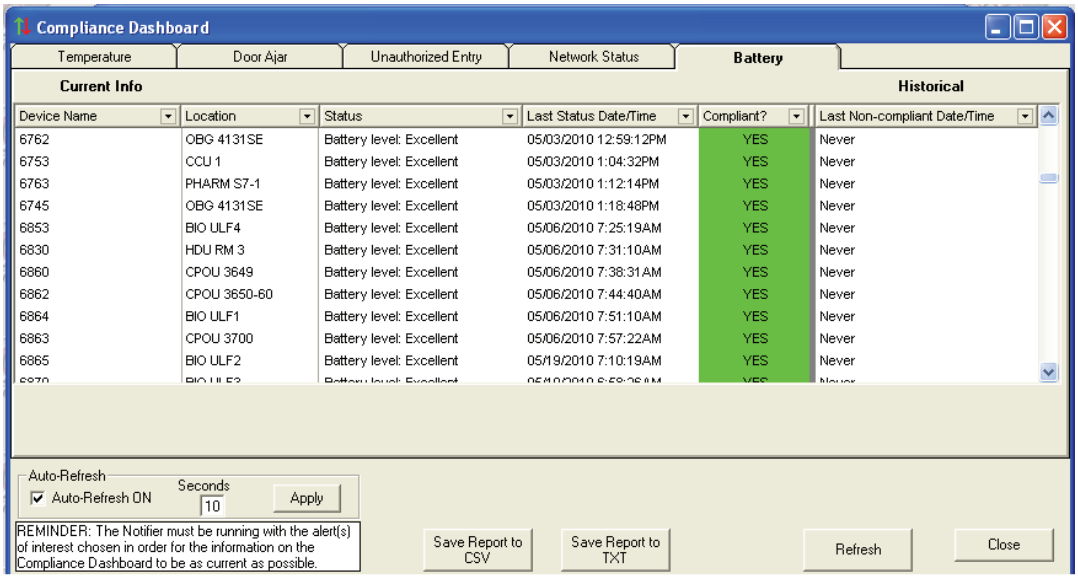
Select the **Network Status** tab to view the Location, network Status, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each networked eLock on the system.



NOTIFIER continued

BATTERY DASHBOARD

Select the **Battery** tab to view the Location, battery Status, Last Status Date/Time, Compliance status, and Last Non-compliant date/time for each eLock on the system.



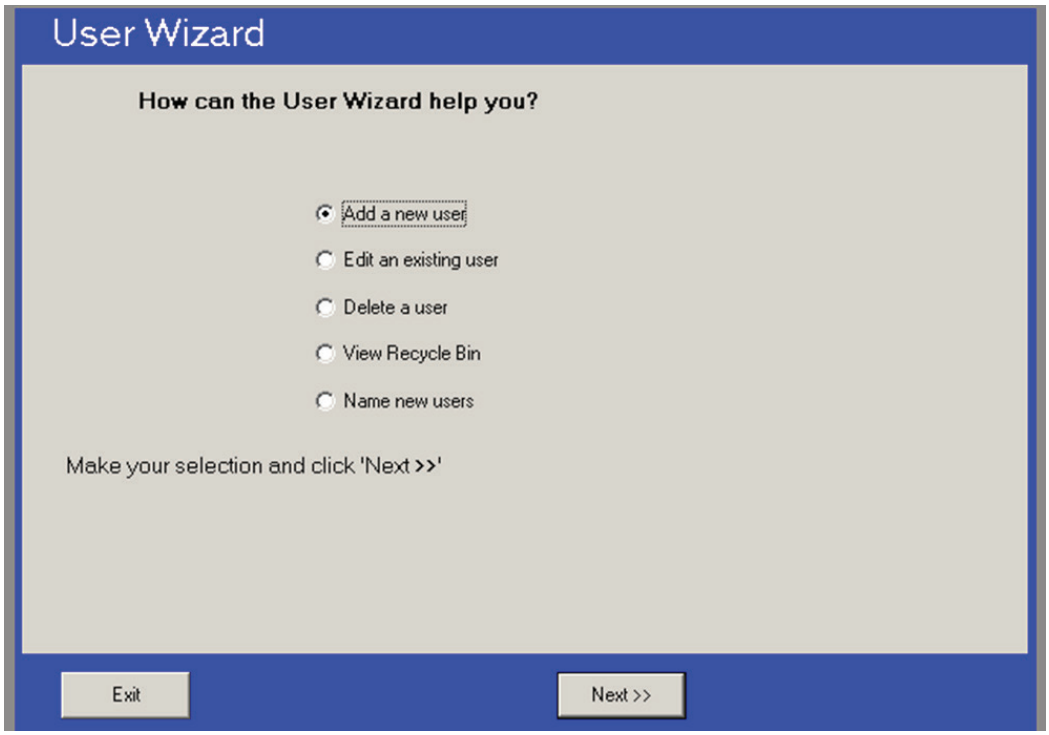
WIZARDS

LockView Wizard is an alternate method to add, edit and delete users and locks. Click the **Wizards** icon to bring up the Wizards menu.

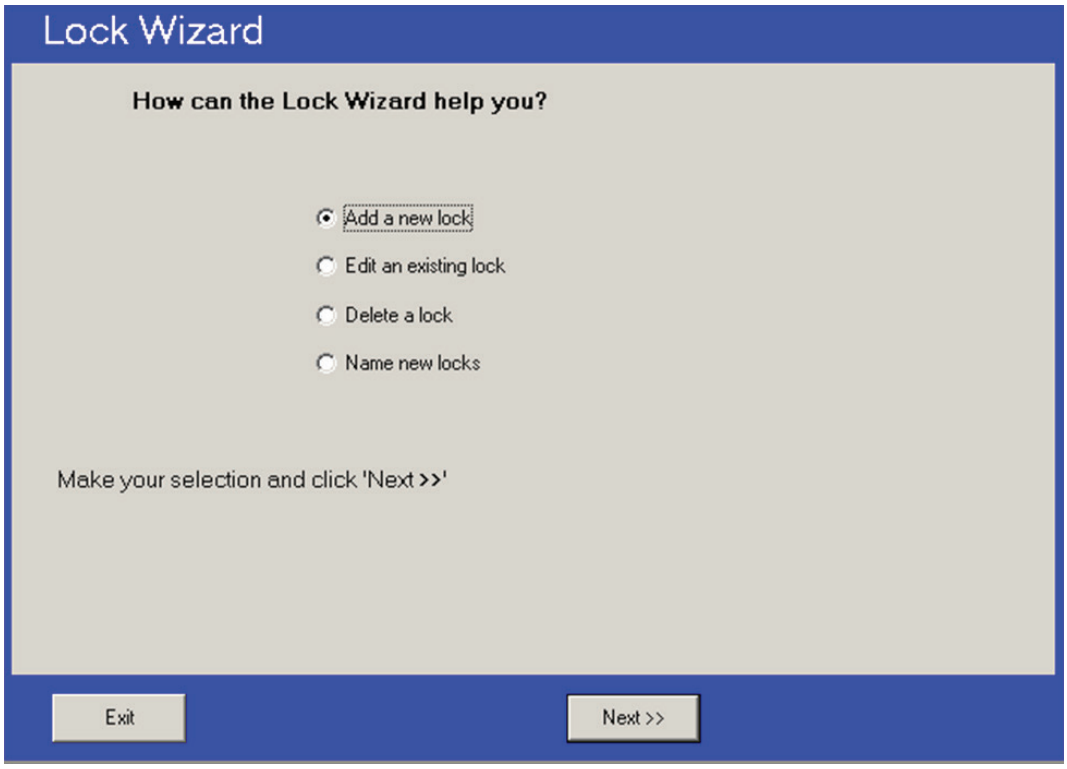
There are three Wizard choices:
CREATE USER DATABASE, CREATE LOCK DATABASE and **CONNECT**

WIZARDS continued

CREATE USER DATABASE
offers 5 choices:
- Add a new user
- Edit an existing user
- Delete a user
- View Recycle bin
- Name New users



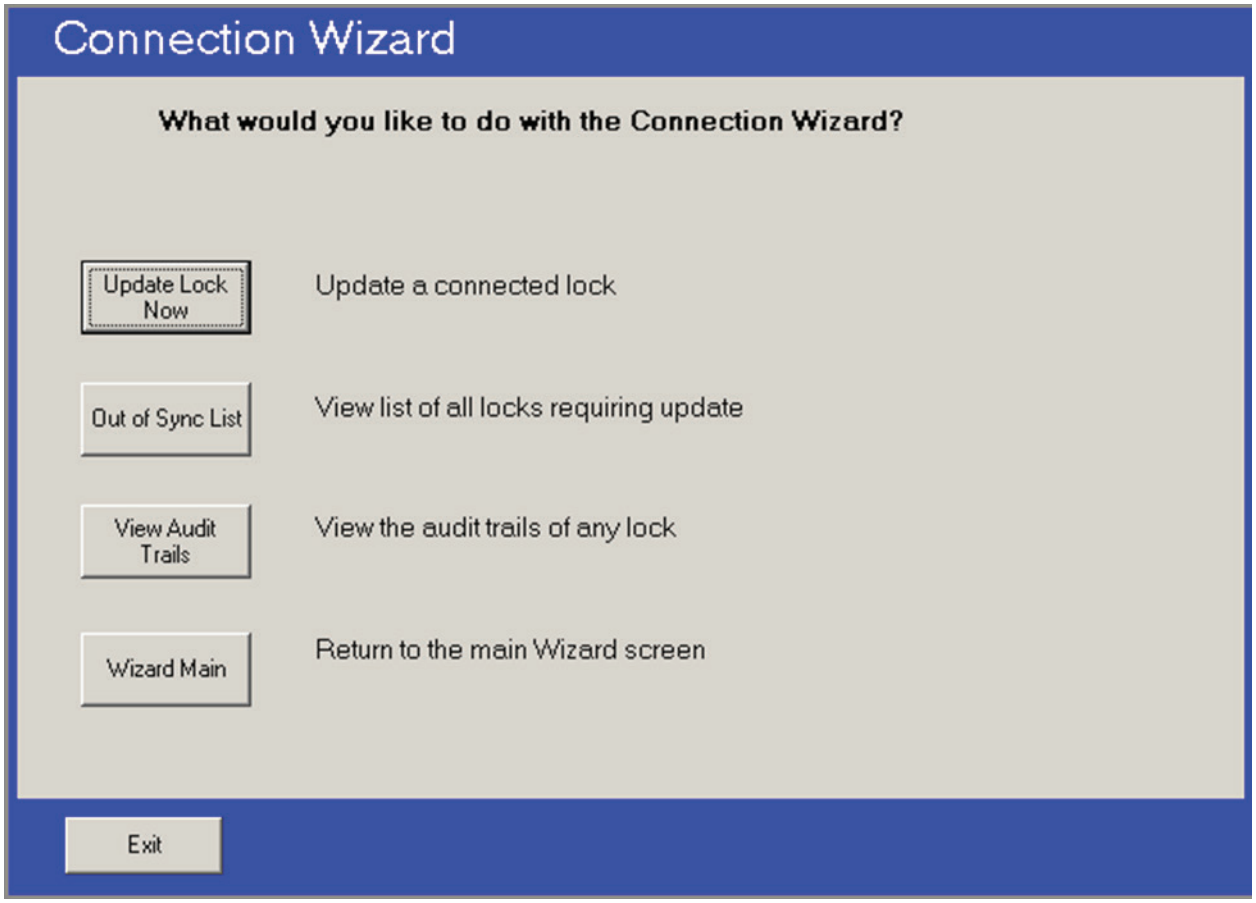
CREATE LOCK DATABASE
offers 4 choices:
- Add a new lock
- Edit an existing lock
- Delete a lock
- Name New users



WIZARDS continued

CONNECT offers 4 main choices:

- **Update Lock Now**: Update a connected lock
- **Out of Sync List**: View list of all eLocks requiring updates
- **View Audit Trails**: View the Audit trails of any eLock
- **Wizard Main**: Returns to the main Wizard



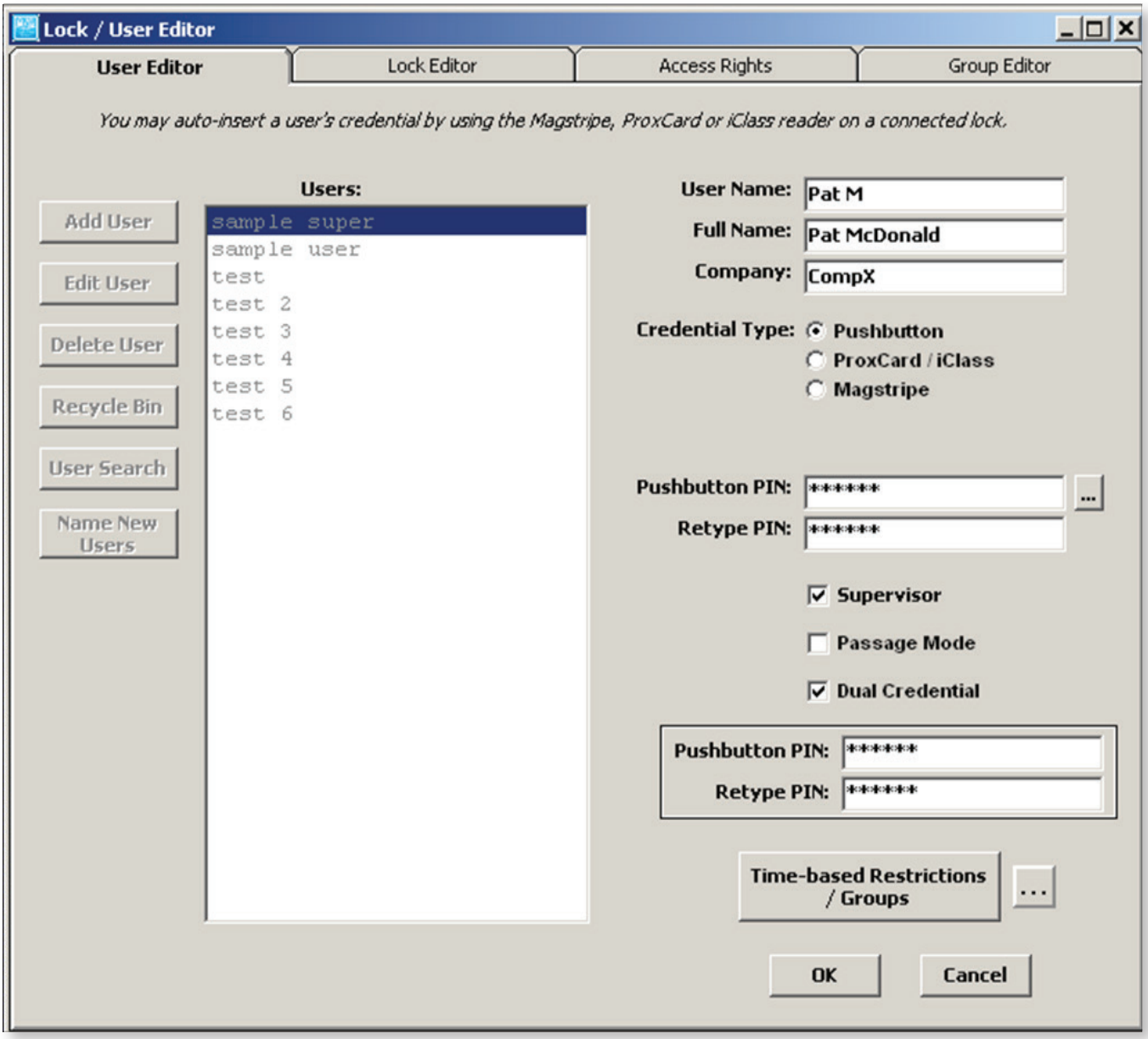
PROGRAMMING EXAMPLE

The below illustrates an example of two new users being added into the computer database and then added into a lock's database.

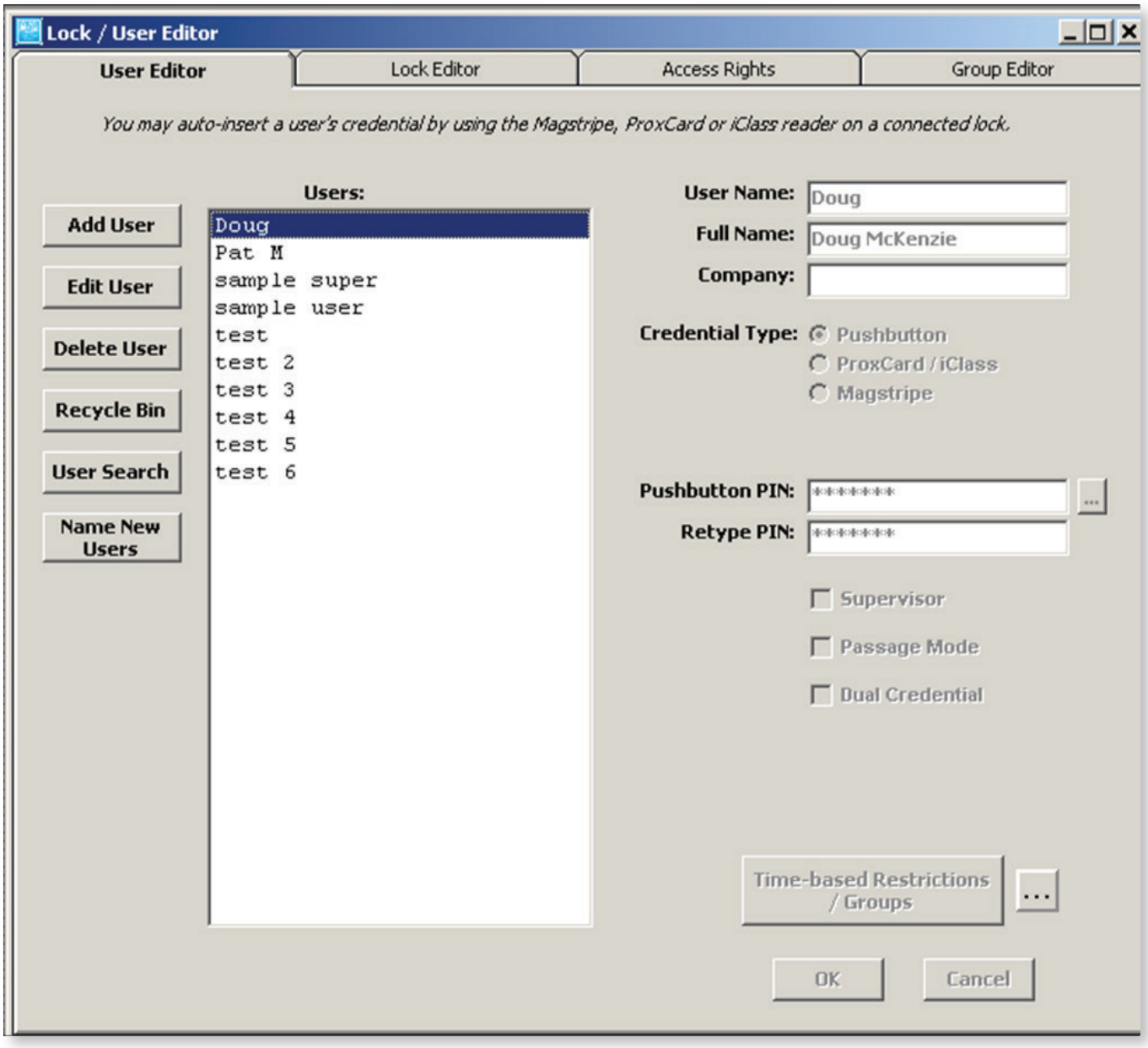
1. Select **Lock/User Editor**.
2. Select **Add User** and enter new user's information.

See pages 9-13 for more information on what each entry in the **User Editor** means.

NOTE: *The following screens show a new user being added to the computer database.*



PROGRAMMING EXAMPLE *continued*



User information for Pat M and Doug is added into the computer database by using the User Editor.

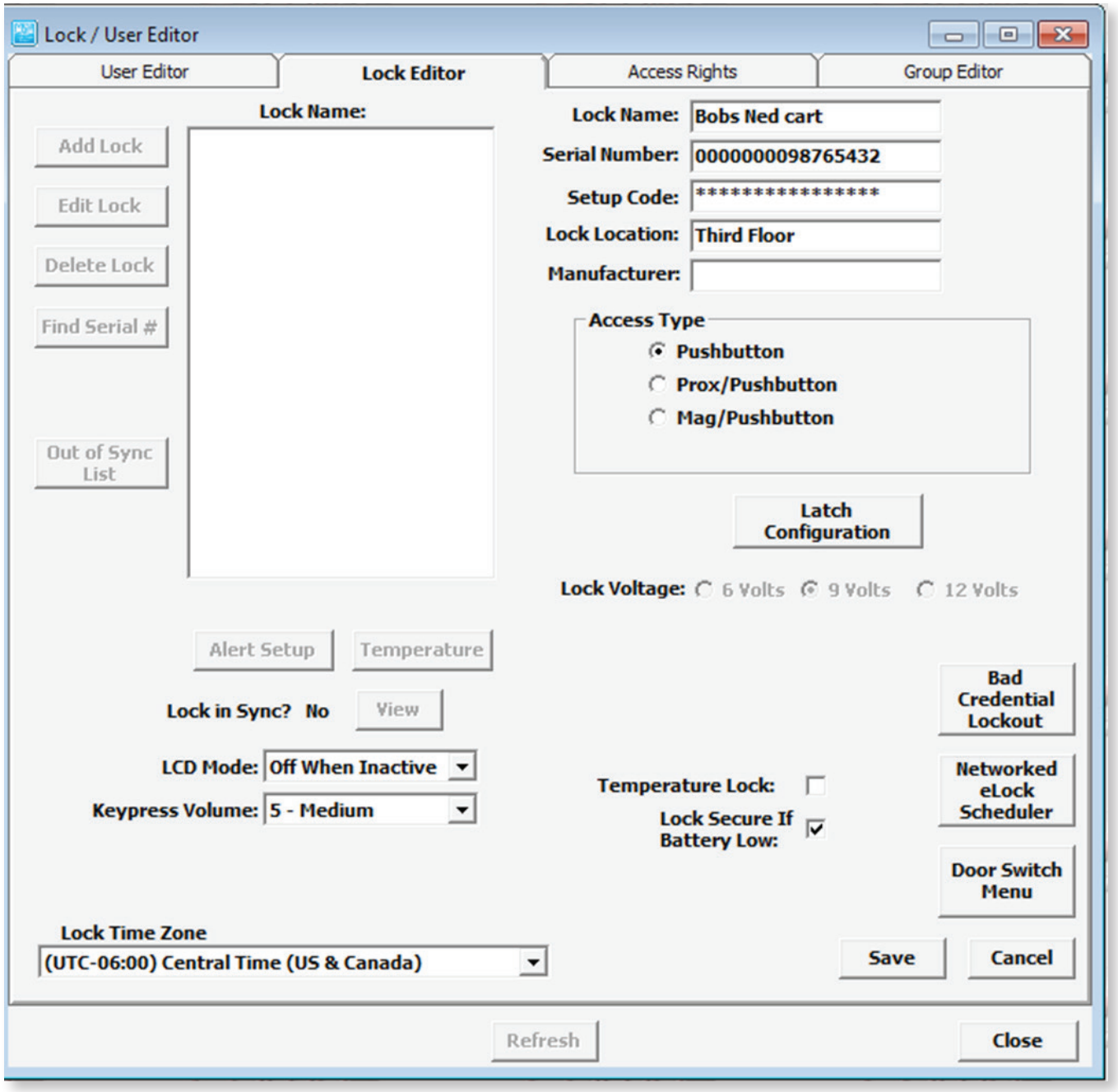
PROGRAMMING EXAMPLE *continued*

The new users do not have any access rights to locks.

3. Open **Lock Editor.**
4. Select **Add Lock**.

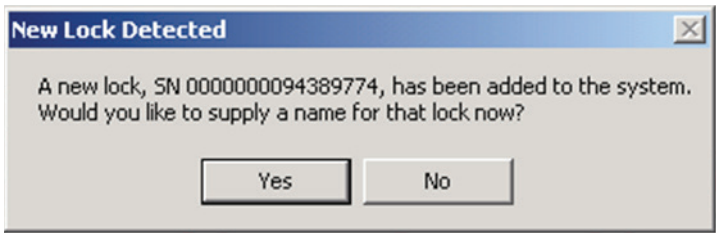
NOTE: *The screen below is of a new lock being added to the computer database.*

5. There are two different ways to enter a lock into the **Lock Editor**; manually or automatically. To enter the information manually, click **Add Lock** and enter the information into the screen. (See pages 14-19 for more information.)

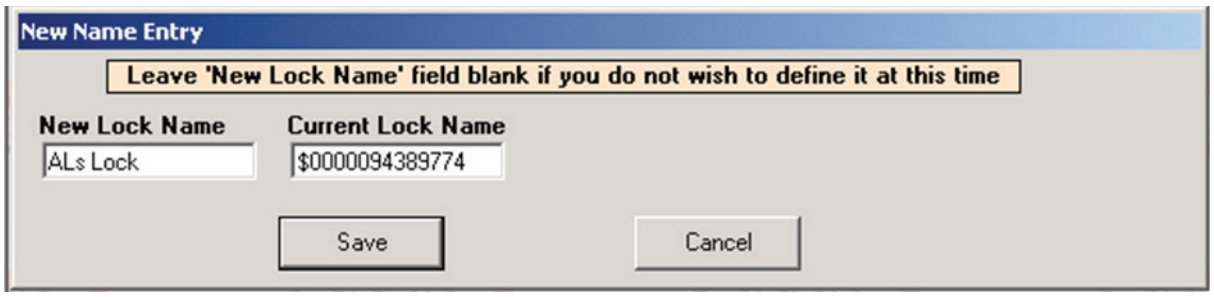


PROGRAMMING EXAMPLE continued

6. Alternately, the lock can automatically be added to the database.
   a. Press and hold "CLEAR" on the keypad. "**ENTER SETUP CODE**" will appear on the display.
   b. Enter the setup code that was provided on the sticker set with the lock into the keypad.
   c. "**SETUP**" will appear on the display.
   d. Connect the USB cable to the computer and to the lock. If a network module is being used and it is setup, press the "NETWORK" button to initiate a manual update.
   e. Within a few seconds, the following window will appear, SNXXXX is the serial number of the lock being added.



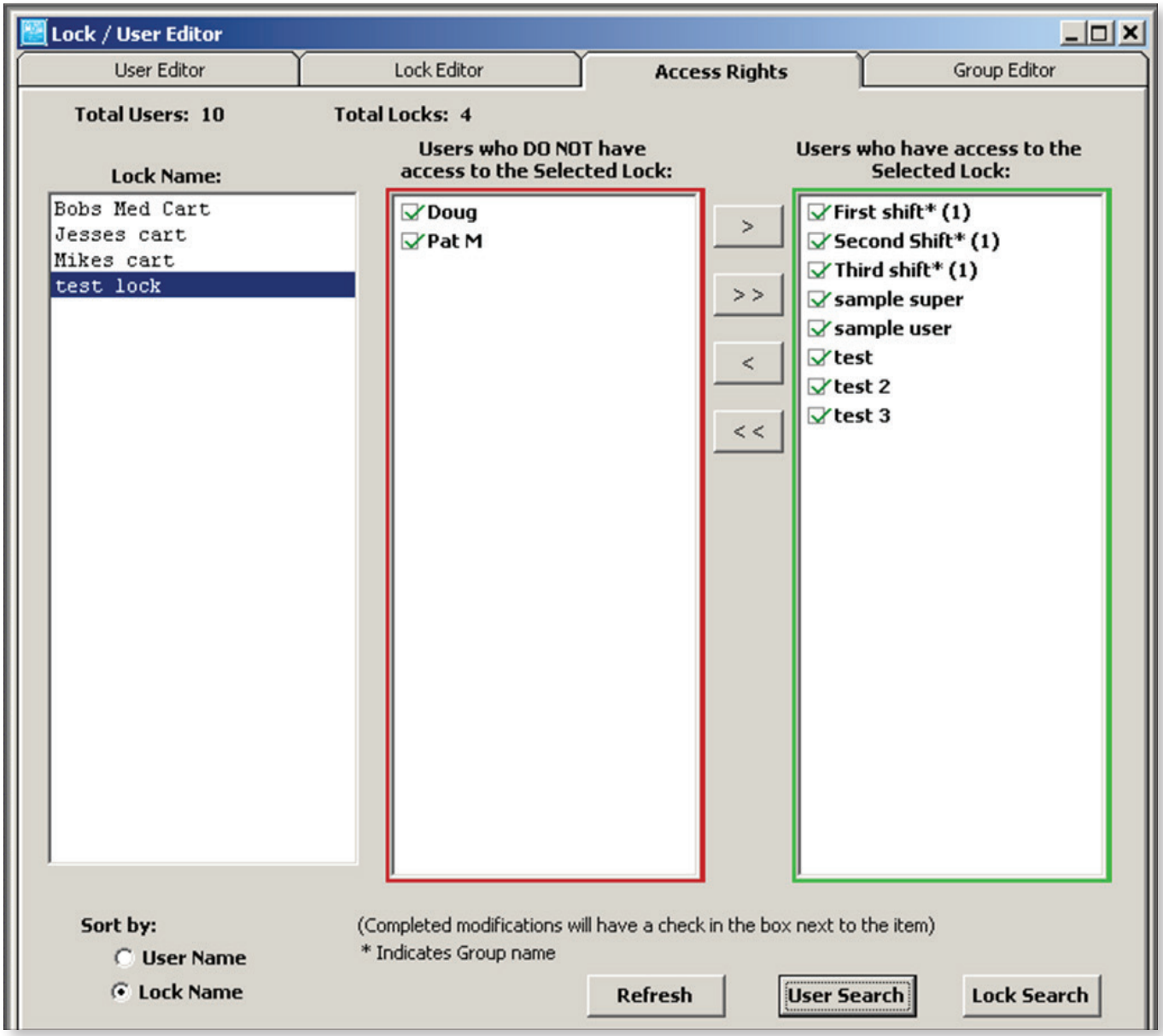
   f. Click **Yes.**
   g. Enter the **New Lock Name**. The lock and all of the settings will be loaded into the database.



   h. Click **Save**.

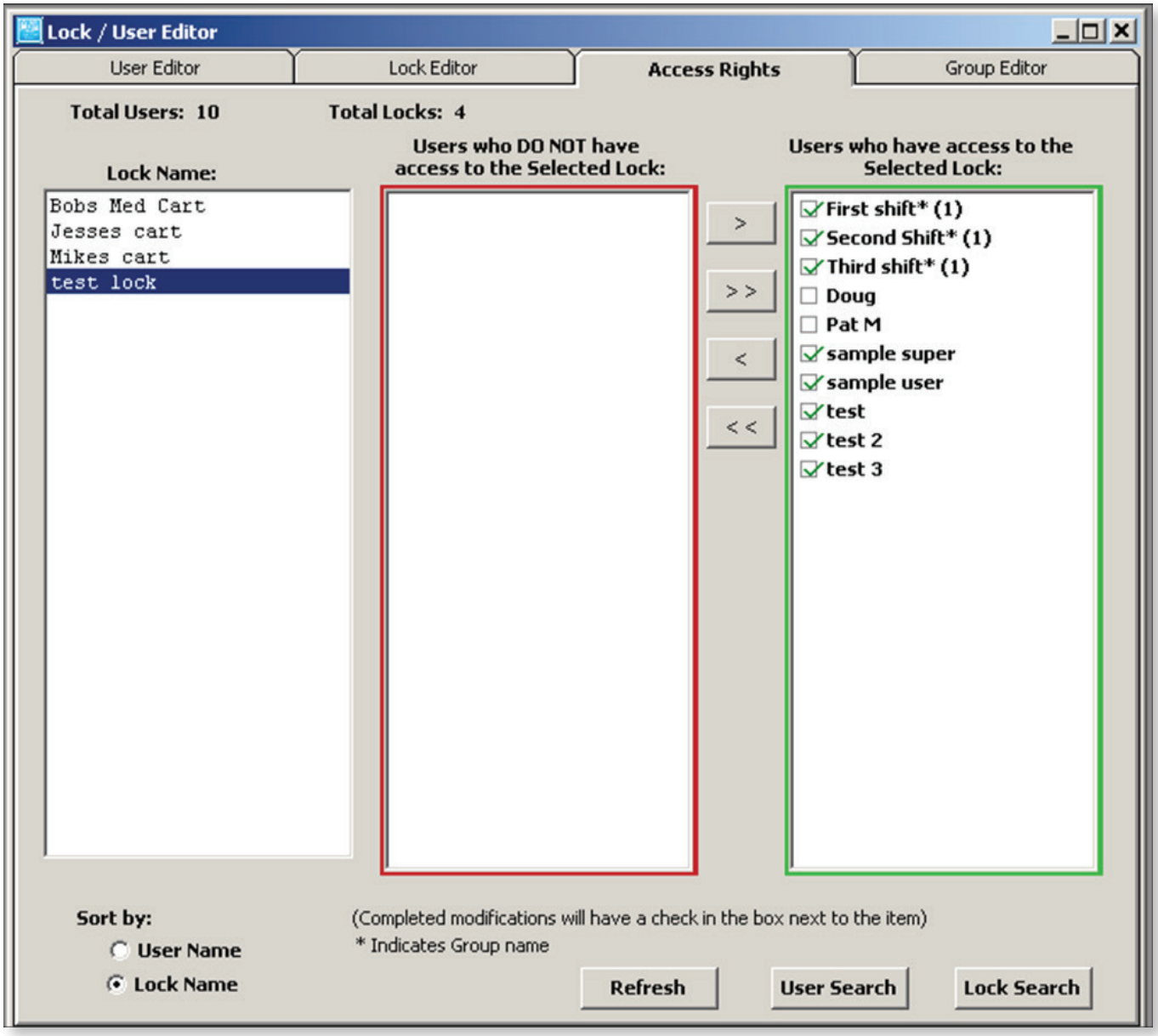
PROGRAMMING EXAMPLE *continued*

Click **Access Rights** tab. The screen below shows users Doug and Pat M DO NOT have access to the **test lock**.



PROGRAMMING EXAMPLE *continued*

By highlighting Doug and Pat M and selecting the appropriate arrow, these two new users are granted access to **test lock** as it shows in the next screen (which is the contents of the computer's database), but they still are not able to open the lock until they are uploaded into the lock's database. The two new users will not have a check mark next to their names and will not be able to open the lock until they are uploaded into the lock's database. When they are uploaded, a check mark will appear in the box next to their names in the right column.

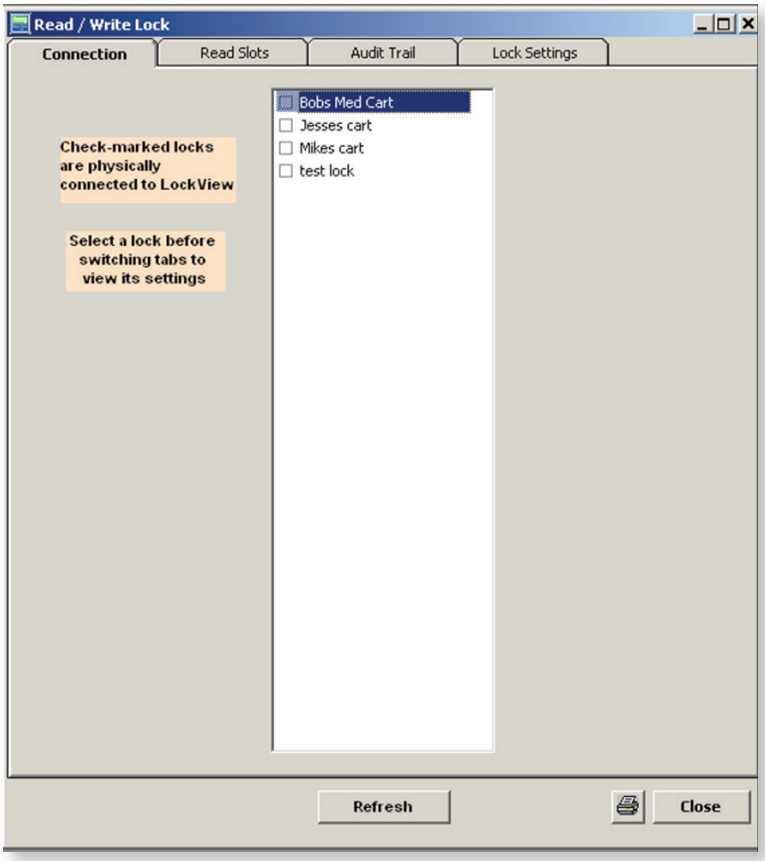


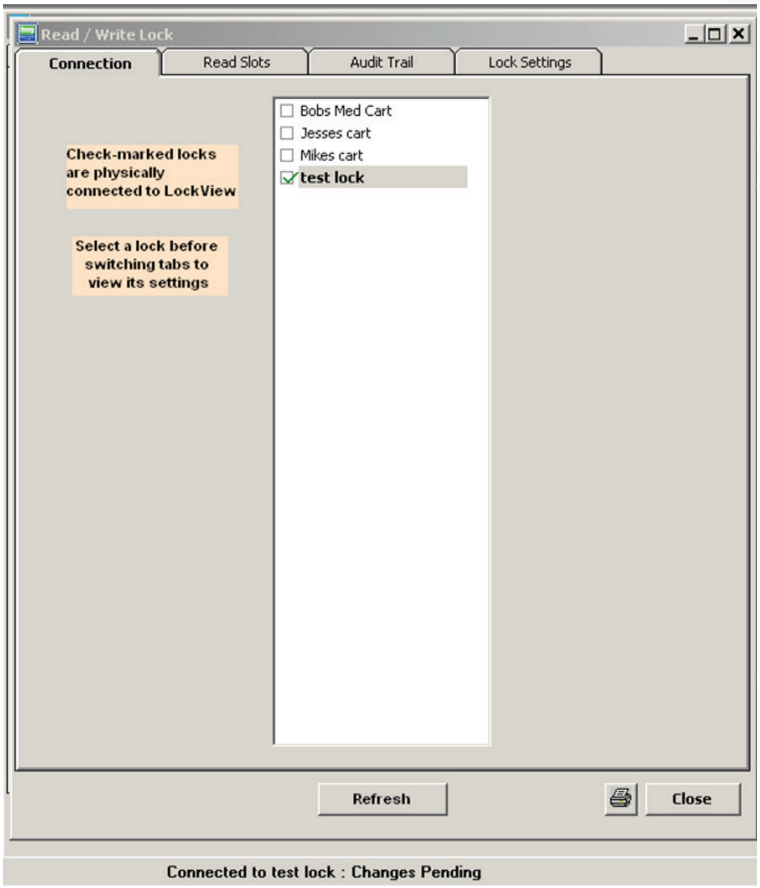
Open the **Read/Write Lock** menu. Choose the **Connection** tab.

PROGRAMMING EXAMPLE *continued*

Note: *There are no highlighted locks or check marks.*

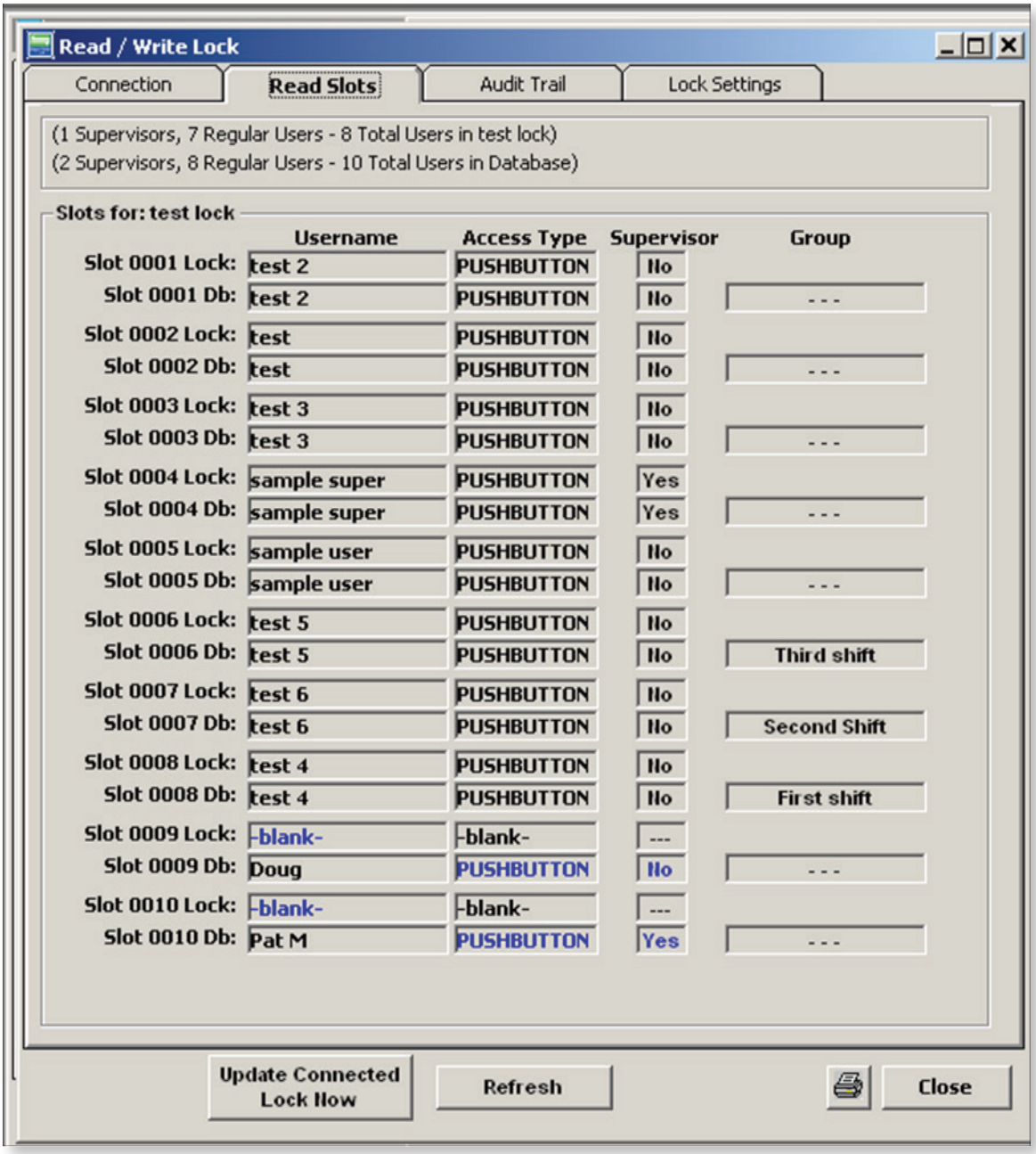
Plug in the USB cable into the computer and into the lock. "**Connected to test lock**" appears on the status bar as well as a check appears next to **test lock**.





PROGRAMMING EXAMPLE *continued*

7. Select **Read Slots**.



This **Read Slots** screen shows the new users Doug and Pat M in the computer's database in slots 0009 and 0010, but not in the Lock database.

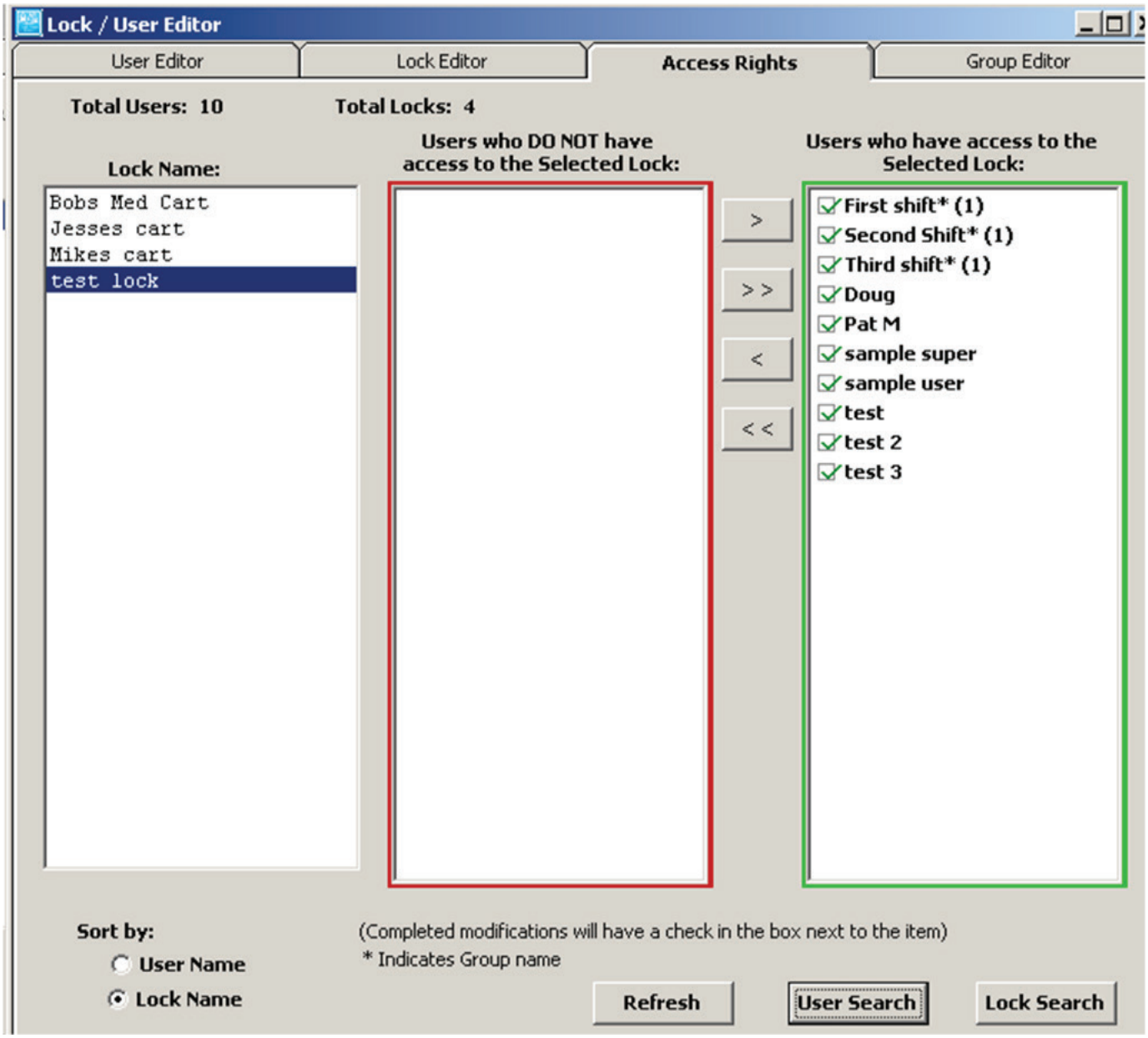
8. Press **Update Connected Lock Now**.
9. Note: it is possible that the update will have occurred before this screen opened, as the system updates itself very quickly.

PROGRAMMING EXAMPLE *continued*

New users Doug and Pat M are now updated in **test Lock**.

PROGRAMMING EXAMPLE *continued*

Open **Lock/User Editor**. Select **Access Rights**.

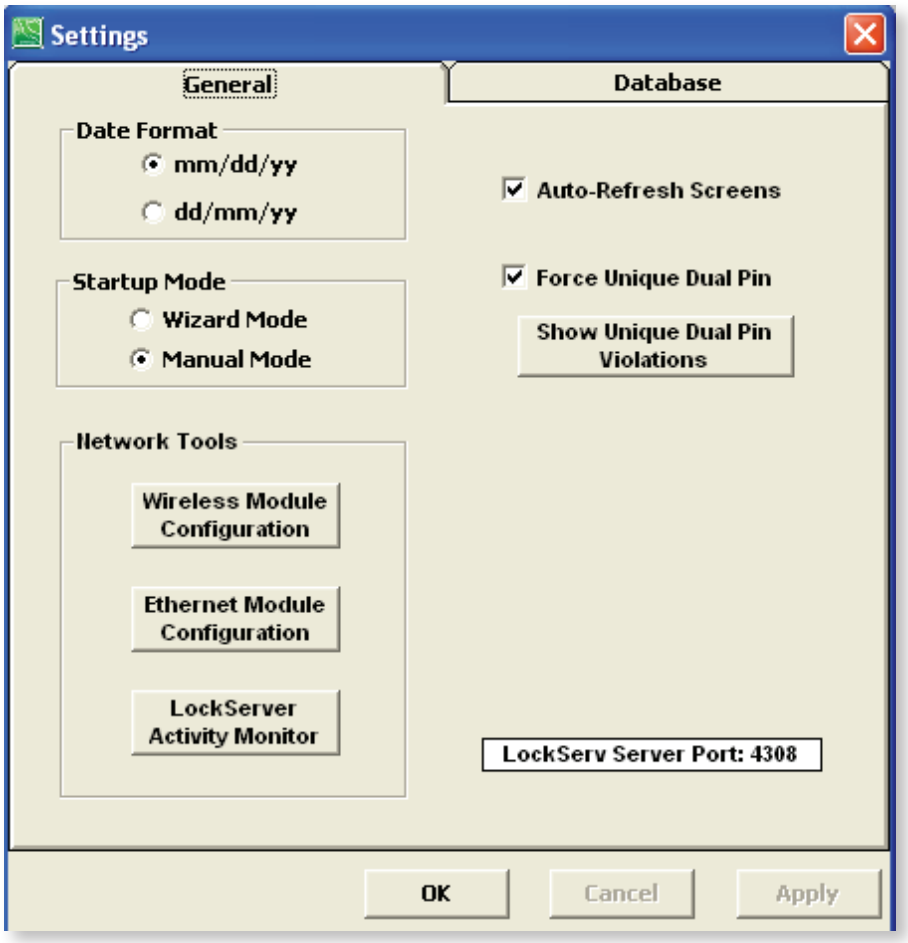


The **Access Rights** screen now shows a check mark next to Doug and Pat M.

SETTINGS

Settings allows the Operator to make changes to the database location on the computer as well as other changes to LockView.

Select the **Settings** window.



General tab
Date Format (Changes date format in Audit Log)
month/day/year
or
day/month/year

Startup Mode – choose which mode LockView will start up in, Wizard mode or Manual mode.

Network Tools (Refer to "Database & Network Configuration & Install Manual")

Auto Refresh Screens - LockView continually updates User Editor, Lock Editor, Access Rights screens.

Note: Turning this feature on may slow the system down.

Force Unique Dual Pin - All dual credential codes in the User Editor must be different; that is, every User with a dual credential code will be forced to have a different dual credential from all other Users with dual credentials.

SETTINGS *continued*

Show Unique Dual Pin Violations - If the Force Unique Dual Pin option was turned on after users were already in the database, clicking this button will display any users that have dual credential codes that match other user's dual credential codes.

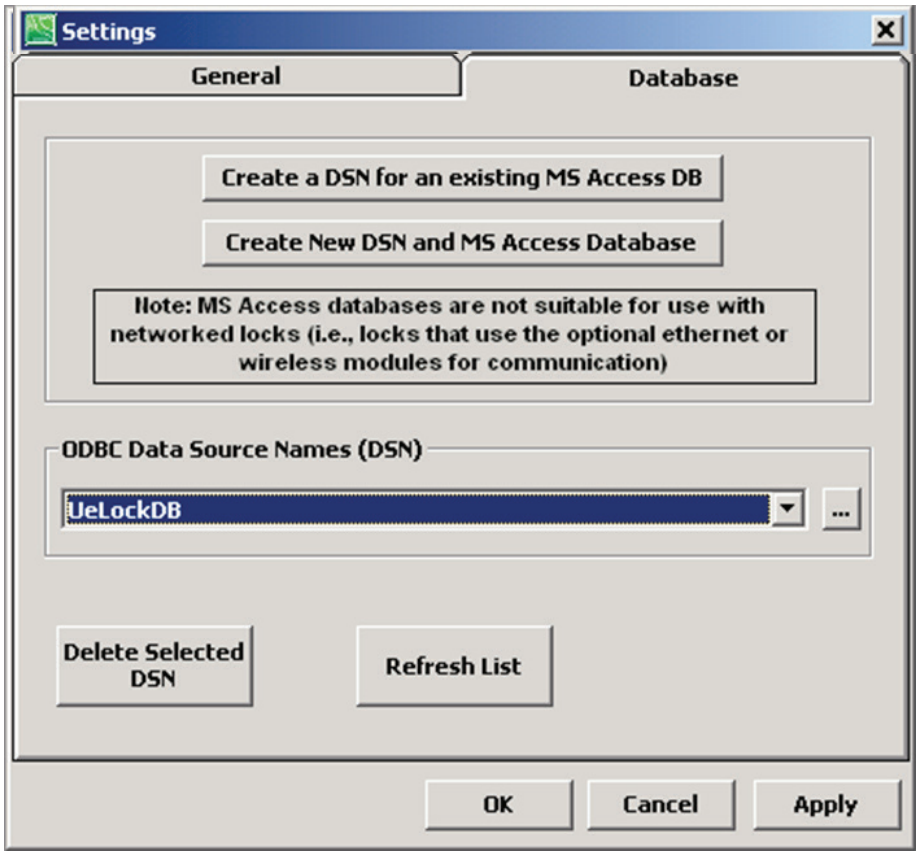
Server Settings (networked systems only)

Maximum Simultaneous Updates: The number of locks LockServer can update simultaneously.
Alter LockView Server Port: TCP/UDP Port 4308 is CompX-LockView owned. No other software should use this port. It is highly recommended NOT to alter the TCP port.

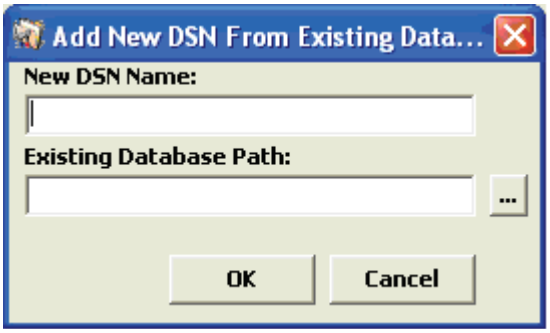
Database tab (Refer to "Database & Network Configuration & Install Manual")

CREATE ODBC CONNECTION FOR AN EXISTING ACCESS DATABASE

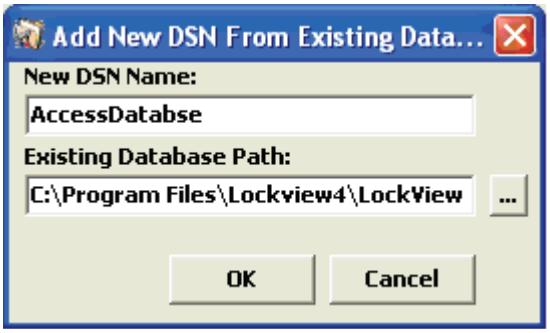
1. Open LockView, open **Settings**, select the **Database** tab.



2. Select '**Create a DSN for an existing MS Access DB**'

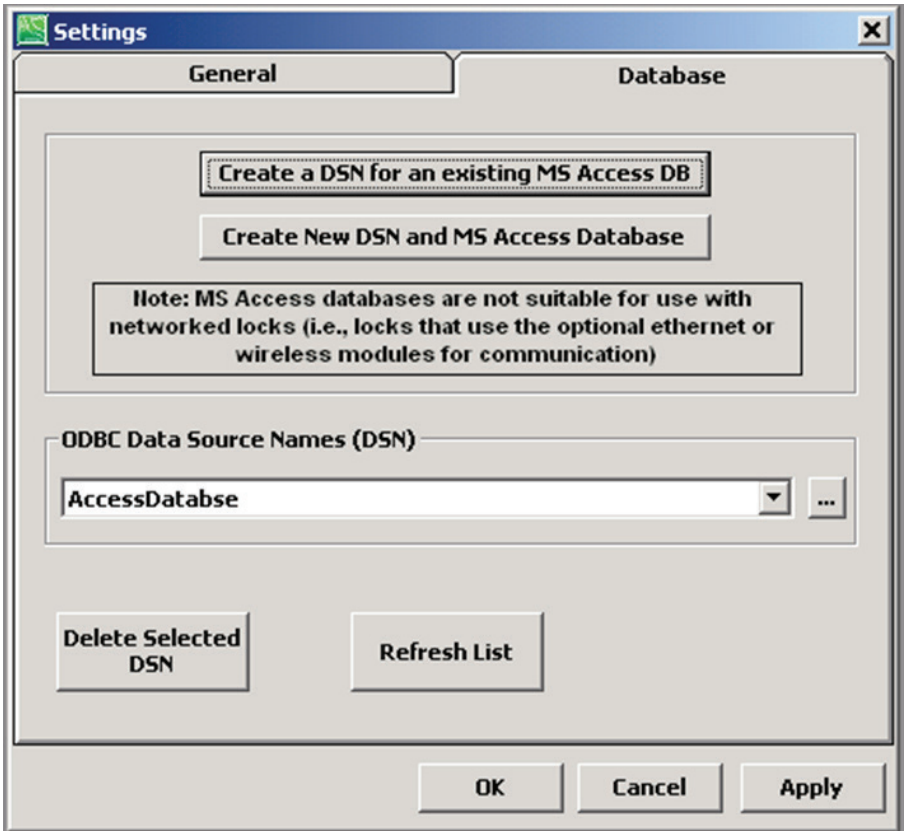


3. Enter a DSN.
   In this case, AccessDatabse was entered for the DSN Name.
   Click on the browse icon (...) and locate the Existing Database,
   Or type in the location and click **OK**.

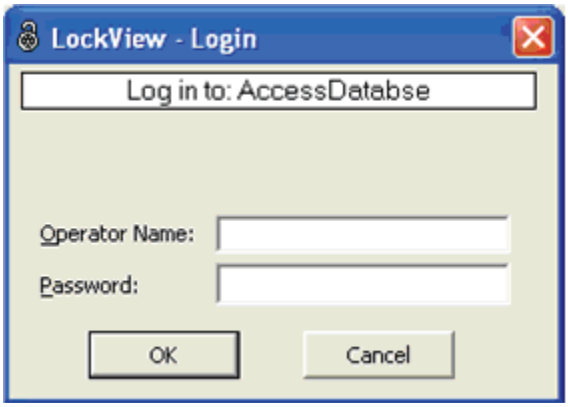


CREATE ODBC CONNECTION FOR AN EXISTING ACCESS DATABASE cont.

4. AccessDatabse is now the current ODBC connection.
   Click '**Apply**.'

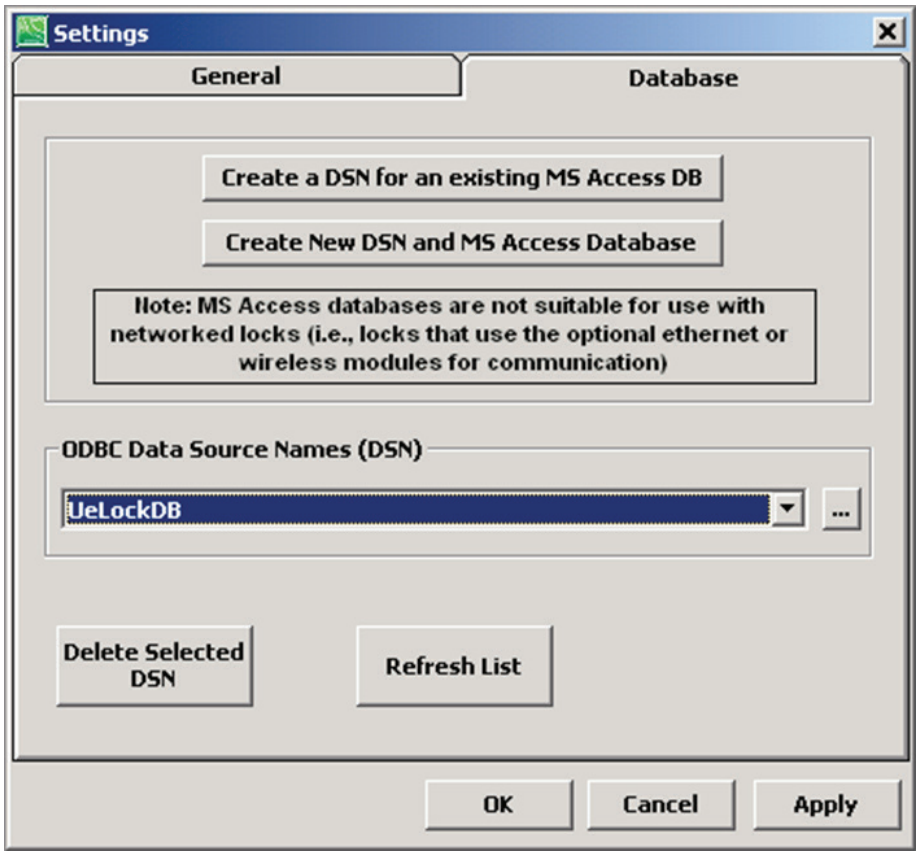


5. Login to database with an Operator that is valid in the chosen database.
   Click **OK**.

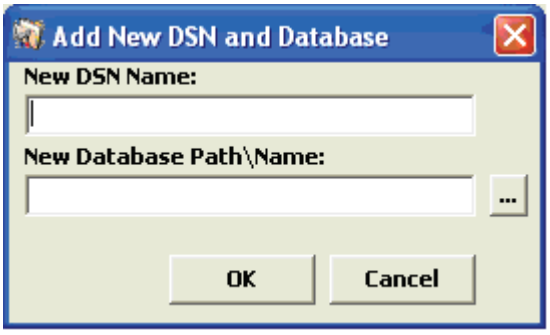


CREATE ODBC CONNECTION FOR A NEW ACCESS DATABASE

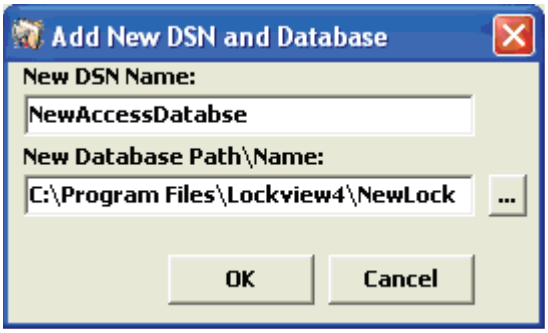
1. Open LockView, select **Settings**, click the **Database** tab.



2. Select '**Create a New DSN and MS Access Database**'

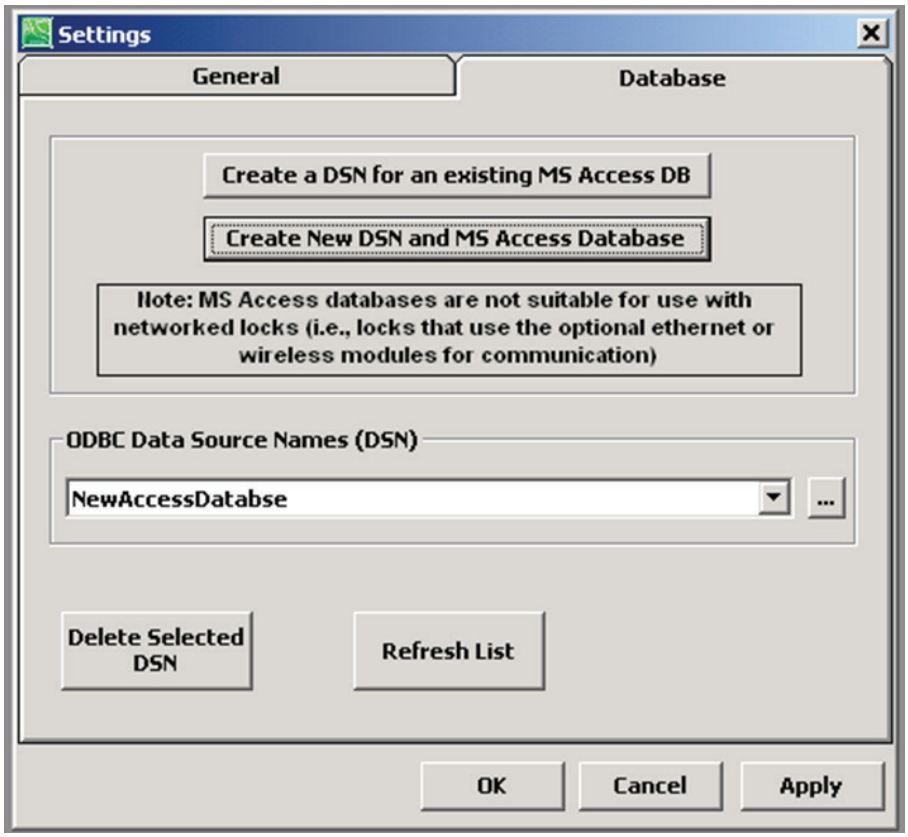


3. Enter a DSN.
   In this case, NewAccessDatabse was entered for the DSN Name.
   Click on the browse icon (...) and select the desired location of the new database.
   Click **OK**.

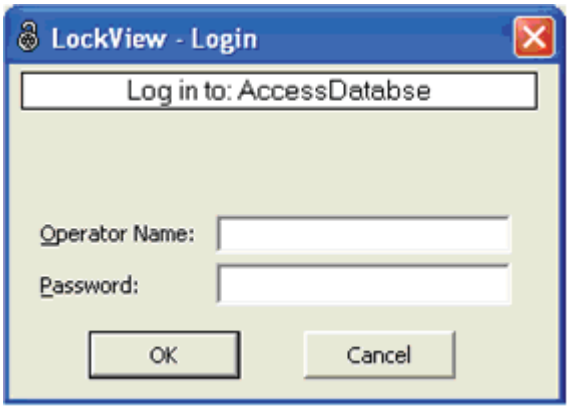


CREATE ODBC CONNECTION FOR A NEW ACCESS DATABASE cont.

4. NewAccessDatabse is now the current ODBC connection.
   Click '**Apply**.'



5. Login to database with:
   Operator Name: *admin*
   Password: *admin*. Click **OK**.



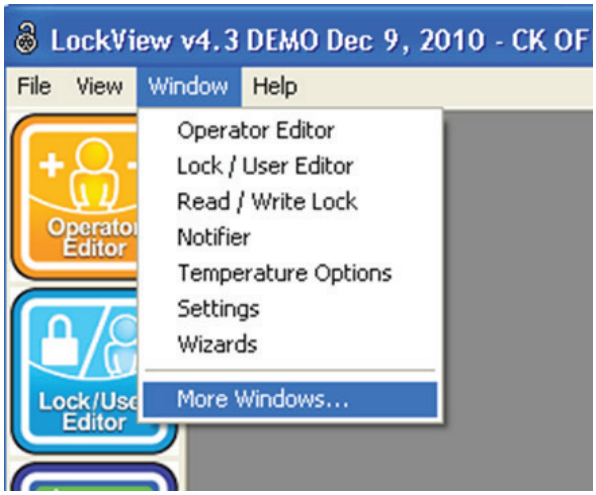
CALIBRATION INSTRUCTIONS

Calibration of the CompX temperature monitoring eLock can only be done in conjunction with LockVIew version 4 software. In the event that NIST certification is required, please contact CompX Security Products. CompX recommends adding the temperature monitoring eLock to an existing calibration schedule.

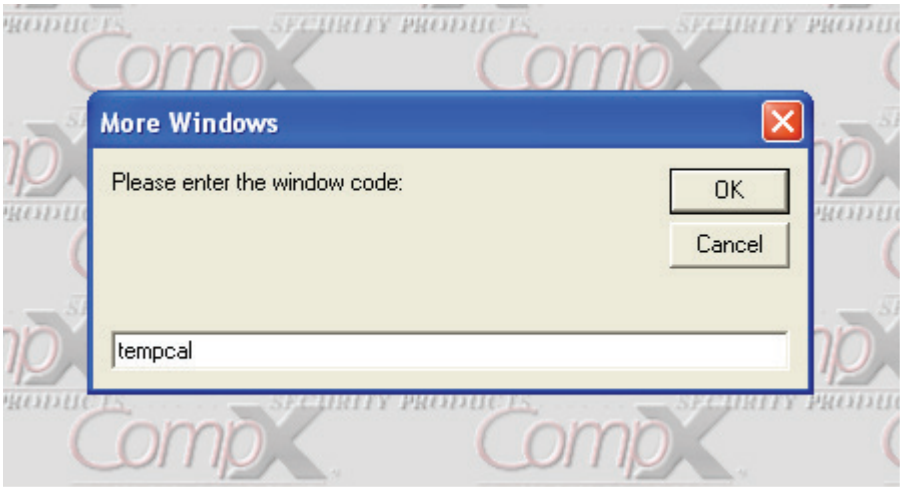
In LockView, click "Window"

Click "More Windows..."

Type: *tempcal*



Click OK



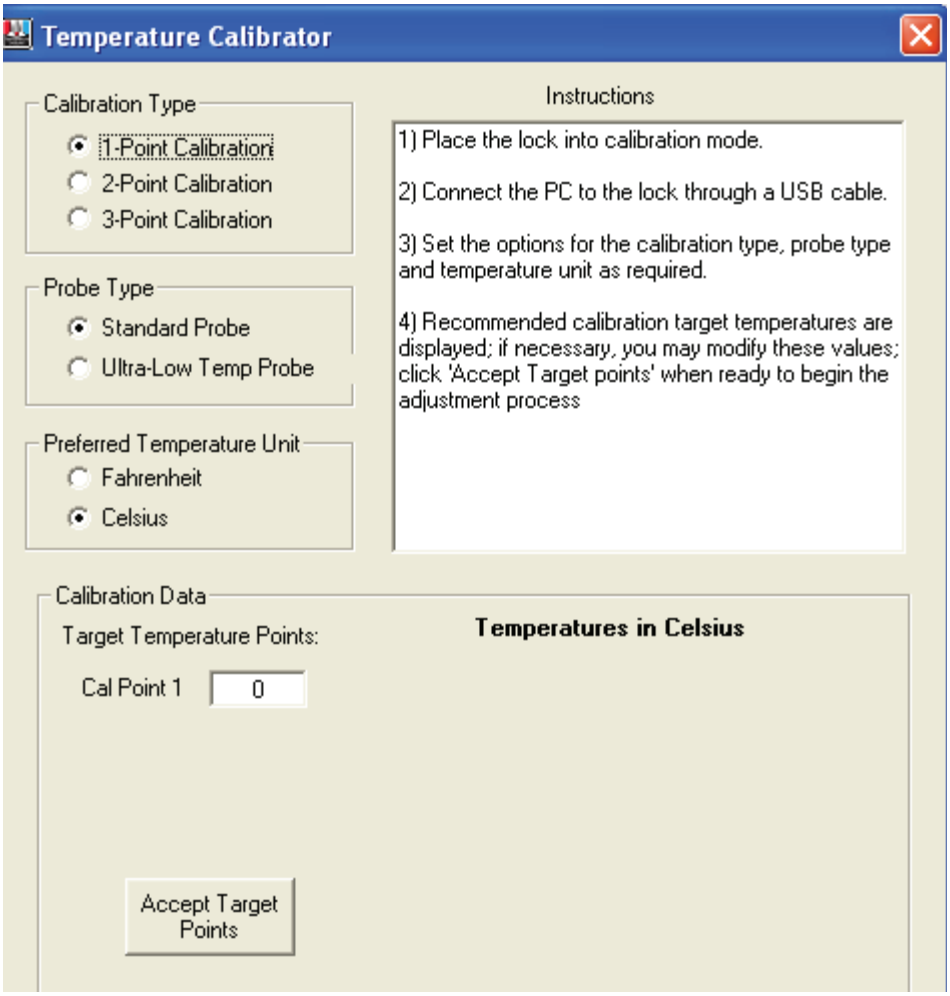
CALIBRATION INSTRUCTIONS *continued*

By following the instructions shown in the Temperature Calibrator, 1-Point, 2-Point, or 3-Point calibration can be performed.

To place the eLock in calibration mode, access to the eLock manual programming screen is required.

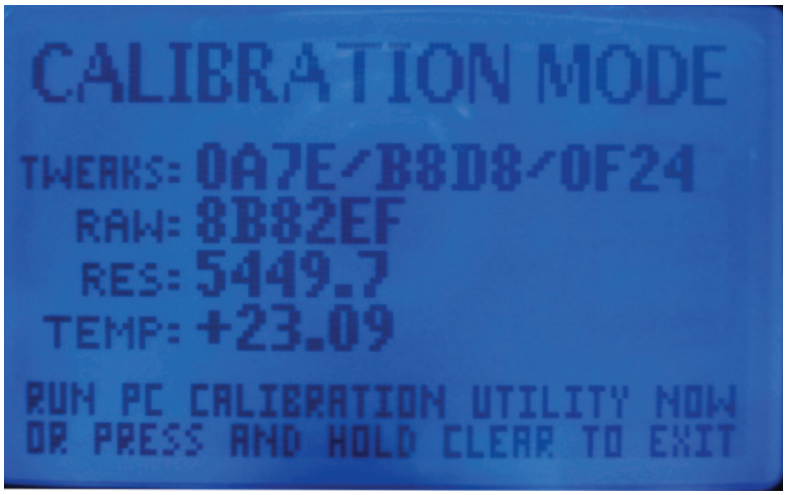
At the eLock:

1) Press "MENU." **LOGIN PLEASE** will be displayed.
2) Scan valid credential or enter a valid 4 – 14 digit PIN and press "ENTER."
3) Press "UP/DOWN" to highlight **TEMPERATURE MENU** and press "NEXT/SELECT."
4) Press "UP/DOWN" to highlight **CALIBRATE MODE** and press "NEXT/SELECT."

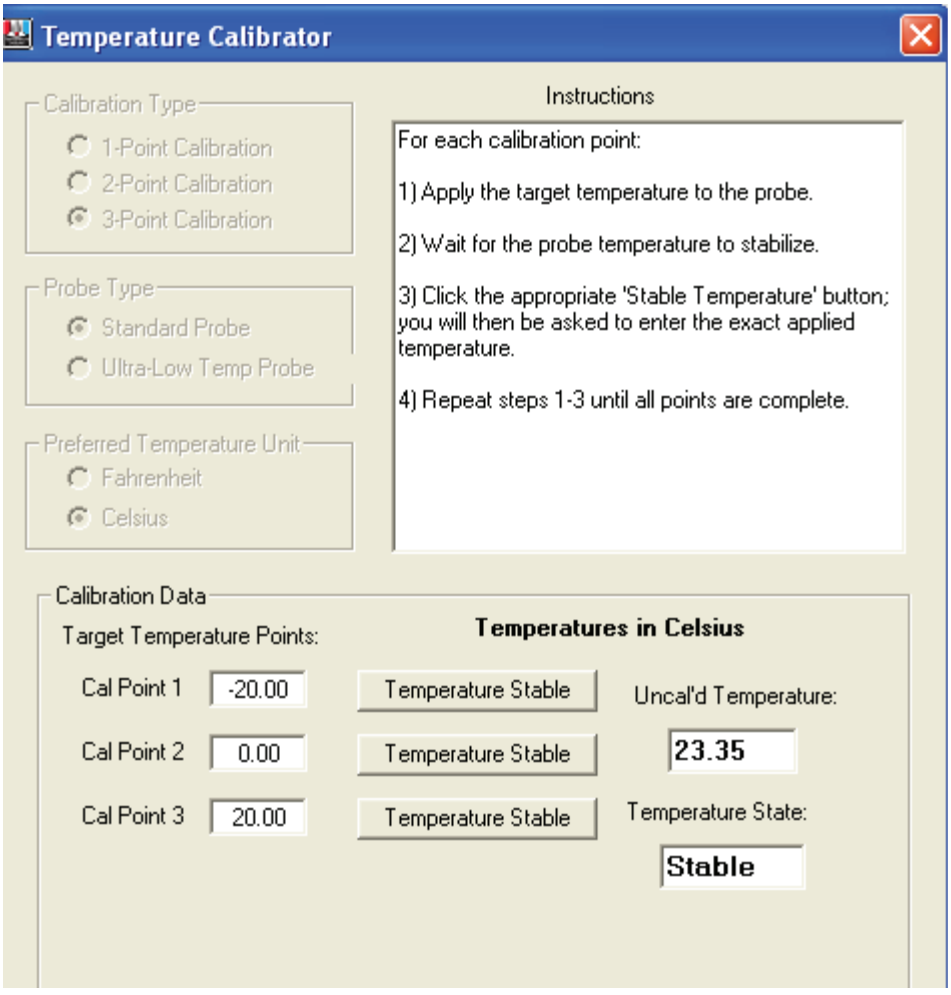


CALIBRATION INSTRUCTIONS *continued*

Screen shot of eLock LCD when in calibration mode.



After the target point(s) have been accepted, follow the instructions for each calibration point.



LockView 5/5Pro

CompX LockView Software Instruction Manual

eLock
TECHNICAL HOTLINE
847-752-2525
M-F: 8 a.m.-5 p.m. Central

CompX SECURITY PRODUCTS

Copyright 2016 © CompX Security Products / 847.752.2500 / compx.com / 715 Center St., Grayslake, IL 60030
Any companies and/or products referred to herein are marks or registered trademarks of their respective companies, owners and/or mark holders.