

Unicon™ CL Series Software

REFERENCE MANUAL



Trademarks

The following items are trademarks or registered trademarks of Kaba Mas in the United States and/or other countries.

- Unicon

Windows, Windows 2000, Windows XP, Windows Vista, and Windows 7 are registered trademarks of Microsoft Corporation.

Notice: The information in this manual is subject to change without notice and does not represent a commitment on the part of the Kaba Mas. Kaba Mas shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

© 2006-2010 Kaba Mas

All rights reserved

Document Number 3076.026
Rev. C - 10/10

Table of Contents

CHAPTER 1

INTRODUCING THE UNICON™ CL SERIES SOFTWARE 1

Kaba Mas Welcome	1
The Unicon™ CL Series Software Program Package	1
System Overview	2
Model CL10 Detail	3
Lock Modes	3
Personnel Classifications	4
Access Combination Requirements	4
Personnel Activity Chart	5
Model CL20 Detail	6
Lock Modes	6
Personnel Classifications	7
Access Combination Requirements	7
Personnel Activity Chart	8
System Processes	9
Program Lock	9
Add/Delete Users to/from Lock	9
Upload Access Schedules to Lock	10
Upload Date & Time to Lock	10
Retrieve & Report on Audit Download from Lock	10
Retrieve & Report on User Table Download from Lock	11

CHAPTER 2

UNICON™ CL SERIES SOFTWARE 13

Software Conventions	13
Database Backup & Restoration	13
Backup A Database	13
Restore A Database Backup	19
Attach A Database	23
Start the Unicon CL Series Software Program	25
Unicon CL Main Menu	27
CL10 Interface Main Menu	27
CL20 Interface Main Menu	28
Current Lock Interface	28
Menu Bar Options	29
Toolbar Options	31

File Menu	33
Exit	33
Access Schedules Menu	35
Create A New Access Schedule	36
Modify Access Schedule	39
Delete Access Schedule	42
Users Menu	45
Manage Users	46
Add A New User	46
Modify User Data	49
Delete User	52
Find Locks	54
Manage User Groups	58
Manage User Groups - CL10 Interface	59
Create A New User Group	59
Modify User Group	66
Delete User Group	70
Manage User Groups - CL20 Interface	72
Create A New User Group	72
Modify User Group	82
Delete User Group	85
Locks Menu - CL10	87
List Locks	88
Delete Lock	89
Show Lock Details Report	90
Program Lock	91
Program Lock - Lock Options	91
Program Lock - Add/Delete Users	93
Assign Users to Lock from User Group	93
Assign Users to Lock	94
Program Lock Users	102
Add Users to the Lock	105
Change User ID Assignment	109
Delete Users from Lock	113
Write to the Key	115
Program Lock Date & Time	116
Locks Menu - CL20	117
List Locks	118
Delete Lock	119
Show Lock Details Report	120
Program Lock	121
Program Lock - Lock Options	122
Program Lock - Add/Delete Users	123
Assign Users to Lock from User Group	124
Assign Users to Lock	125
Program Lock - Access Schedules	133
Assign Access Schedules to Lock from Access Schedule Template ...	134
Assign Access Schedules to Lock	136

Program Lock Users	138
Add Users to the Lock	140
Change User ID Assignment	144
Delete Users from Lock	148
Write to the Key	150
Program Lock Access Schedules	151
Assign Access Schedules to Lock from Access Schedule Template	154
Assign Access Schedules to Lock	156
Program Lock Date & Time	158
Keys Menu	161
Initialize Audit Download Key	162
Initialize User Table Download Key	162
Delete Key Contents	163
Reports Menu	165
Report on Audit Download Key	166
Model CL10 Audit Data Report	167
Model CL10 Transaction Types and Definition	168
Model CL20 Audit Data Report	171
Model CL20 Transaction Types and Definition	173
Report on User Table Download Key	176
Model CL10 User Table Report	177
Model CL20 User Table Report	178
Report on Users	179
Lock List Report	180
Lock Detail Report	181
Integrated Audit Report	182
Settings Menu	185
Current Lock Interface	186
Change Adapter and Port Settings	189
Select Database Server	190
Choose Default Lock	191
Help Menu	193
Help Topics	193
About Unicon CL Series Software	195
Appendices	197
Appendix A - Audit Transaction Records - CL10	199
Appendix B - Audit Transaction Records - CL20	203

INTRODUCING THE UNICON™ CL SERIES SOFTWARE SYSTEM

Kaba Mas Welcome

Kaba Mas, part of the world-wide Kaba group, is the world's leading manufacturer and supplier of high security, electronic safe locks. From sophisticated locks safeguarding classified information and cash supplies stored in automated teller machines to complete systems serving goods-in-transit, Kaba Mas products are world renowned for their ability to greatly reduce incidence of theft. Kaba Mas is dedicated to satisfying end-user needs for security, safety, and convenience. We welcome you to the world of Kaba Mas security and the Unicon™ CL Series Software.

The Unicon™ CL Series Software Program Package

The Unicon CL Series Software implementation package includes:

- Unicon CL Series Software Install CD, Version 2.1.0 (32-bit version)
- Unicon CL Series Software Install CD, Version 2.1.0 (64-bit version)
- Unicon Data Cable
- USB Adapter for Unicon Data Cable
- 1 Programming Key Fob (Teal)
- 1 Reporting Key Fob (Red)
- Unicon CL Series Software Getting Started Guide
- Unicon CL Series Software Reference Manual (Included on Install CD in electronic format)

If you are missing any of the above items, contact Kaba Mas Customer Service at 1(800) 950-4744. Please note that if you are installing the upgrade package, you will not receive all of these items.

Note: *If you do not have an available USB port on your PC but you do have an available serial port, the serial adapter (P/N 202124) can be installed as an alternate to the USB adapter. This item is ordered separately.*

System Overview

The Unicon CL Series Software allows PC based programming of lock data instead of manual entry at the lock. Lock and user data are defined and maintained in a database at the PC. Additionally, the system allows the retrieval and reporting of data stored in the lock.

Upload Data to Lock

As an alternative to defining setup data and user data manually at the lock, certain types of data can be defined at the PC using the Unicon CL Series Software and the information can then be uploaded (transferred) to the lock via a Programming Key Fob.

Download Data from Lock

There are two types of data that can be “downloaded” (retrieved) from the Unicon CL Series locks using the Unicon CL Series Software. Lock audit data and user table data can be retrieved from the lock using a Reporting Key Fob and can then be reported on at the PC.

It is important that you understand how the entire system operates, even though many operations will be carried out by other personnel. Before you start using the program, be sure to read the next few pages. They tell you what this package includes, the equipment you need to use the software, and identify the components of the system and the people who will be working with them.

The **Unicon CL Series System** consists of three basic components:

1) PC Based Computer Program

The PC Based Computer System is actually comprised of hardware and software components, including a Unicon data cable with USB interface. The software component is the PC based Unicon™ CL Series Software.

2) Security Locks with Access Accountability

The Unicon CL locks are secured, advanced design locks with programming and audit capabilities. There are currently 2 different models of the Unicon CL lock family that will operate in conjunction with the Unicon CL Series Software. They are as follows:

- **Unicon Model CL10**
- **Unicon Model CL20**

Some functions of the software will be limited and some menu options will vary depending on which type of lock you are working with at the time.

3) Key Fobs

A Key Fob is actually a Dallas Semiconductor electronic device imbedded in a plastic fob. The keys are designed to be carried on a key ring like a traditional key. The keys are attached to a Unicon data cable at the PC and are initialized with unique data. They can then be inserted into the key port at the lock to upload and download data to and from the lock.

Key Types

There are two types of Key Fobs that are used with the Unicon CL Series Software. They are designated and used as follows:

- **Programming Key Fob** - The teal colored key fob is initialized at the PC with the information needed to take it into the field and program a lock.
- **Reporting Key Fob** - The red Supervisor Audit key is initialized at the PC to retrieve audit records or user tables from a lock. The key can then be read by the computer to provide a record of lock activity or report on lock users.

Model CL10 Detail

This section explains the operational approach to the Model CL10 lock and the details of the personnel who will be working with the lock.

Lock Modes

A lock is shipped from the factory with default lock “setup” values and a pre-set PIN for locking and unlocking the lock. This is referred to as **Factory Mode**.

The lock is shipped with a default factory **Super Master User PIN** that can be set (i.e., changed) when the lock is in Factory Mode. Once the Super Master User PIN is set, the Super Master User combination can be used to shelve the lock in the event that the Master User combination is lost. Refer to the *Unicon CL10 Super Master Operations* (Document # 3109.017) for more detail.

WARNING: *The setting of the Super Master User PIN is optional, however, if you do not set the Super Master User PIN before setting the Master User PIN, all Super Master User capabilities will be permanently lost.*

The lock is removed from Factory Mode when the Master User PIN gets changed.

To remove a lock from an operational mode, one can “shelve” the lock which places it in **Shelved Mode**. Most lock values are returned to the factory default. Refer to the *Shelve Lock* operation for more detail.

Personnel Classifications

There are three different classifications of lock personnel:

- **Master User** - The Master User performs the initial lock setup activities and can also shelve the lock. There is a maximum of one Master User per lock. The Master User combination will also lock and unlock the lock.
- **Manager User** - A user added by the Master User. A Manager User can lock and unlock the lock. A Manager User can also retrieve reporting data from the lock if authorized to do so by the Master User.
- **Lock User** - A user who can take temporary ownership of a locker by setting a combination to lock and unlock the lock.

There can be a maximum of 126 users who can open this lock at specific times:

- There can be a maximum of **one Master User and 124 Manager Users**, programmed and capable of accessing the lock at any given time.
- There can be a maximum of **one Lock User** (not including the Master or Manager users) programmed and capable of accessing the lock at any given time.

Access Combination Requirements

A valid access combination allows a user to lock or unlock a lock.

Master or Manager User Access Combination

An access combination for the Master User and for Manager Users is eight digits long and consists of a 3-digit User ID + a 5-digit User PIN.

Master or Manager User ID

A **User ID** is a three-digit number that represents a user. **User ID 111 is reserved for the Master User.** A maximum of 125 user IDs are available in the lock (Master User ID + 124 other user IDs.) All operations performed by users require the entry of the User's ID as the first three digits of the combination. User IDs are assigned by the Master User or by a Supervisor.

Master or Manager User PIN

A **User Personal Identifier Number (PIN)** is five digits. A User PIN can be defined to any combination of numbers allowed by the keypad. A PIN can also be changed at a later time.

Lock User Access Combination

The **Lock User Access Combination** is a 4-7 digit variable length combination that is set as each new Lock User takes ownership of the unit (locker, cabinet, etc.) that needs to be secured. The access combination can then be used to lock and unlock the lock until the current Lock User relinquishes ownership of the lock (by leaving it in an open state) and a new Lock User sets a new access combination.

Note: *The Lock User does not have an actual assigned User ID like the Master User and Manager Users, but is identified as User 200 for operations recorded in the Audit trail of the lock.*

Personnel Activity Chart

The following chart shows the activities that can be performed by each type of user.

	Keypad Command	Master User	Manager User	Lock User
Set Master User PIN (p.6)	#1	✓		
Change PIN (p.11)	#1	✓	✓	N/A
Set Lock User Access Combination (p.12)	#1	N/A	N/A	✓
Shelve Lock - Master User (p.11)	#3	✓		
Add Manager Users (p.10)	#4	✓		
Delete Manager Users (p.10)	#5	✓		
Set Lock ID (p.8)	##1	✓		
Toggle Sound On/Off (p.8)	##5	✓		
Toggle Daylight Savings Time (p.12)	###1	✓		
Change Reporting Capabilities (p.8)	###2	✓		
Lock/Unlock - Master/Mgr Combo (p.11)		✓	✓	N/A
Lock/Unlock - Lock User Combo (p.12)		N/A	N/A	✓
Upload Data to Lock* (p.13)	#2	✓		
Download Data from Lock* (p.xx)	#2	✓	✓	

* Software Based Operations

Model CL20 Detail

This section explains the operational approach to the Model CL20 lock and the details of the personnel who will be working with the lock.

Lock Modes

A lock is shipped from the factory with default lock “setup” values and a pre-set PIN for unlocking the lock. This is referred to as **Factory Mode**.

The lock is shipped with a default factory **Super Master User PIN** that can be set (i.e., changed) when the lock is in Factory Mode. Once the Super Master User PIN is set, the Super Master User combination can be used to shelve the lock in the event that the Master User combination is lost. Refer to the *Super Master Operations* (Document # 3072.026) for more detail.

WARNING: *The setting of the Super Master User PIN is optional, however, if you do not set the Super Master User PIN before setting the Master User PIN, all Super Master User capabilities will be permanently lost.*

The lock is removed from Factory Mode when the Master User PIN gets changed. The lock has two modes of operation: **Independent Mode** and **Supervisory/Subordinate Mode**. Within each operation mode, two access modes are available: **Single User access** and **Dual User access**. In Single User access, only one combination is required to open the lock. In Dual User access, two combinations must be correctly and consecutively entered to open the lock.

- **Independent Mode** - When operating in Independent Mode, the Master User can add Access Users. One (**Single User access**) or two (**Dual User access**) combinations are required to open the lock. This is the default operation mode for the lock when the Master User PIN first gets changed.
- **Supervisory/Subordinate Mode (Super/Sub Mode)** - When operating in Super/Sub Mode, the Master User can add Supervisors. Subordinate Users must then be added by and assigned to a Supervisor.

In **Single User access**, an enabled Subordinate User combination is required to open the lock.

In **Dual User access**, two enabled Subordinate User combinations are required to open the lock.

If a Supervisor disables lock access for the Subordinate User(s) assigned to a Supervisor ID, the Subordinate User combinations for that Supervisor ID will no longer be valid combinations for lock access.

To remove a lock from an operational mode, one can “shelve” the lock which places it in **Shelved Mode**. **Most** lock values are returned to the factory default.

Personnel Classifications

There are four different classifications of lock personnel:

- **Master User** - The Master User performs the initial lock setup activities and can also shelve the lock. There is a maximum of one Master User per lock. The Master User combination will also open the lock.
- **Access User** - In Independent mode, a user added by the Master User. An Access User can open the lock.
- **Supervisor** - In Super/Sub mode, a user added by the Master User who has the ability to add/delete Subordinate Users. The maximum number of Supervisors per lock varies according to lock model. A Supervisor can open the lock.
- **Subordinate User** - In Super/Sub mode, a user who is added by and assigned to a Supervisor. Subordinates can open the lock when enabled by a Supervisor.

Access Combination Requirements

A valid access combination allows a user to open a lock. By default a combination is eight digits long and consists of a 3-digit User ID + a 5-digit User PIN. The access combination requirement can be changed to require entry of only the User ID. This decreased access requirement lessens the security of the lock and is not recommended in most situations.

Note: *The full 8-digit combination of User ID + PIN is always required for the Master User.*

User ID

A **User ID** is a three-digit number that represents a user. **User ID 111 is reserved for the Master User.** A maximum of 125 users are available in the lock (Master User + 124 other users.) All operations performed by users require the entry of the User's ID as the first three digits of the combination. User IDs are assigned by the Master User or by a Supervisor.

In Super/Sub mode **User IDs 112, 113, 114 and 115 are reserved for Supervisors.** In this mode, the allocation of users allowed is a Master User, 4 Supervisors and 120 Subordinate Users.

User PIN

A **User Personal Identifier Number (PIN)** is five digits. A User PIN can be defined to any combination of numbers allowed by the keypad. A PIN can also be changed at a later time.

Personnel Activity Chart

The following chart shows the activities that can be performed by each type of user.

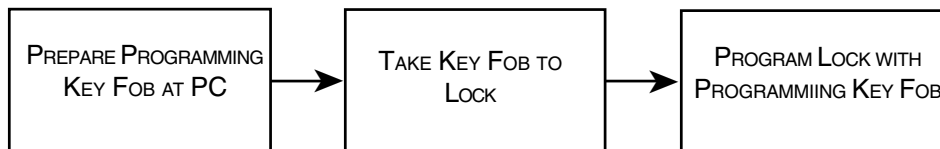
	Keypad Command	Master User	Access User	Supervisor	Subordinate User
Set Master User PIN (p.6)	#1	✓			
Change PIN (p.10)	#1	✓	✓	✓	✓
Shelve Lock - Master User (p.11)	#3	✓			
Add Supervisors or Access Users (p.9)	#4	✓			
Add Subordinate Users (p. 9)	#4			✓	
Delete Supervisors or Access Users (p.9)	#5	✓			
Delete Subordinate Users (p.9)	#5			✓	
Set Access/Operating Mode/Lock ID(p. 6)	##1	✓			
Enable/Disable Lock Access For Subordinates (p.10)	##4		N/A	✓	
Toggle Sound On/Off (p.7)	##5	✓			
Toggle Daylight Savings Time (p.12)	###1	✓			
Change Reporting Capabilities (p.7)	###2	✓			
Toggle Access Combination Req. (p.12)	###3	✓			
Unlock - Independent Mode (p.10)		✓	✓	N/A	N/A
Unlock - Super/Sub Mode (p.10)		✓	N/A	✓	✓
Upload Data to Lock* (p.13)	#2	✓	✓		
Download Data from Lock* (p.14)	#2	✓	✓	✓	✓

* Software Based Operations

System Processes

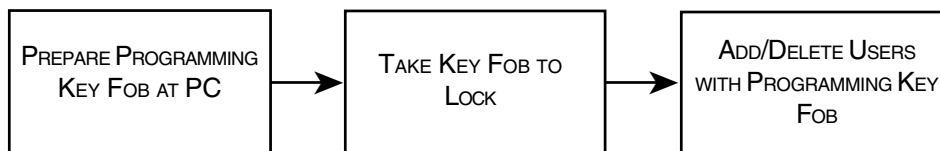
There are several system processes that involve integrating activity at the PC software level with activity at the lock. It is important that these processes be completed in their entirety. These processes are defined as follows in the form of flow charts and accompanying text.

Program Lock



As an alternative to defining setup data and user data manually at the lock, certain types of data can be defined at the PC using the Unicon CL Series Software and the information can then be uploaded (transferred) to the lock via a Programming Key Fob. You can prepare a Programming Key Fob at the PC that can program the lock with setup data, time and date, users, and access schedules (if applicable.) The key is then taken to the lock and the upload data command is entered. The key is inserted into the key reader on the lock while the key's data is written into the lock's memory.

Add/Delete Users to/from Lock



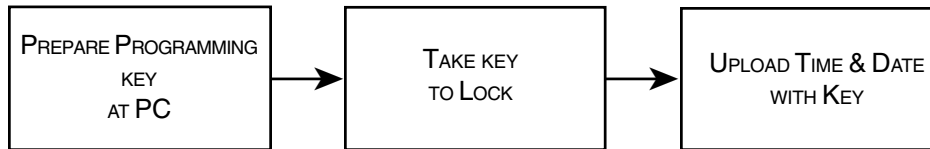
As an alternative to defining user data manually at the lock, the data can be defined at the PC using the Unicon CL Series Software and the information can then be uploaded (transferred) to the lock via a Programming Key Fob. You can prepare a Programming Key Fob at the PC that can program the lock with user data. The key is then taken to the lock and the upload data command is entered. The key is inserted into the key reader on the lock while the key's data is written into the lock's memory.

Upload Access Schedules to Lock (CL20 Only)



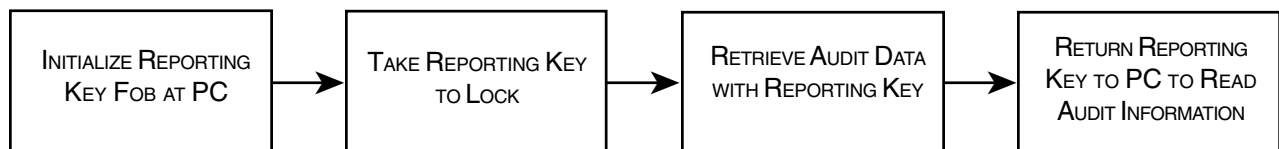
As an alternative to defining access schedule data manually at the lock, the data can be defined at the PC using the Unicon CL Series Software and the information can then be uploaded (transferred) to the lock via a Programming Key Fob. You can prepare a Programming Key Fob at the PC that can program the lock with the access schedule data. The key is then taken to the lock and the upload data command is entered. The key is held inserted into the key reader on the lock while the key's data is written into the lock's memory.

Upload Date & Time to Lock



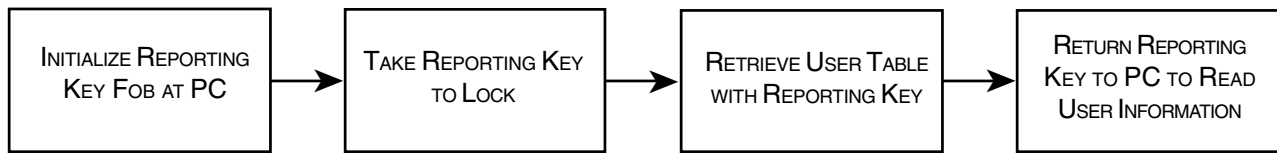
As an alternative to defining time window data manually at the lock, the data can be defined at the PC using the Auditcon 2 Series Software and the information can then be uploaded (transferred) to the lock via a Smart Key. You can prepare an SA Key at the PC that can program the lock with the time window data. The key is then taken to the lock. The lock is powered and the upload data command is entered. The key is inserted into the key reader on the lock while the key's data is written into the lock's memory.

Retrieve & Report on Audit Download from Lock



The audit records recorded in a lock may be written to a Reporting Key Fob which is then taken to the PC to be printed. The procedure is to use the Unicon CLSeries Software to initialize a red Reporting Key Fob for the retrieval of the audit data. The key is then taken to the lock and the retrieve audit command is entered. The key is inserted into the key reader on the lock while the data is written into its memory. The key with the data now written in it is taken to the PC where the data is read and a report is either printed or displayed.

Retrieve & Report on User Table Download from Lock



The user table defined in a lock may be written to a Reporting Key Fob which is then taken to the PC to be printed. The procedure is to use the Unicon CL Series Software to initialize a red Reporting Key Fob for the retrieval of the user table. The key is then taken to the lock and the retrieve user table command is entered. The key is inserted into the key reader on the lock while the data is written into its memory. The key with the data now written in it is taken to the PC where the data is read and a report is either printed or displayed.

Software Conventions

The Unicon™ CL Series Software program is operated through several windows. It conforms to Windows conventions so Windows users should have no trouble using it. Enough detail is included in this manual to enable a non-experienced user to follow the required procedures.

Note: *The screens shown in the Unicon CL Series Software manuals were captured on a Windows XP system. If your PC is running under a different operating system, your screens may look slightly different.*

Data Conventions

By default, SQL Server is case insensitive in regard to data handling; i.e., it will not differentiate between upper and lower case letters/characters when doing sorts or searches to retrieve records. For example, “Inpatient Services” would be seen the same as “inpatient services”. For more detail see the Microsoft web site.

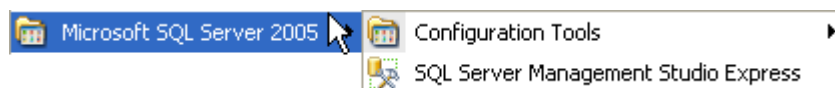
Database Backup & Restoration

It is recommended that the Unicon™ CL Series Database files be backed up on a regular basis so that data is not lost in the case of a system crash, fire, or other disaster. Frequency of backup should be based on the usage of the system; i.e., how often the data changes. The method to restore data will depend on how you have backed up the data; i.e., appending data with restore points or overwriting data each time you back up the data.

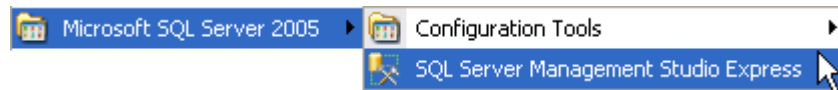
Back Up A Database

(source: <http://msdn2.microsoft.com/en-us/library/ms187510.aspx>)

1. Select the **Start** icon from the Windows task bar.
2. Select the **Programs** menu item.
3. Select the **Microsoft SQL Server 2005** menu item.



4. Select the **SQL Server Management Studio Express** icon.

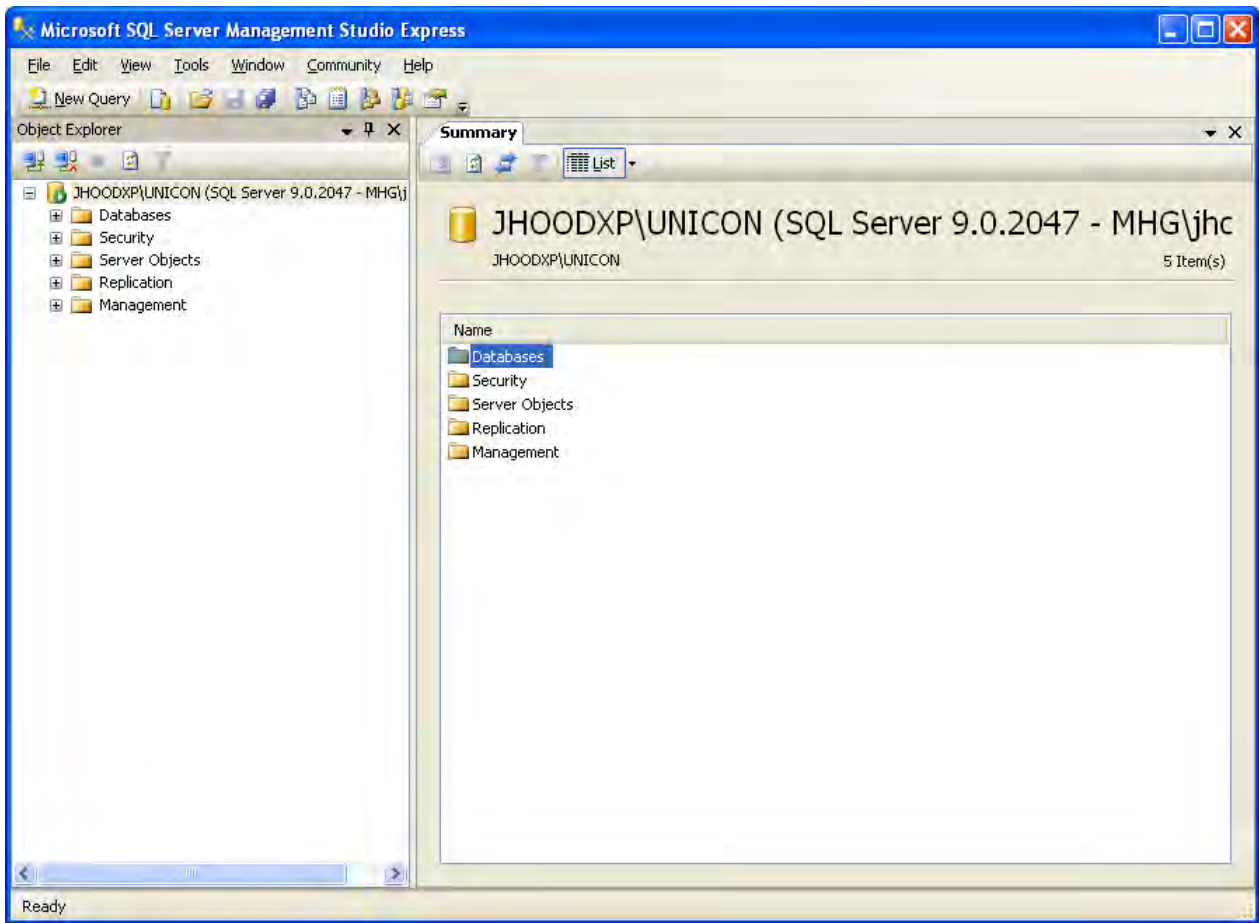


The Connect to Server window is displayed.

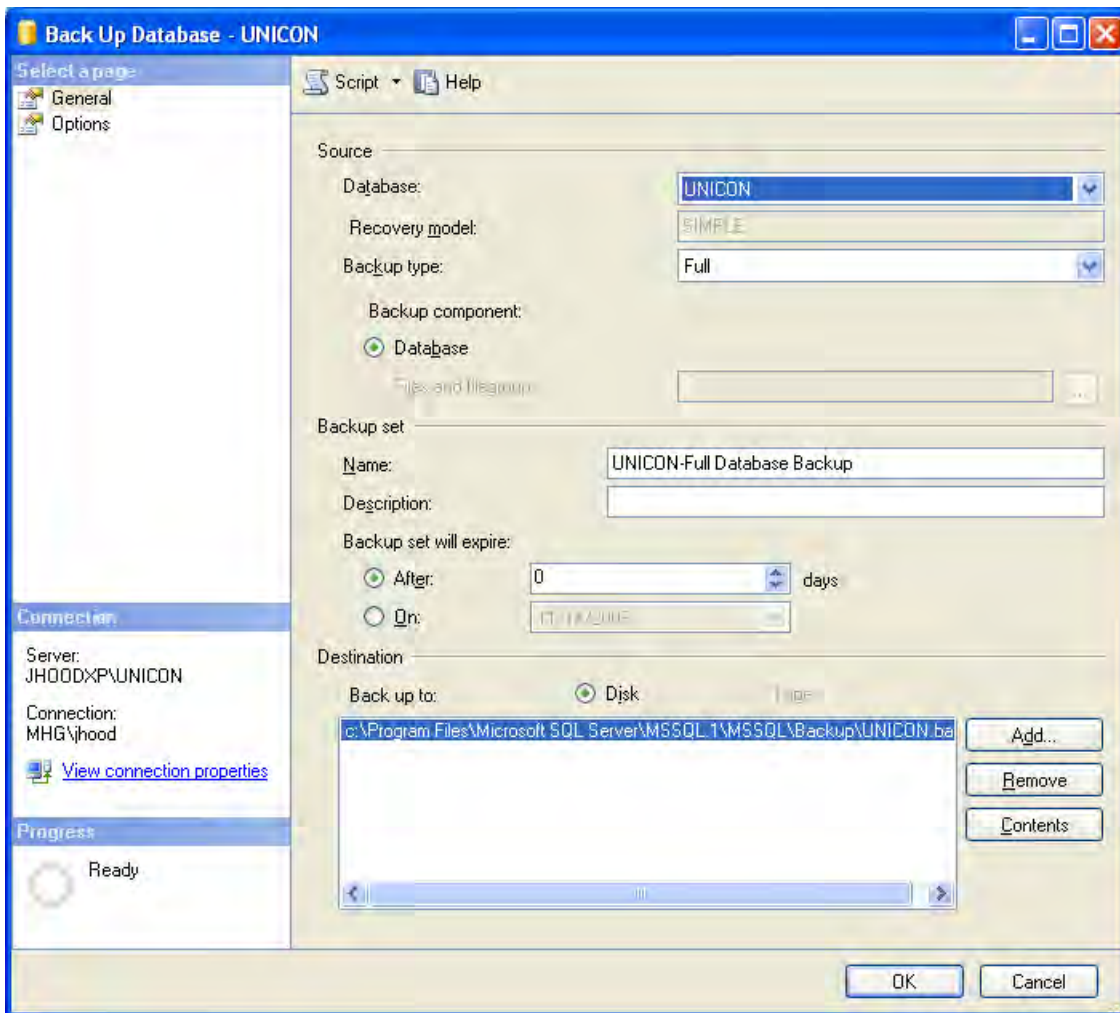


5. Click on **Connect** to connect to the UNICON instance of the Microsoft SQL Server Database Engine.

The SQL Server Management Studio Express Object Explorer is displayed.



6. In Object Explorer click the server name (for e.g. JHOODXP/UNICON) to expand the server tree, if necessary.
7. Expand **Databases**, and select **UNICON** database.



9. In the **Database** list box, verify the database name (UNICON).

10. In the **Backup type** list box, select **Full**.

Note: *After creating a full database backup, you can create a differential database backup.*

11. Either accept the default backup set name suggested in the **Name** text box, or enter a different name for the backup set.

12. Optionally, in the **Description** text box, enter a description of the backup set.

13. Specify when the backup set will expire and can be overwritten without explicitly skipping verification of the expiration data:
 - To have the backup set expire after a specific number of days, click **After** (the default option), and enter the number of days after set creation that the set will expire. This value can be from 0 to 99999 days; a value of 0 days means that the backup set will never expire.
 - To have the backup set expire on a specific date, click **On**, and enter the date on which the set will expire.
14. To view or select the advanced options, click **Options** in the **Select a page** pane.
15. Select an **Overwrite Media** option, by clicking one of the following:
 - **Back up to the existing media set**

For this option, click either **Append to the existing backup set** or **Overwrite all existing backup sets**.
 - Optionally, select **Check media set name and backup set expiration** to cause the backup operation to verify the date and time at which the media set and backup set expire.

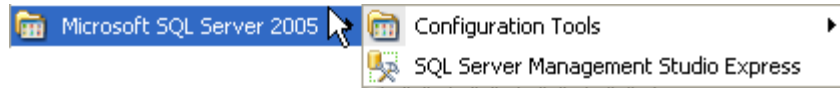
Optionally, enter a name in the **Media set name** text box. If no name is specified, a media set with a blank name is created. If you specify a media set name, the media (tape or disk) is checked to see whether the actual name matches the name you enter here.
 - **Back up to a new media set, and erase all existing backup sets**

For this option, enter a name in the **New media set name** text box, and, optionally, describe the media set in the **New media set description** text box.
16. In the **Reliability** section, optionally check:
 - **Verify backup when finished**.
 - **Perform checksum before writing to media**, and, optionally, **Continue on checksum error**.
17. When finished, click on **OK** to complete the backup.

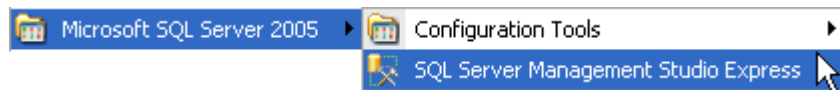
Restore A Database Backup

(source: <http://msdn2.microsoft.com/en-us/library/ms177429.aspx#>)

1. Select the **Start** icon from the Windows task bar.
2. Select the **Programs** menu item.
3. Select the **Microsoft SQL Server 2005** menu item.



4. Select the **SQL Server Management Studio Express** icon.

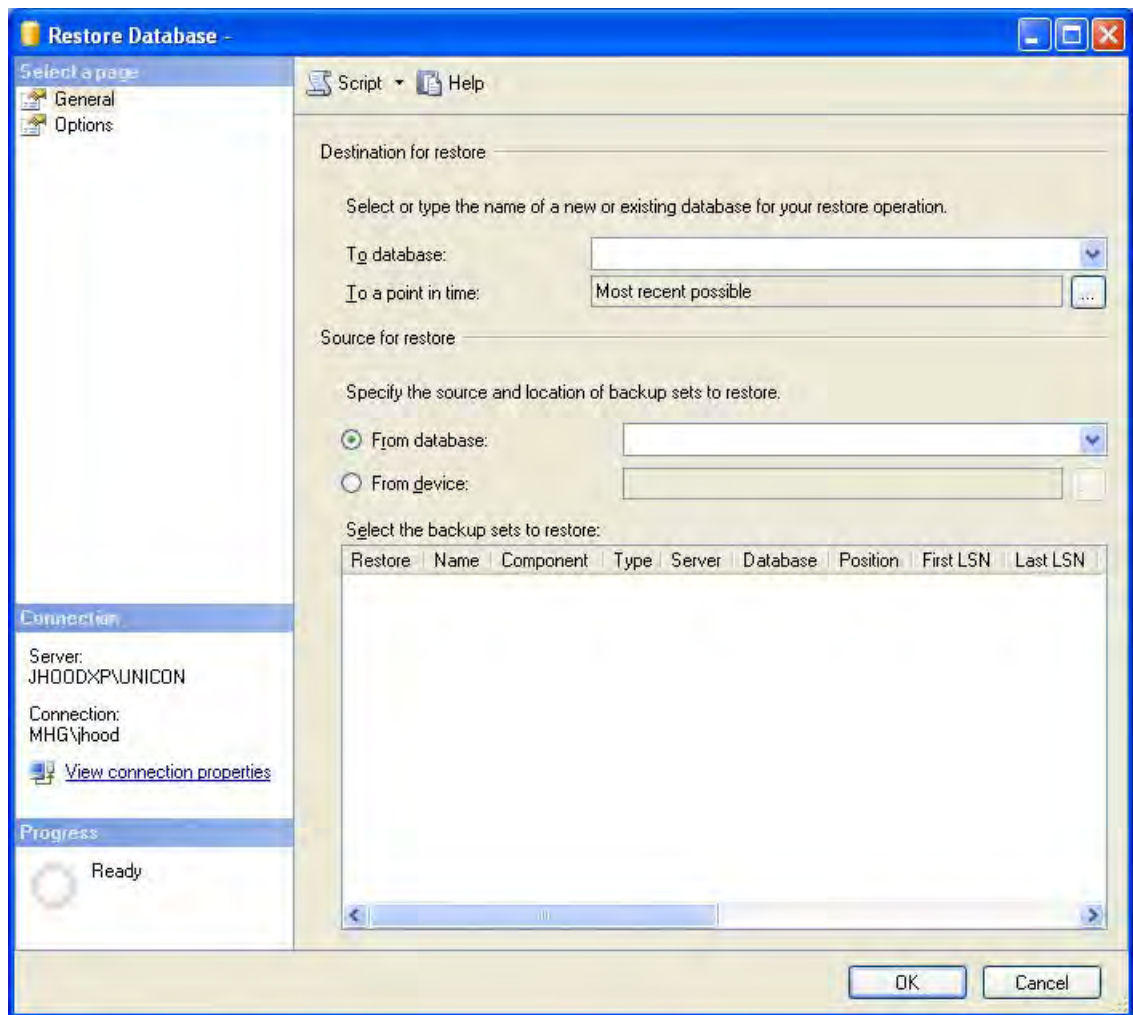


The Connect to Server window is displayed.



5. Click on **Connect** to connect to the UNICON instance of the Microsoft SQL Server Database Engine.

The SQL Server Management Studio Express Object Explorer is displayed.



7. On the **General** page, the name of the restoring database (in this case **UNICON**) appears in the **To database** list box. If the Unicon Database has been deleted, enter the database name of **Unicon** in the **To database** list box so as to look for Unicon's backups.
8. In the **To a point in time** text box, either retain the default (**Most recent possible**) or select a specific date and time by clicking the browse button, which opens the **Point in Time Restore** dialog box.
9. To specify the source and location of the backup sets to restore, click one of the following options:
 - **From database**
Enter/Choose a database name (UNICON) in the list box.
 - **From device**
Click the browse button, which opens the **Specify Backup** dialog box. In the **Backup media** list box, select one of the listed device types. To select one or more devices for the **Backup location** list box, click **Add**.

After adding the desired devices to the **Backup location** list box, click **OK** to return to the **General** page.

10. In the **Select the backup sets to restore** grid, select the backups to restore. This grid displays the backups available for the specified location. By default, a recovery plan is suggested. To override the suggested recovery plan, you can change the selections in the grid. Any backups that depend on a deselected backup are deselected automatically.
11. To view or select the advanced options, click **Options** in the **Select a page pane**.
 - a) In the **Restore options** panel, you can choose any of the following options, if appropriate for your situation:
 - **Overwrite the existing database**
 - **Preserve the replication settings**
 - **Prompt before restoring each backup**
 - **Restrict access to the restored database**
 - b) Optionally, you can restore the database to a new location by specifying a new restore destination for each file in the **Restore the database files as grid**.
 - c) The **Recovery state** panel determines the state of the database after the restore operation. The default behavior is:
 - **Leave the database ready to use by rolling back the uncommitted transactions. Additional transaction logs cannot be restored. (RESTORE WITH RECOVERY)**

Note: *Choose this option only if you are restoring all of the necessary backups now.*

Alternatively, you can choose either of the following options:

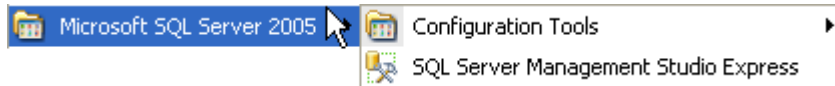
- **Leave the database non-operational, and do not roll back the uncommitted transactions. Additional transaction logs can be restored. (RESTORE WITH NORECOVERY)**
 - **Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a standby file so that recovery effects can be reverted. (RESTORE WITH STANDBY)**
12. Click on **OK** to complete the restoration of the UNICON database.

Note: *If you are simply moving your Unicon system to a different PC, you can follow a similar process to copy the files from the old PC and then **Attach** the database files to the database instance on the new PC. See the following section for detailed instruction.*

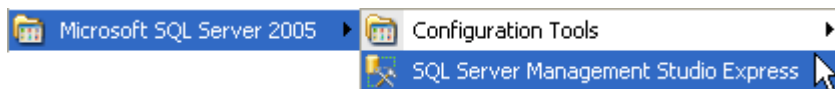
Attach A Database

(source: <http://msdn2.microsoft.com/en-us/library/ms190209.aspx>)

1. Copy the Unicon database files to the same location on the new PC as where they had been on the original PC.
2. Select the **Start** icon from the Windows task bar.
3. Select the **Programs** menu item.
4. Select the **Microsoft SQL Server 2005** menu item.



5. Select the **SQL Server Management Studio Express** icon.



The Connect to Server window is displayed.

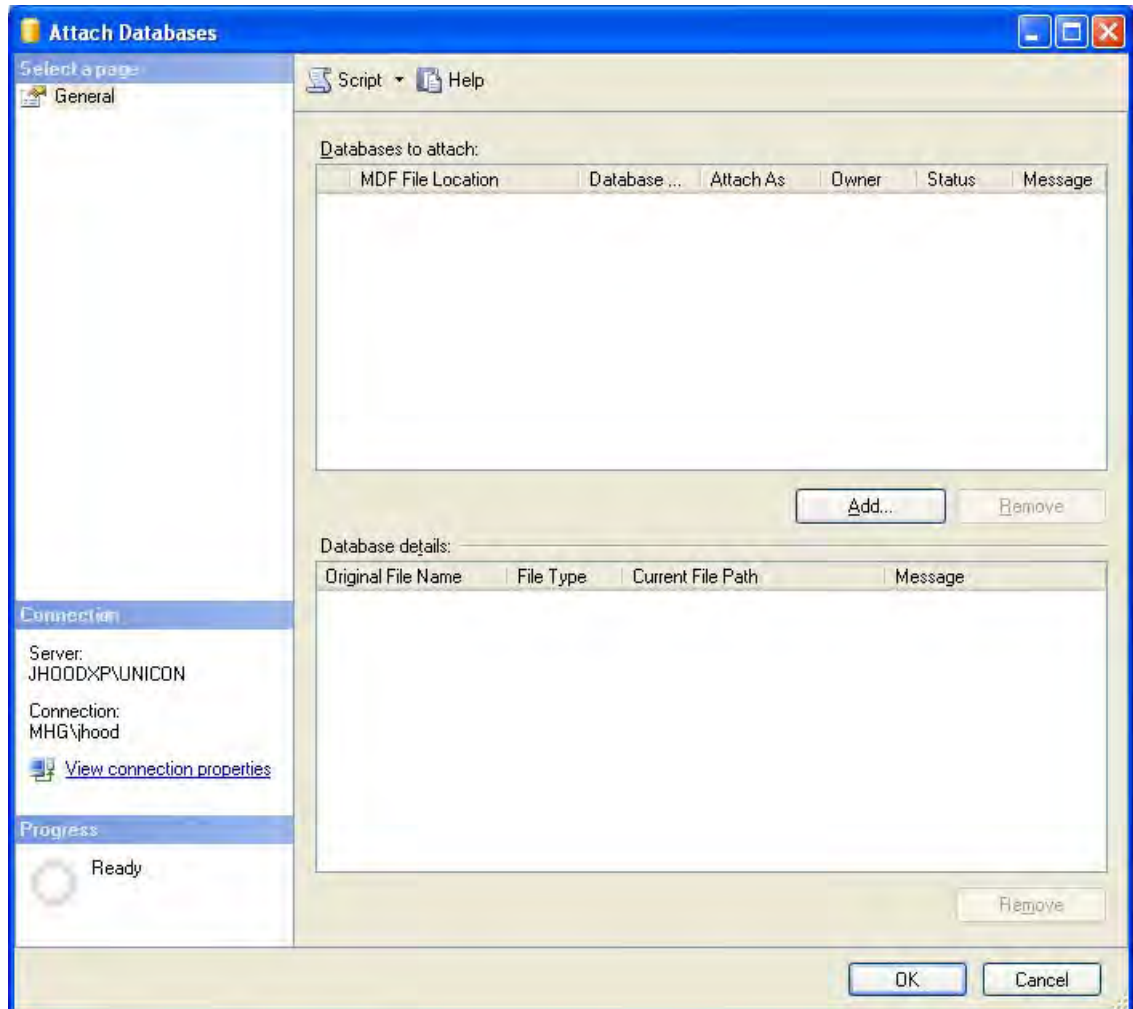


6. Click on **Connect** to connect to the UNICON instance of the Microsoft SQL Server Database Engine.

The SQL Server Management Studio Express Object Explorer is displayed.

7. Right click on Databases and choose **Attach...**

This opens the **Attach** dialog box.



8. In the **Attach Databases** dialog box, click on **Add** and specify the database to be attached.
9. In the **Locate Database Files** dialog box, select the disk drive where the **UNICON** database resides and expand the directory tree to find and select the .mdf file of the database (UNICON.mdf).
10. When you are ready to attach the database, click on **OK**.

Start the Unicon™ CL Series Program

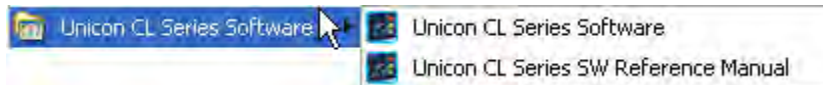
Note: *Before loading the Unicon CL Series Software program, ensure that the data cable and adapter are plugged into the appropriate port on the PC.*

You can start the Unicon™ CL Series Software Program at the PC by clicking on the Unicon™ CL Series Software icon from the desktop.



If you prefer, you can complete the following steps to start the Unicon™ CL Series Software Program from the Programs Menu:

1. Select the **Start** icon from the Windows task bar.
2. Select the **Programs** menu item.
3. Select the **Unicon CL Series Software** menu item.



4. Select the **Unicon CL Series Software** icon.



Note: *The Unicon CL Series Software Reference Manual is also available in PDF format from the Unicon CL Series Software Menu for printing or for online assistance.*

Default Lock Selection Setting

The Unicon CL Series Software allows programming and reporting for both Model CL10 and Model CL20 locks. If this is the first time that you (as a unique user with a unique user profile) have loaded the software, you will be prompted to select the default lock model for your Unicon CL software activity. This setting determines whether the CL10 or the CL20 lock interface for the software will be presented when you start the program. This default setting will be associated with your User profile as it is known to the Windows operating system. This setting will determine the lock interface that is presented when the software is loaded.



5. Select your personal default lock setting for the Unicon CL Series software and click on Save.

Note: *The default lock setting can be changed at any time from the Settings Menu after the software is loaded.*

Distributed Transaction Coordinator Service

The Microsoft Distributed Transaction Coordinator (MSDTC) service needs to be running for Unicon CL Series Software database operations. On program startup, the Unicon CL Series Software checks to see if the Distributed Transaction Coordinator service is running. If it is not running, the following message is displayed to give the user the option to start the service.

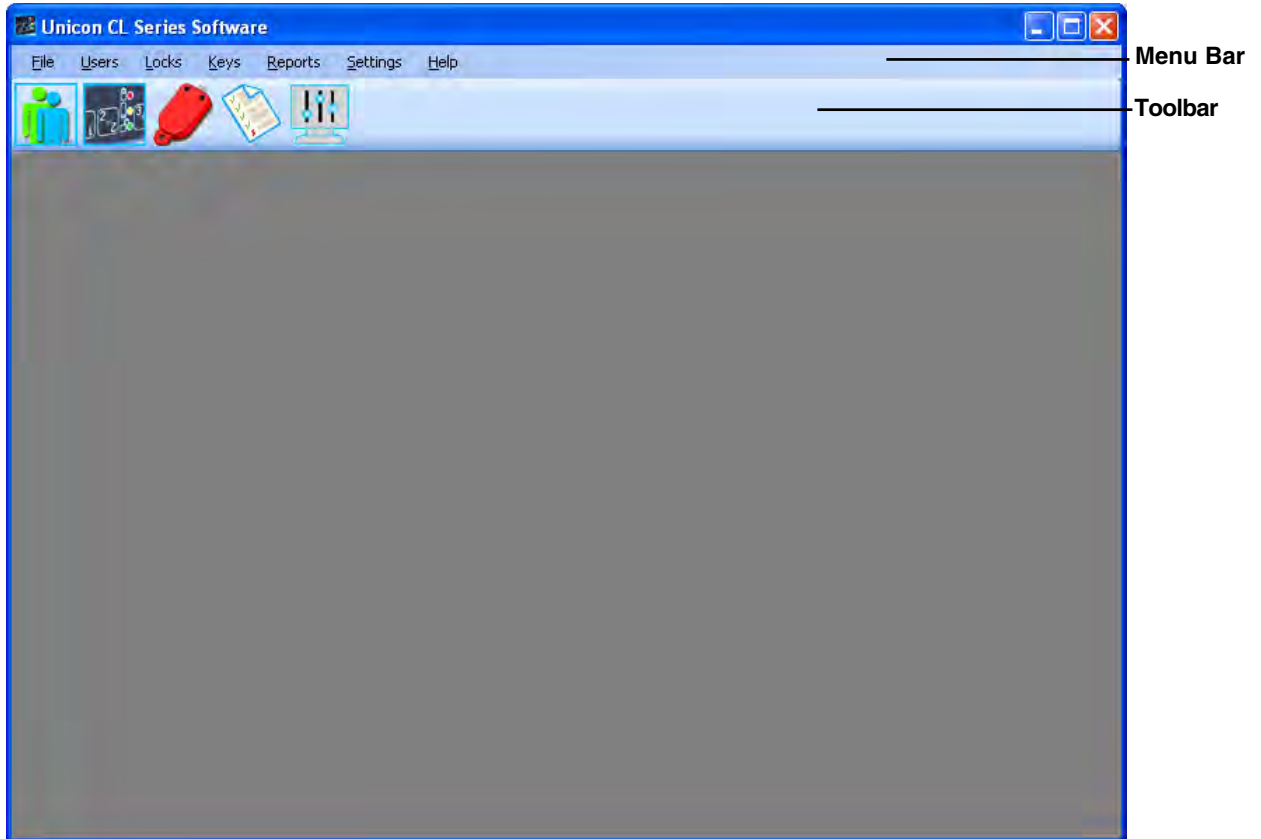


6. Click on **OK** to start the Distributed Transaction Coordinator and continue loading the Unicon CL Series Software.

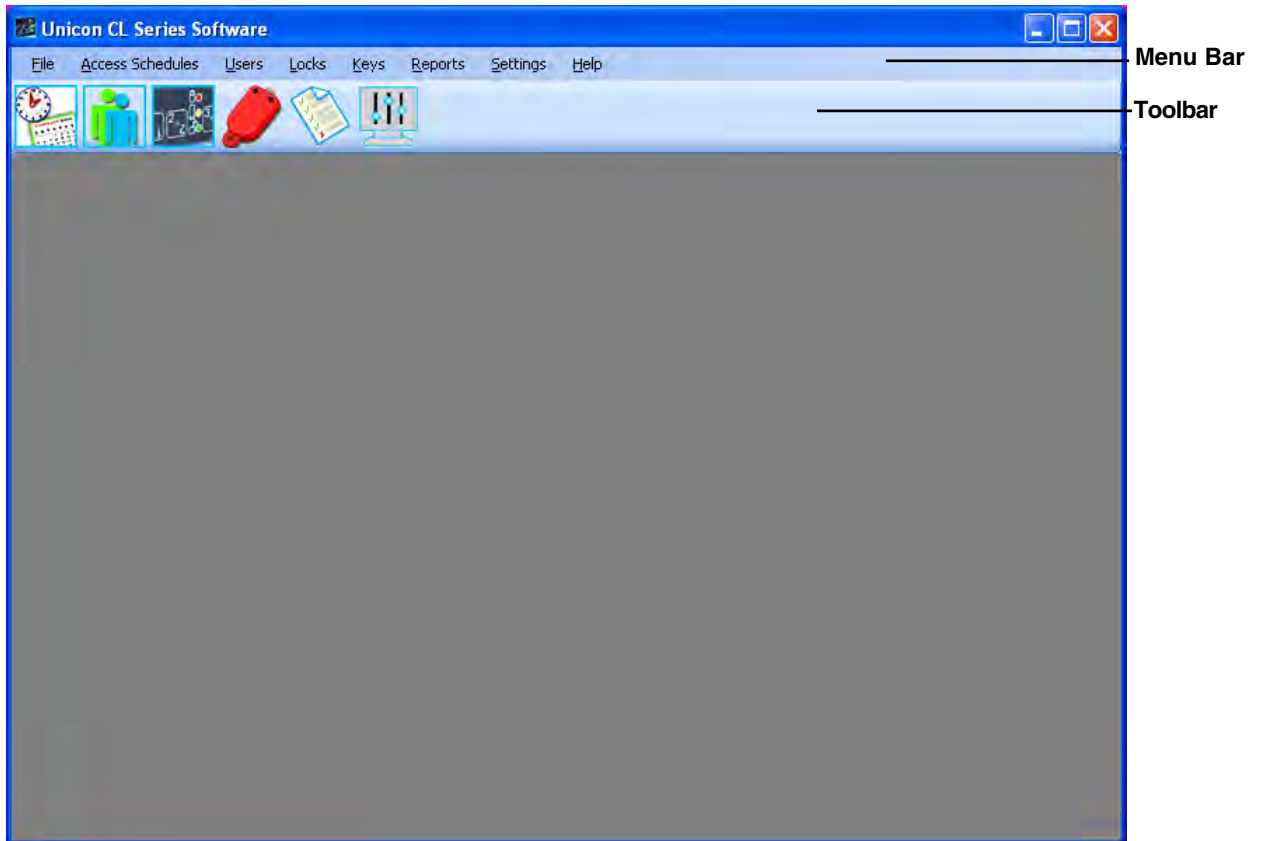
Unicon CL Main Menu

The Unicon CL Main Menu that is displayed at program startup will vary depending on whether you chose the Model CL10 lock as your Default Lock Interface selection or the Model CL20.

For Default Lock Interface selection of the Model CL10, the following screen is displayed.



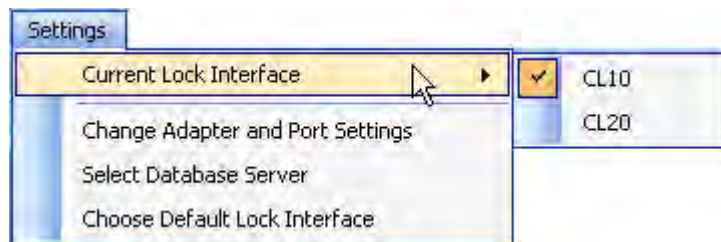
For Default Lock Interface selection of the Model CL20, the following screen is displayed.



Current Lock Interface

The Current Lock Interface setting indicates whether the CL10 or the CL20 lock interface for the software is currently presented. At program startup this setting defaults to the Default Lock Interface setting as defined in the user profile for the user who is logged on to the PC.

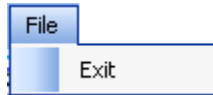
The current lock interface can easily be toggled at anytime during operation of the software for customer applications where both types of locks are installed. This option is available from the Settings Menu.



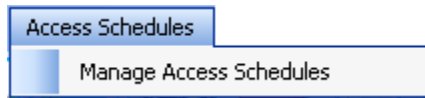
Menu Bar Options

The Menu Bar displays the available menu options for the Current Lock Interface. Some of these options are also available from the toolbar. The menu options available from the Unicon CL Series Software are listed below and the corresponding toolbar icon (if applicable) can be found in the following Toolbar section. Remember that the available menu bar options vary depending on the lock interface that is selected.

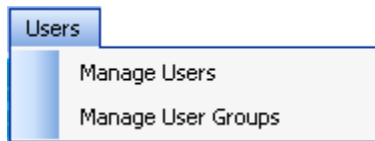
File - Exit the Unicon CL Series Software.



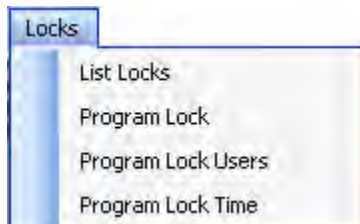
Access Schedules - Manage Access Schedules (CL20 Only)



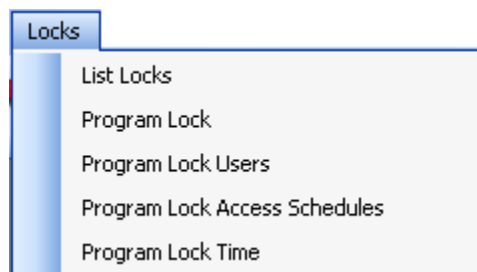
Users - Manage Users or User Groups



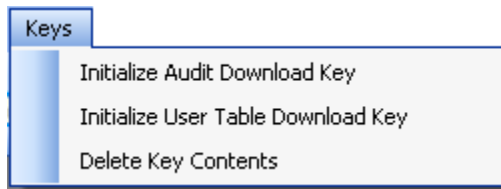
Locks CL10 Interface - List Locks or Program Lock Information



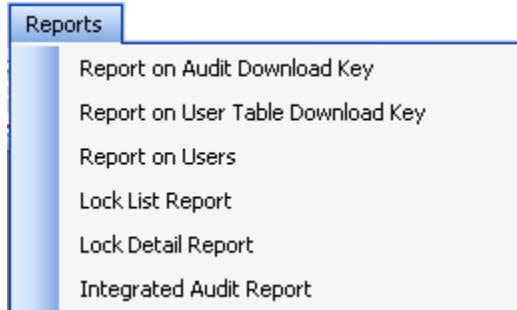
Locks CL20 Interface - List Locks or Program Lock Information



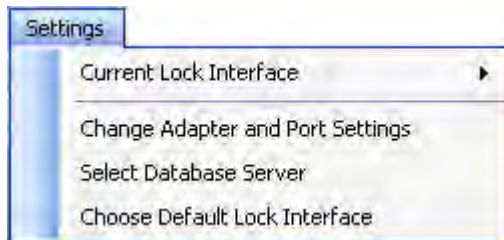
Keys - Initialize or Delete Reporting Keys



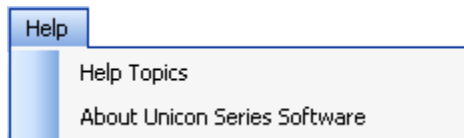
Reports - View or Print Reports



Settings - Define or Maintain System Settings & Data



Help - 1) Display the Unicon CL Series Software basic program information, version number and copyright or 2) access the online system help information.



You can select an option on the menu bar by 1) positioning the mouse pointer on the option name and clicking the left mouse button one time, 2) using the shortcut keys underlined on the option's label. For example, for the option label Locks, you can select the option by pressing the **Alt** and **L** keys at the same time (Alt + L).

Note: *Online help is also available by pressing the F1 function key at any time. This method of accessing online help will take you directly to the help for the particular screen or area of the software you are accessing.*

Toolbar Options

The Toolbar is located directly below the menu bar and displays the icons for the menu bar options. You can select an icon on the toolbar by positioning the mouse pointer on the icon and clicking the left mouse button one time. The toolbar icons available from the Unicon CL Series Software are pictured and described below. Remember that the available toolbar options vary depending on the lock interface that is selected.



Access Schedules - Manage Access Schedules **(CL20 Only)**



Users - Manage Users or User Groups



Locks - List Locks or Program Lock Information



Keys - Initialize or Delete Reporting Keys

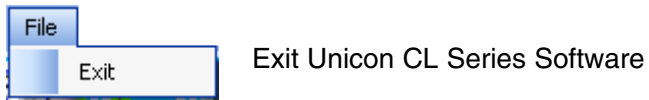


Reports - View or Print Reports



Settings - Define or Maintain System Settings & Data

File Menu



The File menu option allows you to exit the software. From the Main menu:

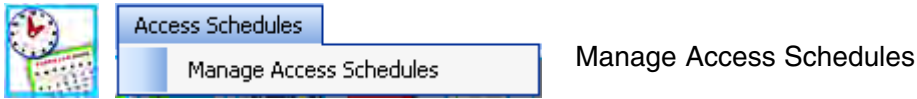
1. Select **File**.

Exit

The Exit option is used to end the Unicon CL Series program.

Access Schedules Menu*

* Available for CL20 only.



The Access Schedules Menu options (available only for the CL20 interface) allow you to define and manage access schedule templates that can be assigned to the locks. The Access Schedules menu options can also be accessed by selecting the Access Schedules icon from the Toolbar.

From the Main menu:

1. Select the **Access Schedules Menu**.

Manage Access Schedules

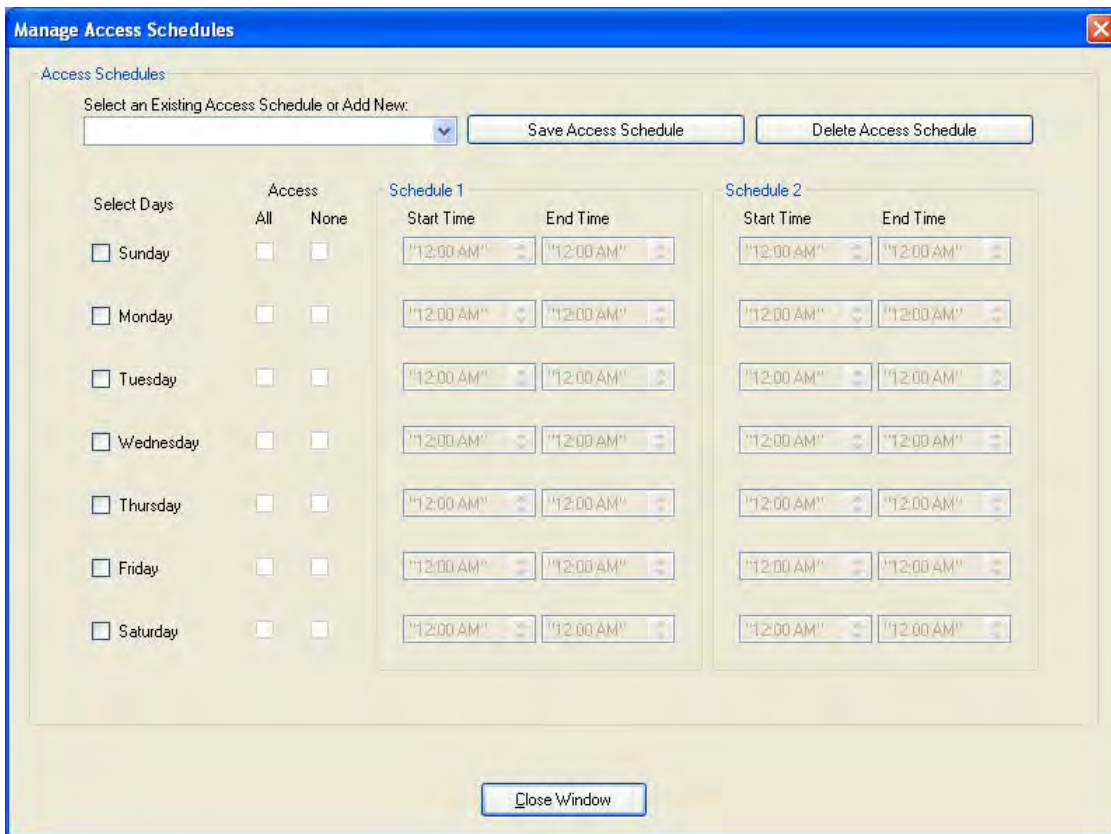
The only option available from the Access Schedules menu is “Manage Access Schedules”. This menu item is used to define and maintain access schedules in the system. It should be selected to add access schedules to the system database, modify access schedules or delete access schedules.

1. Select **Manage Access Schedules** from the Access Schedules Menu or select the



toolbar icon.

The “Manage Access Schedules” screen is displayed.



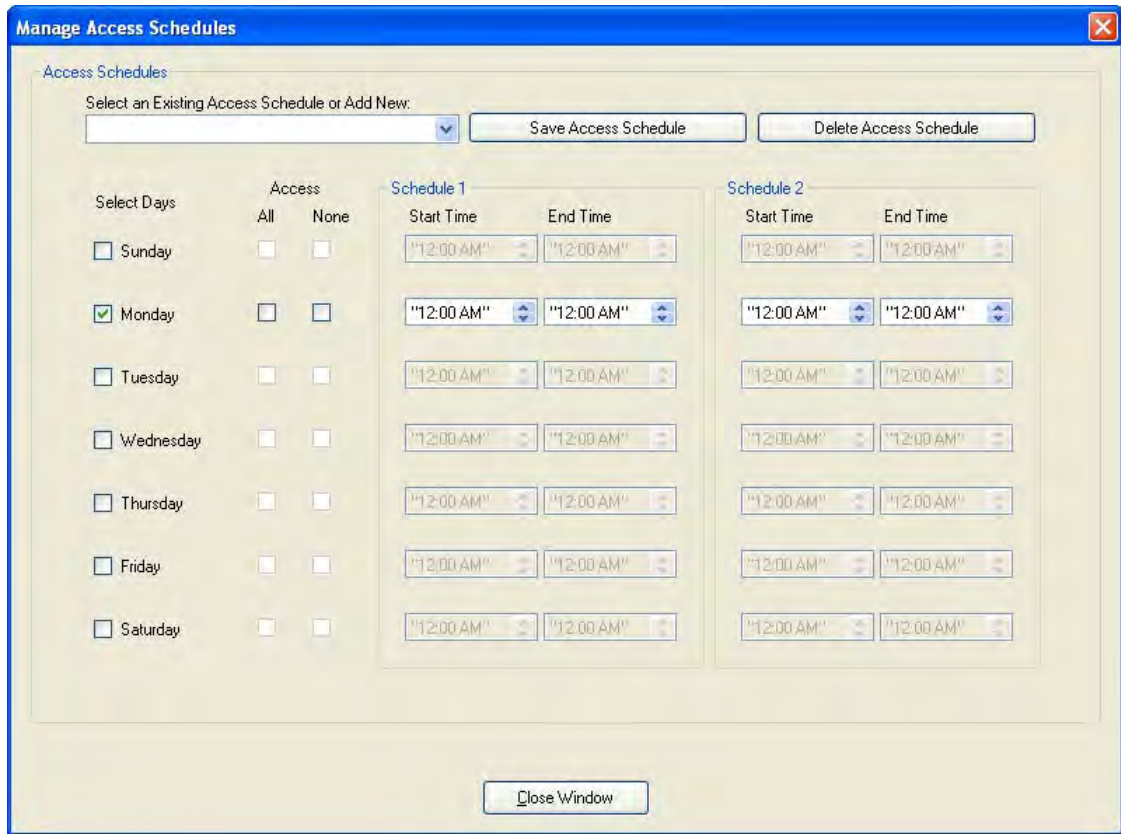
Create A New Access Schedule

To create a new access schedule, you must decide which days and what hours of the week access will be allowed. Then you can proceed to define the access schedule in the system. Once defined, you will save it under an assigned name that can be retrieved when programming user access for a lock.

1. To change the access schedule settings for a given day, click on the Select Days box for that day. If the box is not checked, the lock window settings will not be affected for that day and will remain set to the default values.

Note: *The access schedule settings will default to “all access” at the lock unless defined otherwise via manual programming at the lock or via data upload to the lock from the software.*

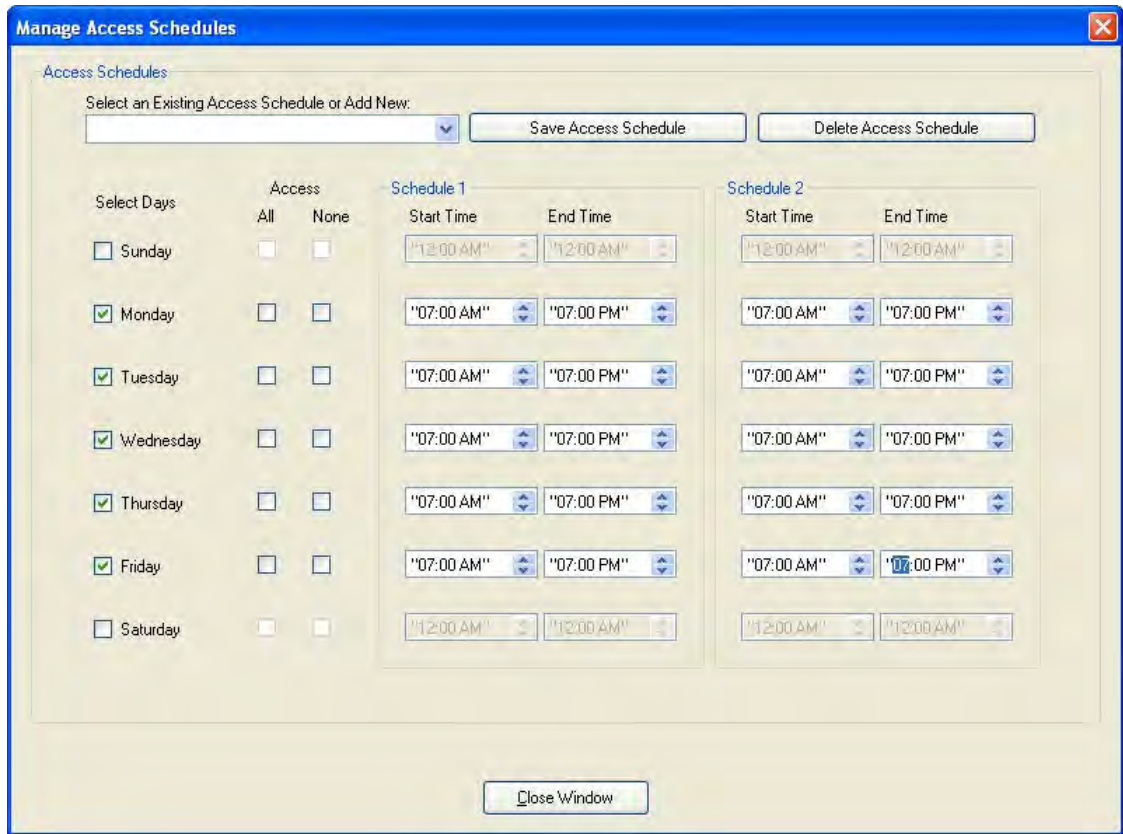
Once the Select Days box has been selected for a specific day, the other input fields for that day will become enabled for data entry.



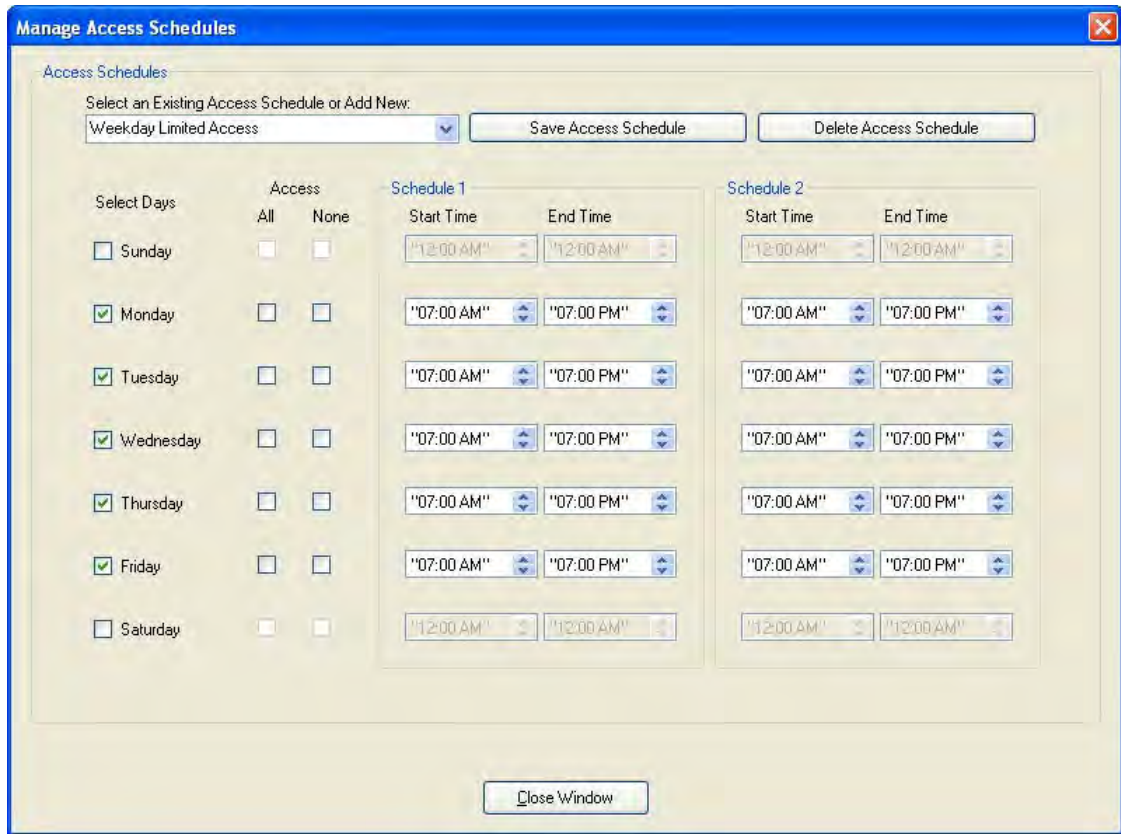
- 2a. If you want No Access Restriction (24 hour access) for the selected day, select the appropriate box for “All Access”. All other input fields will become unavailable for that day.
- 2b. If you want no lock access allowed for the selected day, select the “None” box. All other input fields will become unavailable for that day.
- 2c. If you want to limit access to a certain time period of the selected day, define an access time window by entering a Start Time and End Time under the Schedule 1 section of the screen. Specify all times in HH:MM format. Enter times as they would be set at the lock.

Note: *When data is entered for Schedule 1, the same Start and End Time will automatically be filled in for Schedule 2 once you click into the second window.*

3. Tab to the Start Time in Schedule 2. If you want to define a second access time window for the selected day, update the Start Time and End Time under the Schedule 2 section of the screen to the values for the second window.
4. Continue repeating Steps 1-3 for each day that you want to change from the default access.

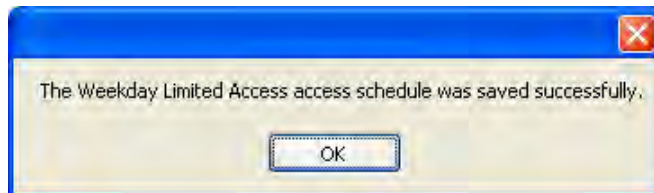


5. Click on the field to “Select an Existing Access Schedule or Add New” and enter the name of the access schedule.



6. Click on the **Save Access Schedule** tab to save the access schedule template to a file.

A message window is displayed indicating that the access schedule was saved successfully.



7. Click on **OK** to continue.

Modify Access Schedule

Once an access schedule template has been created, you have the option to modify it by changing the access restrictions.

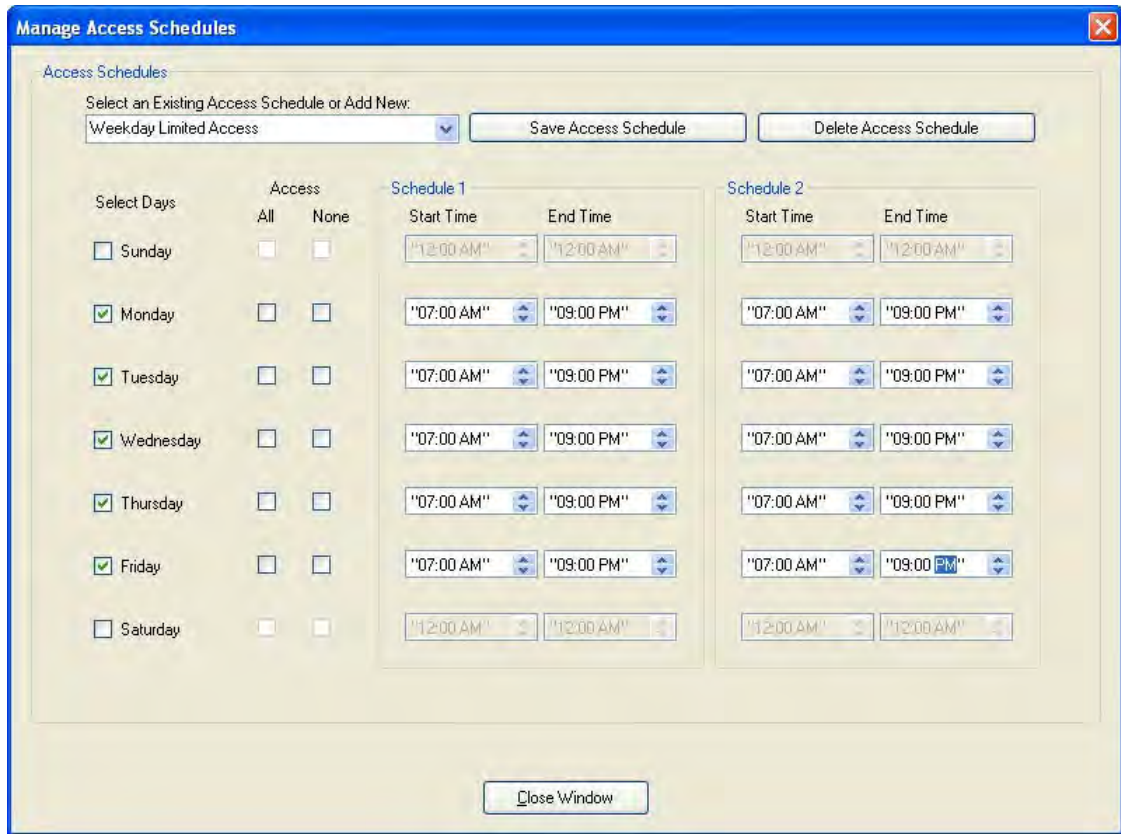
1. Click on the field to “Select an Existing Access Schedule or Add New” and enter or select the name of the access schedule to be updated.

The available access times will be displayed for the access schedule template.

The screenshot shows a software window titled "Manage Access Schedules". At the top, there is a dropdown menu set to "Weekday Limited Access", a "Save Access Schedule" button, and a "Delete Access Schedule" button. Below this, the interface is divided into sections for "Select Days" and "Access" (All/None). The "Select Days" section has checkboxes for Sunday through Saturday, with Sunday through Friday checked. The "Access" section has checkboxes for "All" and "None" for each day. To the right, there are two columns for "Schedule 1" and "Schedule 2", each with "Start Time" and "End Time" dropdown menus. For Schedule 1, the start time is "07:00 AM" and the end time is "07:00 PM" for all days. For Schedule 2, the start time is "07:00 AM" and the end time is "07:00 PM" for Sunday through Friday, and "12:00 AM" for Saturday. A "Close Window" button is located at the bottom center.

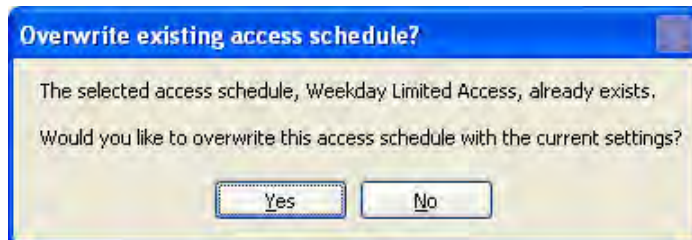
Select Days	Access		Schedule 1		Schedule 2	
	All	None	Start Time	End Time	Start Time	End Time
<input checked="" type="checkbox"/> Sunday	<input type="checkbox"/>	<input type="checkbox"/>	"07:00 AM"	"07:00 PM"	"07:00 AM"	"07:00 PM"
<input checked="" type="checkbox"/> Monday	<input type="checkbox"/>	<input type="checkbox"/>	"07:00 AM"	"07:00 PM"	"07:00 AM"	"07:00 PM"
<input checked="" type="checkbox"/> Tuesday	<input type="checkbox"/>	<input type="checkbox"/>	"07:00 AM"	"07:00 PM"	"07:00 AM"	"07:00 PM"
<input checked="" type="checkbox"/> Wednesday	<input type="checkbox"/>	<input type="checkbox"/>	"07:00 AM"	"07:00 PM"	"07:00 AM"	"07:00 PM"
<input checked="" type="checkbox"/> Thursday	<input type="checkbox"/>	<input type="checkbox"/>	"07:00 AM"	"07:00 PM"	"07:00 AM"	"07:00 PM"
<input checked="" type="checkbox"/> Friday	<input type="checkbox"/>	<input type="checkbox"/>	"07:00 AM"	"07:00 PM"	"07:00 AM"	"07:00 PM"
<input type="checkbox"/> Saturday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"

2. Adjust available access times as necessary.



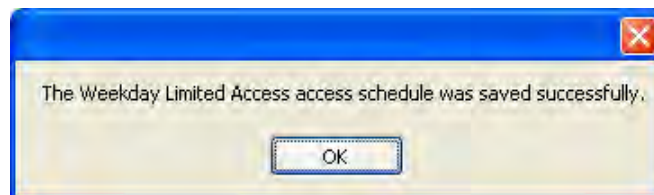
3. Once all changes have been made to the user group, click on the **Save Access Schedule** tab.

A prompt window is displayed asking for confirmation to overwrite the existing access schedule information with the modified information.



4. Click on **Yes** to save the changes for the selected access schedule.

A message window is displayed indicating that the changes to the access schedule template were changed successfully.



5. Click on **OK** to continue.

Delete Access Schedule

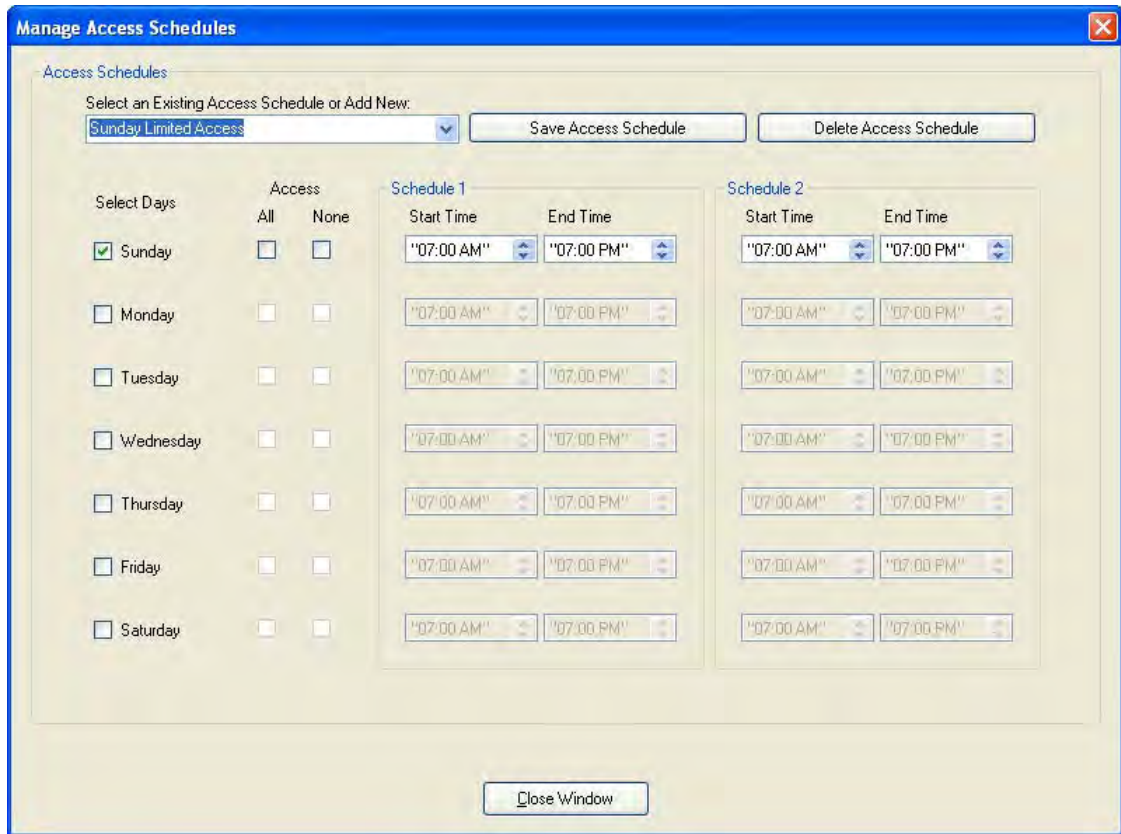
Another option on the Manage Access Schedules screen is “Delete Access Schedule”. This item is used to delete an access schedule template that no longer needs to be maintained in the system.

1. Click on the field to “Select an Existing Access Schedule or Add New” and enter or select the name of the access schedule to be deleted.

The screenshot shows the 'Manage Access Schedules' window. At the top, there is a dropdown menu labeled 'Select an Existing Access Schedule or Add New:' with a list of options: 'Sunday Limited Access', 'Weekday Limited Access', and 'Weekend Limited Access'. Below the dropdown are two buttons: 'Save Access Schedule' and 'Delete Access Schedule'. The main area contains a table for selecting days and setting start/end times for two schedules. The table has columns for 'All', 'None', 'Start Time', and 'End Time' for both 'Schedule 1' and 'Schedule 2'. The 'All' and 'None' columns have checkboxes. The 'Start Time' and 'End Time' columns have time selection boxes. A 'Close Window' button is located at the bottom center.

Select Days	All		None		Schedule 1		Schedule 2	
	Start Time	End Time	Start Time	End Time	Start Time	End Time	Start Time	End Time
<input type="checkbox"/> Sunday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"
<input type="checkbox"/> Monday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"
<input type="checkbox"/> Tuesday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"
<input type="checkbox"/> Wednesday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"
<input type="checkbox"/> Thursday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"
<input type="checkbox"/> Friday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"
<input type="checkbox"/> Saturday	<input type="checkbox"/>	<input type="checkbox"/>	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"	"12:00 AM"

The available access times will be displayed for the access schedule template.



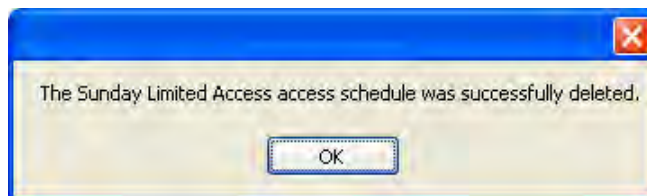
2. Click on the **Delete Access Schedule** tab.

A prompt window is displayed asking for confirmation to delete the access schedule.



3. Click on **Yes** to delete the selected access schedule.

A message window is displayed to indicate that the access schedule was deleted successfully.

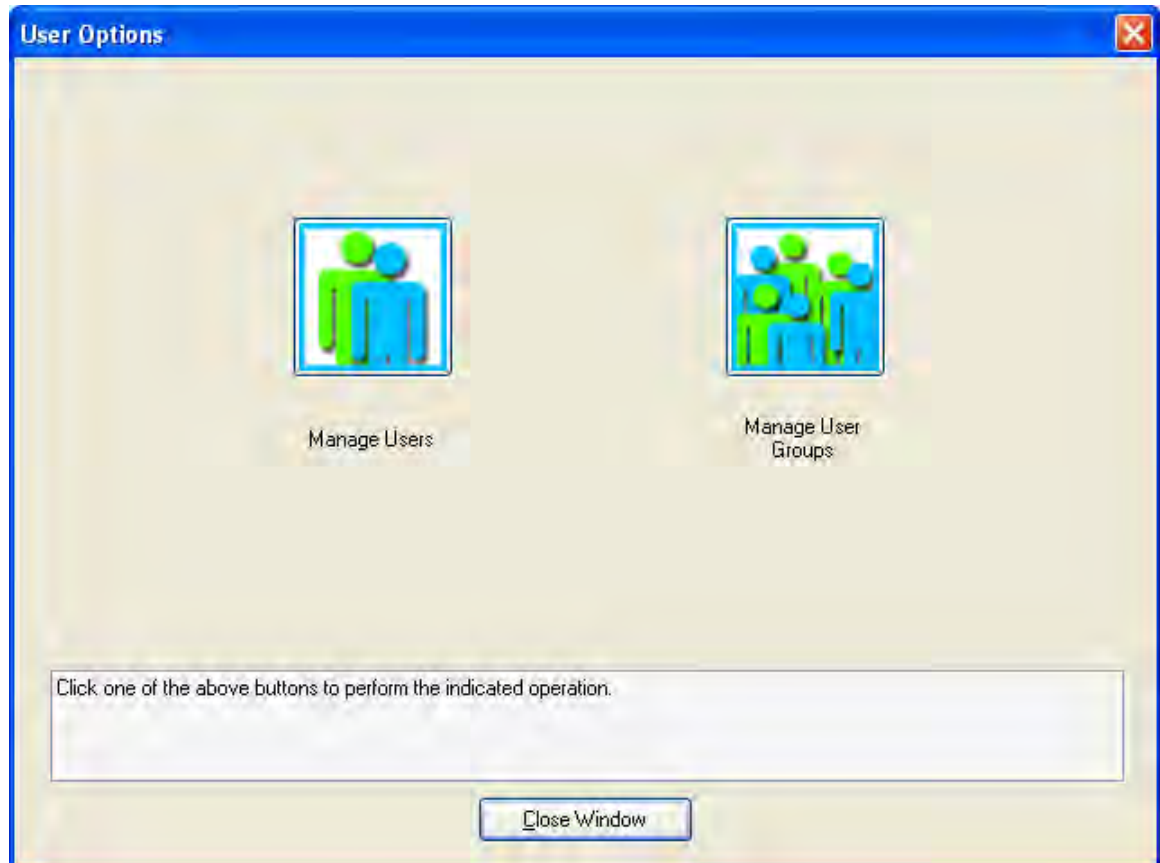


4. Click on **OK** to continue.


Users Menu



The Users Menu options allows you to define and maintain users in the Unicon system database along with managing groups of users. The Users menu options can also be accessed by selecting the Users icon from the Toolbar.




From the Main menu:

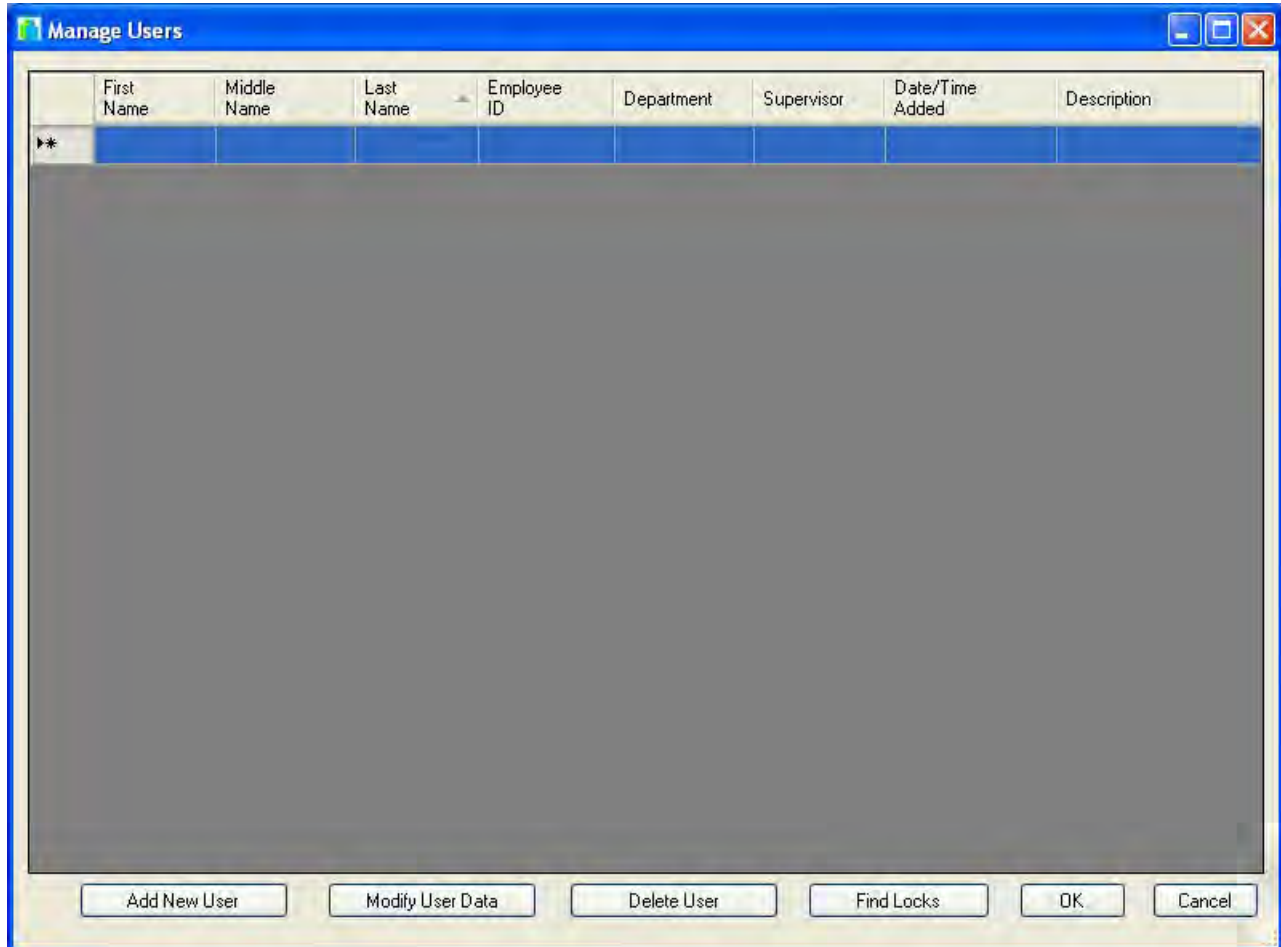
1. Select the **Users Menu** or the  toolbar icon.

Manage Users

The first option on the Users menu is “Manage Users”. This menu item is used to define and maintain users in the system. It should be selected to add users to the system database, modify user data or delete users.

1. Select **Manage Users** from the Users Menu or select the  icon from the User Options screen.

The Manage Users screen is displayed.



Add a New User

The first tab option on the Manage Users screen is “Add A New User”. This item is used to add new users to the system. Once added to the database, users can be assigned access to locks.

1. Click on **Add A New User**.

The Add New User to the Database screen is displayed.

Note: An asterisk (*) indicates a required field.

First Name: *

Middle Name:

Last Name: *

Employee ID: *

Description:

Department:

Supervisor:

* Required Fields

OK Cancel

2. Enter the First Name of the user.
3. Enter the Middle Name of the user. (Optional)
4. Enter the Last Name of the user.
5. Enter the user's Employee ID.
6. Enter a description of the user. (Optional)
7. Enter Department information for the user. (Optional)
8. Enter the name of the user's Supervisor. (Optional)

Add New User to the Database

First Name: *

Middle Name:

Last Name: *

Employee ID: *

Description:

Department:

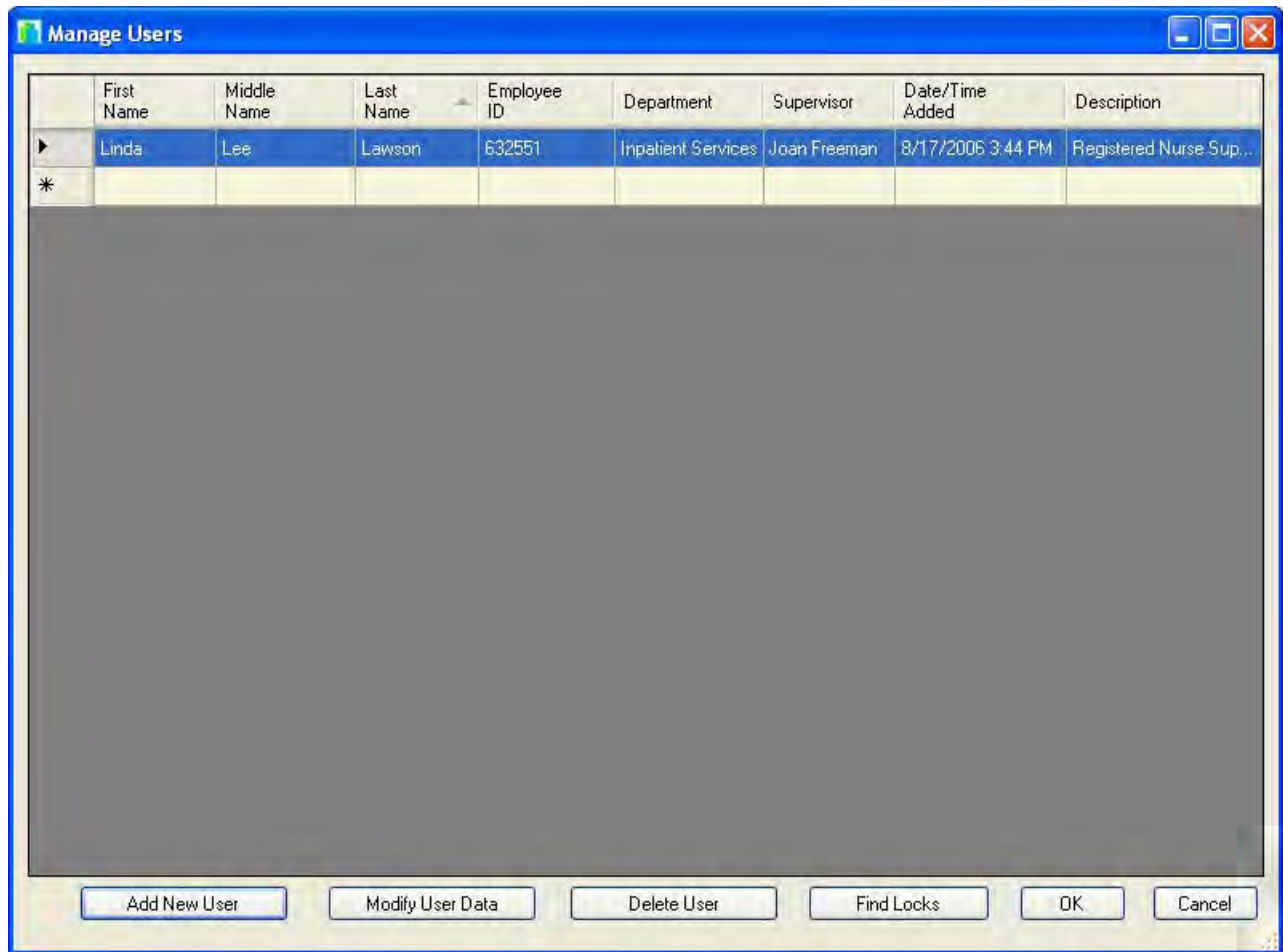
Supervisor:

* Required Fields

OK Cancel

9. Click on **OK** to accept and save the user information.

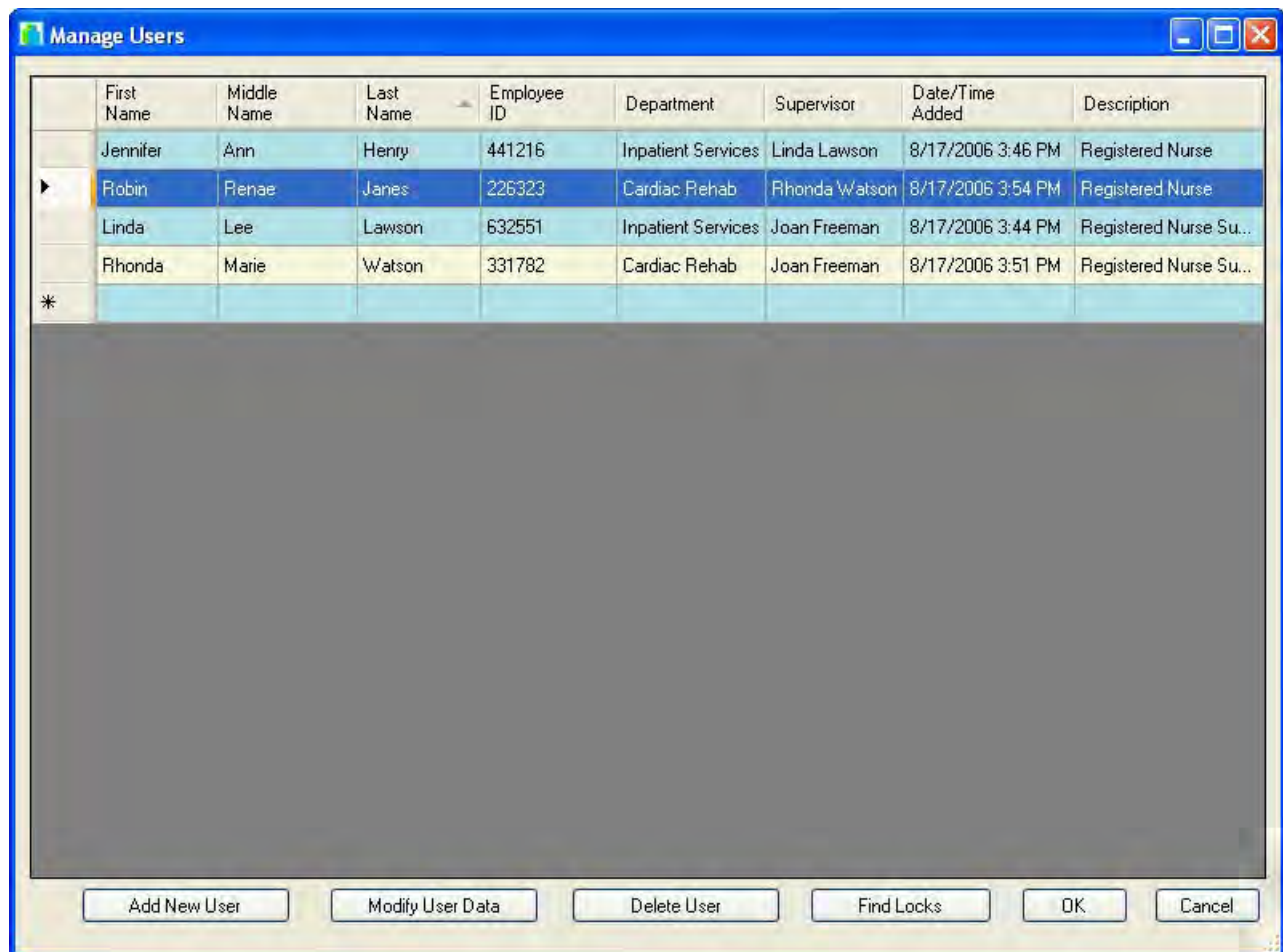
The new user will be reflected in the User List.



Modify User Data

The second tab option on the Manage Users screen is “Modify User Data”. This item is used to update information for existing users in the system.

1. Select the user from the list for whom information is to be modified.



2. Click on **Modify User Data**.

The Modify User Data to the Database screen is displayed.

Note: *An asterisk (*) indicates a required field.*

Modify User Data

First Name: Robin *

Middle Name: Renae

Last Name: Janes *

Employee ID: 226323 *

Description: Registered Nurse

Department: Cardiac Rehab

Supervisor: Rhonda Watson

* Required Fields

OK Cancel

3. Modify user information as necessary.

Modify User Data

First Name: Robin *

Middle Name: Rena

Last Name: Hayder *

Employee ID: 226323 *

Description: Registered Nurse

Department: Cardiac Rehab

Supervisor: Rhonda Watson

* Required Fields

OK Cancel

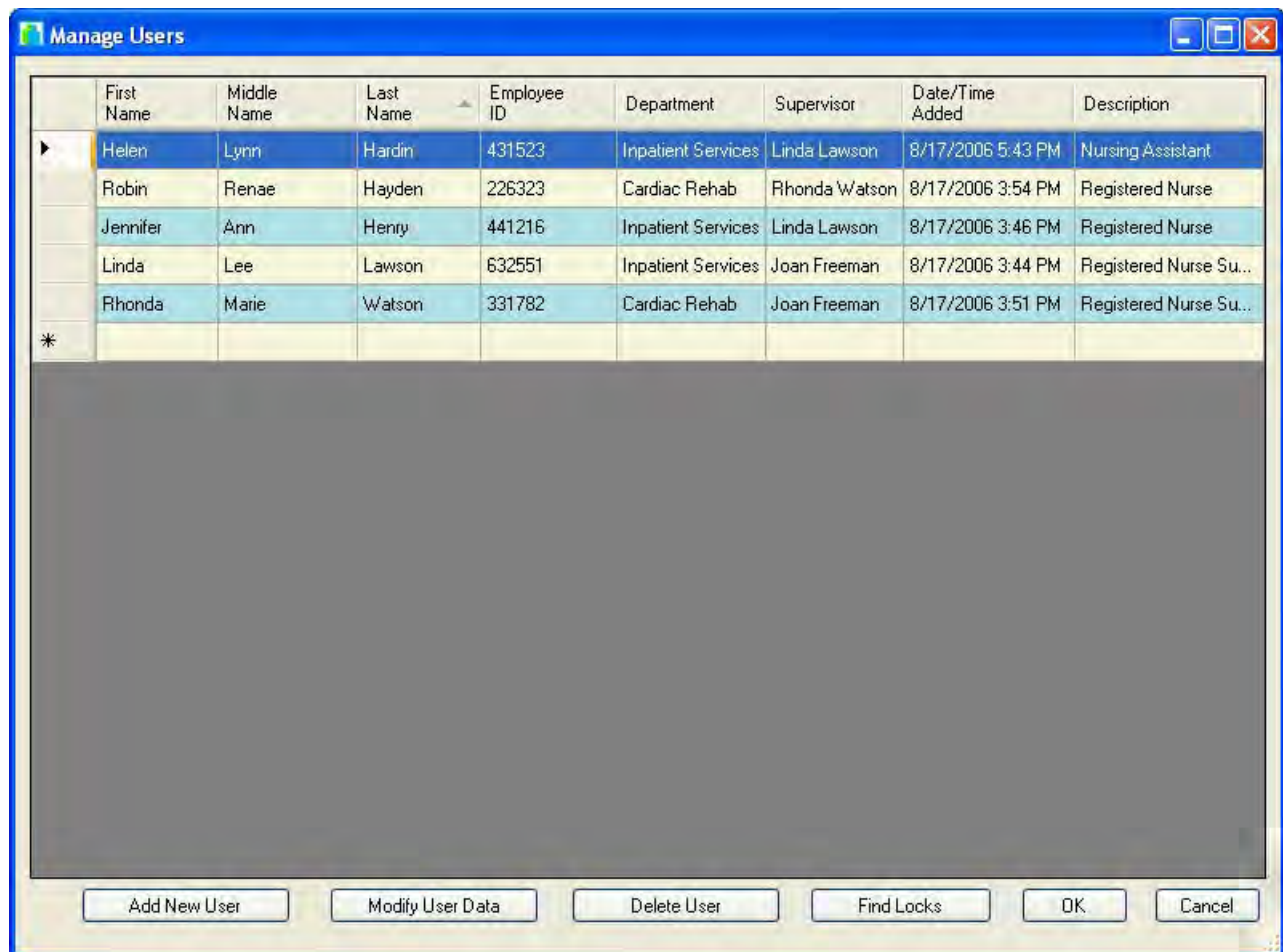
3. Click on **OK** to accept and save the user information.

The updated information will be reflected in the User List.

Delete User

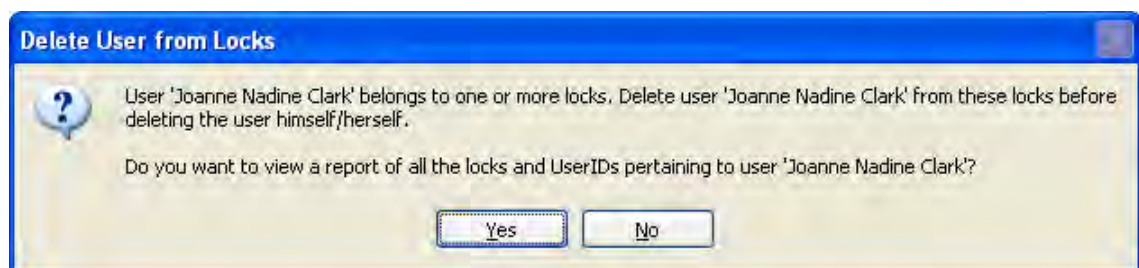
The third tab option on the Manage Users screen is “Delete User”. This item is used to delete a user who no longer needs to be maintained in the system.

1. Select the user who is to be deleted from the list.

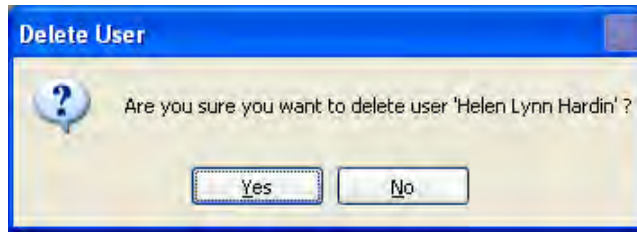


2. Click on **Delete User**.

If the user is currently attached to a one or more locks, a prompt window is displayed indicating that the user must be removed from all locks before being deleted. Click on **Yes** to display a report of all the lock and User IDs pertaining to the user. Otherwise, click on **No**.

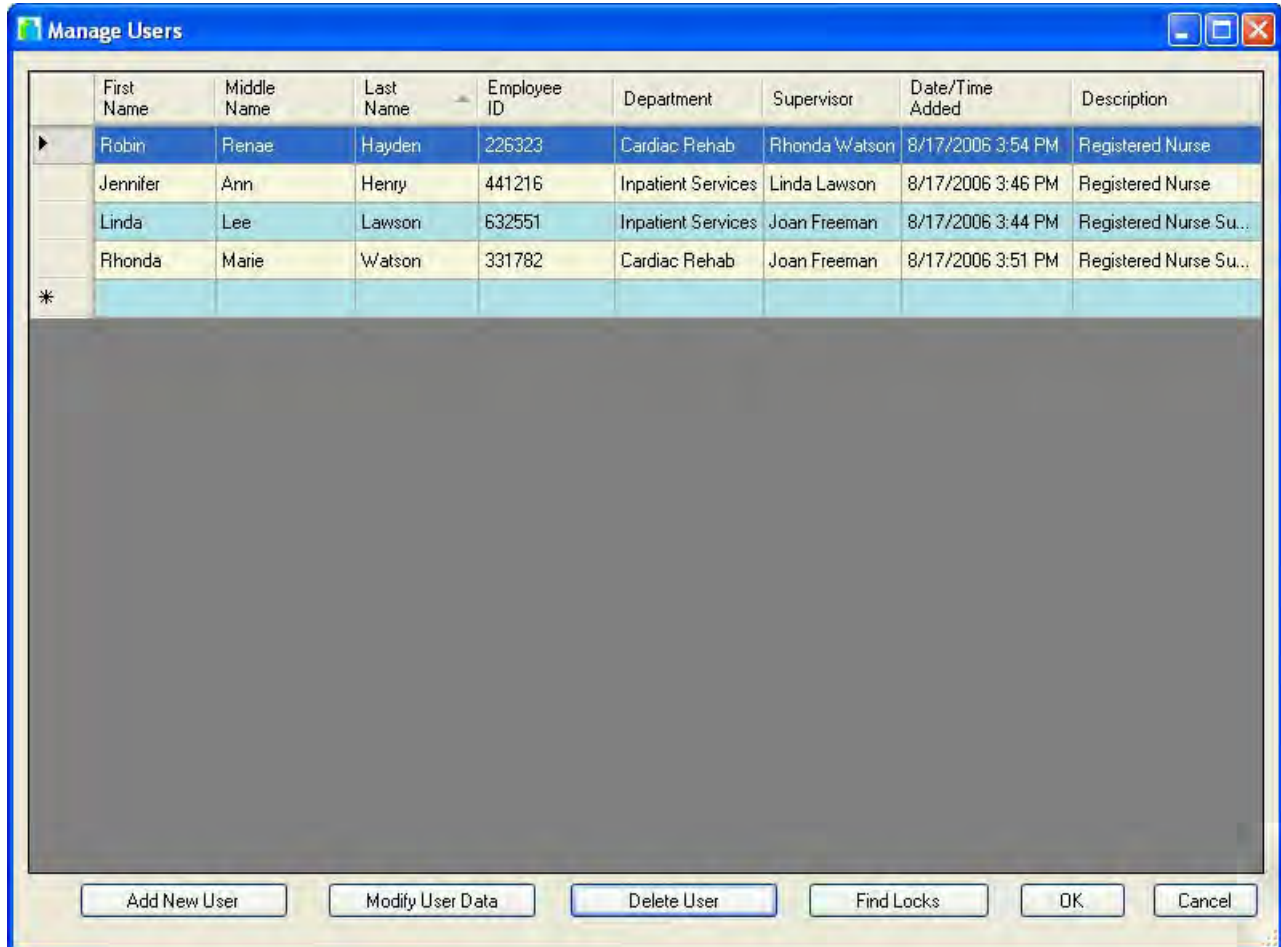


If the user is not currently attached to any lock, a prompt window is displayed asking for confirmation to delete the user.



3. Click on **Yes** to delete the selected user.

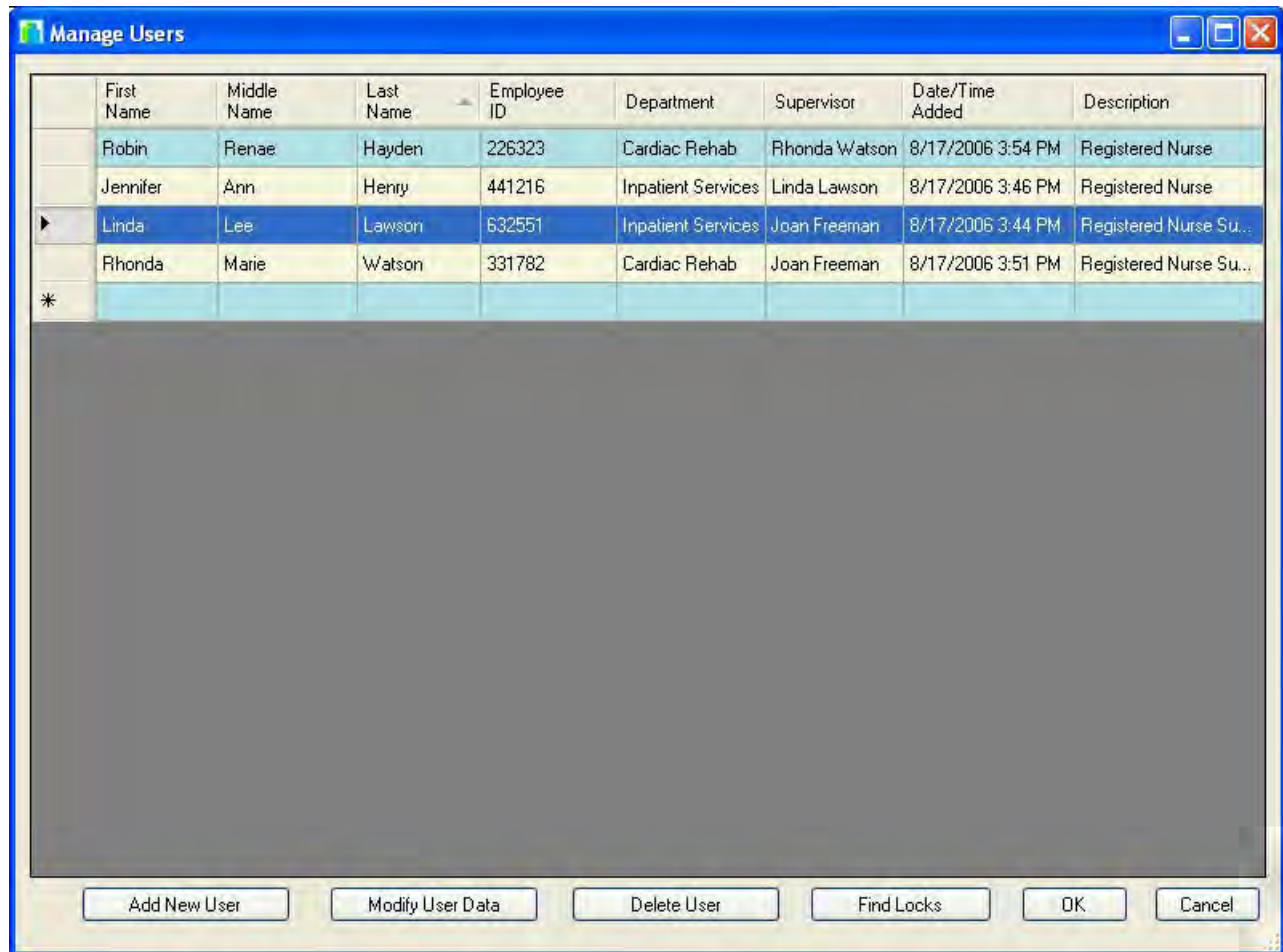
The user will be deleted from the User List.



Find Locks

The fourth tab option on the Manage Users screen is "Find Locks". This option allows you to identify all of the locks to which a particular user has been assigned access

1. Select the user from the list for whom you wish to identify assigned locks.



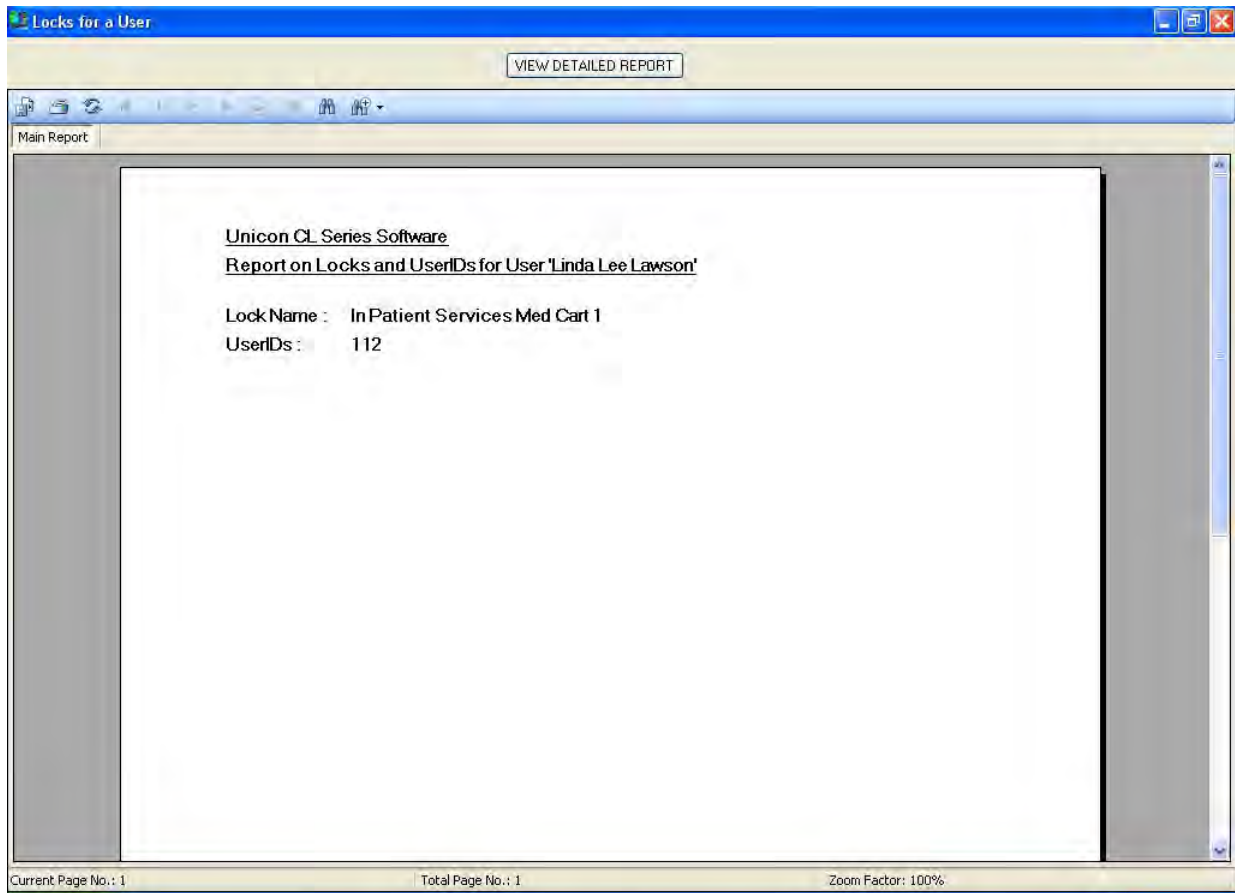
2. Click on **Find Locks**.

If the user has not been assigned access to any locks, the following message window will be displayed.



Click on **OK** to continue

If the user has been assigned access to locks, a list of those locks (a Crystal Report) will be generated and displayed.

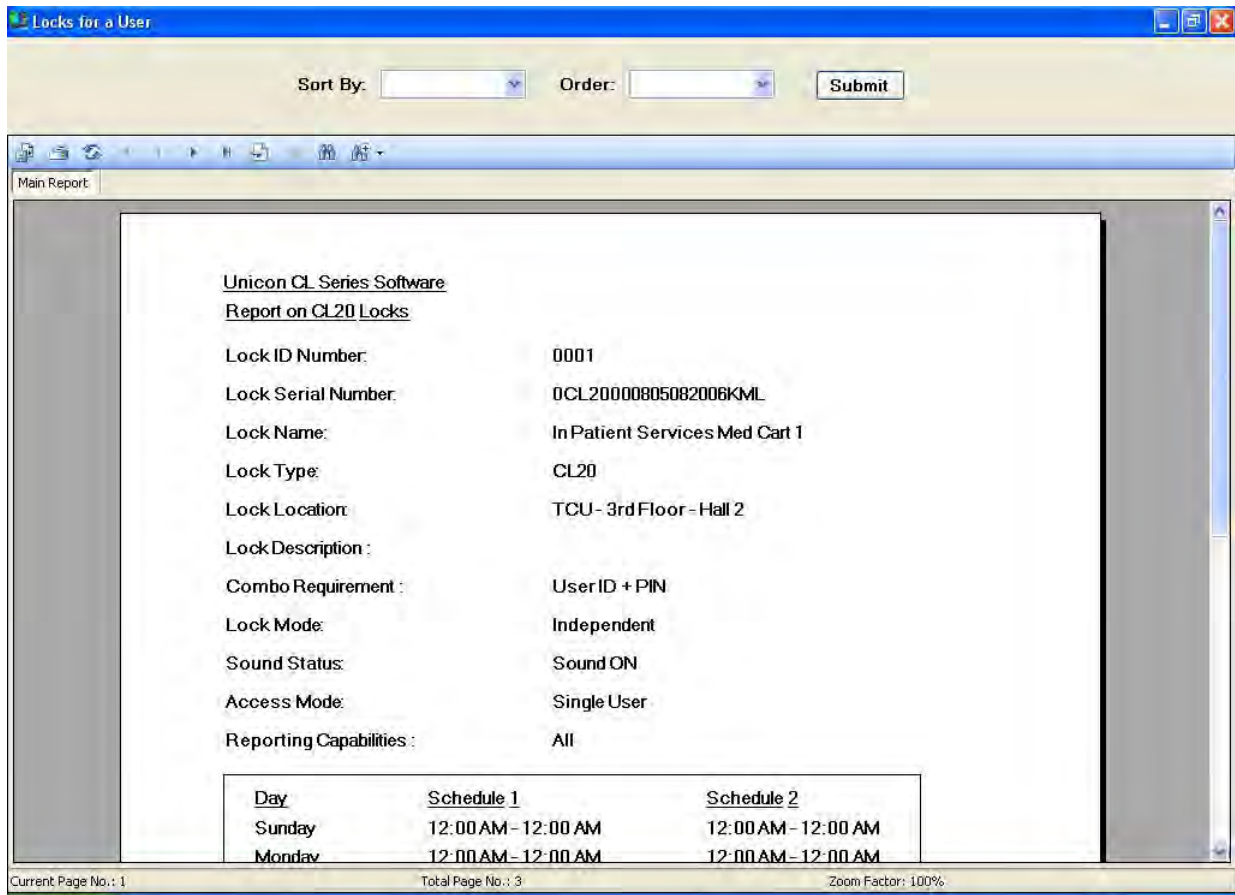


A list of the lock names and the User ID assigned to the user for that lock will be shown.

You may print the report by clicking on the **Print** button.



You also have the option of exporting the report data to a file on your disk drive. To export the report data to a file, click on the **Export** button. The Export Report window will be displayed. Enter the name of the file where you want the data stored, select the type of file, and click on the **Save** button to export it. The report data will be saved and the following confirmation screen will be displayed.

3. If you would like to view the detailed report, click on the **View Detailed Report** tab. The detailed report will be generated and will display detail lock information for each of the locks to which the user is assigned.



Once again as with the standard report, you have the option to print the report or export it to a file.


Additionally on the detailed report, you have the option to sort the data differently than what is shown in the default sort. Select the field by which you would like to sort the data and then select the order of the sort (ascending or descending).

4. Click on the red X Close button  in the upper right hand corner to close the detail report window.
5. Click on the red X Close button  in the upper right hand corner to close the standard report window.

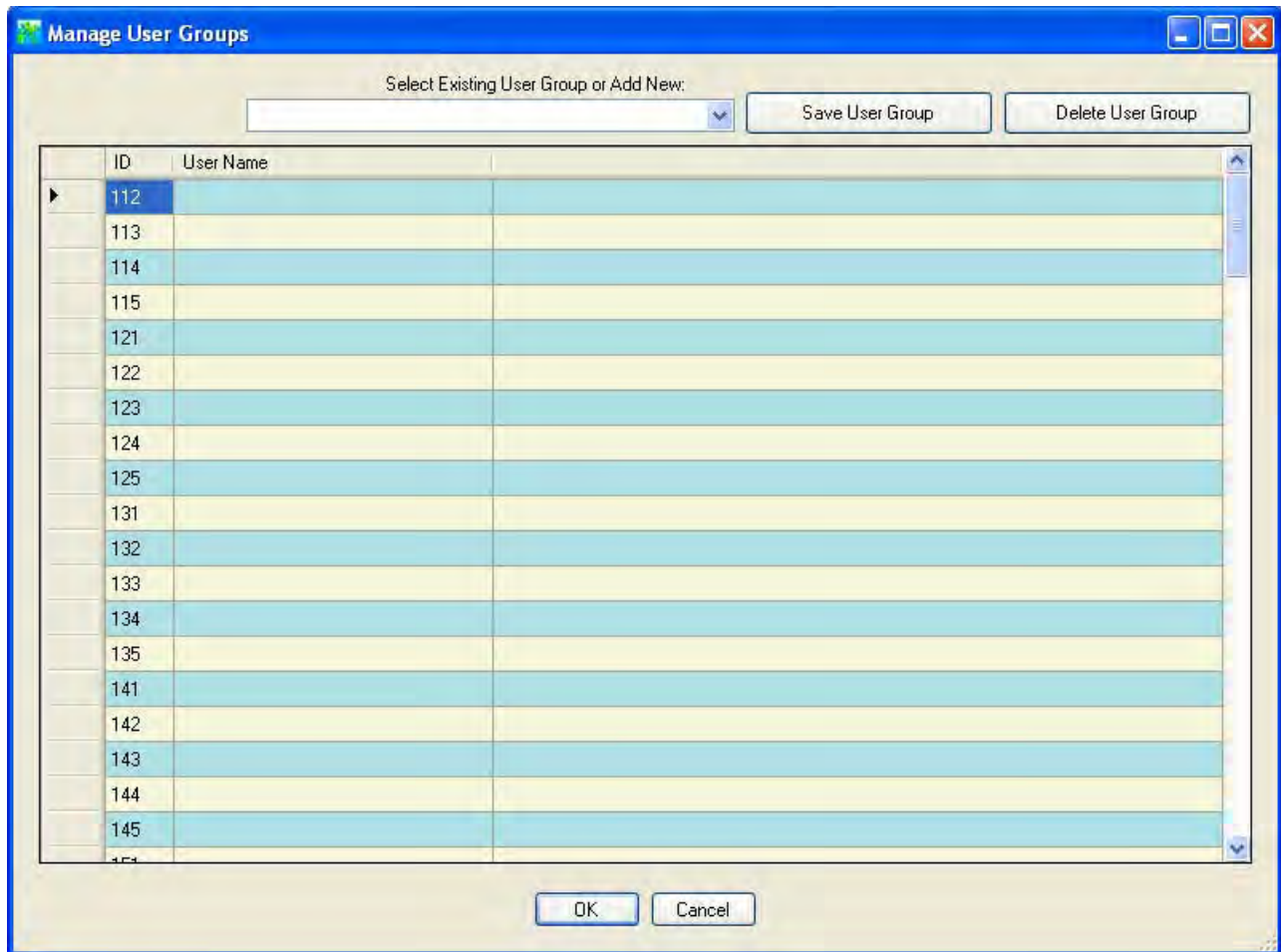
Manage User Groups

The second option on the Users menu is “Manage User Groups”. This menu item is used to define and maintain groups of users in the system. Once defined, an entire user group can be given access to a particular lock without having to identify each of the individual users when programming the lock.

Note: *It is highly recommended to use this software feature, especially when you will be assigning the same users to multiple locks. This feature is also very useful in situations of lock recovery or replacement.*

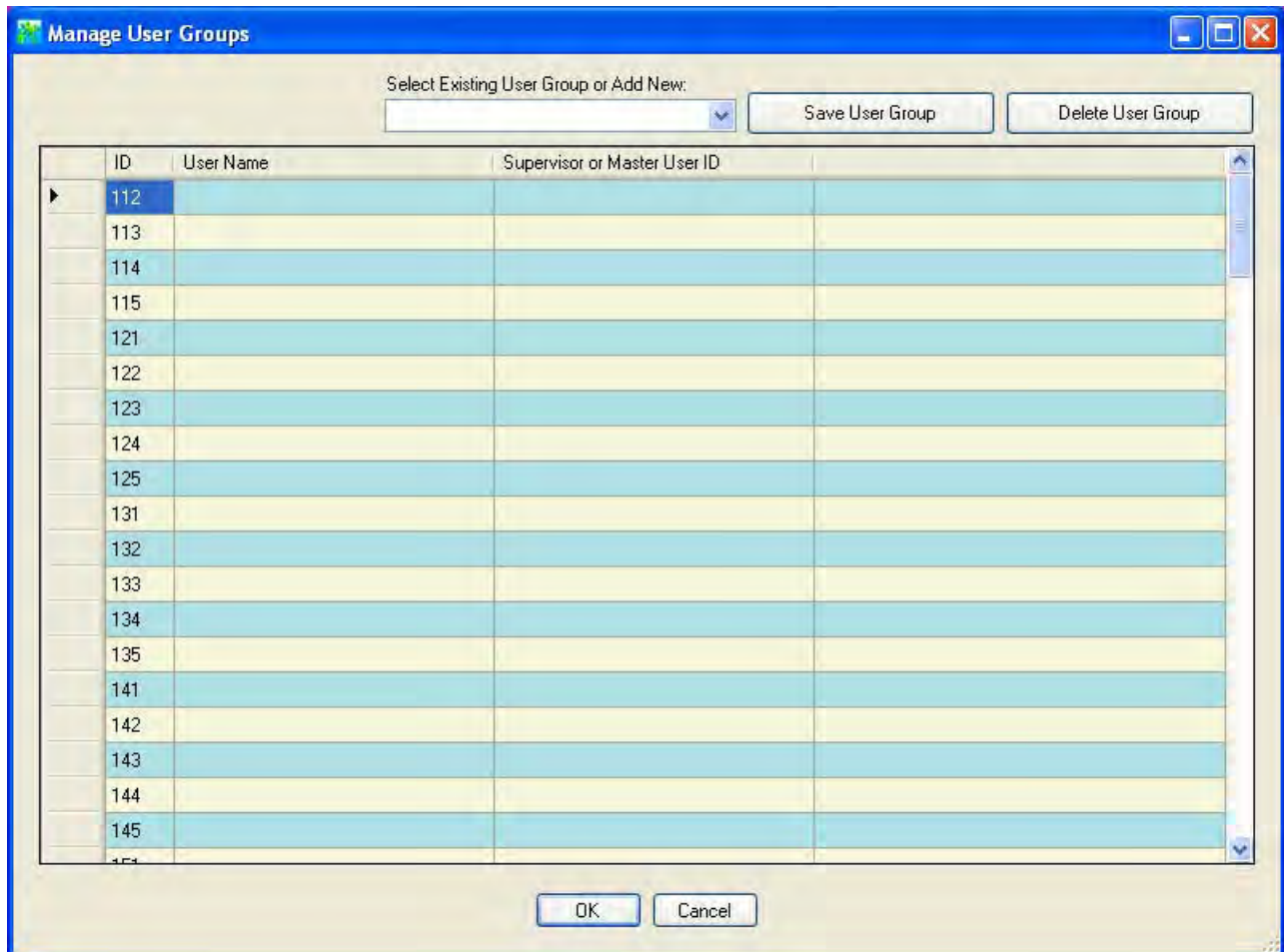
1. Select the **Manage User Groups** icon  from the User Options screen.

If the Current Lock Interface setting is CL10, the following Manage User Groups screen is displayed.



ID	User Name
112	
113	
114	
115	
121	
122	
123	
124	
125	
131	
132	
133	
134	
135	
141	
142	
143	
144	
145	

If the **Current Lock Interface setting is CL20**, the following Manage User Groups screen is displayed.



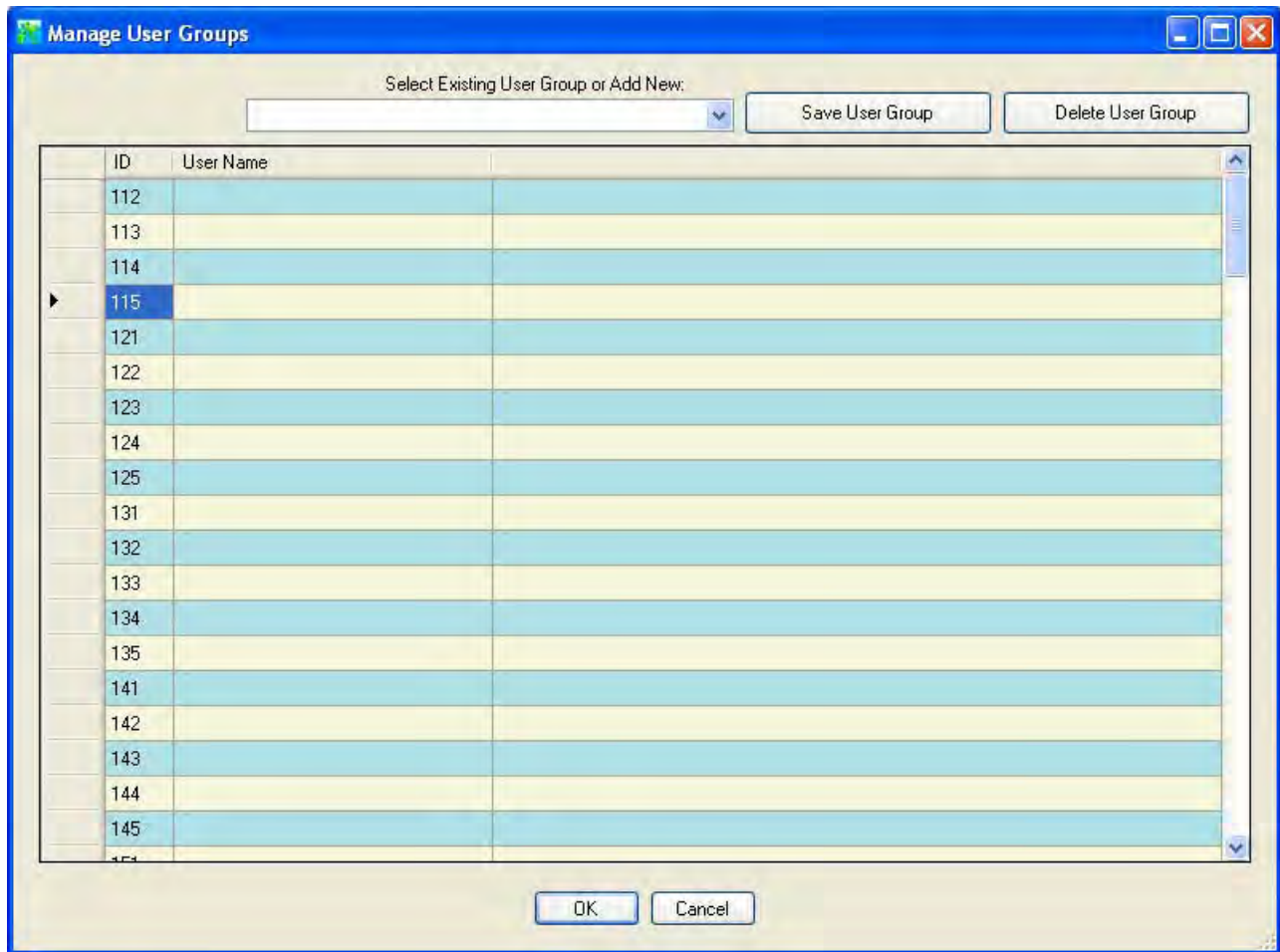
Manage User Groups - CL10 Interface

The options available from the Manage User Groups CL10 interface allow you to create new user groups or to modify or delete existing user groups.

Create A New User Group

To create a new user group, you must decide which users will belong to the group and you must identify the user ID assignment for each member of the group. Then you can proceed to define the user group in the system. Once defined, you will save it under an assigned name that can be retrieved when programming user access for a lock.

1. Select the User ID to which you want to assign a user.

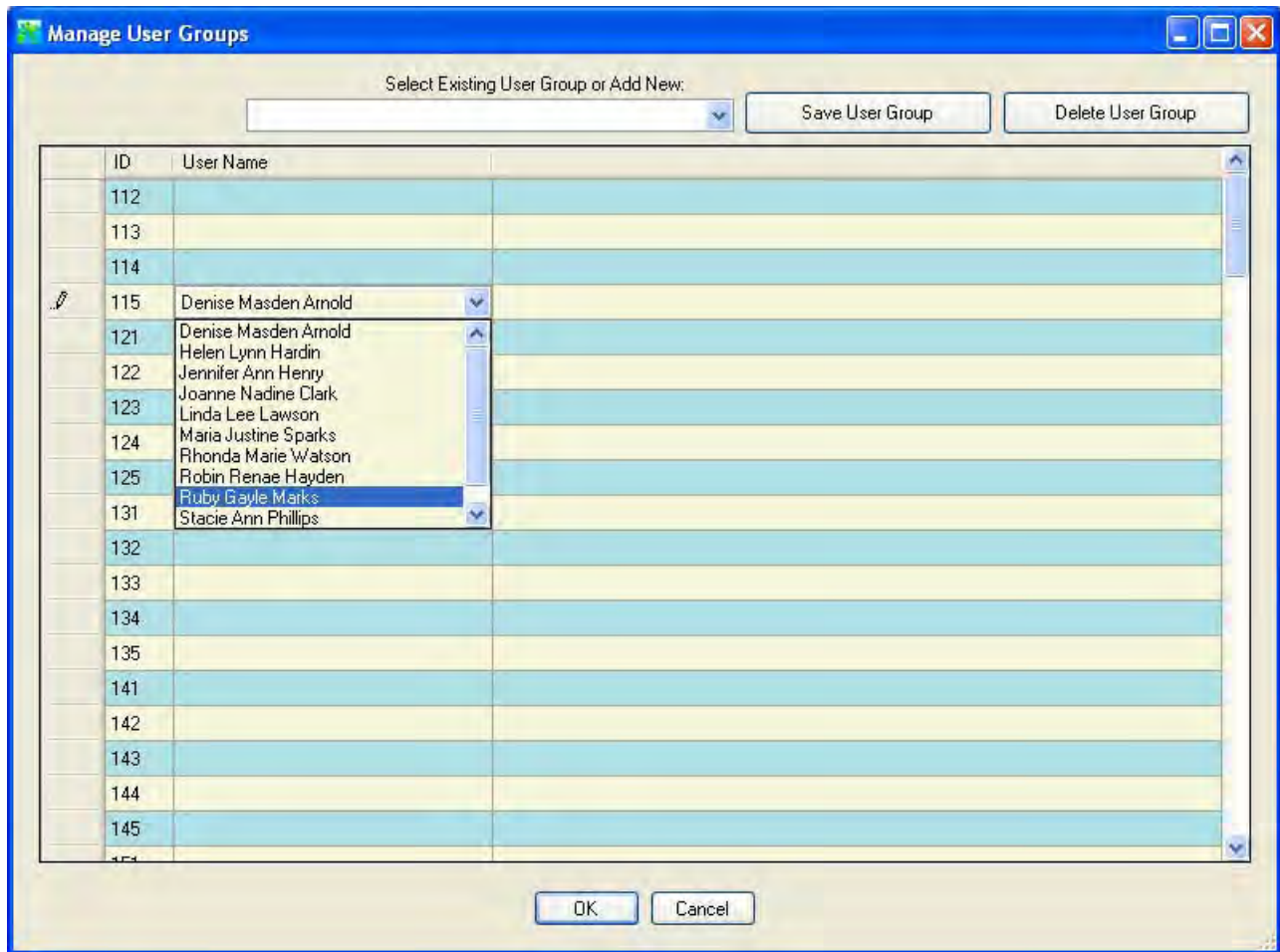


2. Click on the User Name field in the same line as the selected User ID.

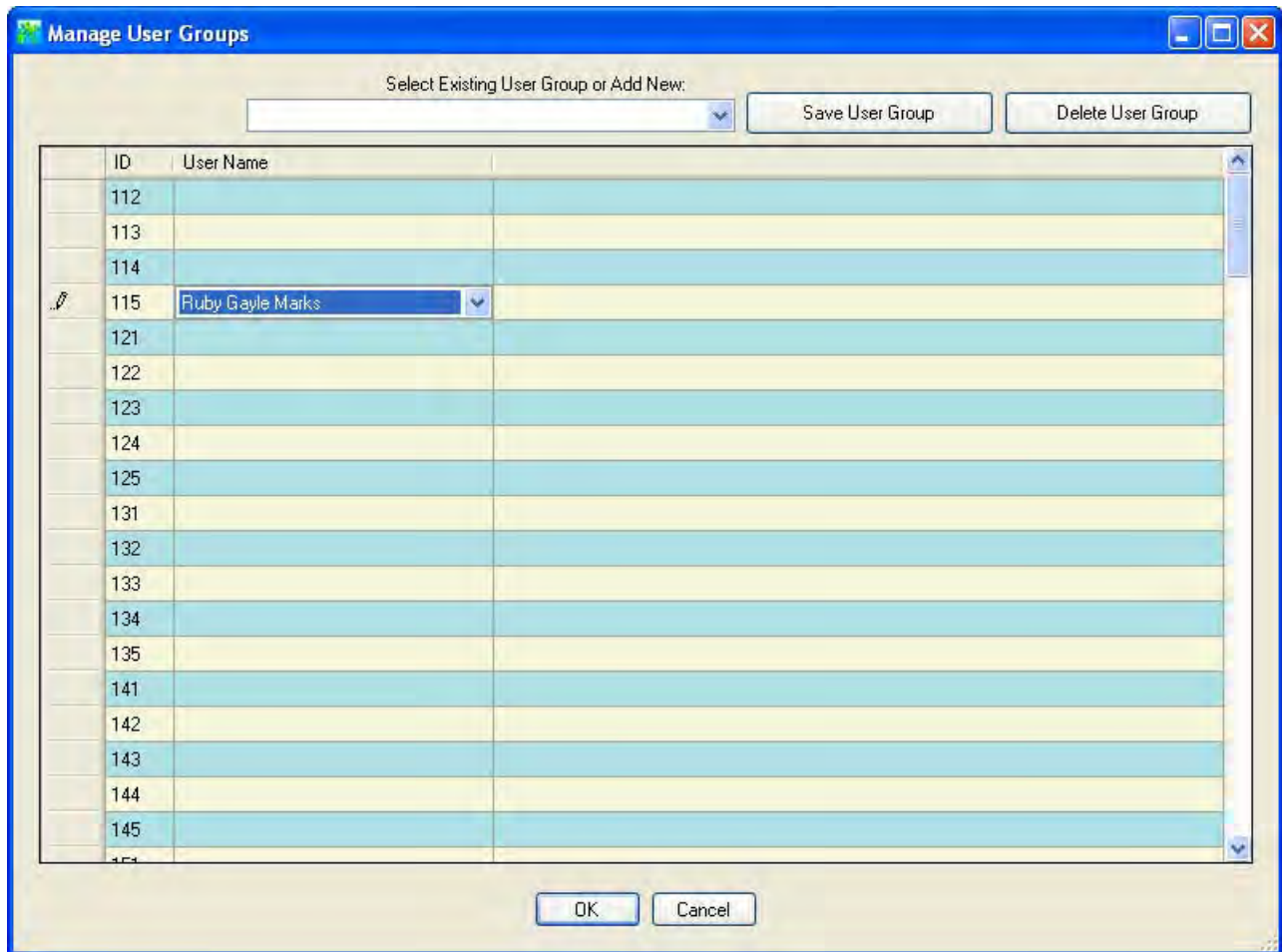
A dropdown box arrow will appear on the right hand side of the field.

3. Select a user name from the dropdown selection box.

Helpful Hint: *You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.*



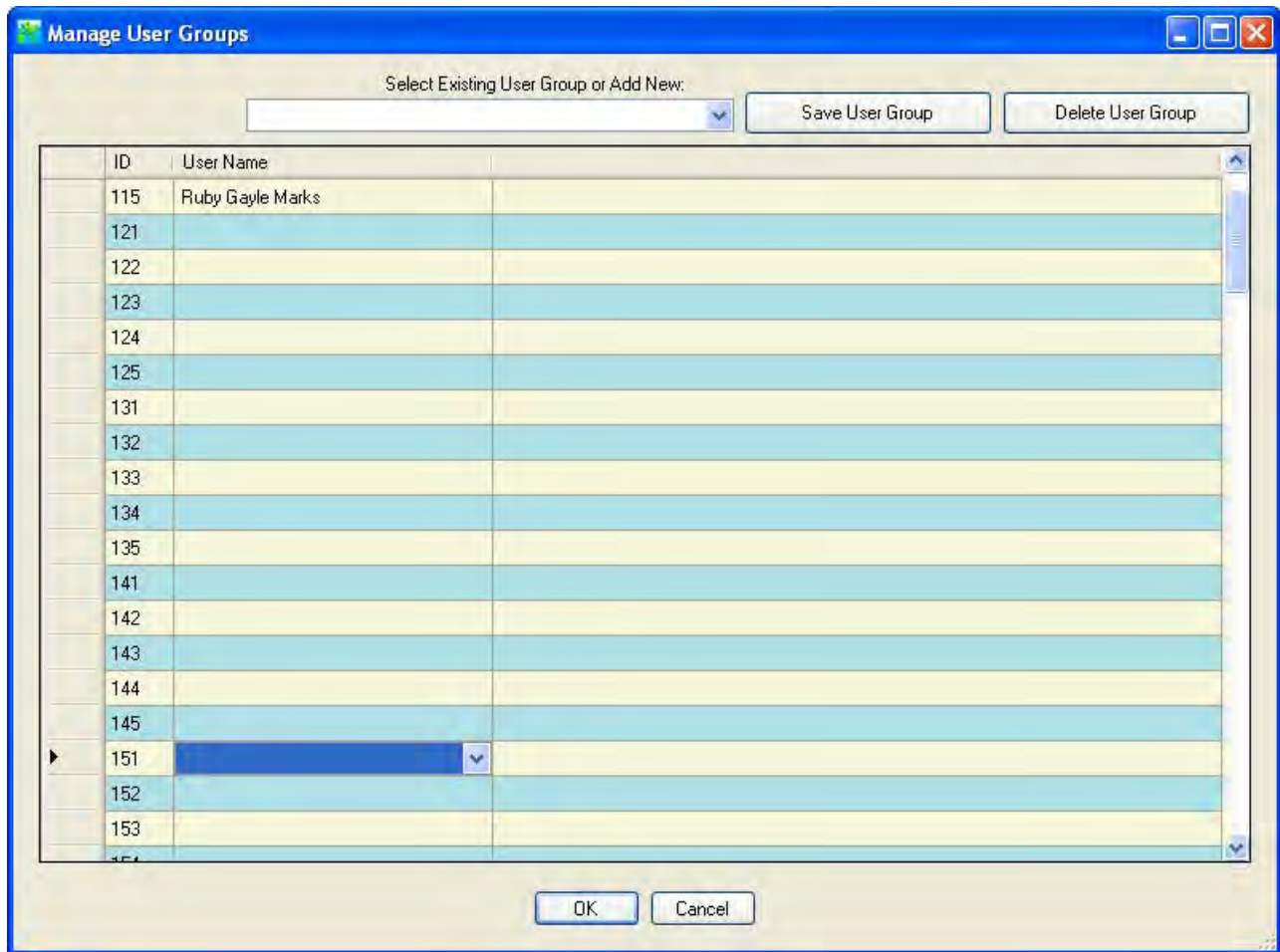
The selected name will fill the window.



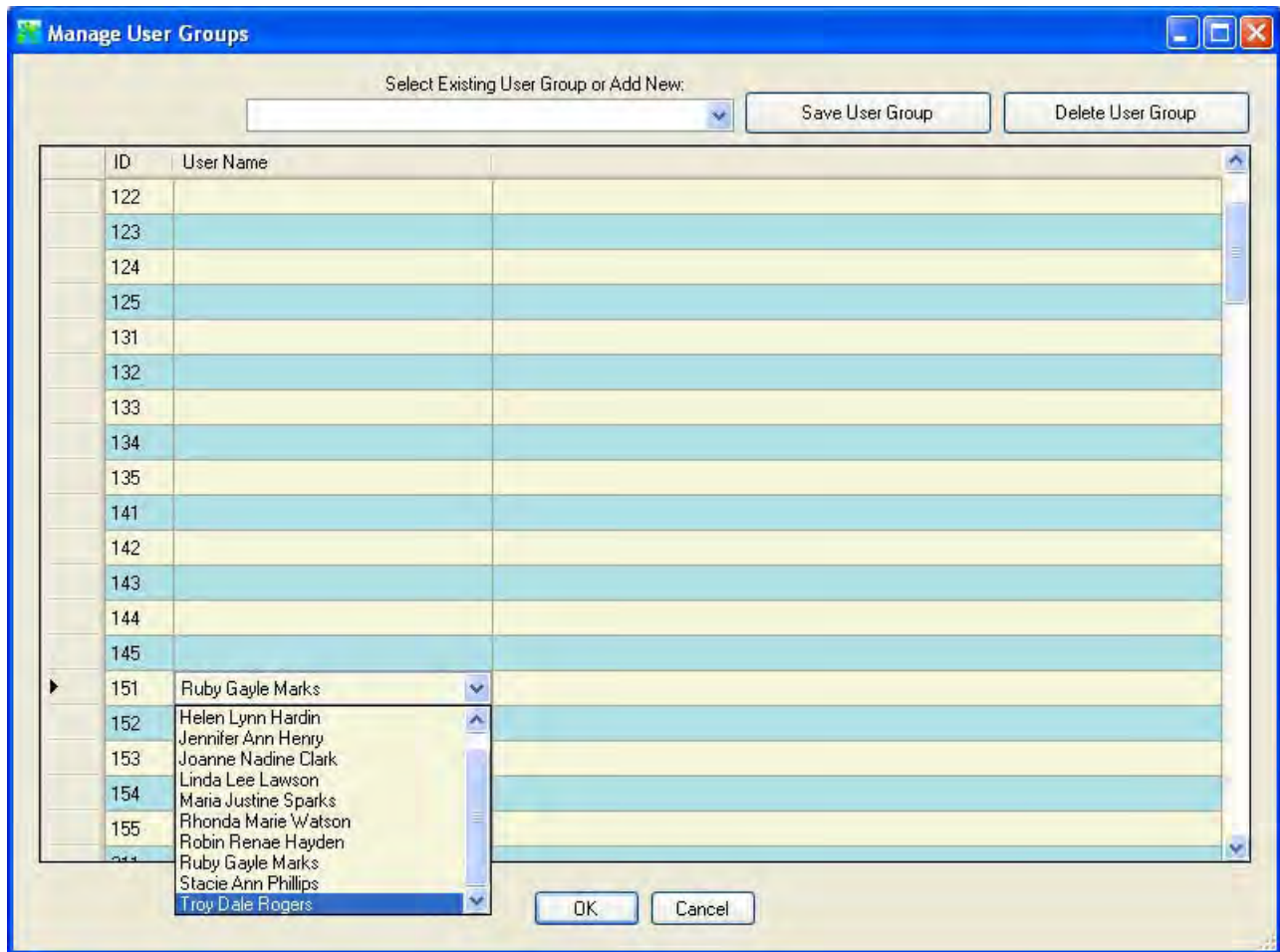
Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name and then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

5. Select the next User ID you want to assign to a user for this user group.
6. Click on the User Name field in the same line as the selected User ID.

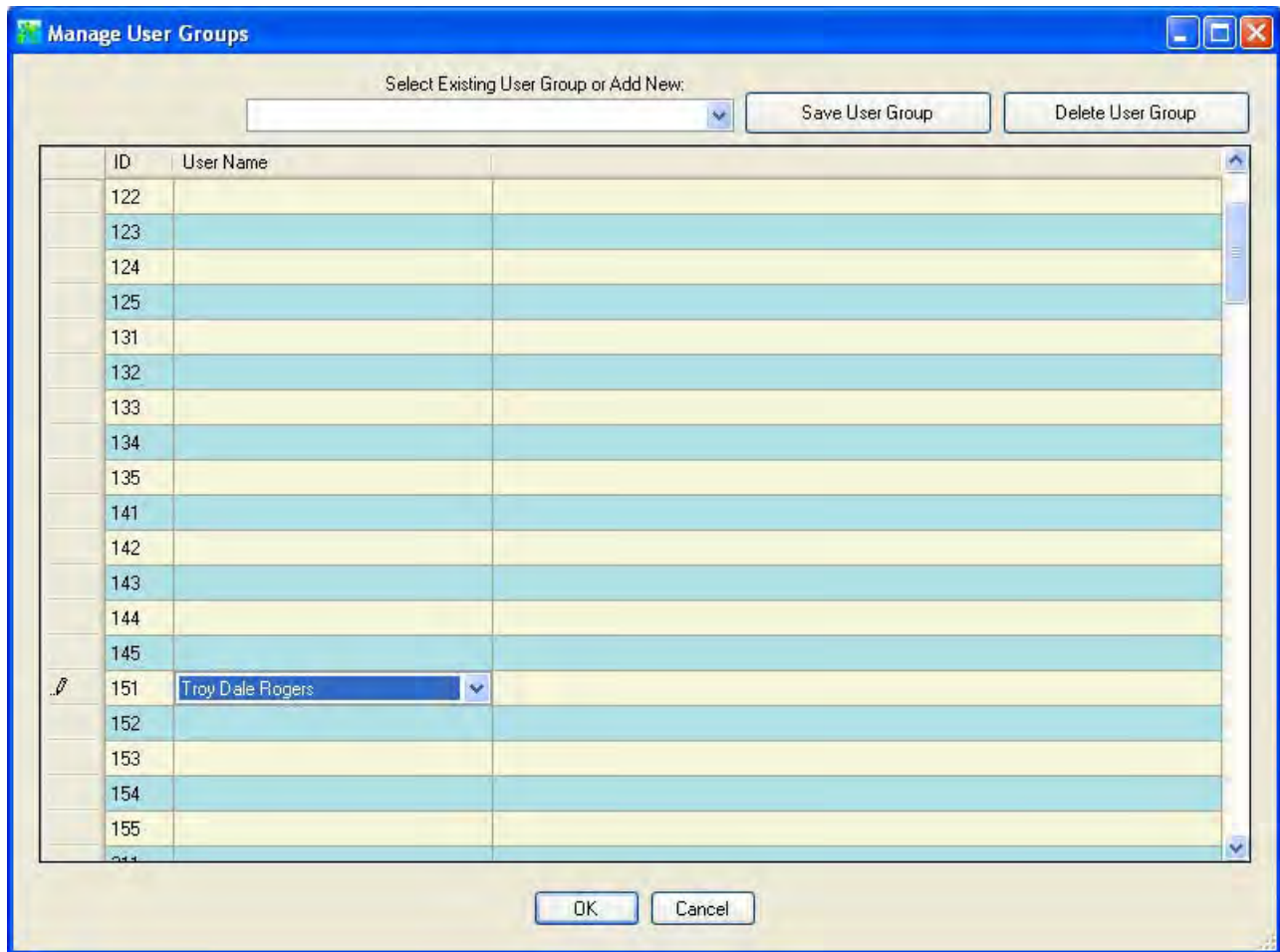
A dropdown box arrow will appear on the right hand side of the field.



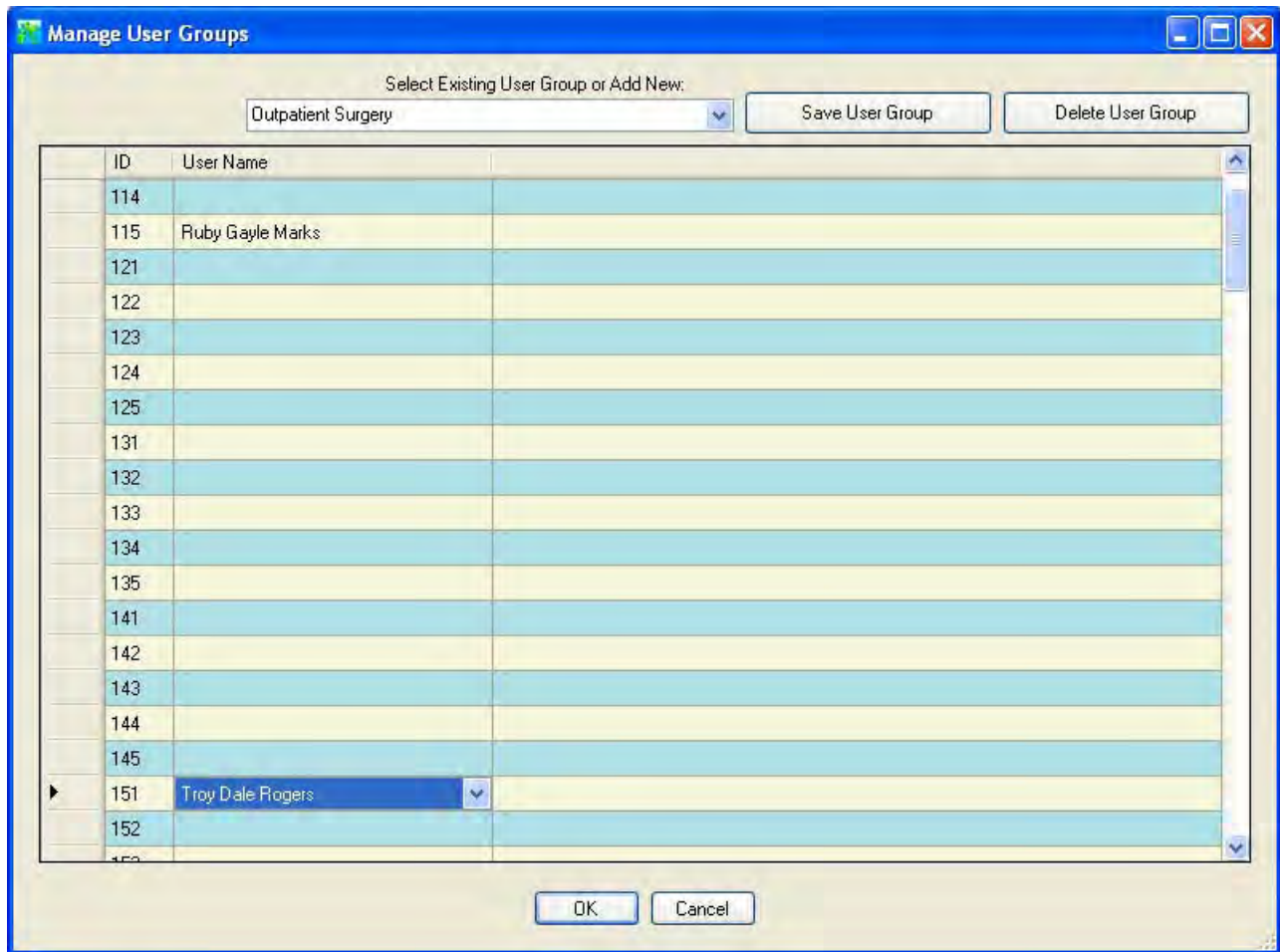
7. Select a user name from the dropdown selection box.



The selected name will fill the window.

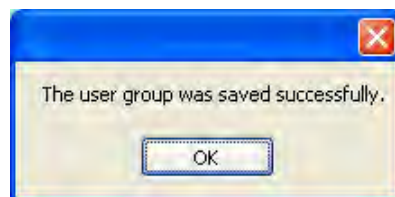


9. Continue repeating the steps to add another user to the user group until the user group members have all been defined.
10. Click on the field to “Select Existing User Group or Add New” and enter the name of the user group.



11. Click on the **Save User Group** tab to save the user group members to a file.

A message window is displayed indicating that the user group was saved successfully.

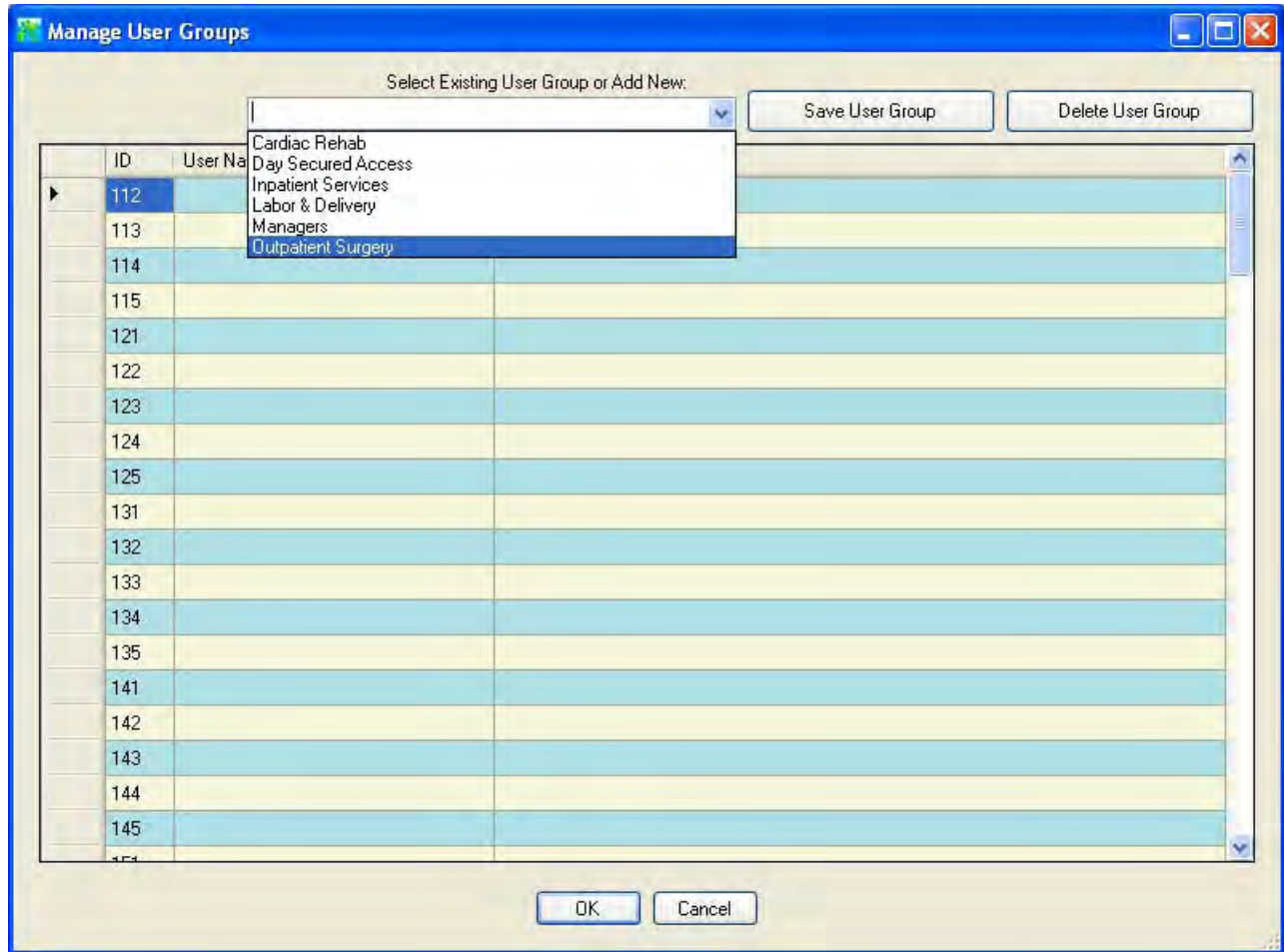


12. Click on **OK** to continue.

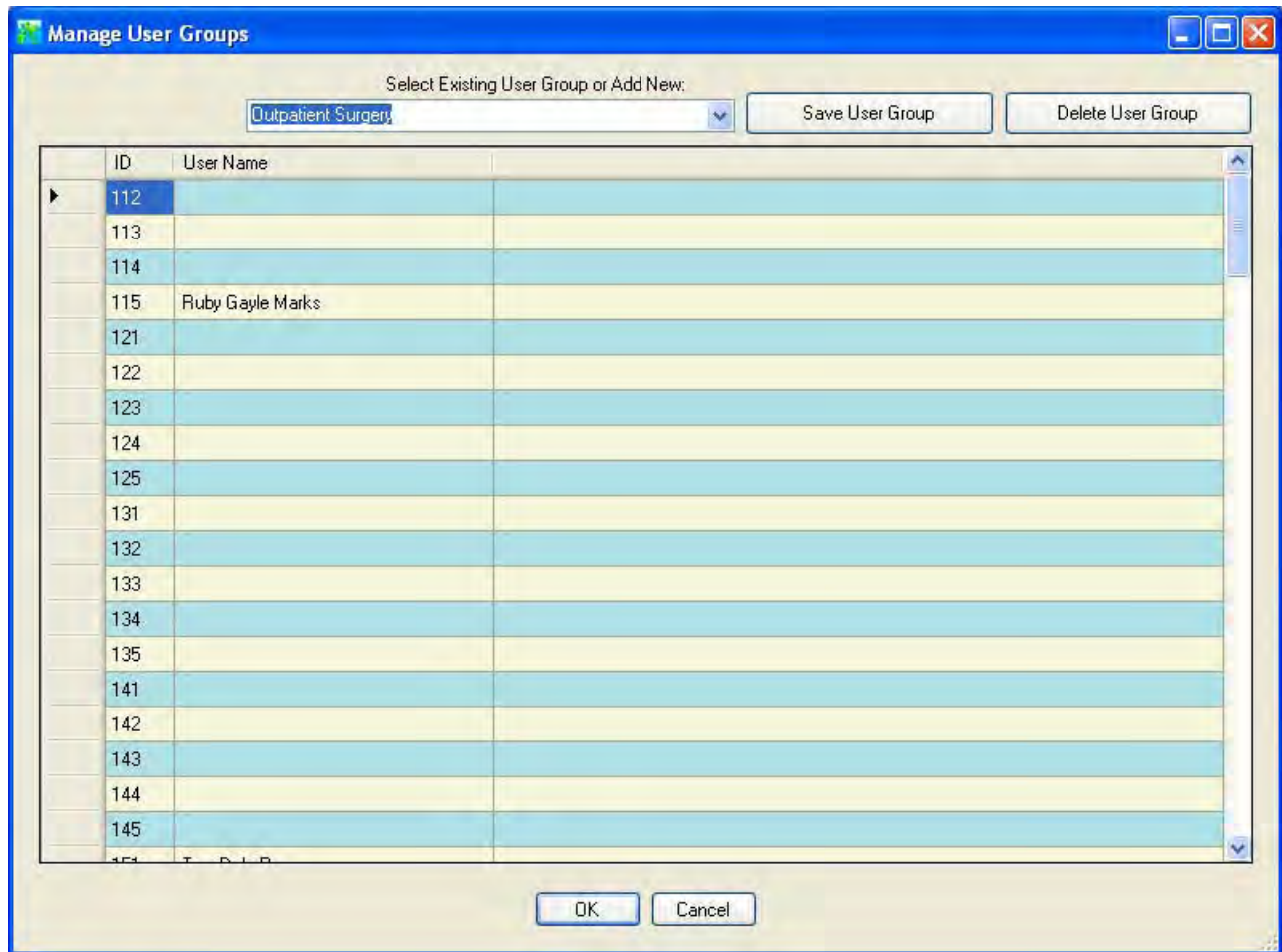
Modify User Group

Once a user group has been created, you have the option to modify it by adding, deleting, and reassigning users.

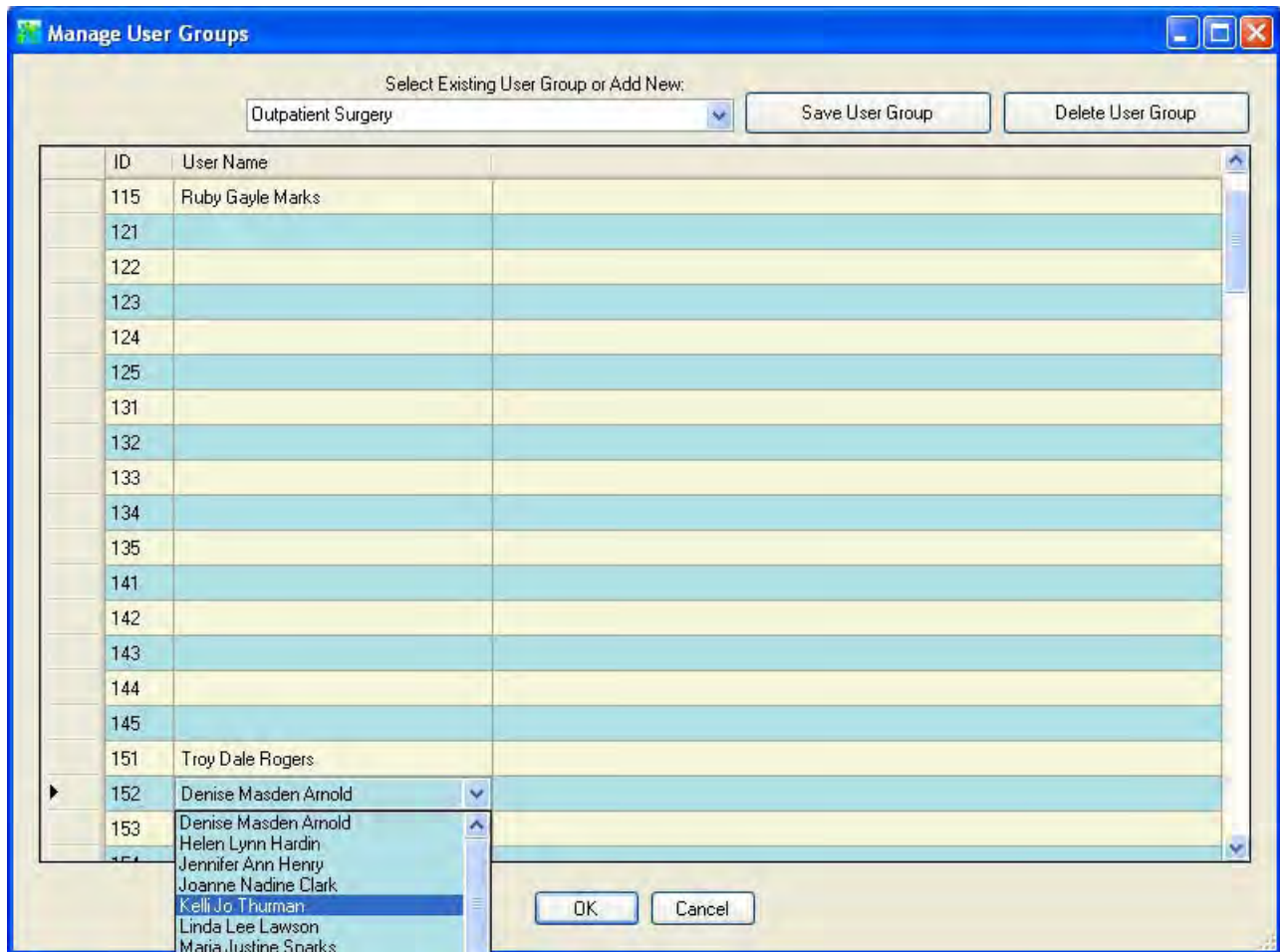
1. Click on the field to “Select Existing User Group or Add New” and enter or select the name of the user group to be updated.



The members of the user group will be displayed.

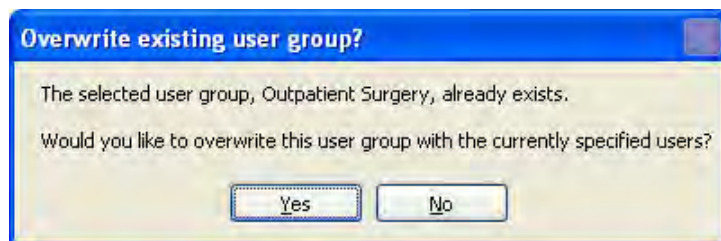


2. Add new members, delete members or reassign members of the user group as necessary.



- Once all changes have been made to the user group, click on the **Save User Group** tab.

A prompt window is displayed asking for confirmation to overwrite the existing the user group information with the modified information.



- Click on **Yes** to save the changes for the selected user group.

A message window is displayed indicating that the changes to the user group were changed successfully.

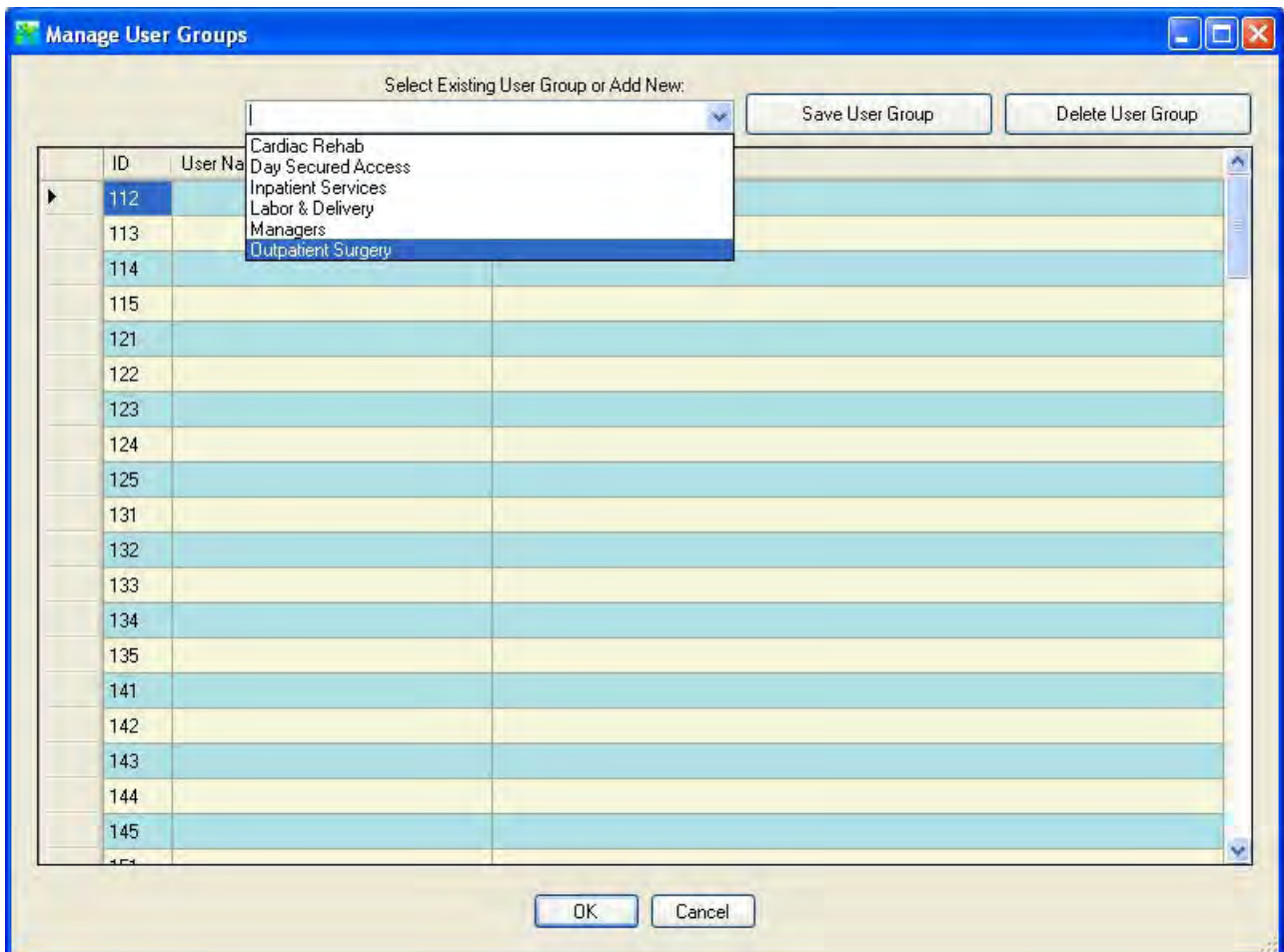


5. Click on **OK** to continue.

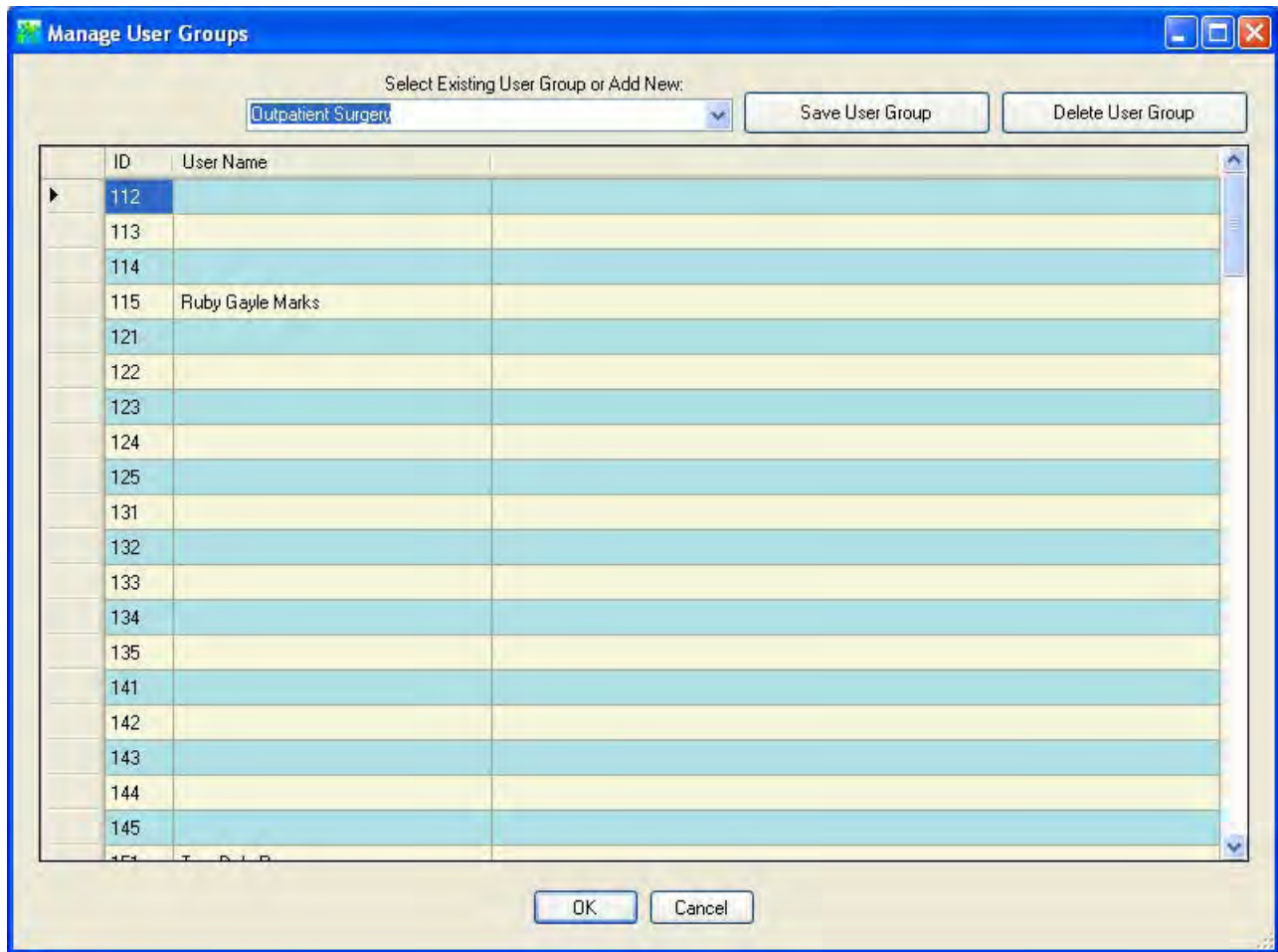
Delete User Group

Another option on the Manage Users screen is “Delete User Group”. This item is used to delete a user group that no longer needs to be maintained in the system.

1. Click on the field to “Select Existing User Group or Add New” and enter or select the name of the user group to be deleted.

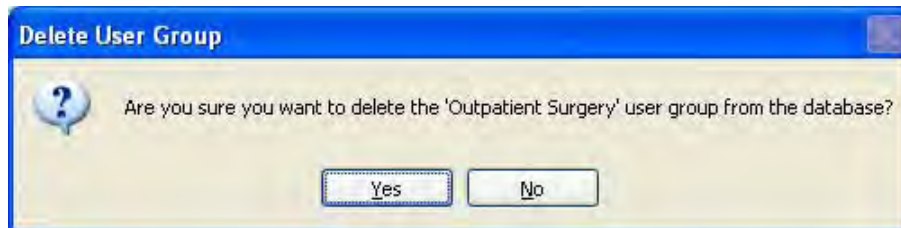


The members of the user group will be displayed.



2. Click on the **Delete User Group** tab.

A prompt window is displayed asking for confirmation to delete the user group.



3. Click on **Yes** to delete the selected user group.

A message window is displayed to indicate that the user group was deleted successfully.



4. Click on **OK** to continue.

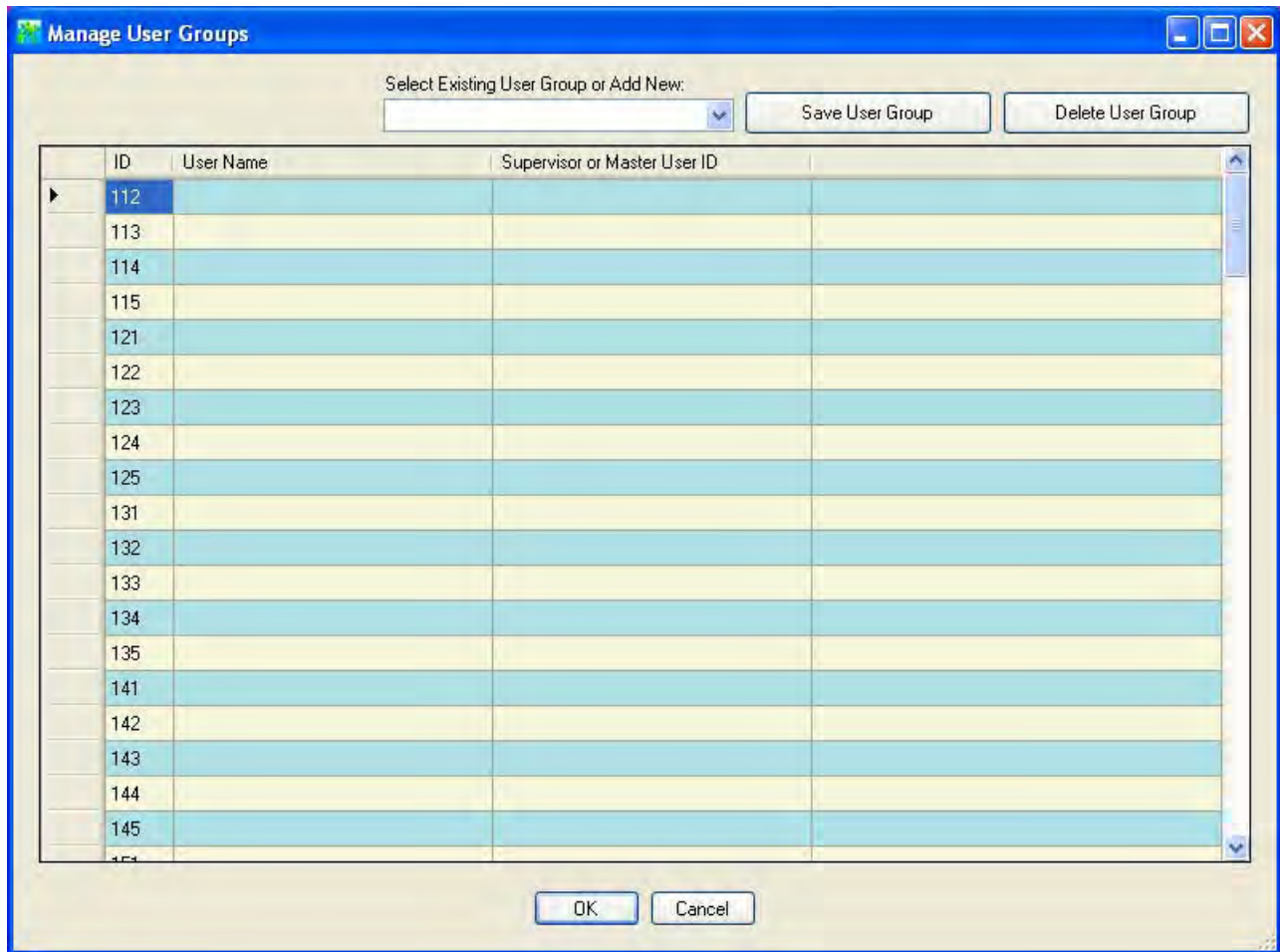
Manage User Groups - CL20 Interface

The options available from the Manage User Groups CL20 interface allow you to create new user groups or to modify or delete existing user groups.

Create A New User Group

To create a new user group, you must decide which users will belong to the group and you must identify the user ID assignment for each member of the group. Then you can proceed to define the user group in the system. Once defined, you will save it under an assigned name that can be retrieved when programming user access for a lock.

1. Select the User ID to which you want to assign a user.

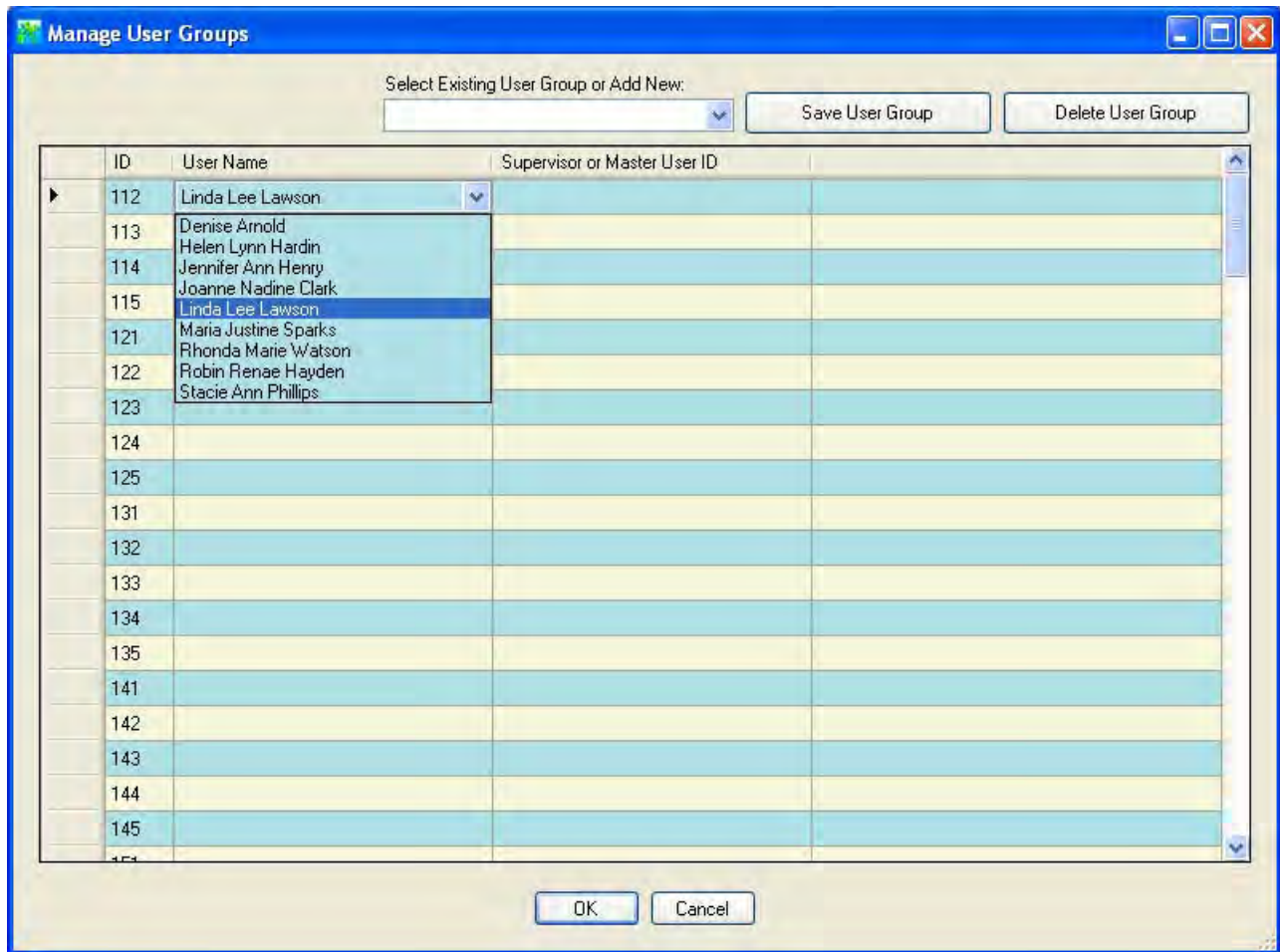


2. Click on the User Name field in the same line as the selected User ID.

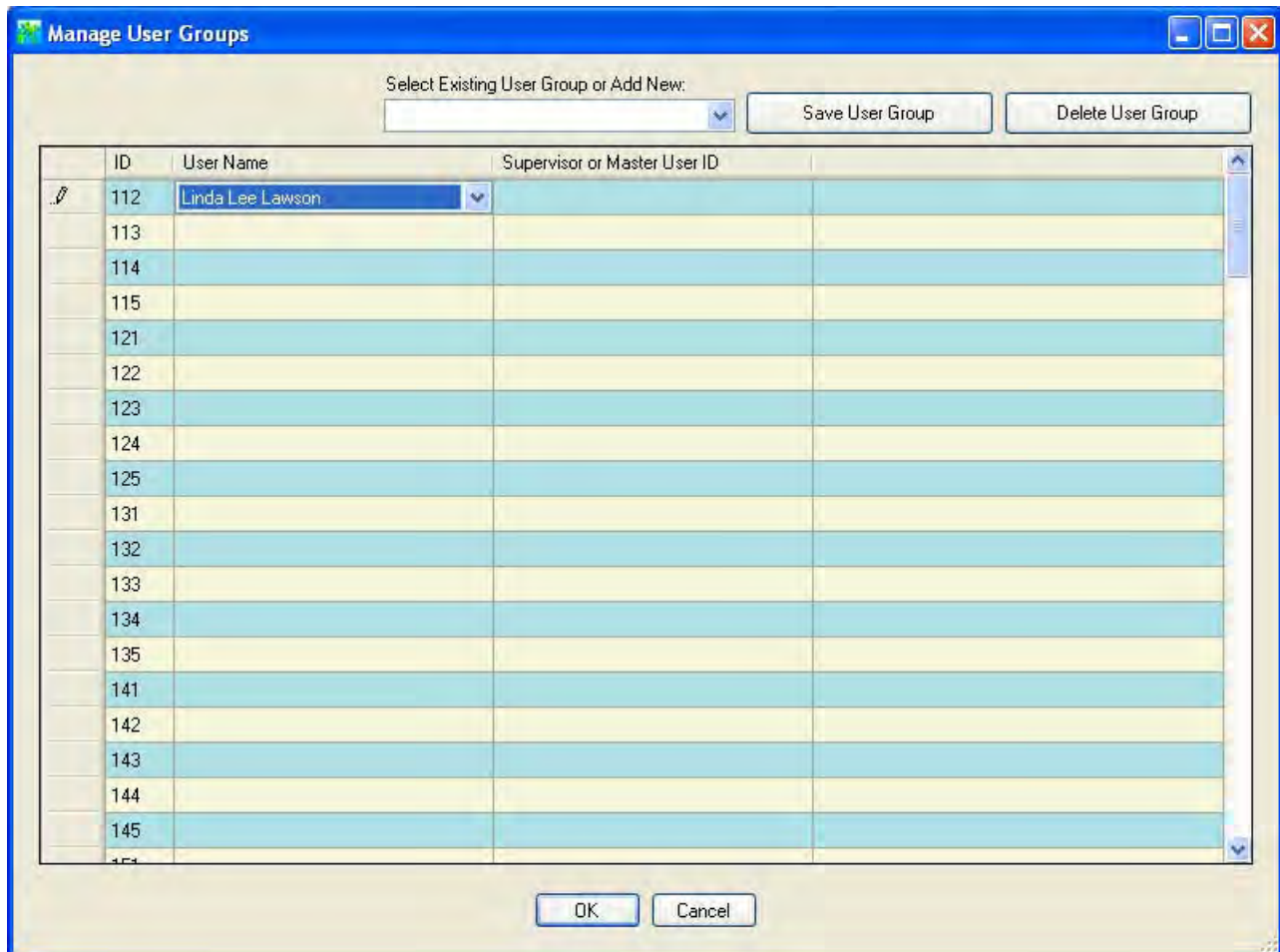
A dropdown box arrow will appear on the right hand side of the field.

3. Select a user name from the dropdown selection box.

Helpful Hint: *You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.*



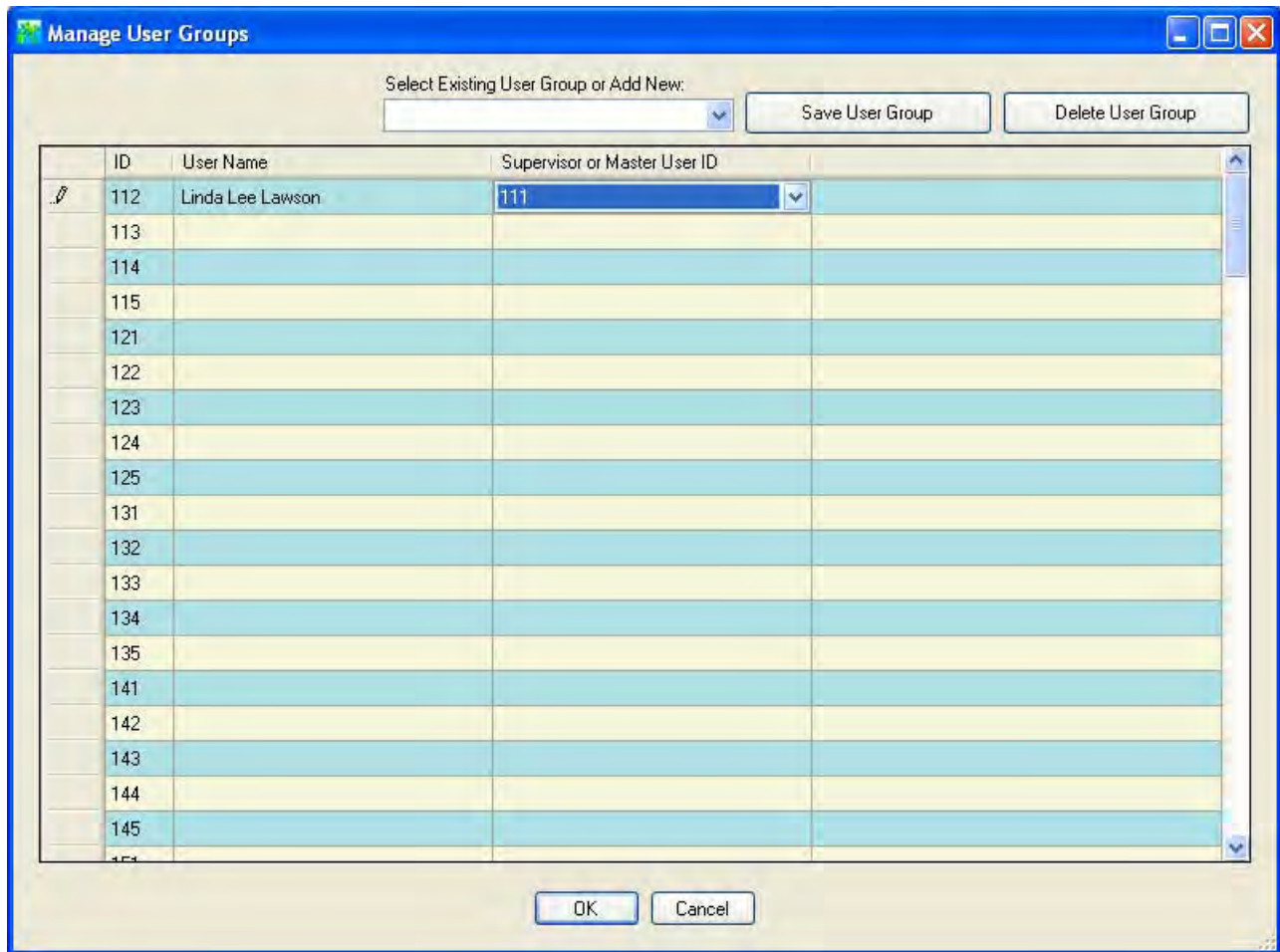
The selected name will fill the window.



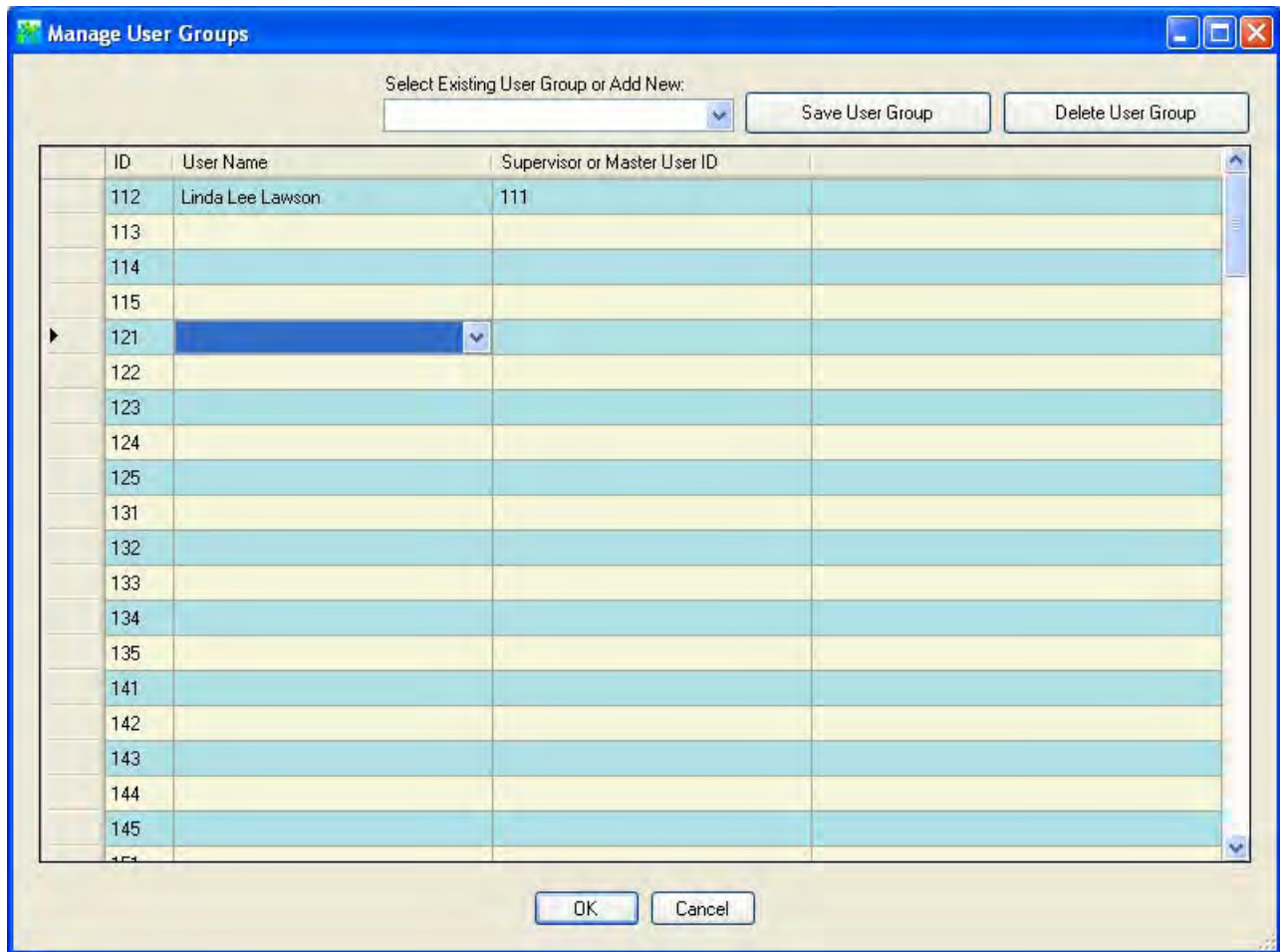
Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name and then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

- If you wish to assign a Supervisor or a Manager to the user, click on the Supervisor or Master User ID field and type in the appropriate User ID, or you can make a selection from the dropdown box.

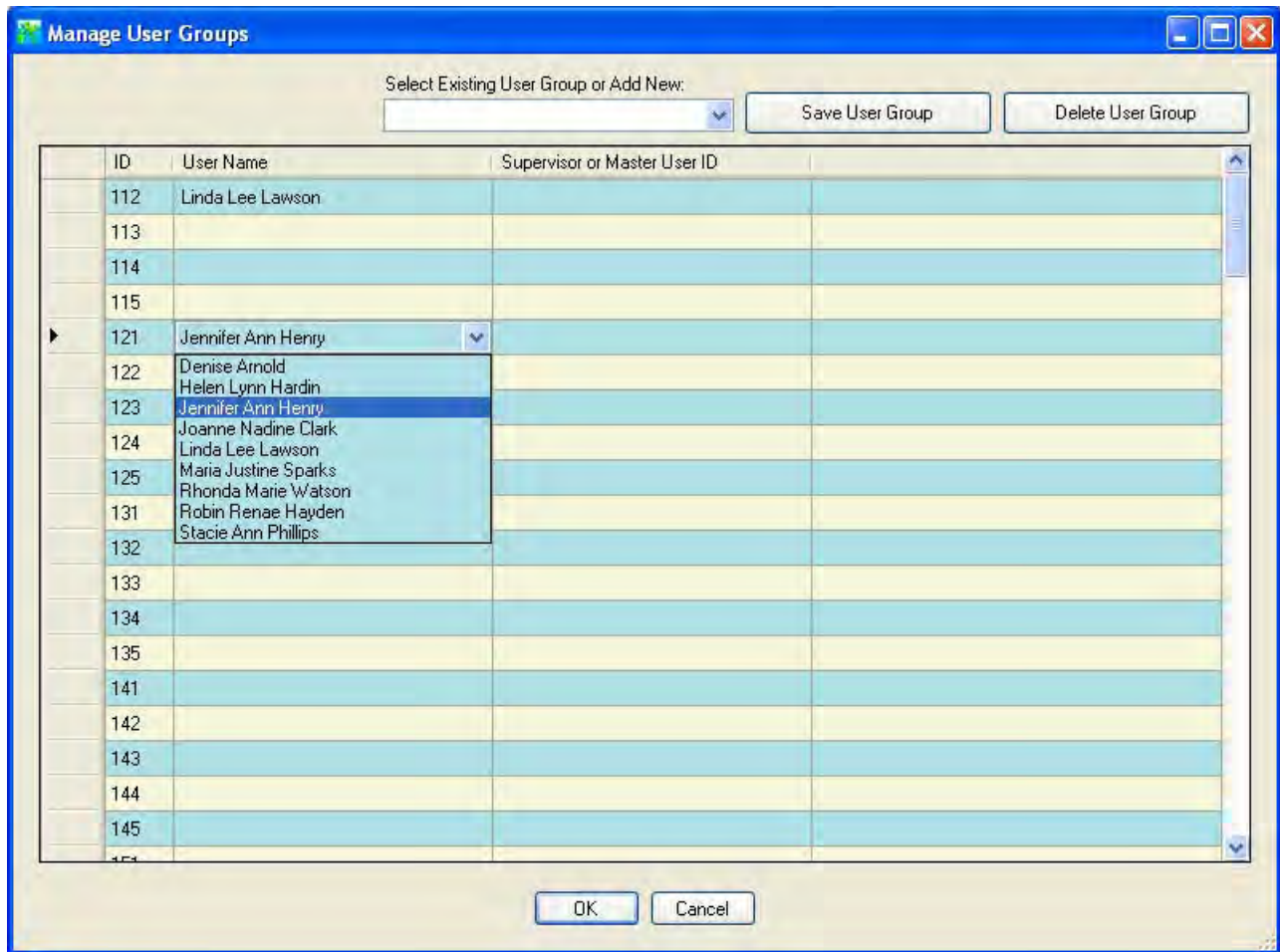
Note: *For a designated Supervisor ID (i.e., 112, 113, 114, 115), the only selection choice is the Master User ID of 111. For all other User IDs, the choices are limited to the designated Supervisor of 112, 113, 114, and 115.*



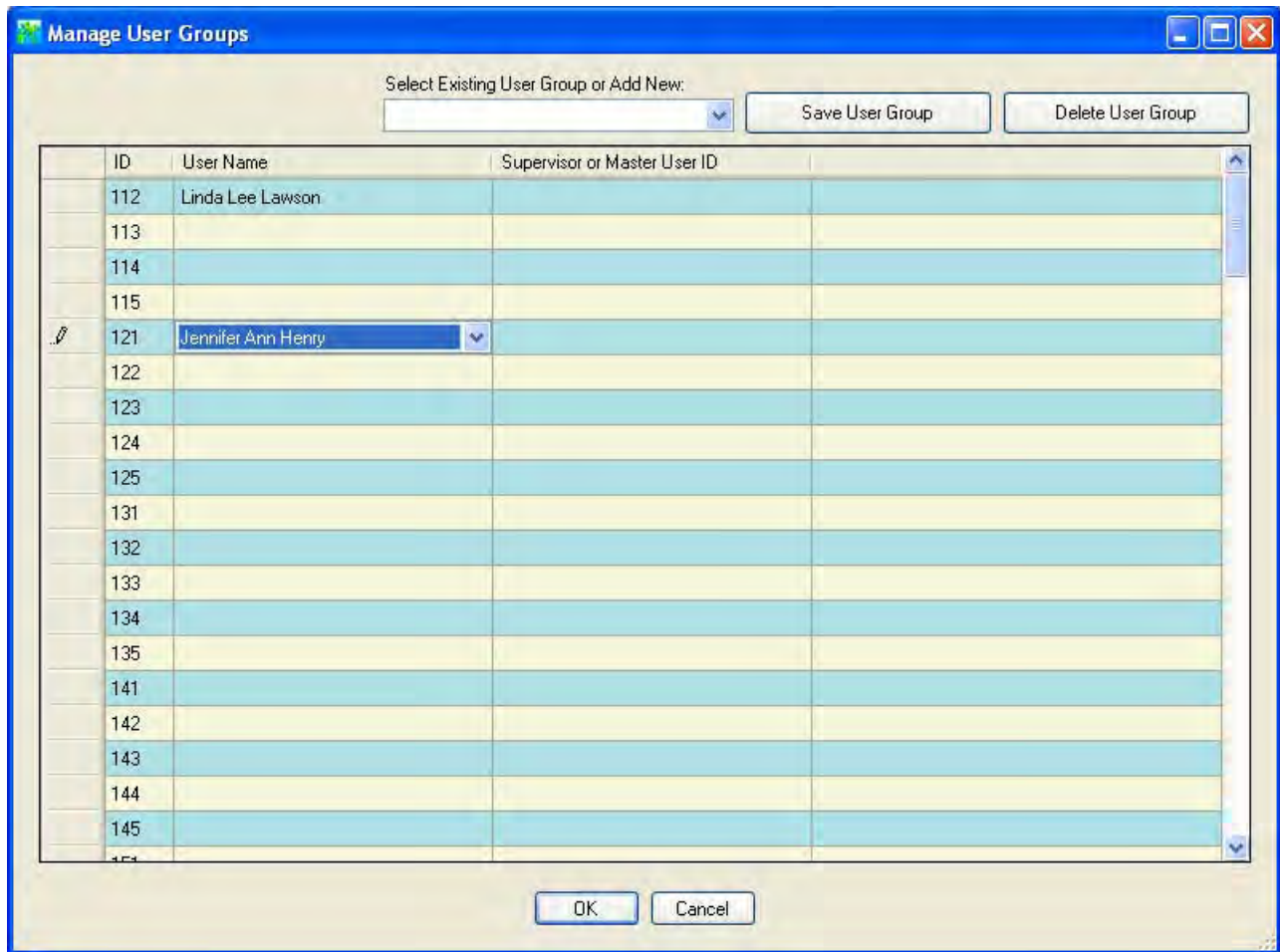
5. Select the next User ID you want to assign to a user for this user group.
6. Click on the User Name field in the same line as the selected User ID.
A dropdown box arrow will appear on the right hand side of the field.



7. Select a user name from the dropdown selection box.

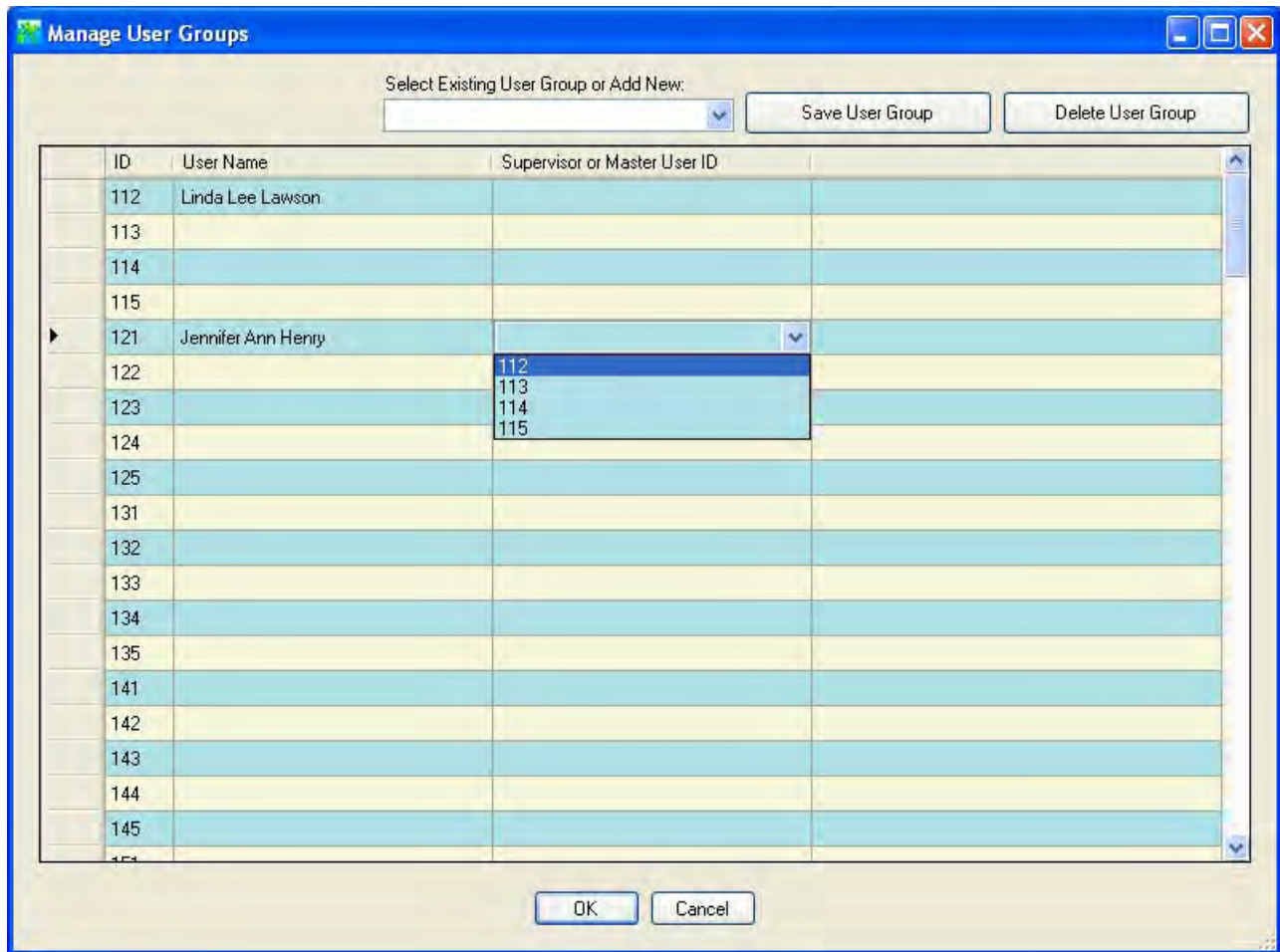


The selected name will fill the window.

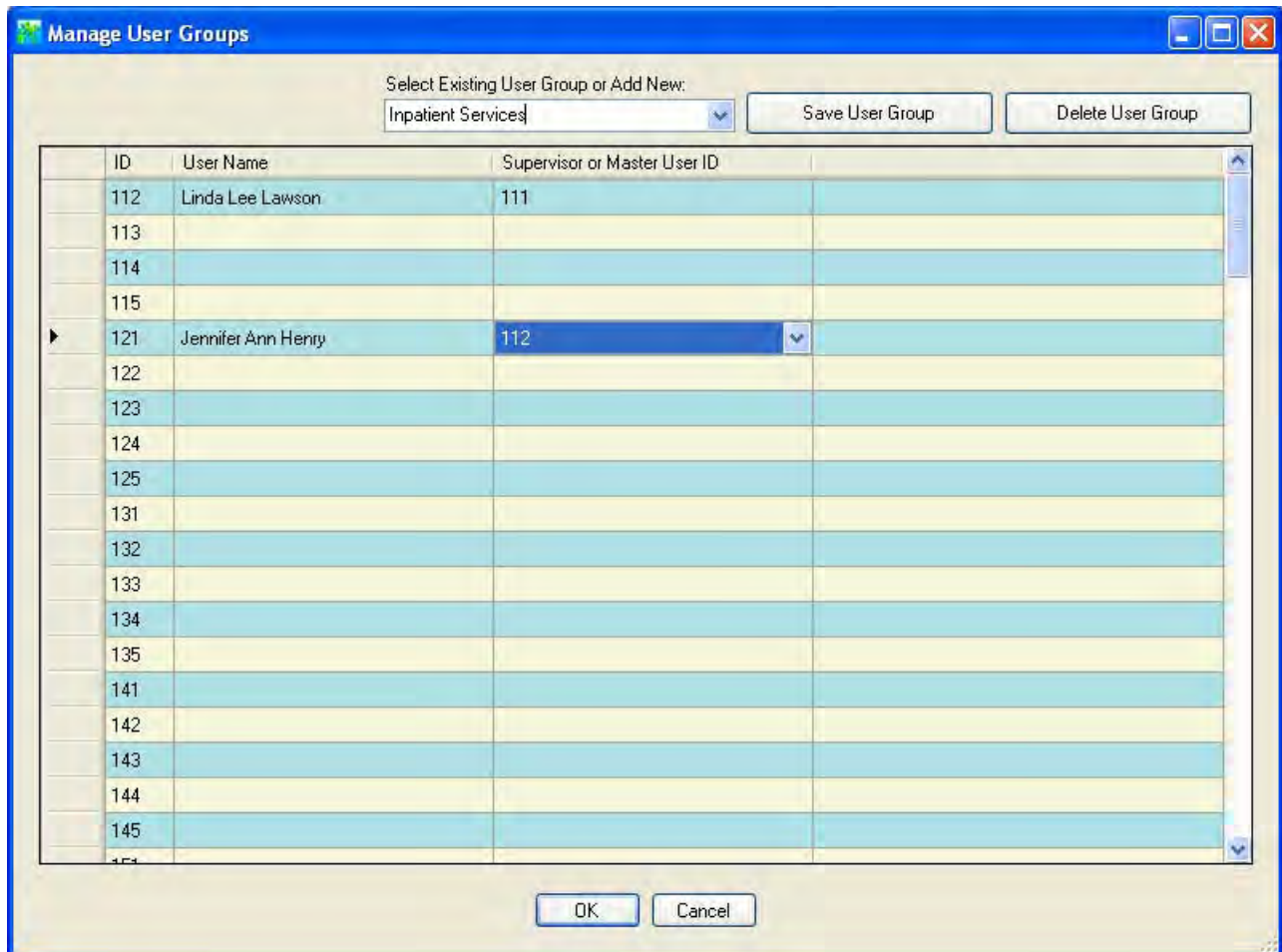


8. If you wish to assign a Supervisor or a Manager to the user, click on the Supervisor or Master User ID field and type in the appropriate User ID, or you can make a selection from the dropdown box.

Note: For a designated Supervisor ID (i.e., 112, 113, 114, 115), the only selection choice is the Master User ID of 111. For all other User IDs, the choices are limited to the designated Supervisor of 112, 113, 114, and 115.

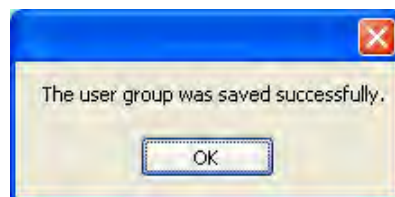


9. Continue repeating the steps to add another user to the user group until the user group members have all been defined.
10. Click on the field to “Select Existing User Group or Add New” and enter the name of the user group.



11. Click on the **Save User Group** tab to save the user group members to a file.

A message window is displayed indicating that the user group was saved successfully.

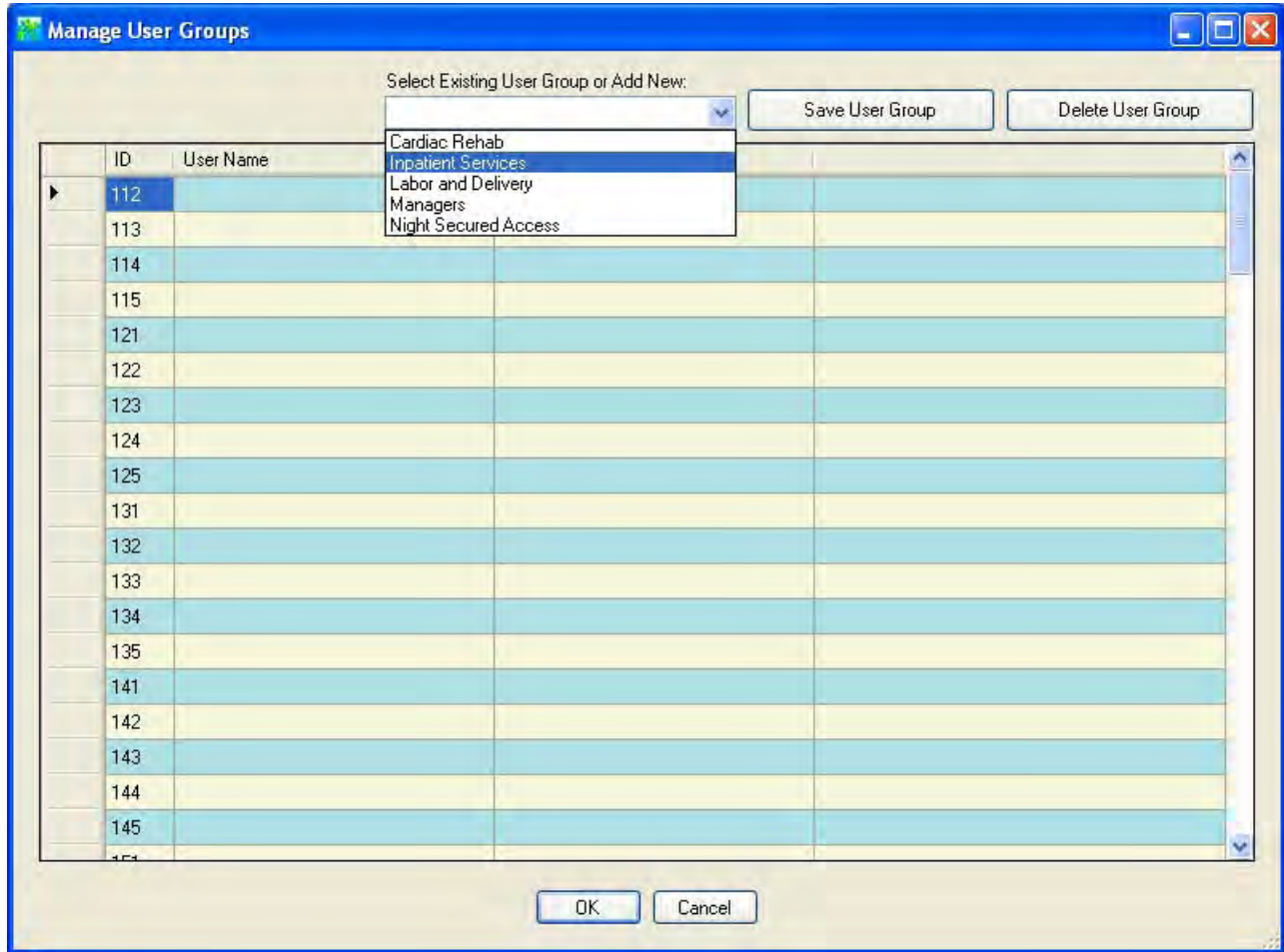


12. Click on **OK** to continue.

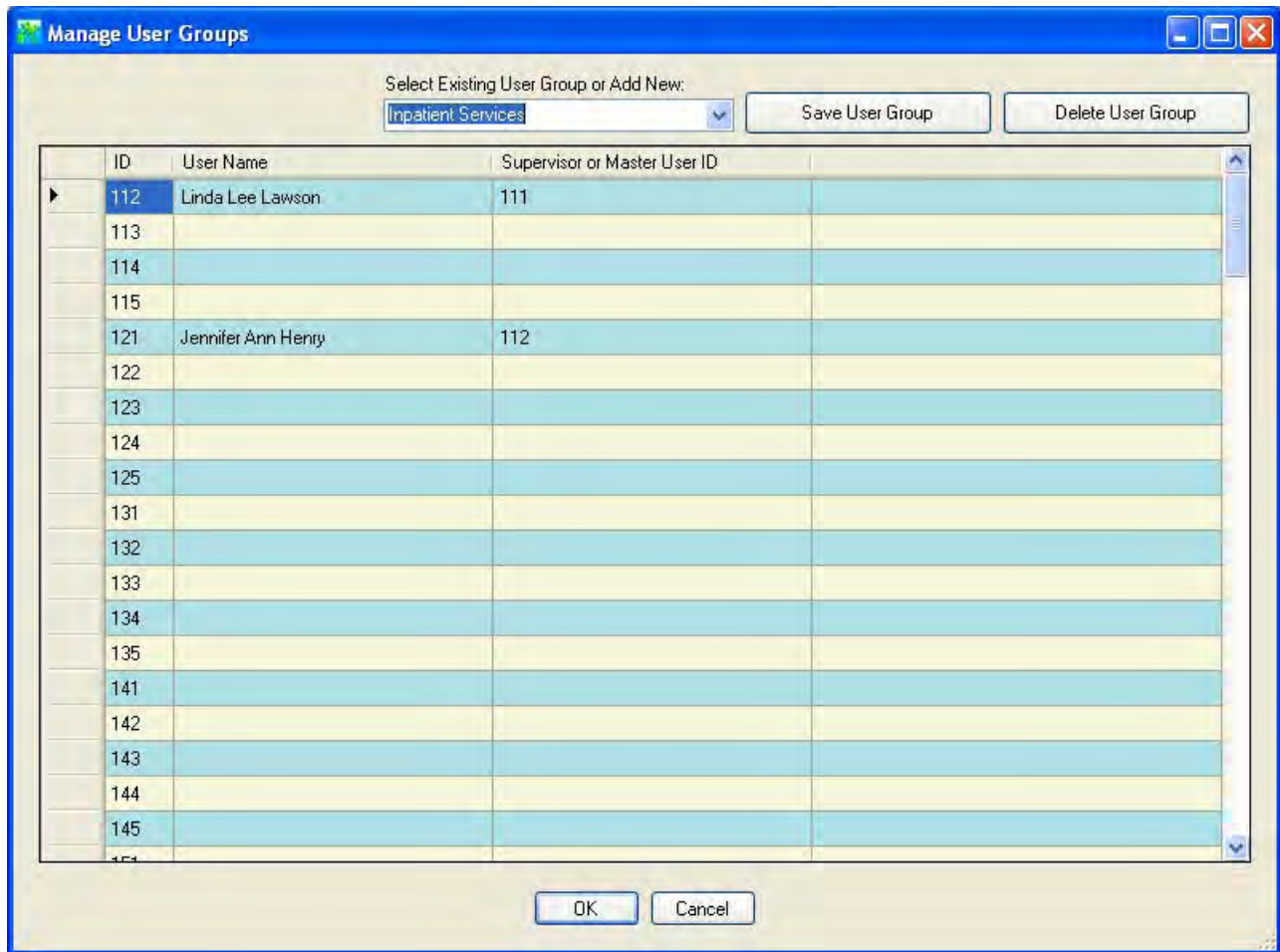
Modify User Group

Once a user group has been created, you have the option to modify it by adding, deleting, and reassigning users.

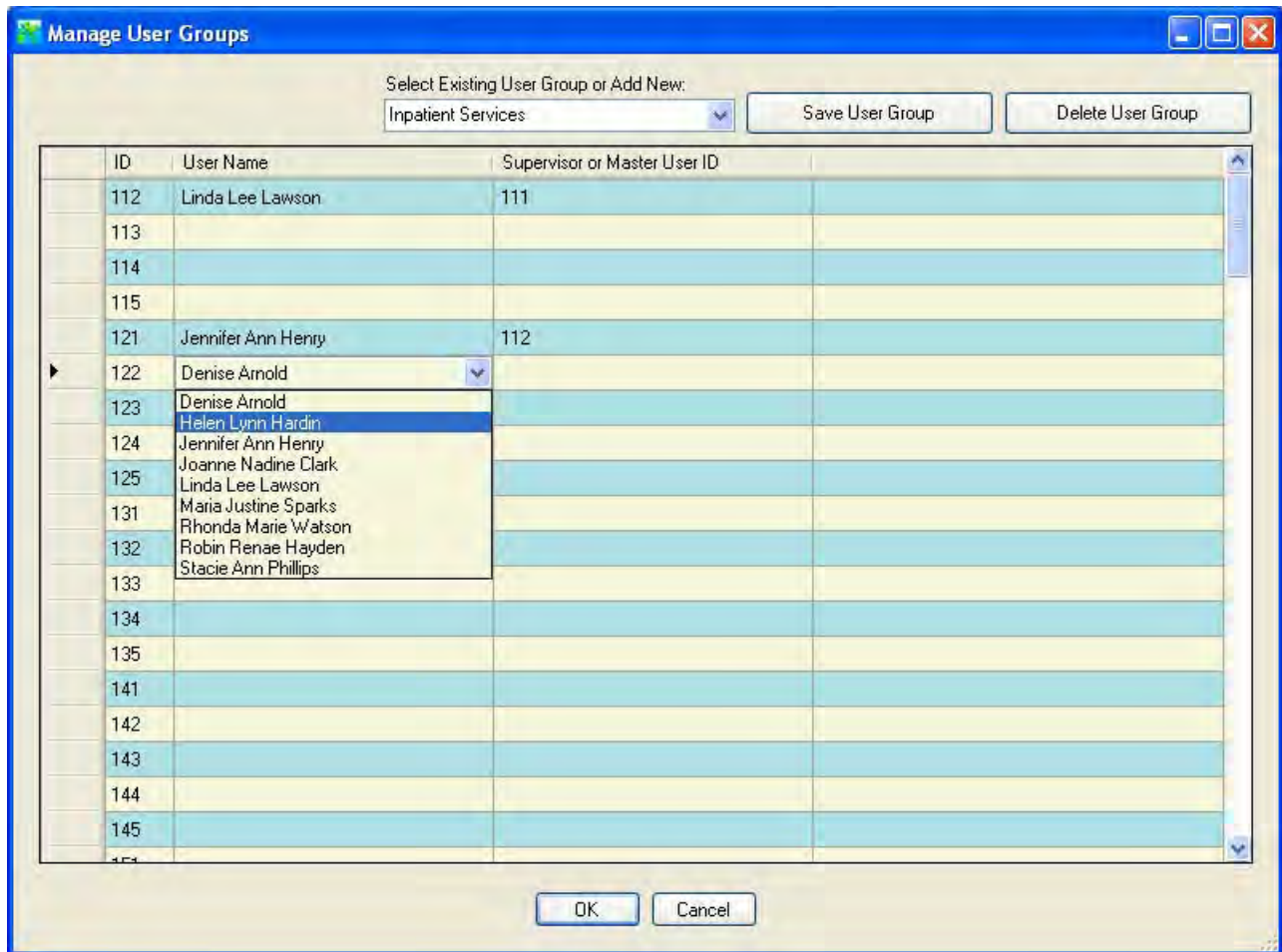
1. Click on the field to “Select Existing User Group or Add New” and enter or select the name of the user group to be updated.



The members of the user group will be displayed.



2. Add new members, delete members or reassign members of the user group as necessary.



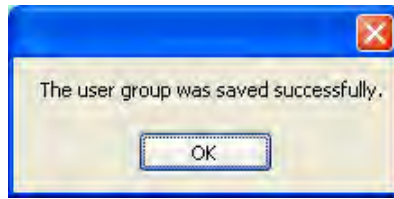
- Once all changes have been made to the user group, click on the **Save User Group** tab.

A prompt window is displayed asking for confirmation to overwrite the existing the user group information with the modified information.



- Click on **Yes** to save the changes for the selected user group.

A message window is displayed indicating that the changes to the user group were changed successfully.

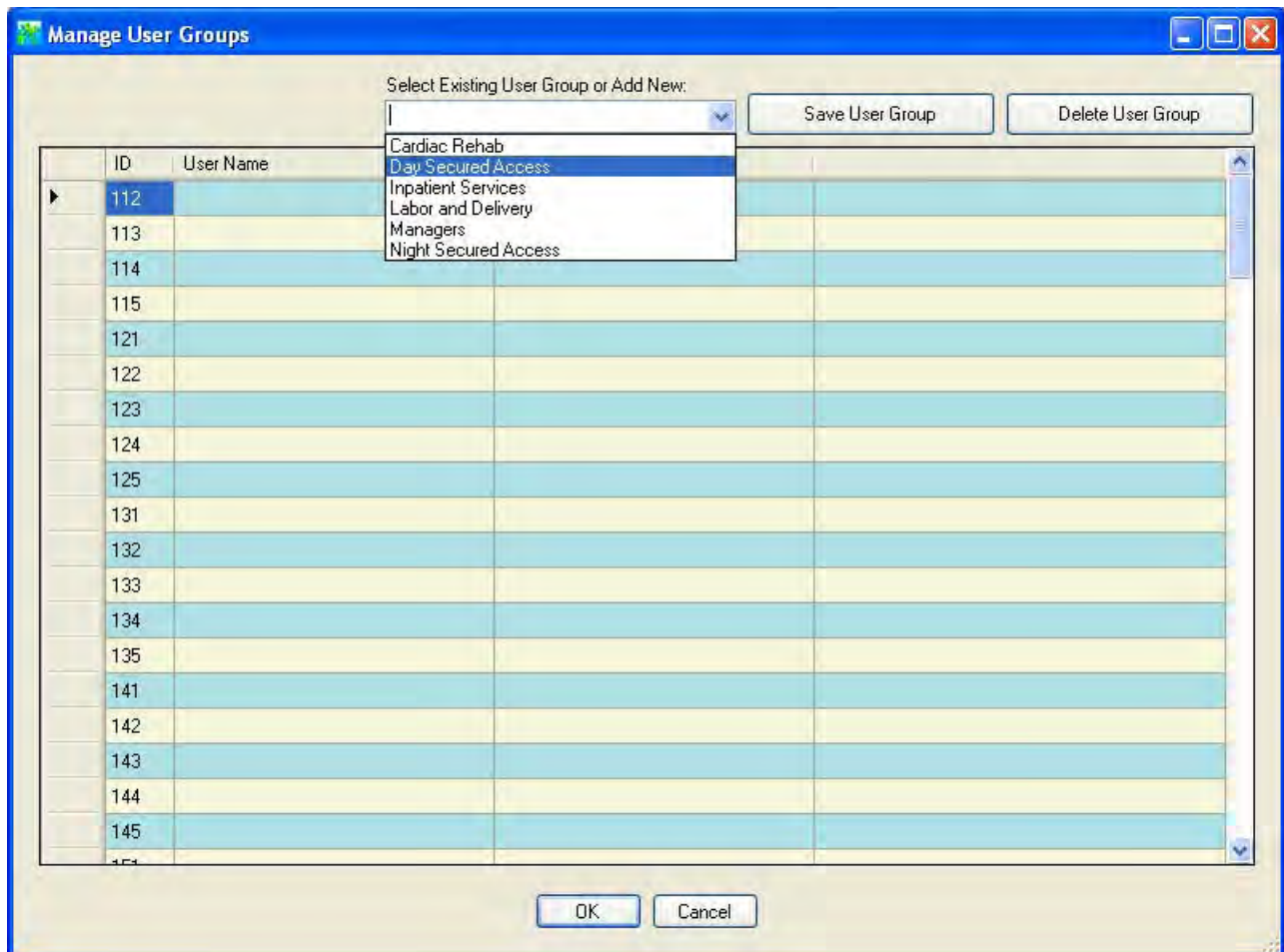


5. Click on **OK** to continue.

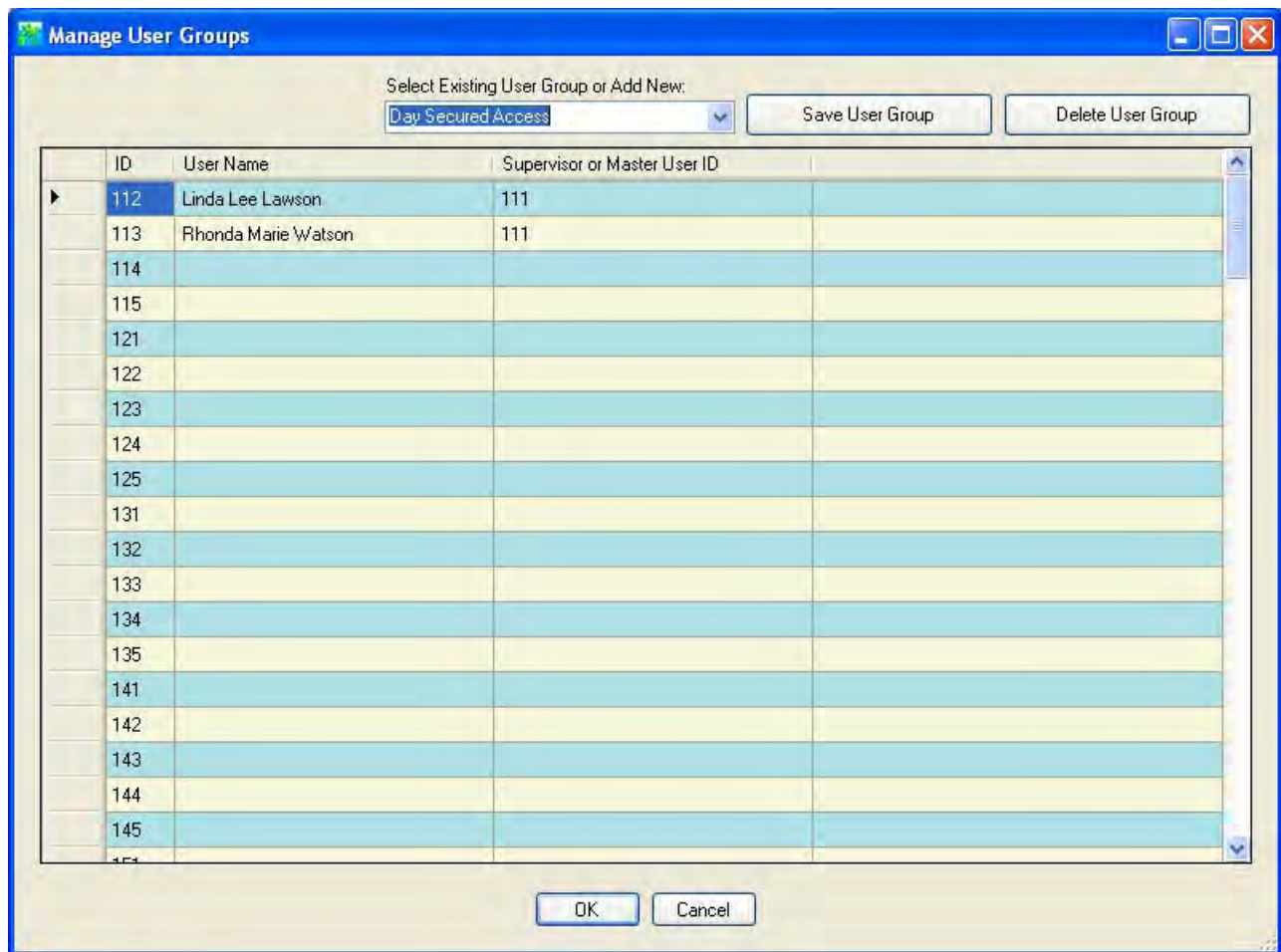
Delete User Group

Another option on the Manage Users screen is “Delete User Group”. This item is used to delete a user group that no longer needs to be maintained in the system.

1. Click on the field to “Select Existing User Group or Add New” and enter or select the name of the user group to be deleted.

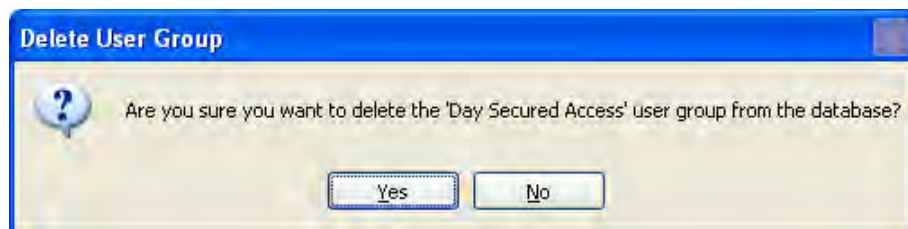


The members of the user group will be displayed.



2. Click on the **Delete User Group** tab.

A prompt window is displayed asking for confirmation to delete the user group.



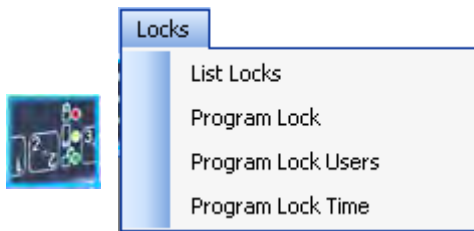
3. Click on **Yes** to delete the selected user group.

A message window is displayed to indicate that the user group was deleted successfully.



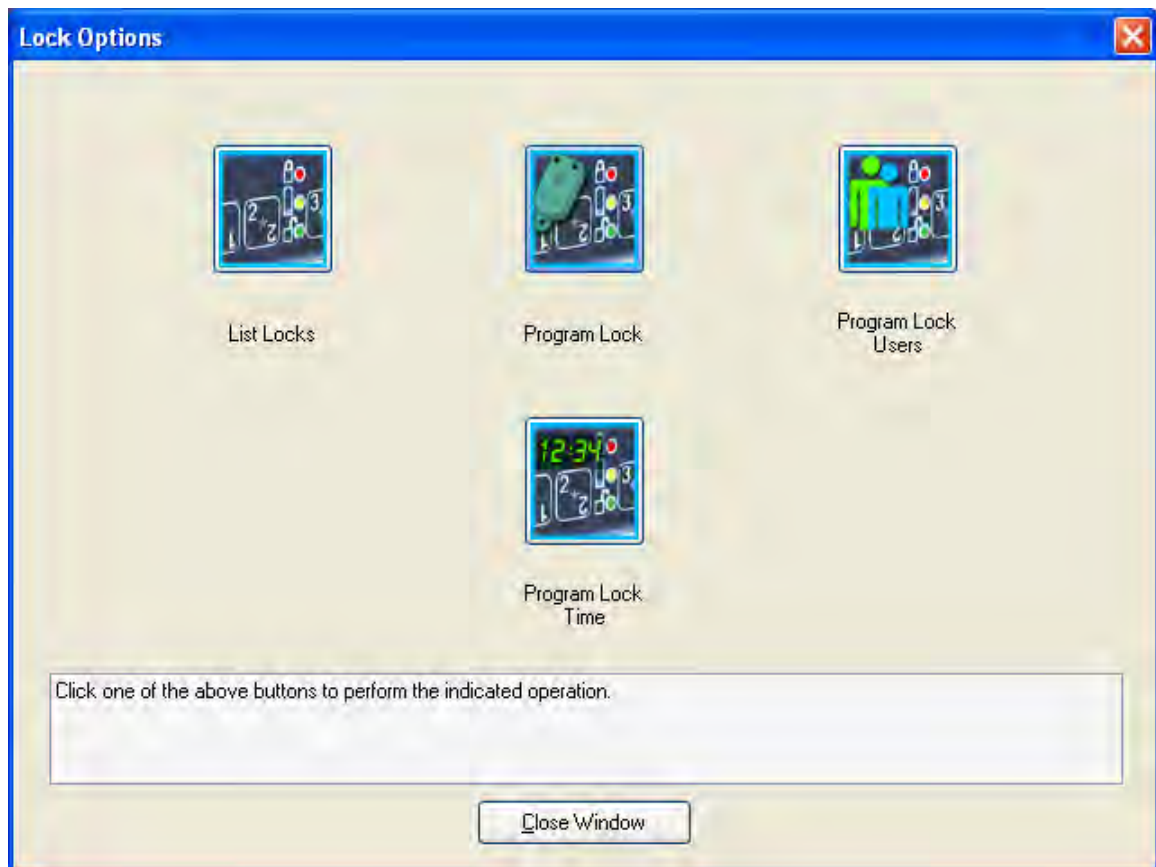
4. Click on **OK** to continue.

Locks Menu - CL10



List Locks or Program Lock Information

The Locks Menu options for the Model CL10 software interface allow you to program the lock, add/delete users, or set the date and time in the lock. The Locks menu options can also be accessed by selecting the Locks icon from the Toolbar.




From the Main menu:

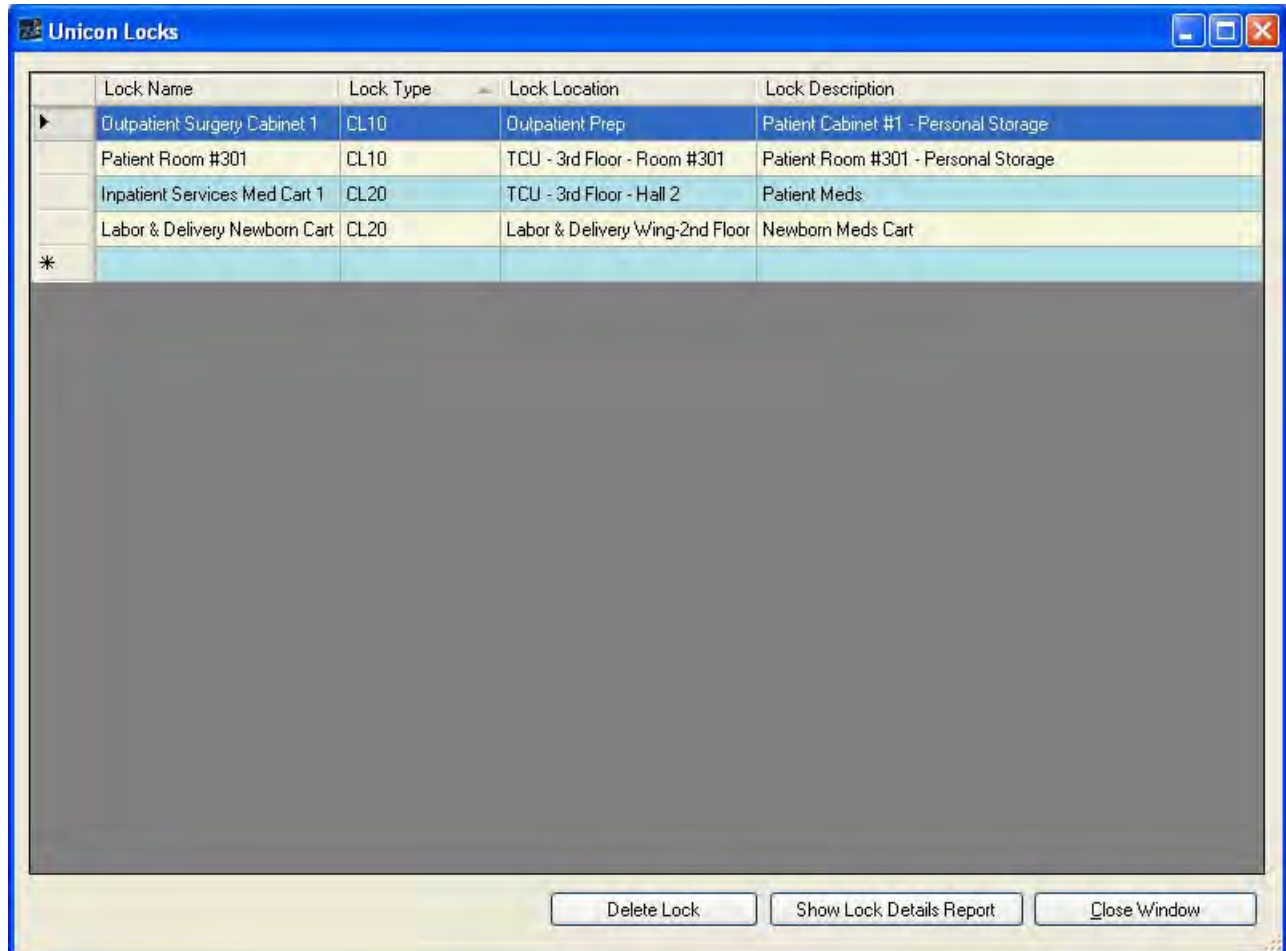
1. Select the **Locks Menu** or the  toolbar icon.

List Locks

This menu item is used to display all locks (CL10 and CL20) that have been defined in the PC system. It also allows the details of each lock to be displayed in report format. Locks can also be deleted from the database.

1. Select **List Locks** from the Program Locks Menu or select the  icon from the Program Locks screen.

The Unicon Locks List screen is displayed.



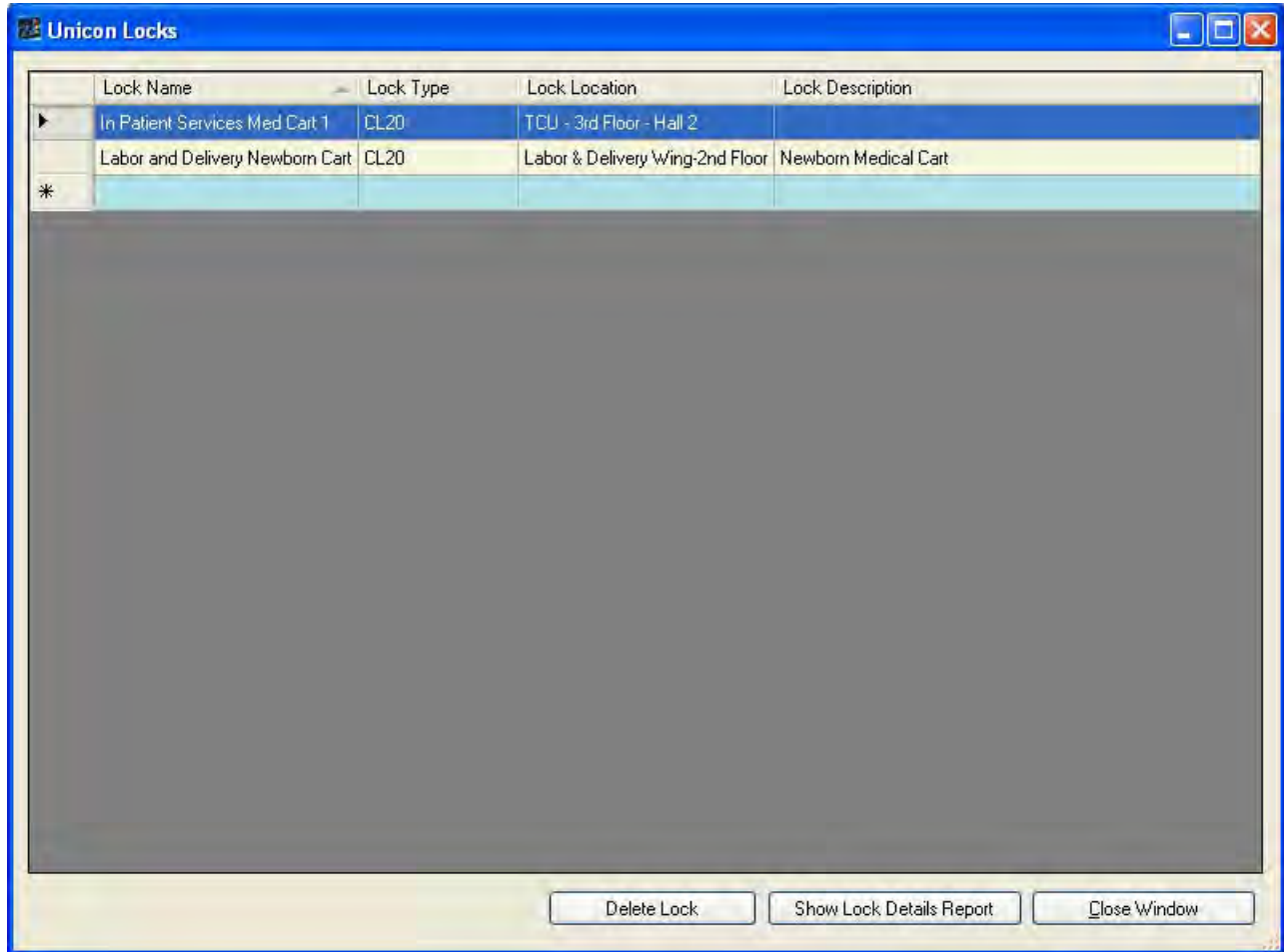
The list will display the locks specified for the Current Lock Interface (i.e., CL10) followed by any CL20 locks that have also been defined in the system.

The lock list display grid can be sorted on any of the four field columns by clicking on a specific column name tab at the top of the grid.

Delete Lock

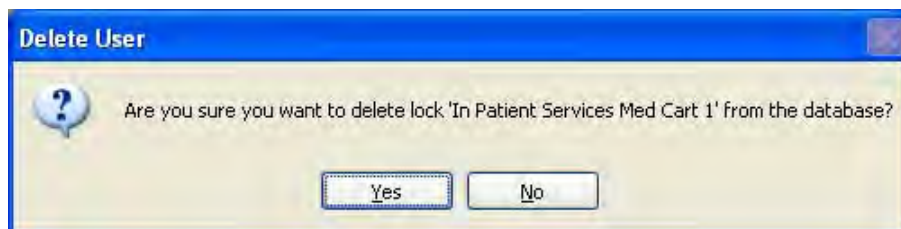
One option on the List Unicon Locks screen is “Delete Lock”. This item is used to delete a lock that no longer needs to be maintained in the system.

1. Select the lock in the list that is to be deleted from the system.



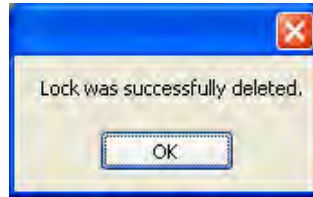
2. Click on the **Delete Lock** tab.

A prompt window is displayed asking for confirmation to delete the lock.



3. Click on **Yes** to delete the selected lock.

A message window is displayed to indicate that the lock was deleted successfully.

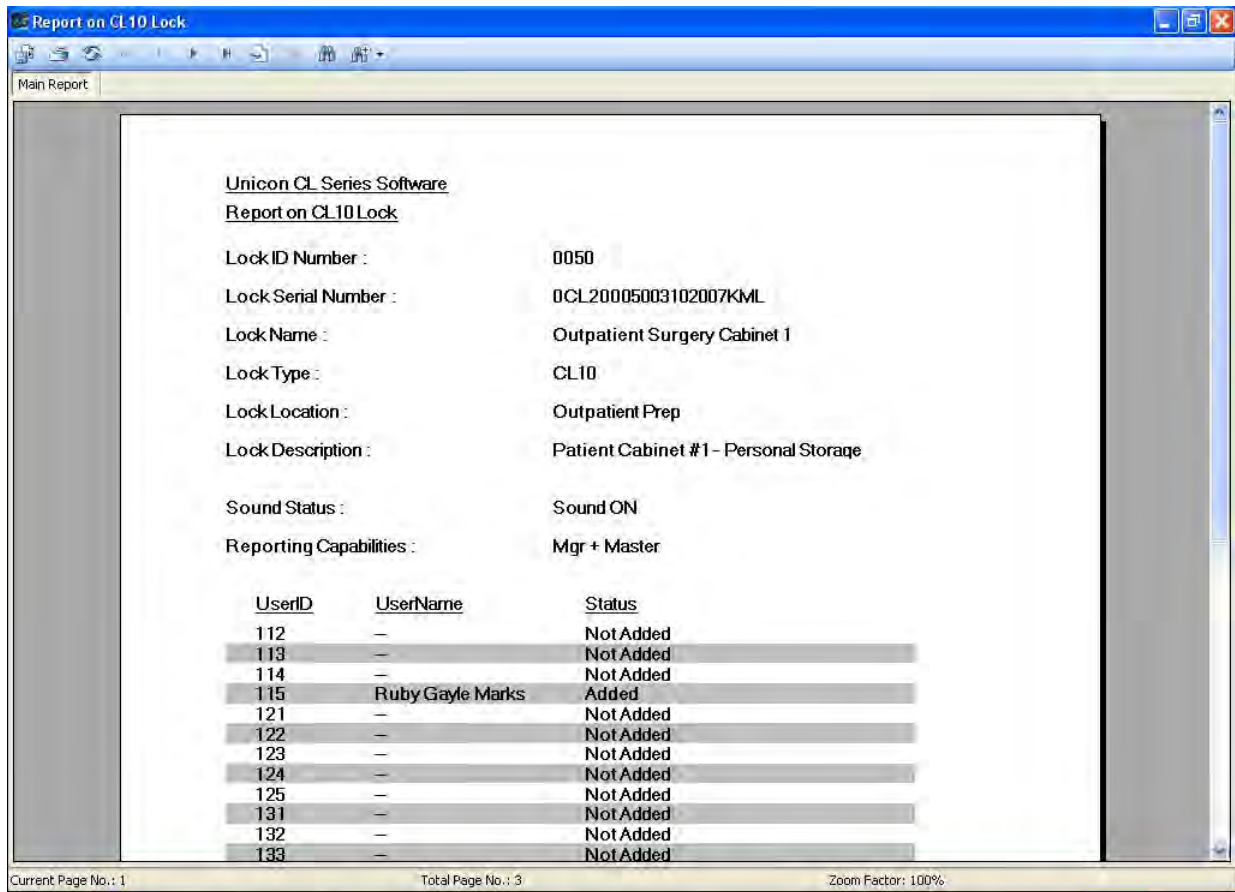


4. Click on **OK** to continue.

Show Lock Details Report

Another option on the List Unicon Locks screen is “Show Lock Details Report”. This option allows the details defined for an individual lock to be shown in Crystal report format.

1. Select the lock in the list for which you would like to view the Lock Details report.



There are standard functions available from the toolbar in all of the Crystal report formats.



The toolbar supports paging forward, backward, to the first, the last or a specific page within a report. It also supports a search function which allows users to search for a string within a report. The toolbar allows users to zoom in or out of a report with a zoom factor between 25 and 400. Additionally, the toolbar supports the ability to close or refresh a report page, print a report, and export a report.

You can change the Zoom on the report or page down to see more of the lock detail data.

Program Lock

The second option on the Locks menu is “Program Lock”. This menu item is used to initiate the program locks wizard. It should be selected to define the original lock setup data, users, and time windows for a lock.

Note: *The Program Lock operation requires a the teal programming key fob.*

If you choose the “Program the Lock” menu option from the Unicon CL Series PC software, you can define the following data in a lock:

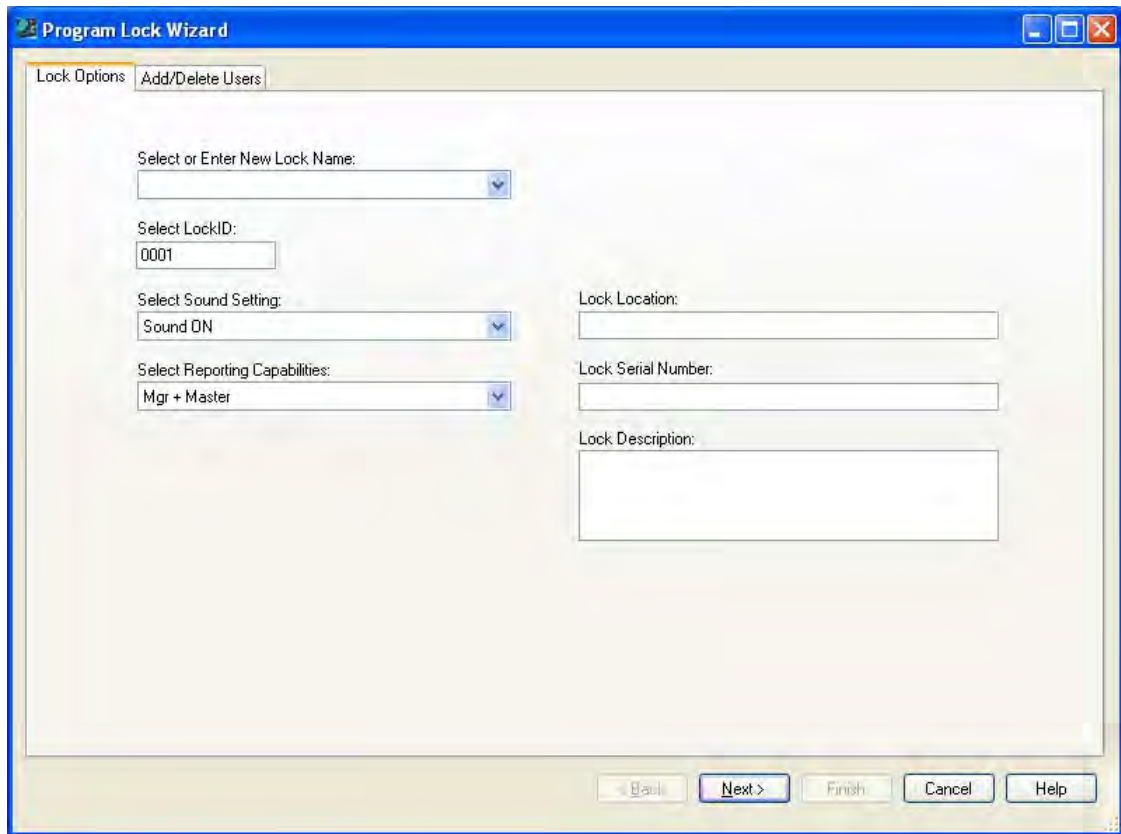
- Lock ID
- Sound ON/OFF
- Reporting Capabilities
- Users

Note: *The date and time in the lock will automatically be set to match the date and time of the PC when the lock is programmed with the programming key fob.*

1. Select **Program Lock**.

Program Lock - Lock Options

The **Program Lock - Lock Options** screen is displayed.



1. Enter the name for a new lock or select the name of a pre-existing lock that is being reprogrammed.

Note: *To program a new lock to replace a lock that had been previously programmed and is no longer functional, simply select the old lock name from the dropdown window.*

2. If you would like to assign a lock ID to the lock, enter a four-digit number (0001-9999) for the lock ID. Otherwise, you may leave the default of "0001" for no lock ID assignment. This ID can serve to uniquely identify a lock in an audit report.
3. Select whether you would like to have Sound turned "On or "Off" in the lock. The default value for the lock sound is "on".
4. Select the reporting capabilities for the lock. The default is Master and Manager Users, but you can also choose to restrict the reporting capabilities to only the Master User.
5. Enter a descriptive Lock Location.
6. Enter the Lock Serial Number.

Note: *The lock serial number can be found on the side of the lock chamber and also on the side of the box in which the lock was shipped.*

7. Enter a Lock Description.
8. Click on **Next** to continue.

Program Lock - Add/Delete Users

You will be prompted with the **Program Lock - Add/Delete Users** screen. You can assign users to a lock from a predefined User Group, assign users to the lock individually, or a combination of both.

Lock Options: Add/Delete Users

Lock Name: Outpatient Surgery Cabinet 1

Select User Group: [Empty Dropdown]

ID	User Name	Add or Update	Delete	Description
112		<input type="checkbox"/>	<input type="checkbox"/>	
113		<input type="checkbox"/>	<input type="checkbox"/>	
114		<input type="checkbox"/>	<input type="checkbox"/>	
115		<input type="checkbox"/>	<input type="checkbox"/>	
121		<input type="checkbox"/>	<input type="checkbox"/>	
122		<input type="checkbox"/>	<input type="checkbox"/>	
123		<input type="checkbox"/>	<input type="checkbox"/>	
124		<input type="checkbox"/>	<input type="checkbox"/>	
125		<input type="checkbox"/>	<input type="checkbox"/>	
131		<input type="checkbox"/>	<input type="checkbox"/>	
132		<input type="checkbox"/>	<input type="checkbox"/>	
133		<input type="checkbox"/>	<input type="checkbox"/>	
134		<input type="checkbox"/>	<input type="checkbox"/>	
135		<input type="checkbox"/>	<input type="checkbox"/>	
141		<input type="checkbox"/>	<input type="checkbox"/>	
142		<input type="checkbox"/>	<input type="checkbox"/>	

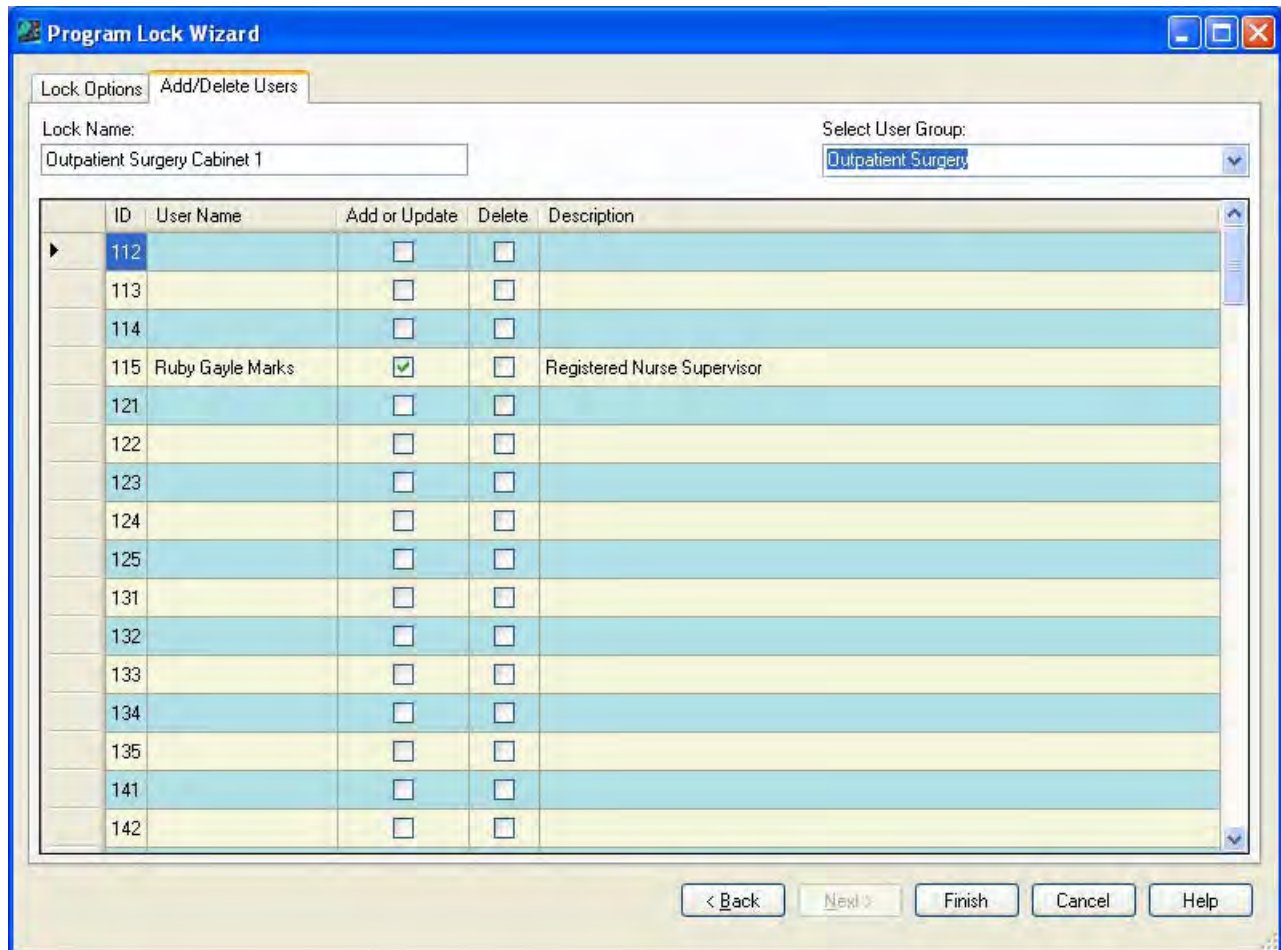
< Back Next > Finish Cancel Help

Assign Users to Lock from User Group

If you want to assign users to the lock from a predefined User Group, complete the following steps:

1. Select the User Group from the Select User Group dropdown window.

The fields will be filled with the predefined users for the User Group.

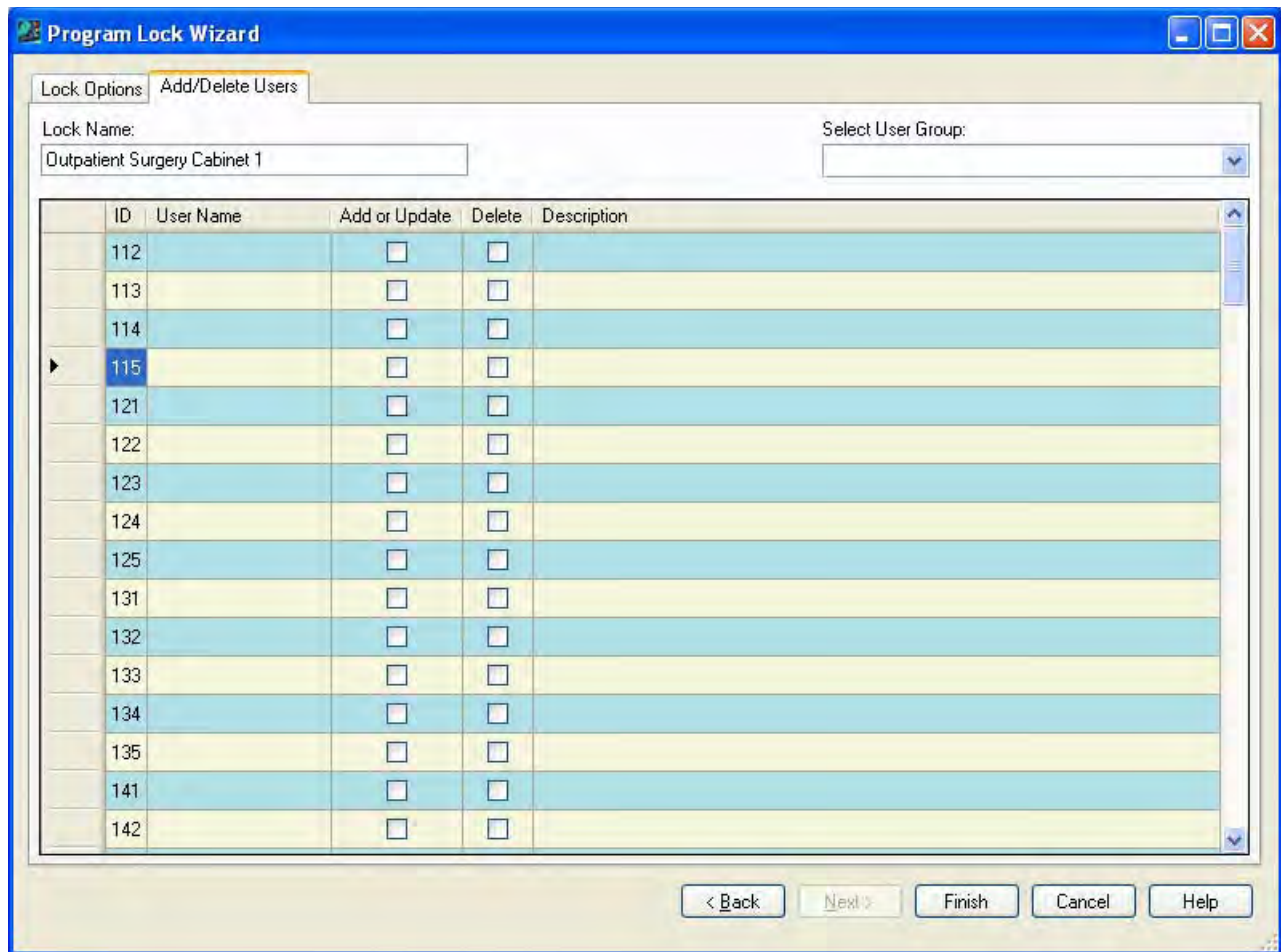


2. Click on **Next** to continue.

Assign Users to Lock

If you want to assign users to the lock individually, complete the following steps:

1. Select the User ID to which you want to assign a user for the lock.

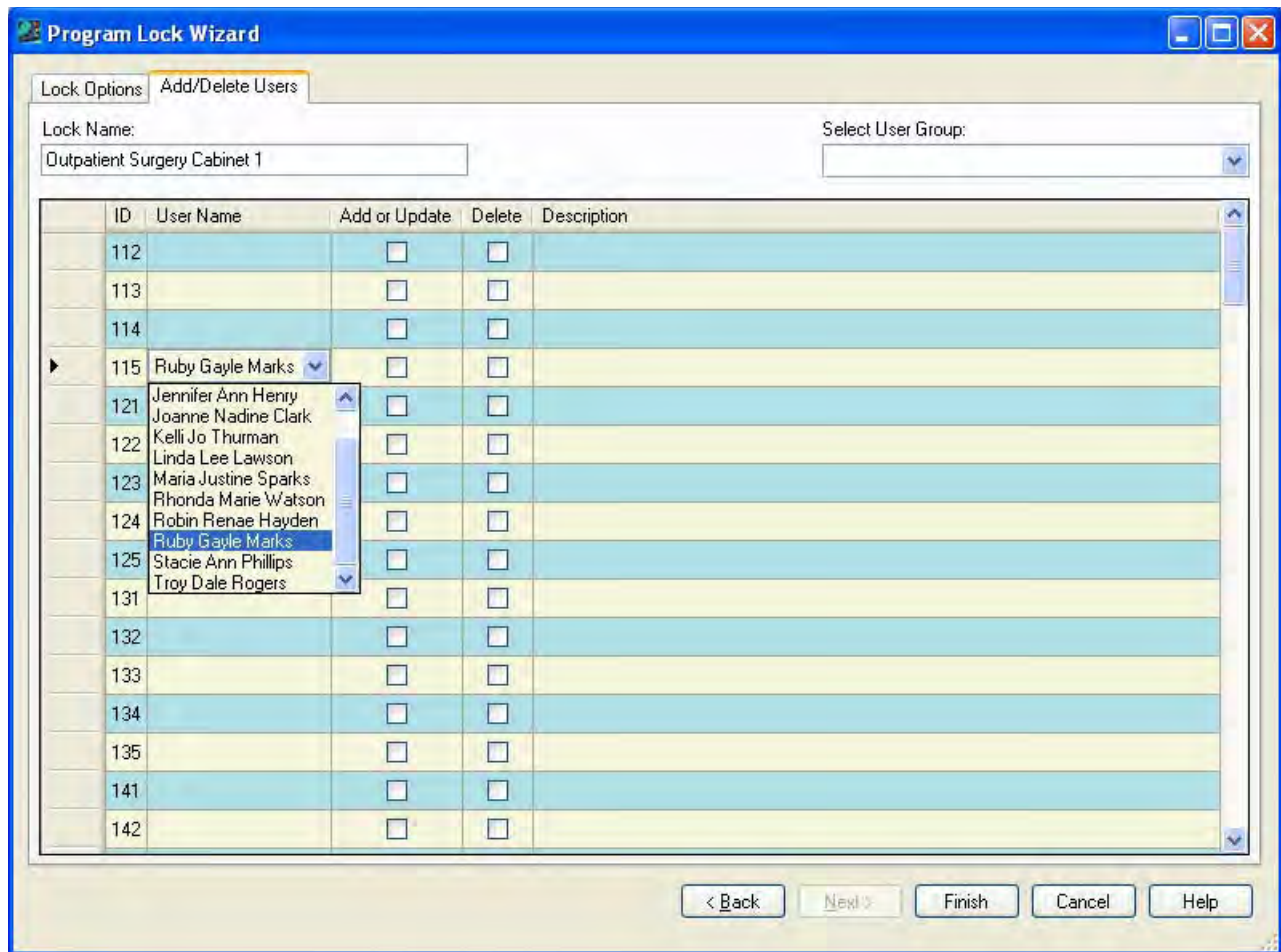


2. Click on the User Name field in the same line as the selected User ID.

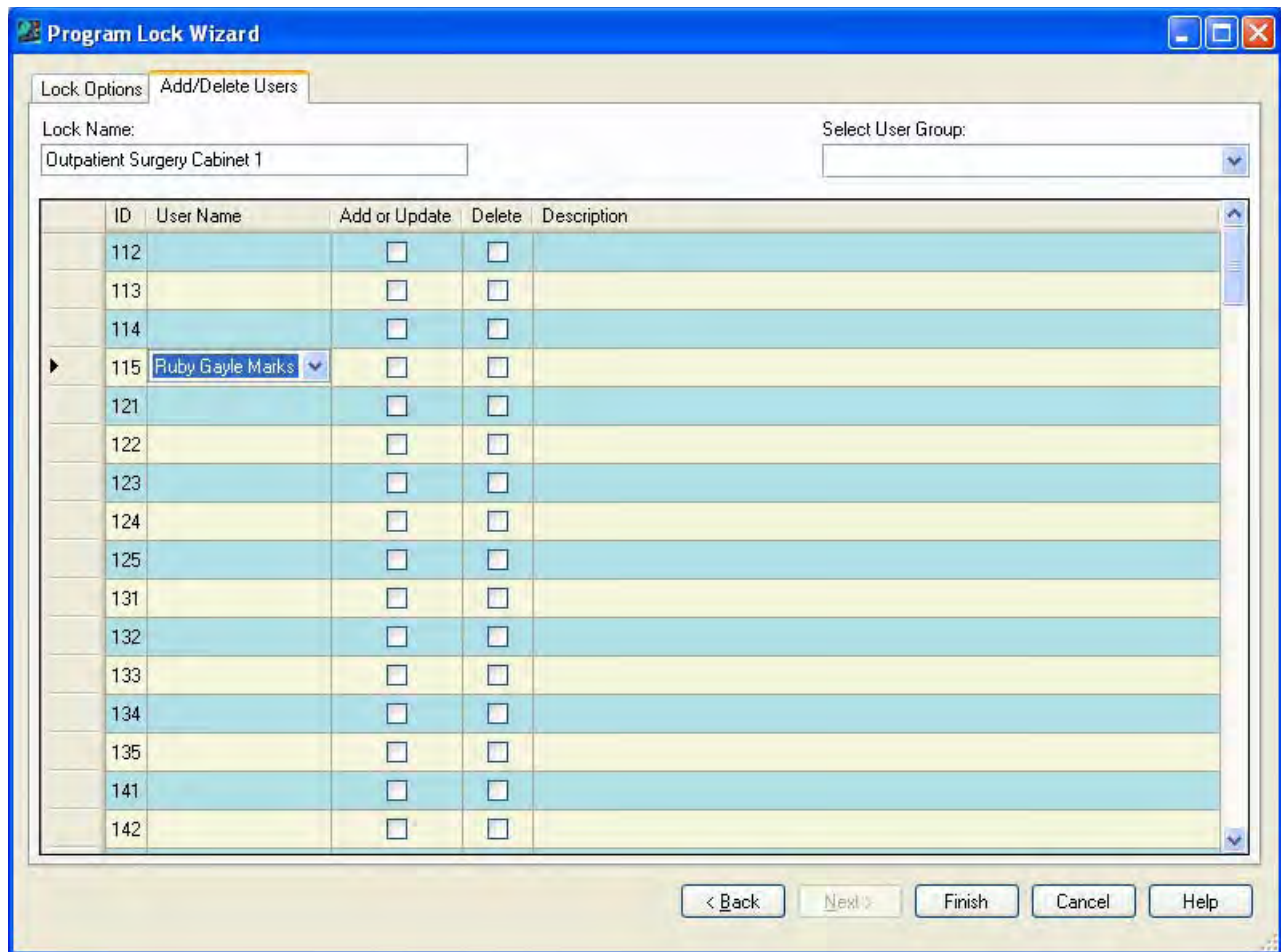
A dropdown box arrow will appear on the right hand side of the field.

3. Select a user name from the dropdown selection box.

Helpful Hint: You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.



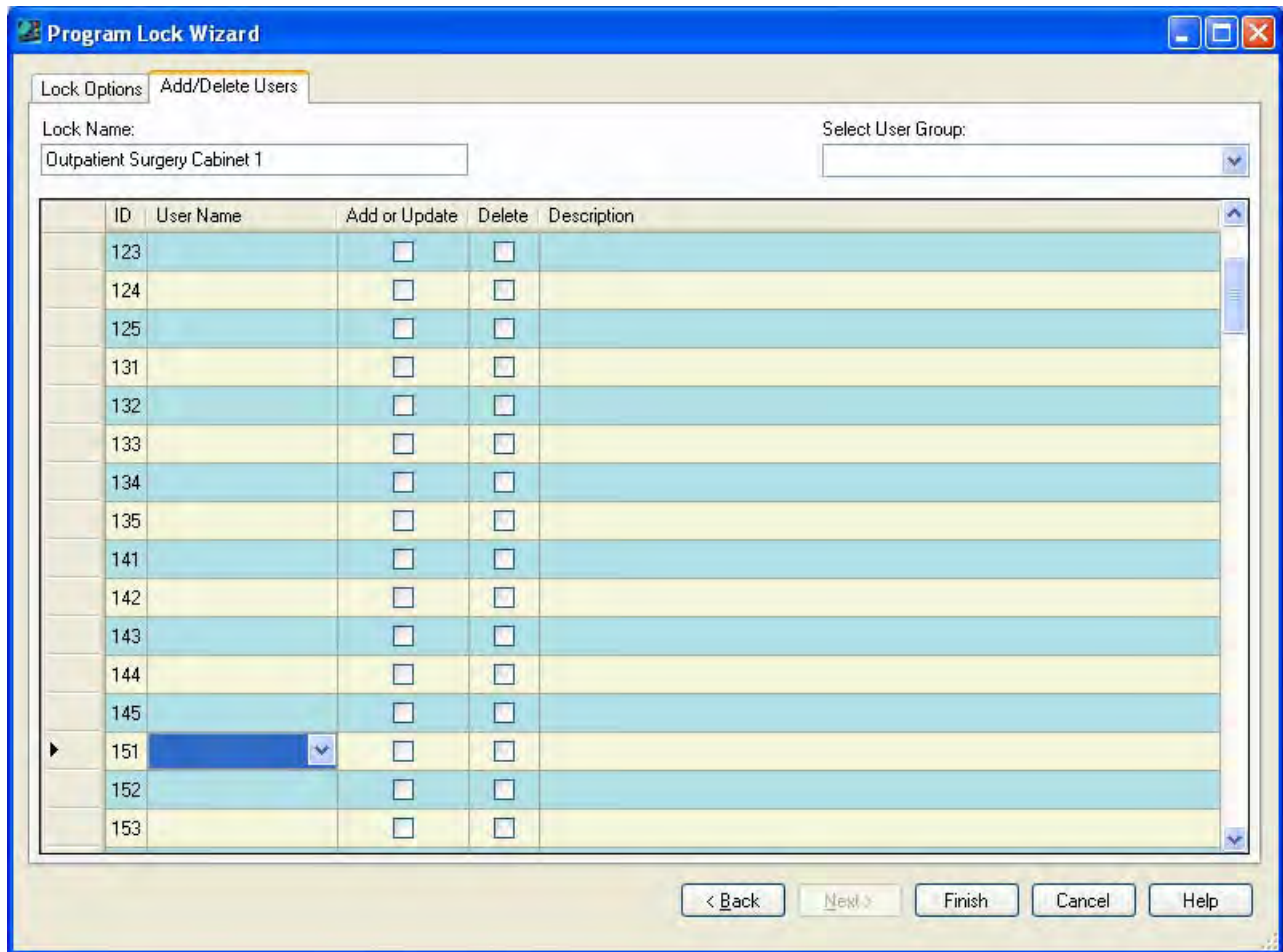
The selected name will fill the window.



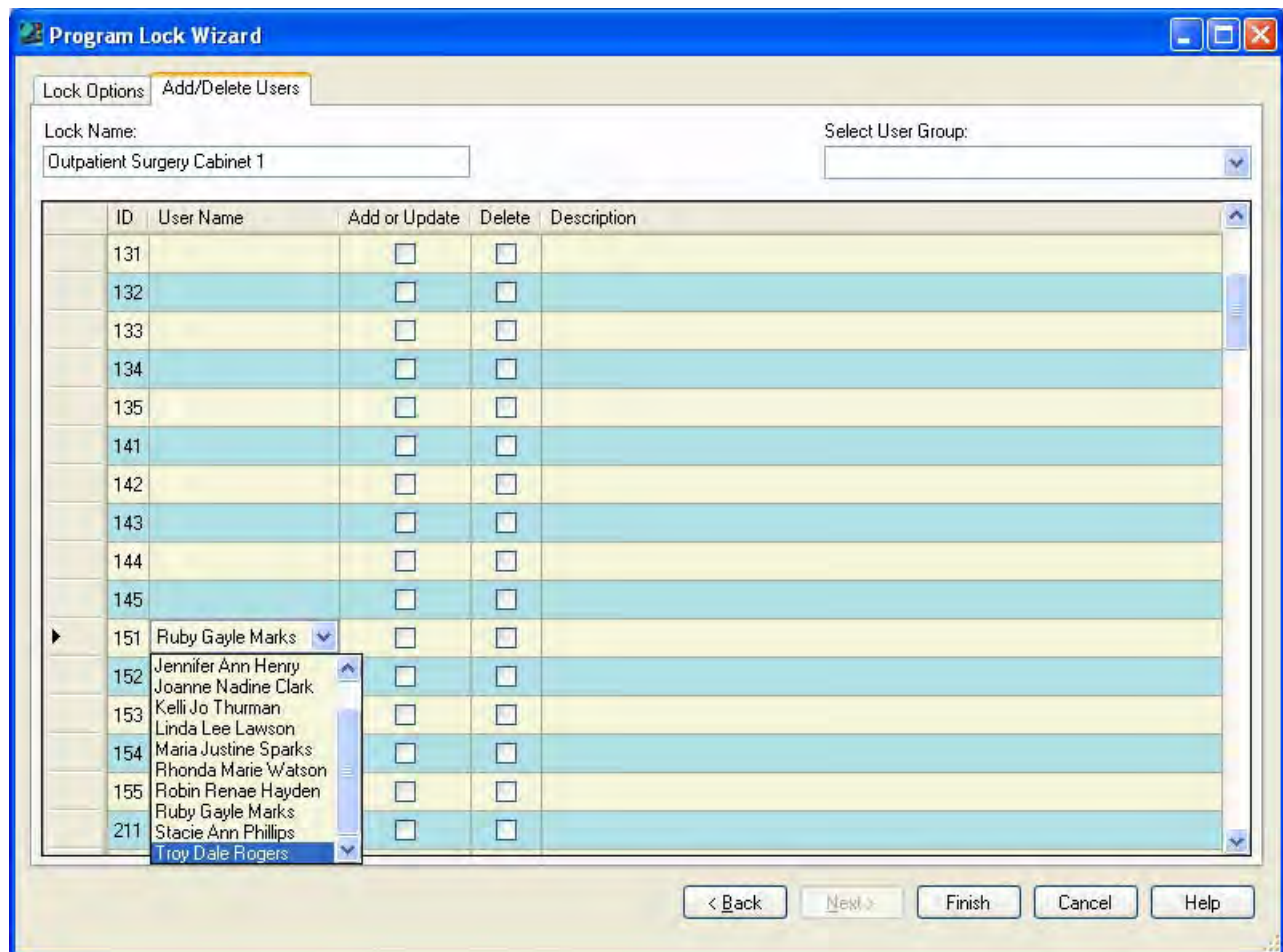
Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

4. Select the next User ID you want to assign to a user for this user group.
5. Click on the User Name field in the same line as the selected User ID.

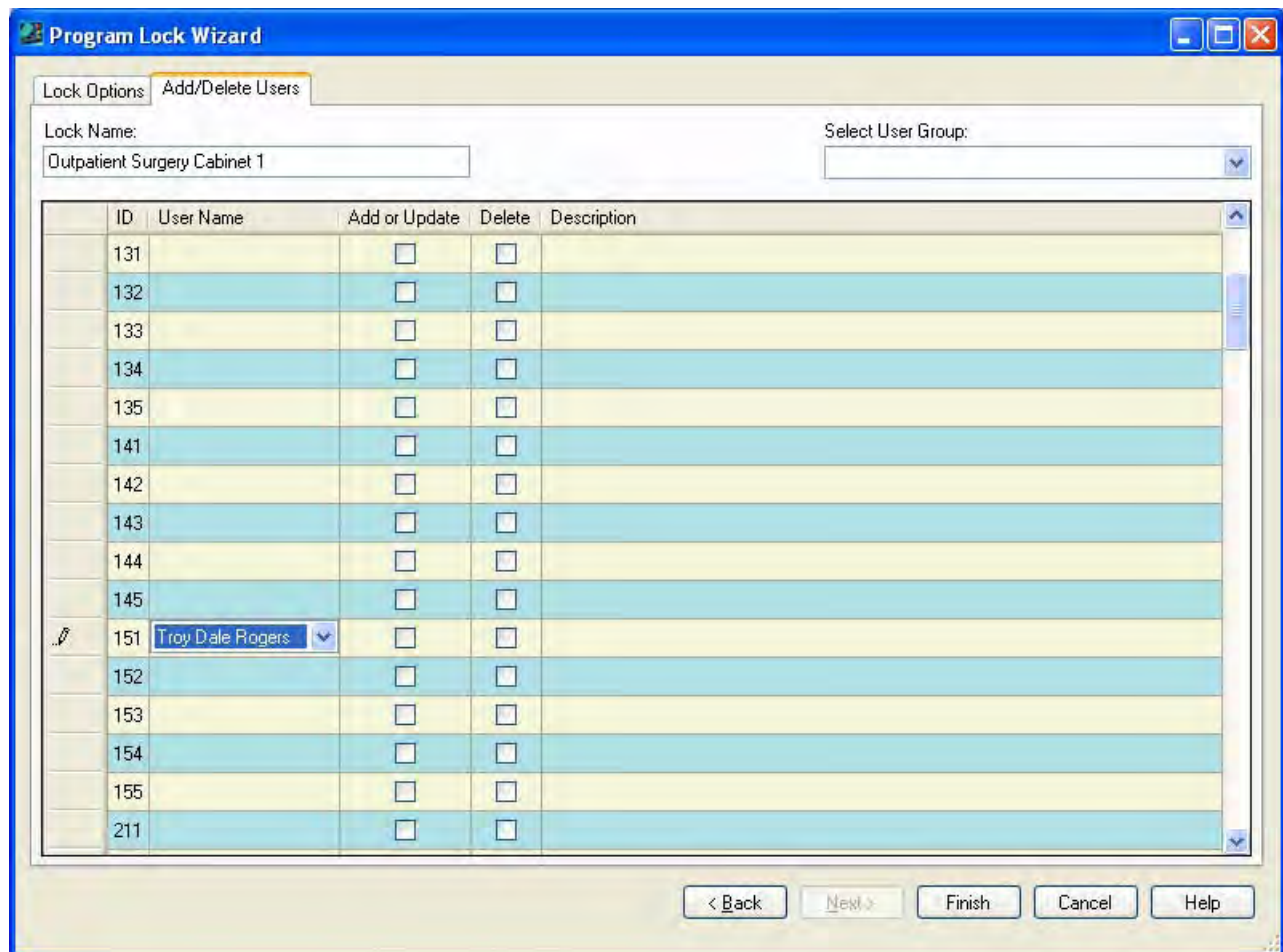
A dropdown box arrow will appear on the right hand side of the field.



6. Select a user name from the dropdown selection box.

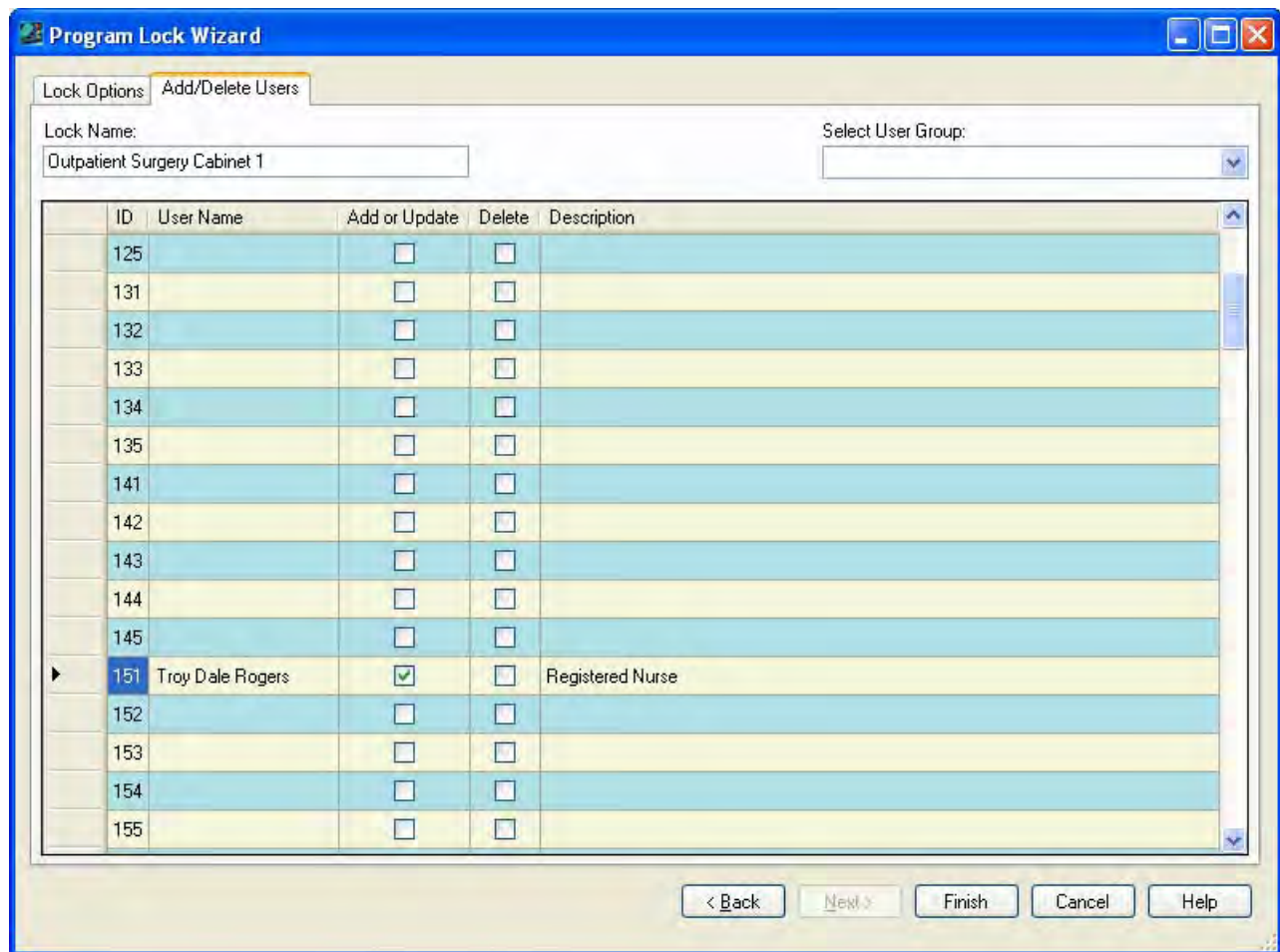


The selected name will fill the window.



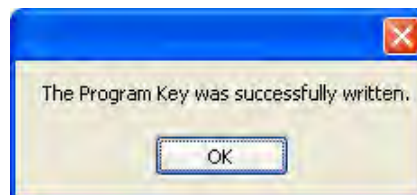
7. Click on the User ID field for the user just added.

The **Add or Update** column should now be checked for the user to be added to the lock.



8. Continue repeating the steps to add another user to the lock until all users have been defined.
9. Once all user assignments are defined, ensure that the appropriate columns are checked for the users to be added to the lock and that a Programming Key Fob has been attached to the data cable.
10. Click on **Finish**.

The following message window is displayed to indicate that the Program Key was written successfully.



11. Click on **OK**.

12. The programming key fob should now be taken to the lock to program the lock data.

Note: *Previous to uploading any data to a lock, the Master User PIN must be "set" in the lock. The default PIN assigned to the Master User is "12345". The default PIN assigned to new Manager Users is "55255". A Manager User must change this default PIN before any lock operations can be performed. See the **Unicon CL10 Operating Instructions** for further detail.*

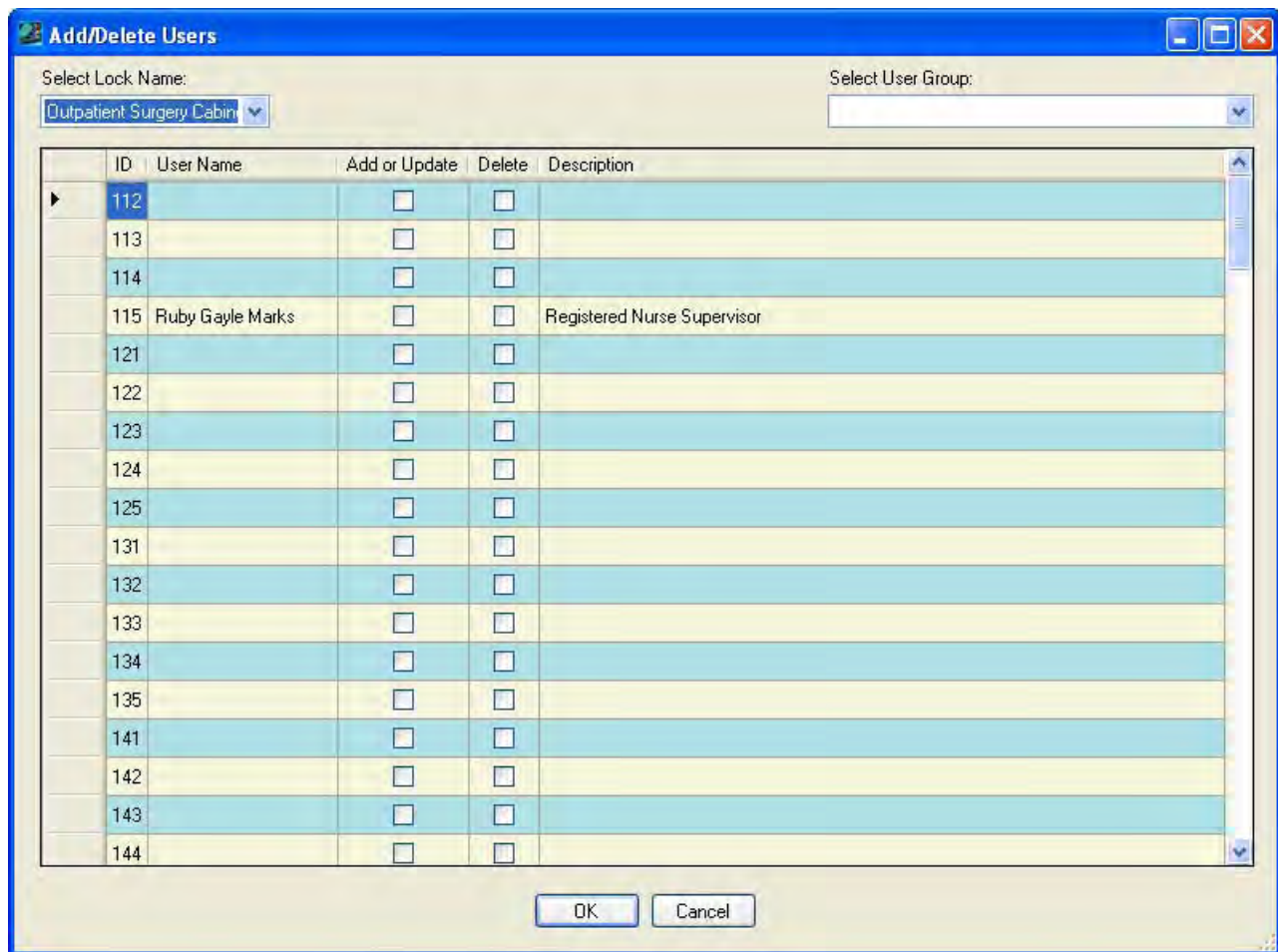
Program Lock Users

This option is used to add and/or delete users to or from a lock using a Programming Key Fob. The option should be selected only to add or delete users to a lock that has already been programmed.

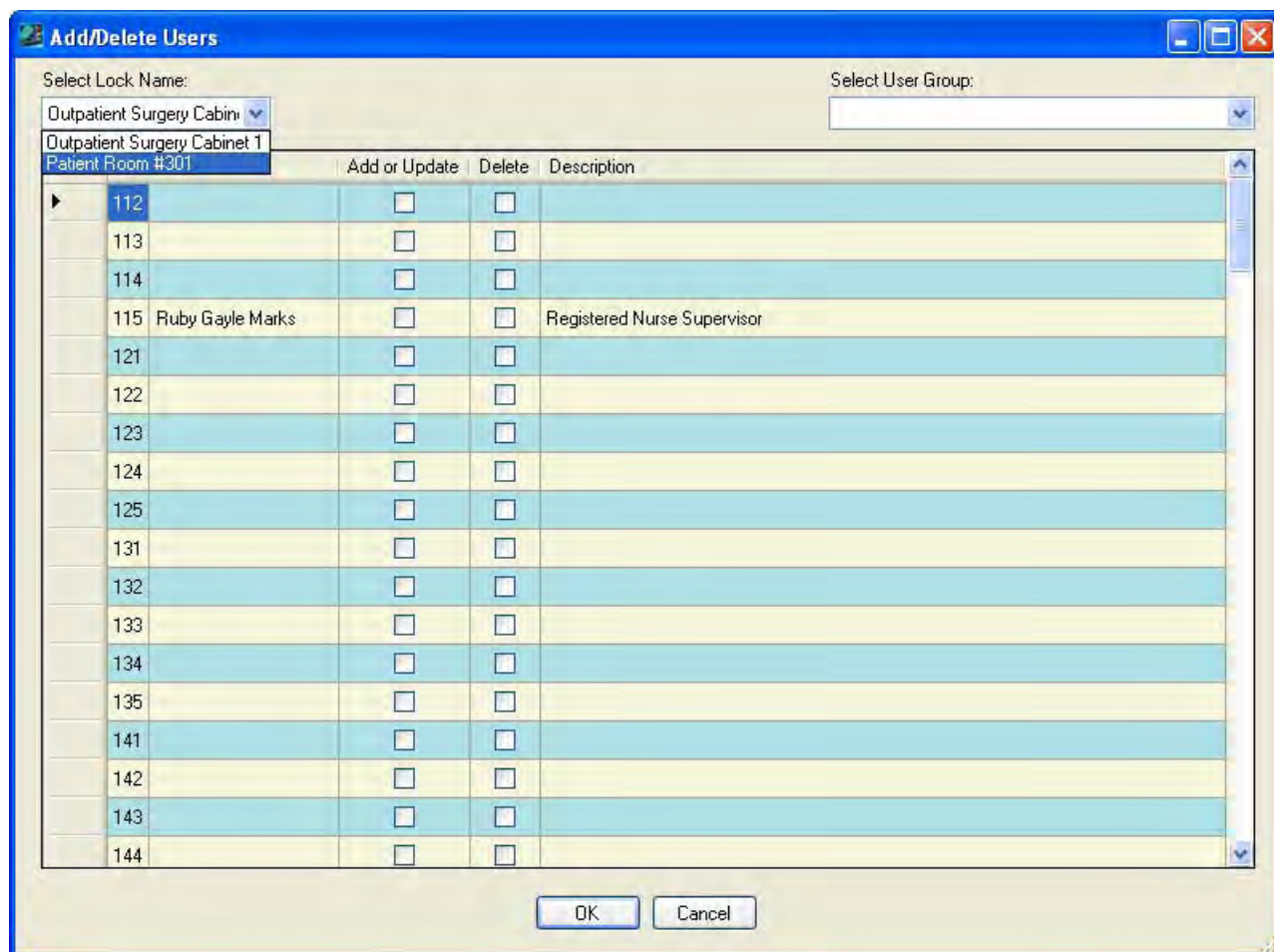
1. Select **Program Lock Users**.

The "Add/Delete Users" screen is displayed.

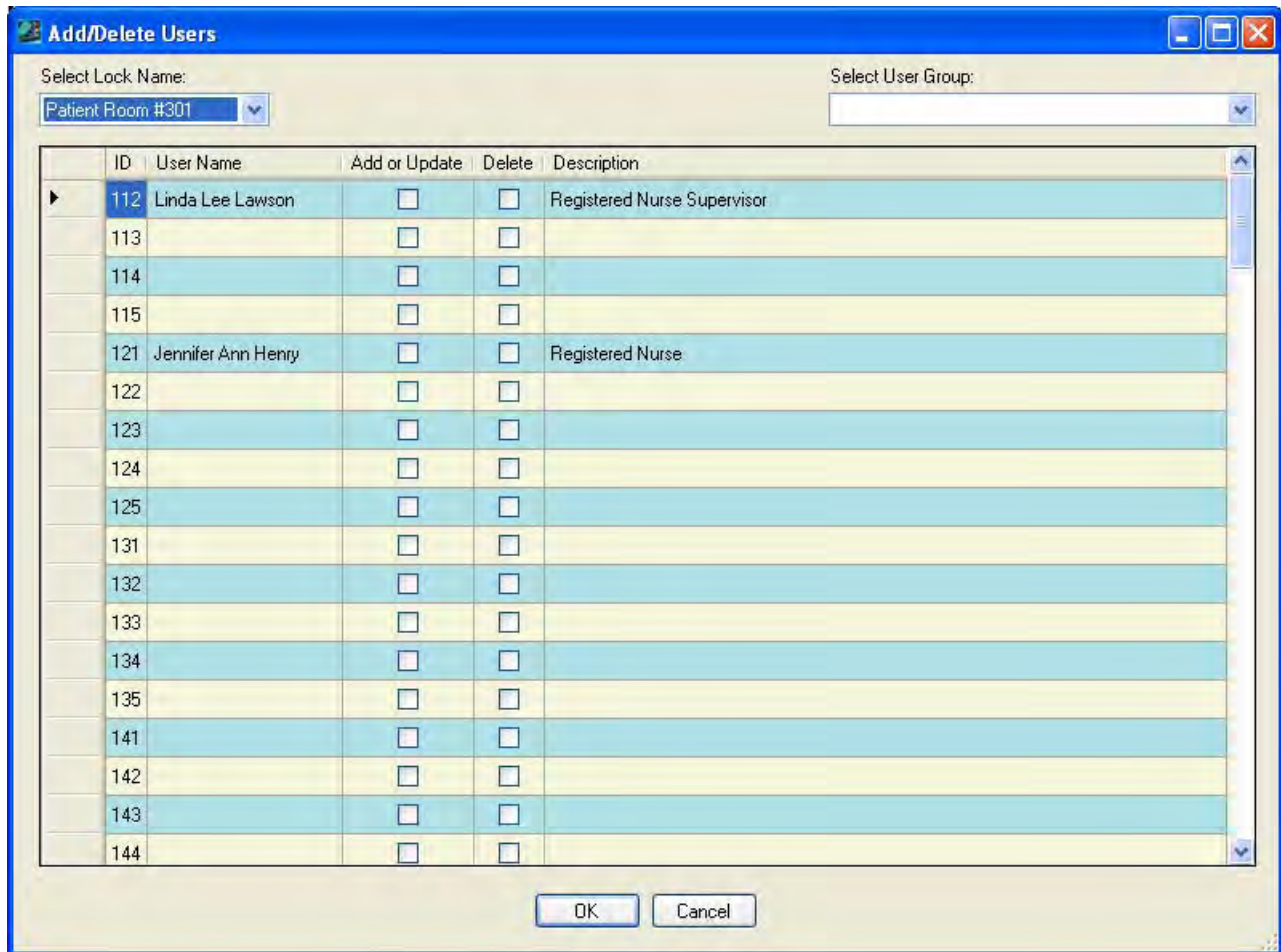
Note: *The first lock (in alphabetical order) is shown as the default.*



2. Select the name of the lock to which you want to add/delete users.



Once the lock is selected, the lock mode will be displayed along with the users currently assigned to the lock.

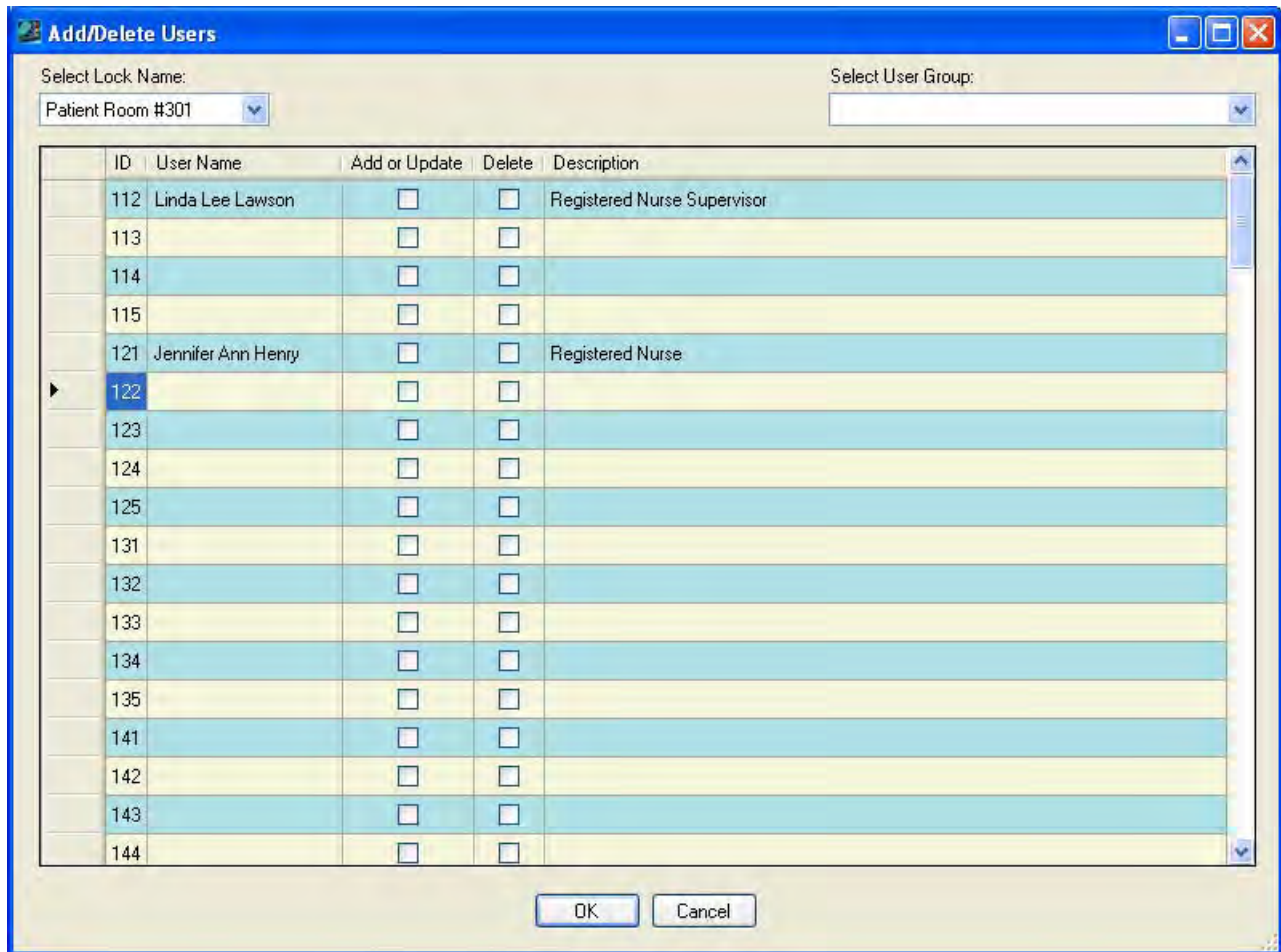


Caution: Do not click on **OK** until you have completed **all** user changes for the lock. Clicking on **OK** will actually write the add/update/delete user information to the database and to the Programming Key Fob.

Add Users to the Lock

If you want to add new users to the lock, complete the following steps for each user to be added:

- 3a. Select the User ID to which you want to assign a new user for the lock.

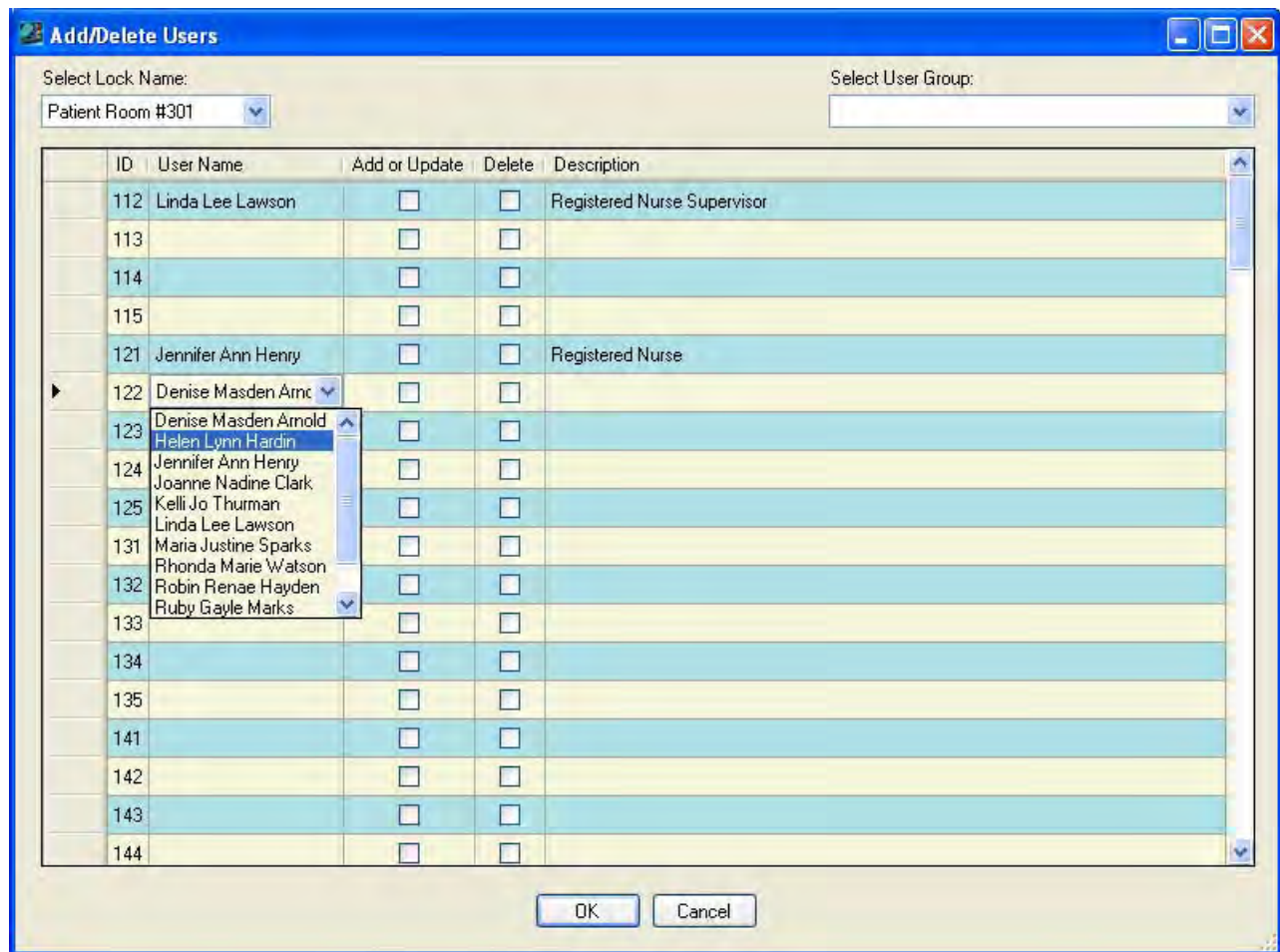


3b. Click on the User Name field in the same line as the selected User ID.

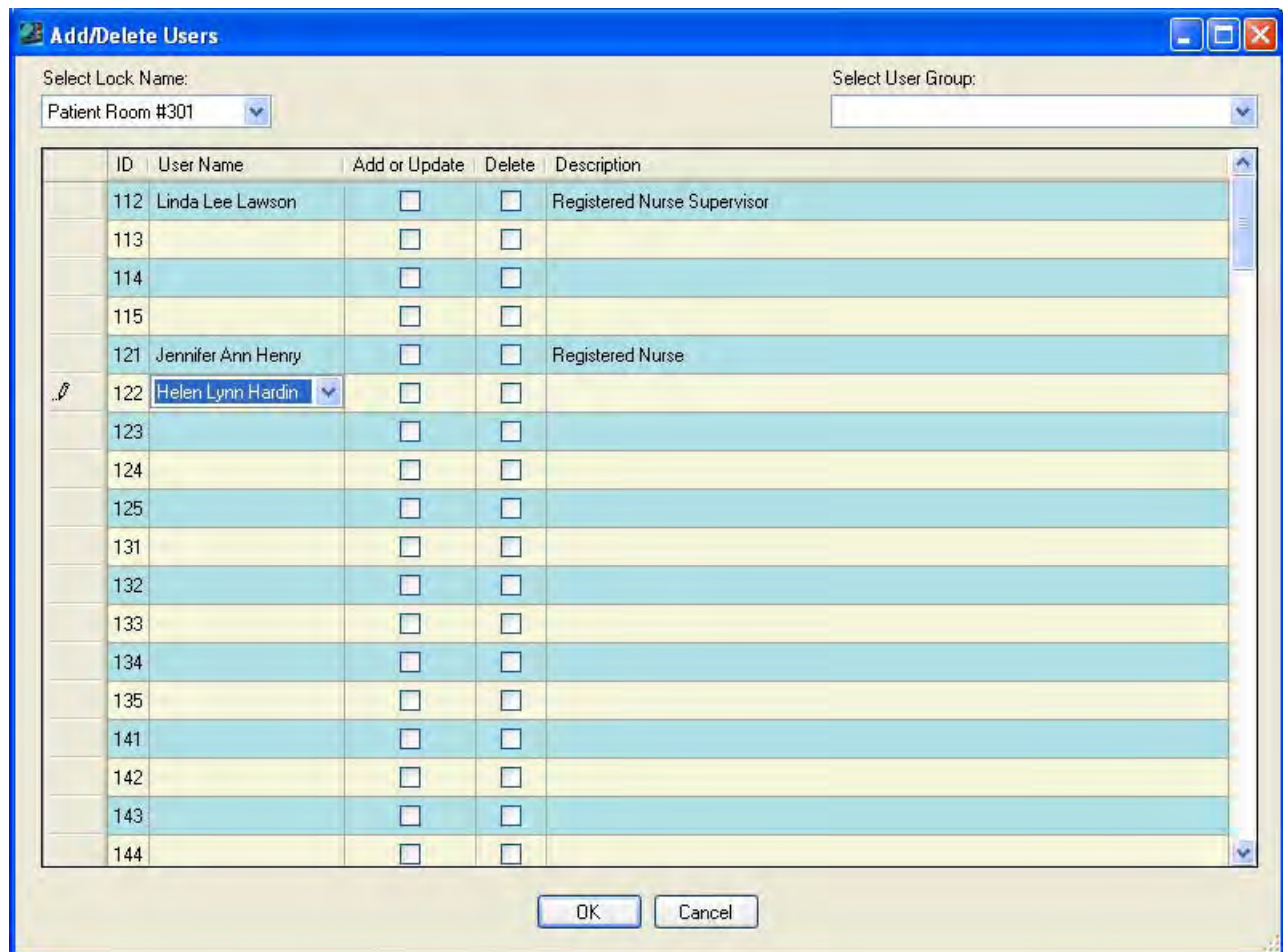
A dropdown box arrow will appear on the right hand side of the field.

3c. Select a user name from the dropdown selection box.

Helpful Hint: You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.

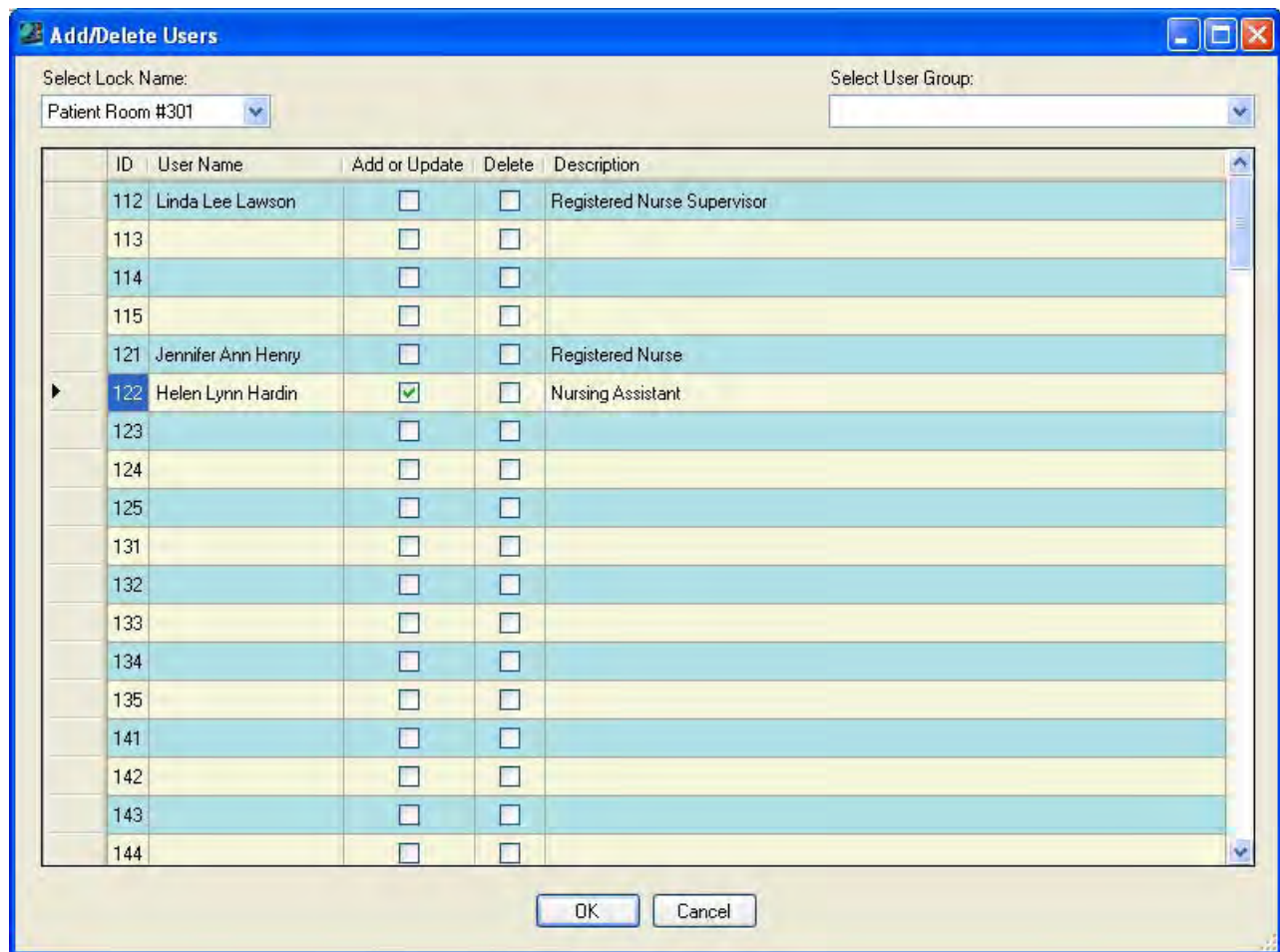


The selected name will fill the window.



Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name and then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

3d. Click on the User ID field for the user just added.

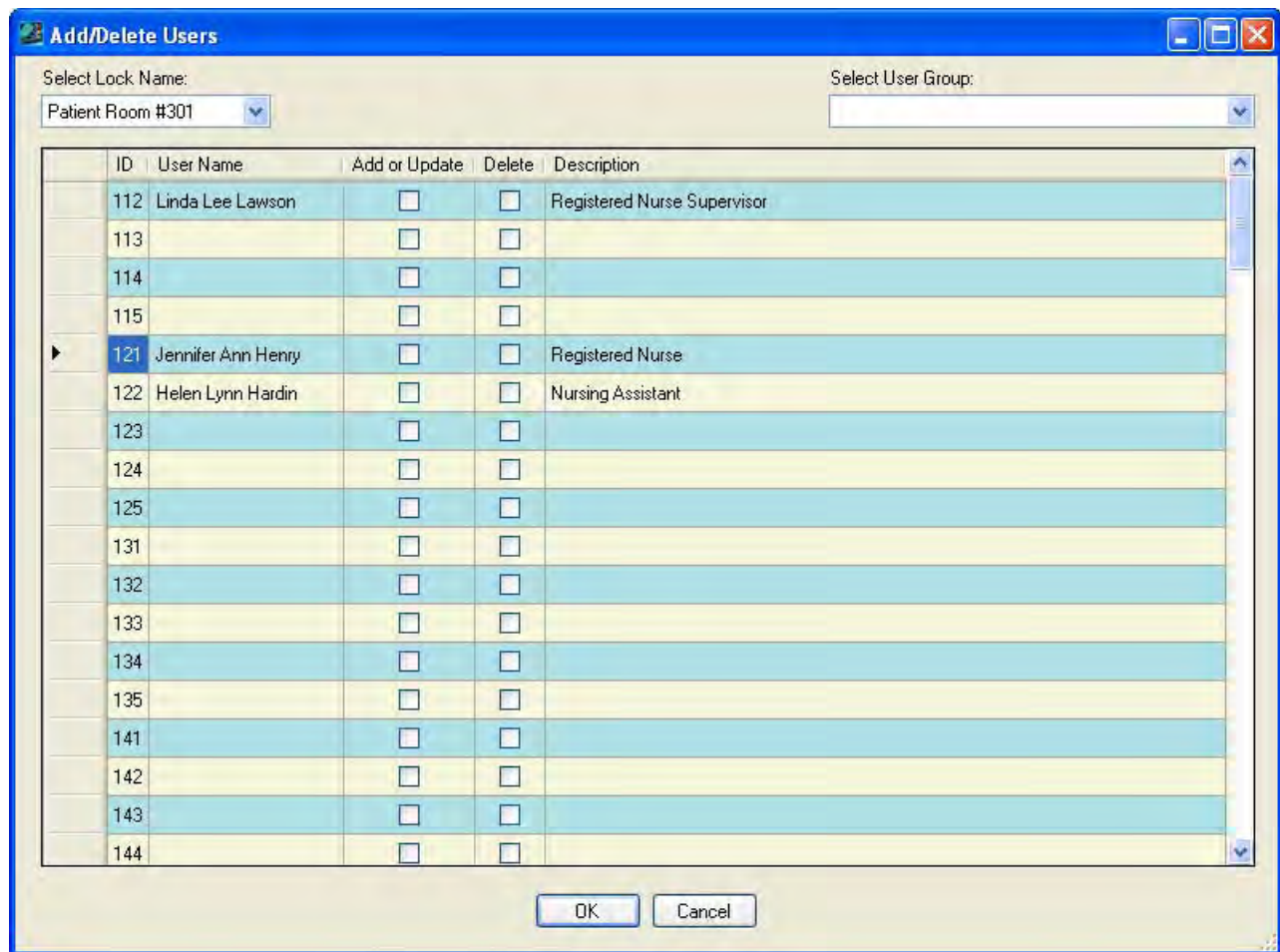


The **Add or Update** column should now be checked for the user to be added to the lock.

Change User ID Assignment

If you want to change the user who is currently assigned to a User ID, complete the following steps for each User ID assignment to be changed:

- 3a. Select the User ID to which you want to assign a different user for the lock.

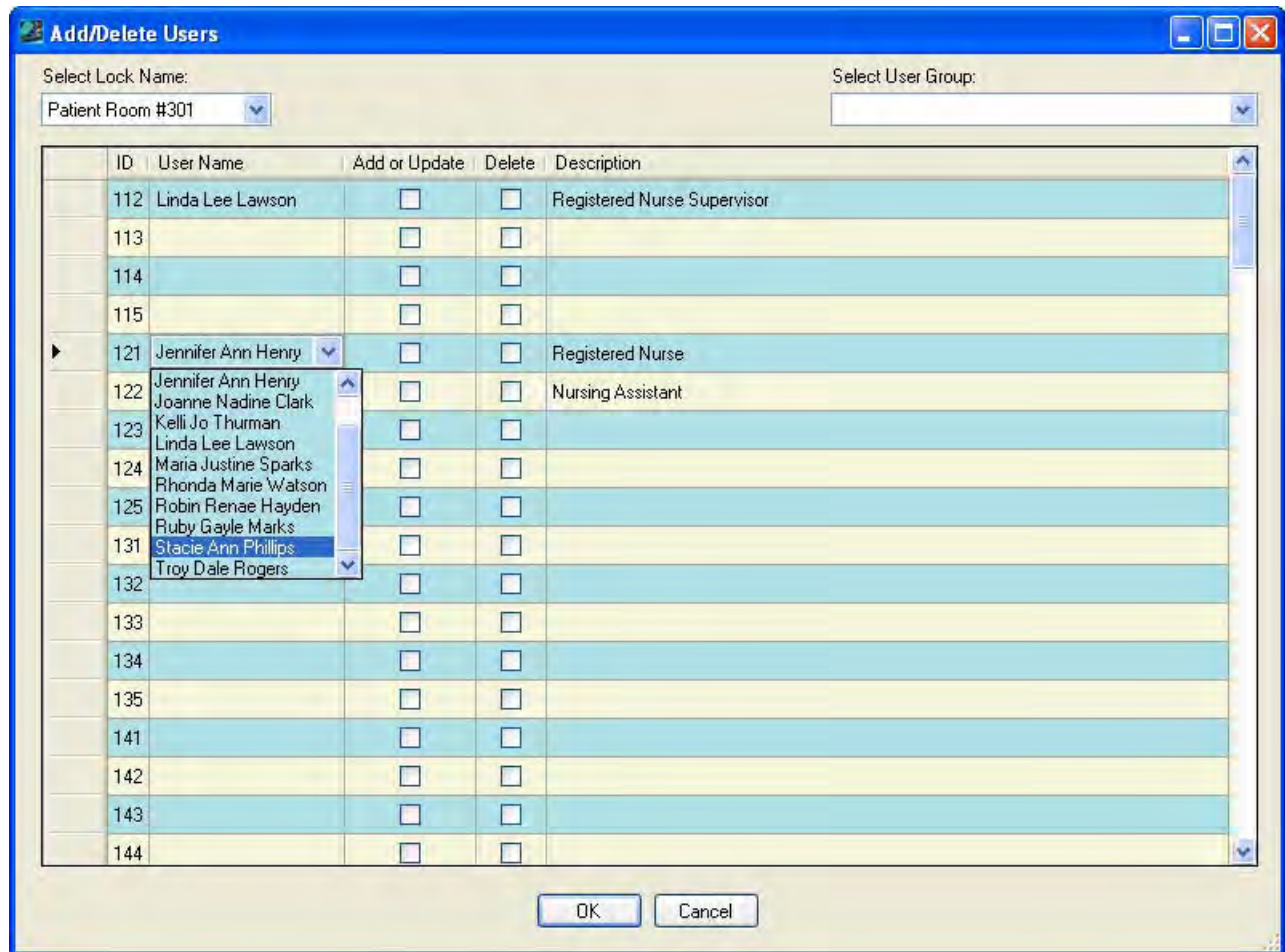


3b. Click on the User Name field in the same line as the selected User ID.

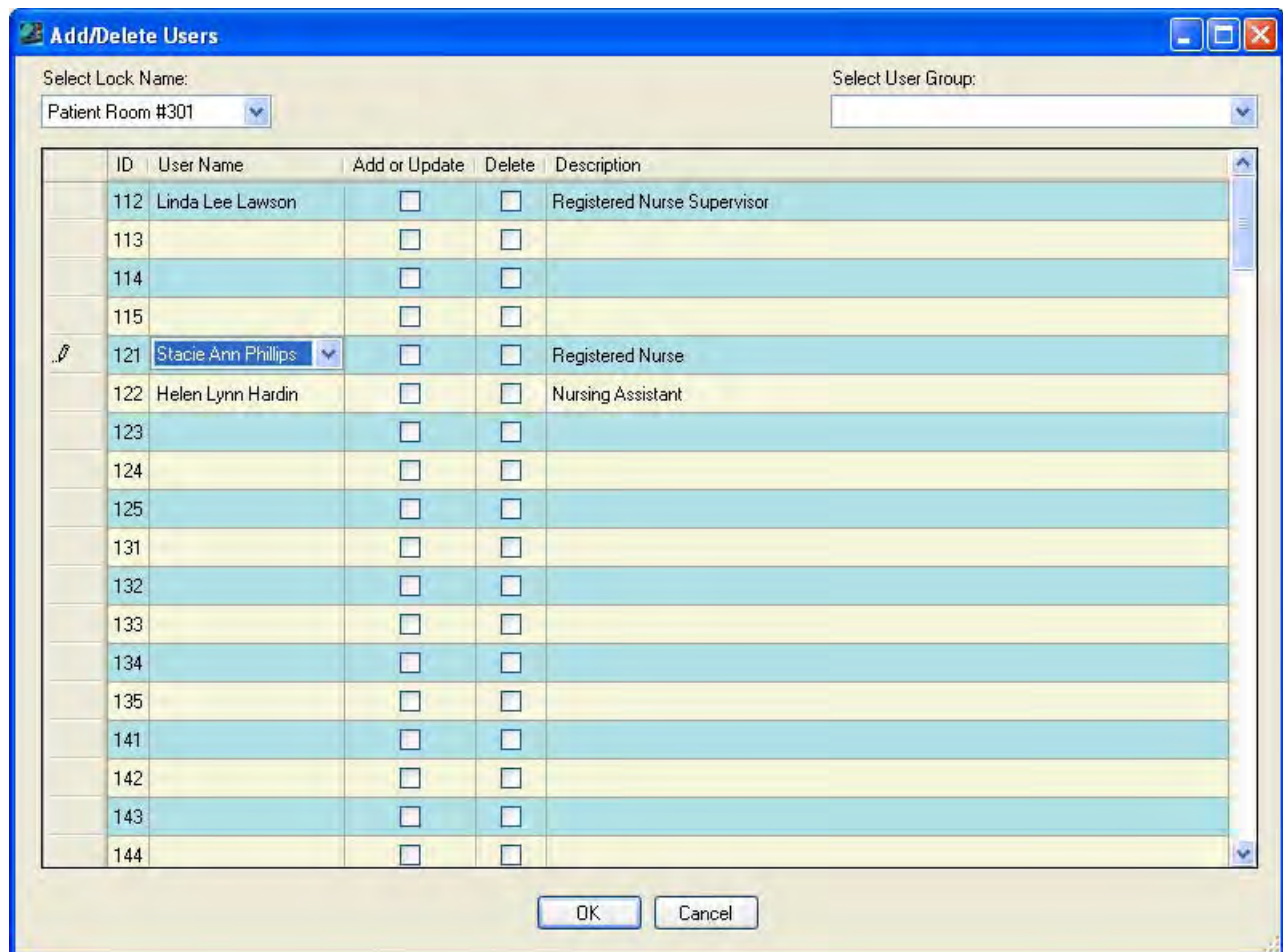
A dropdown box arrow will appear on the right hand side of the field.

3c. Select a different user name from the dropdown selection box.

Helpful Hint: You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.

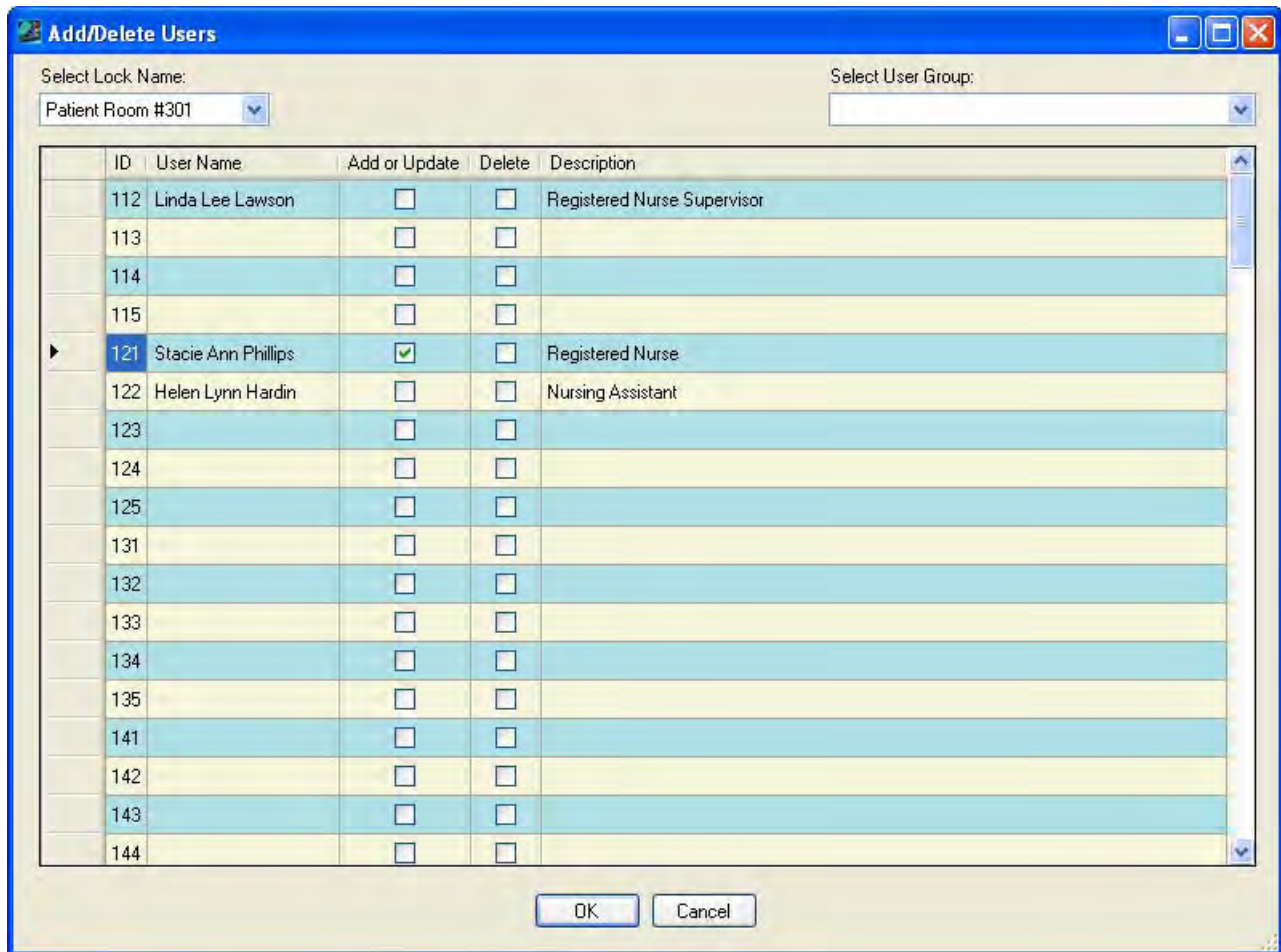


The selected name will fill the window.



Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name and then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

3d. Click on the User ID field for the user just updated.

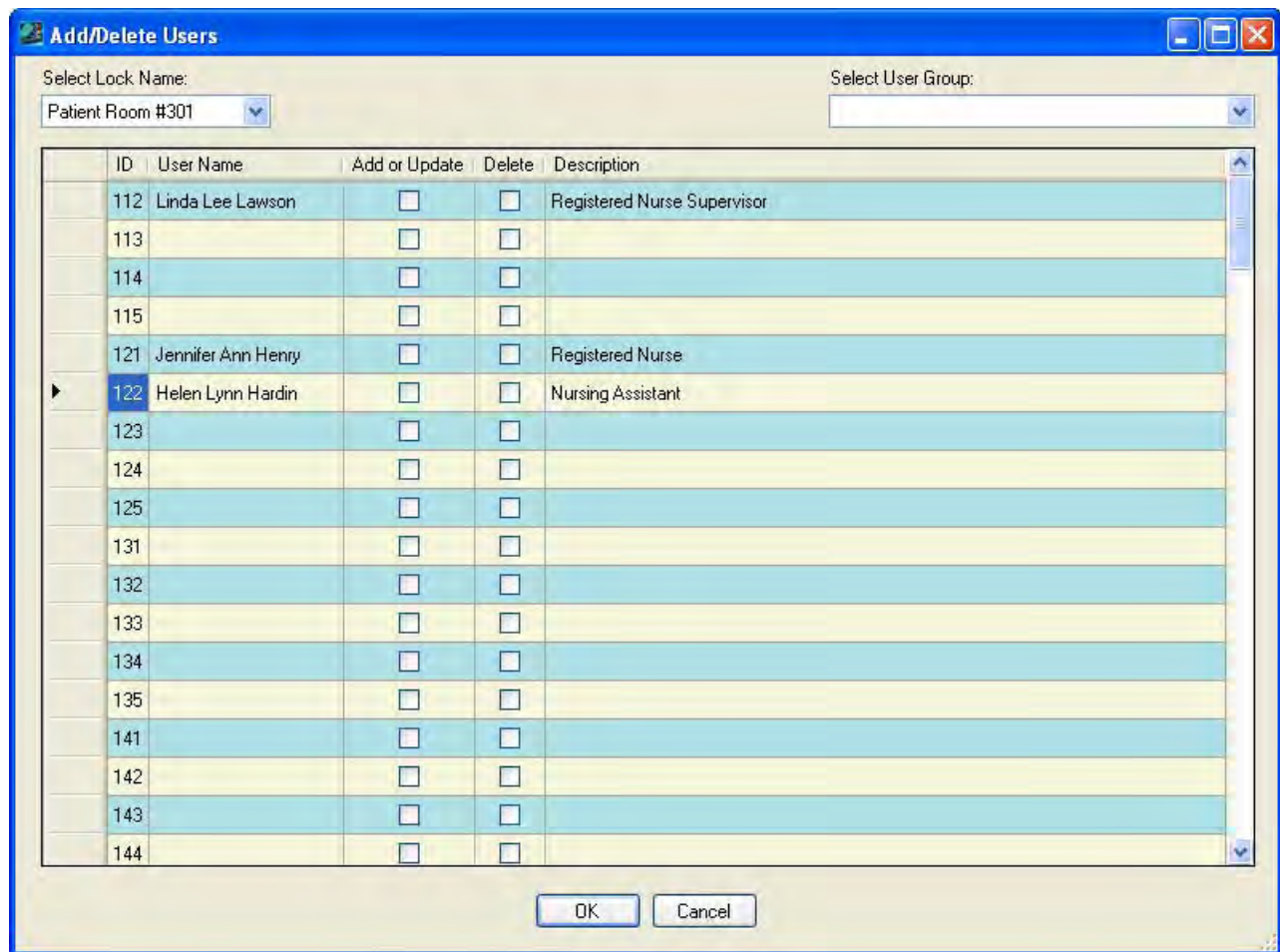


The **Add or Update** column should now be checked for the user to be updated in the lock.

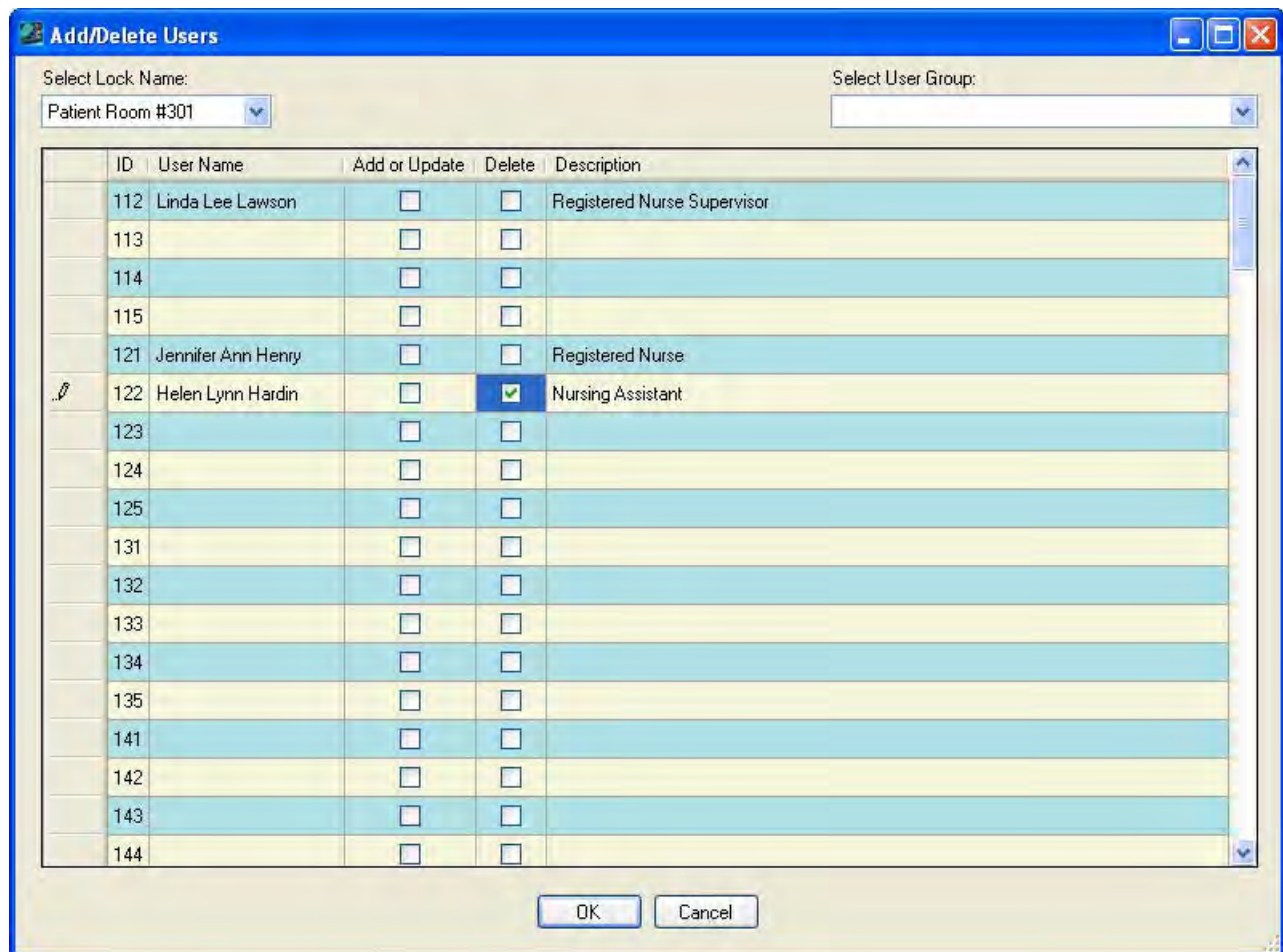
Delete Users from Lock

If you want to delete users from the lock, complete the following steps for each user to be deleted:

- 3a. Select the User ID that you want to delete from the lock.



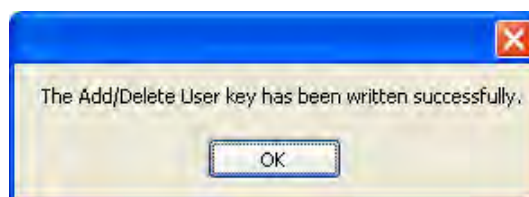
3b. Click on the **Delete** box for the User ID that you want to delete from the lock.



Write to the Key

- When all settings are complete and all desired users have been added/updated/ deleted appropriately, ensure that the Programming Key Fob has been attached to the Unicon data cable.
- Click on the **OK** button.

A message window will be displayed indicating that the Add/Delete key was written successfully.



- Click on **OK** to return to the Lock Options screen.

7. The key should now be taken to the lock to add/delete users to/from the lock.

Note: *Previous to uploading any data to a lock, the Master User PIN must be "set" in the lock. The default PIN assigned to the Master User is "12345". The default PIN assigned to a new Manager User is "55255". A Manager User must change this default PIN before any lock operations can be performed. See the **Unicon CL10 Operating Instructions** for further detail.*

Program Lock Date & Time

This option allows the current date and time to be uploaded to the lock.

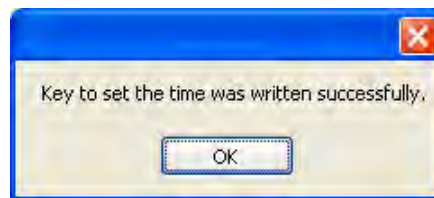
Time in the Unicon locks does not automatically adjust for Daylight Savings Time so must be adjusted via manual programming at the lock or via a Programming Key Fob programmed at the software.

If you change the batteries in the lock, you might also need to reset the date and time in the lock.

From the Locks menu:

1. Ensure that a programming key fob has been attached to the Unicon data cable and select **Program Lock Time**.

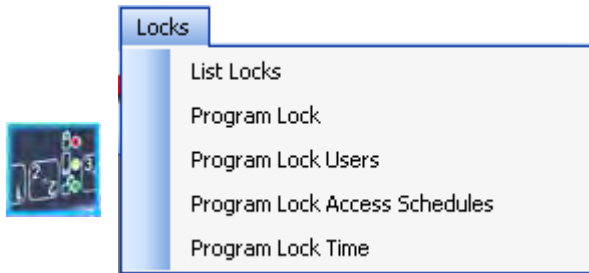
The following message window is displayed to indicate that the key to set the date and time was written successfully.



2. Click on **OK**.
3. The programming key fob should now be taken to the lock to program the lock date and time.

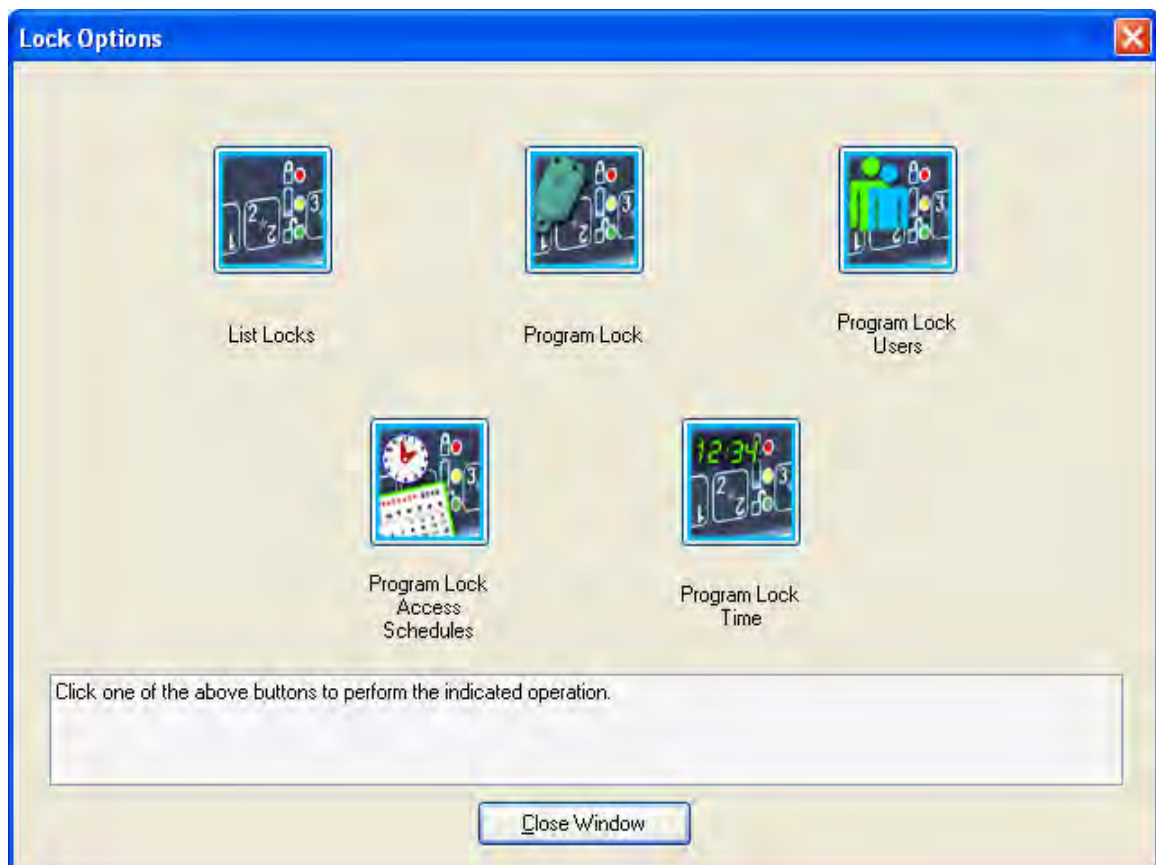
Note: *Previous to uploading any data to a lock, the Master User PIN must be "set" in the lock. The default PIN assigned to the Master User is "12345". See the **Unicon CL10 Operating Instructions** for further detail.*

Locks Menu - CL20




List Locks or Program Lock Information

The Locks Menu options for the Model CL20 software interface allow you to program the lock, add/delete users, set access schedules, or set the date and time in the lock. The Locks menu options can also be accessed by selecting the Locks icon from the Toolbar.




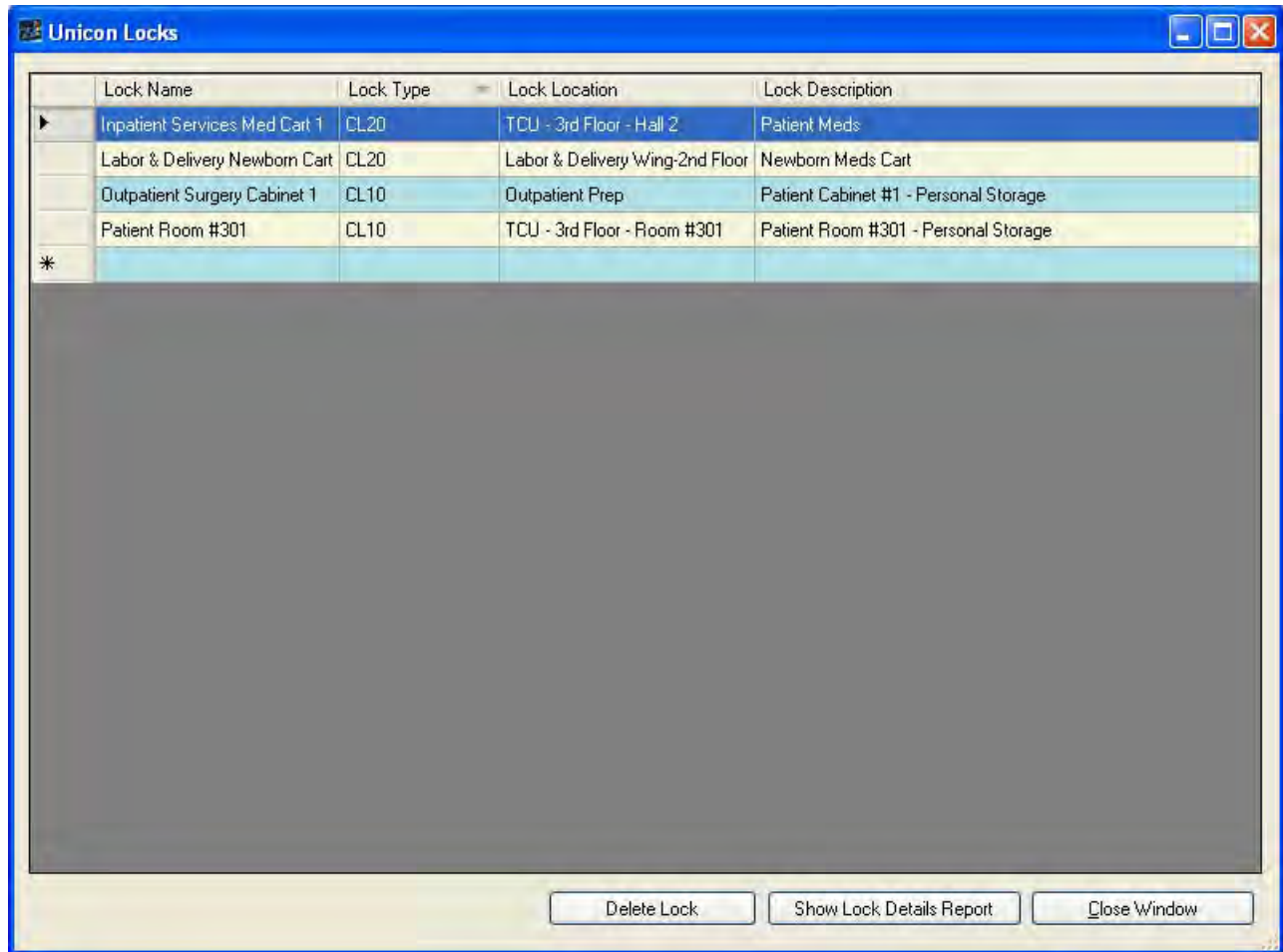
From the Main menu:

1. Select the **Locks Menu** or the  toolbar icon.

List Locks

This menu item is used to display all locks (CL10 and CL20) that have been defined in the PC system. It also allows the details of each lock to be displayed in report format. Locks can also be deleted from the database.

1. Select **List Locks** from the Program Locks Menu or select the  icon from the Program Locks screen.



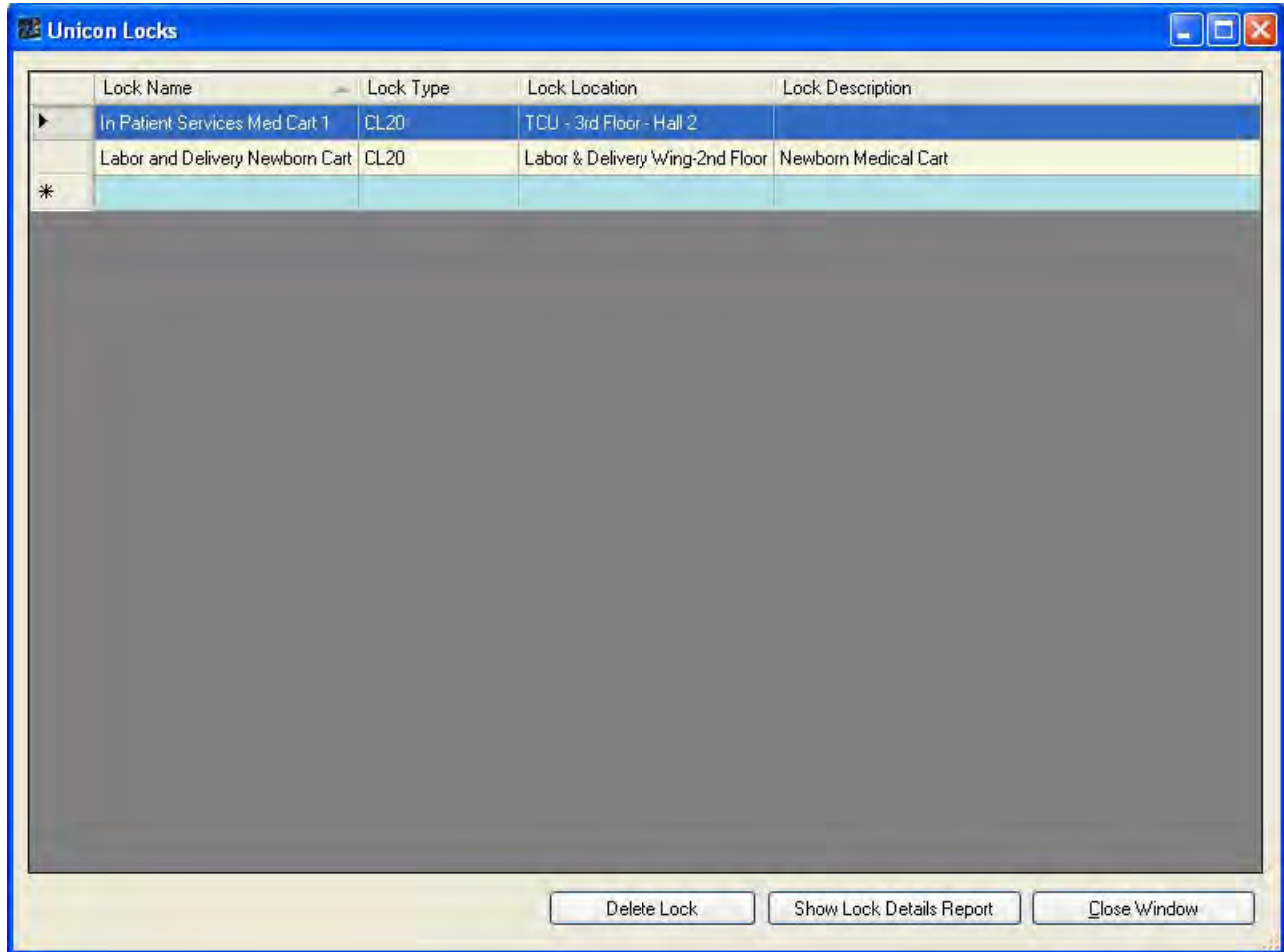
The list will display the locks specified for the Current Lock Interface (i.e., CL20) followed by any CL10 locks that have also been defined in the system.

The lock list display grid can be sorted on any of the four field columns by clicking on a specific column name tab at the top of the grid.

Delete Lock

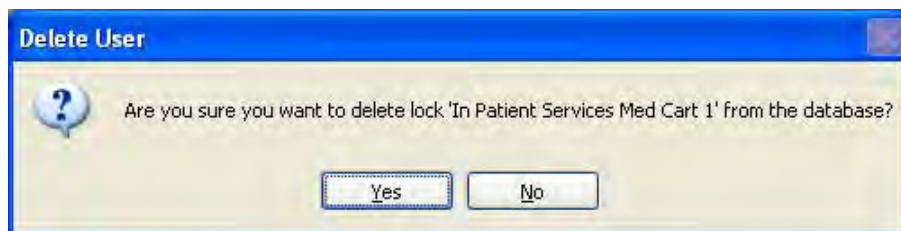
One option on the List Unicon Locks screen is “Delete Lock”. This item is used to delete a lock that no longer needs to be maintained in the system.

1. Select the lock in the list that is to be deleted from the system.



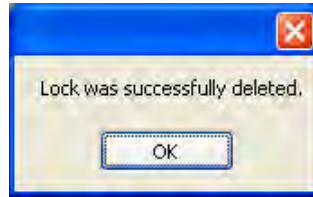
2. Click on the **Delete Lock** tab.

A prompt window is displayed asking for confirmation to delete the lock.



3. Click on **Yes** to delete the selected lock.

A message window is displayed to indicate that the lock was deleted successfully.



4. Click on **OK** to continue.

Show Lock Details Report

Another option on the List Unicon Locks screen is “Show Lock Details Report”. This option allows the details defined for an individual lock to be shown in Crystal report format.

1. Select the lock in the list for which you would like to view the Lock Details report.

Unicon CL Series Software
Report on CL20 Lock

LockID Number : 0001
Lock Serial Number : 0CL20000805082006KML
Lock Name : In Patient Services Med Cart 1
Lock Type : CL20
Lock Location : TCU - 3rd Floor - Hall 2
Lock Description :
Combo Requirement : User ID + PIN
Lock Mode : Independent
Sound Status : Sound ON
Access Mode : Single User
Reporting Capabilities : All

<u>Day</u>	<u>Schedule 1</u>	<u>Schedule 2</u>
Sunday	12:00 AM - 12:00 AM	12:00 AM - 12:00 AM
Monday	12:00 AM - 12:00 AM	12:00 AM - 12:00 AM
Tuesday	12:00 AM - 12:00 AM	12:00 AM - 12:00 AM
Wednesday	12:00 AM - 12:00 AM	12:00 AM - 12:00 AM
Thursday	12:00 AM - 12:00 AM	12:00 AM - 12:00 AM

Current Page No.: 1 Total Page No.: 3 Zoom Factor: 100%

There are standard functions available from the toolbar in all of the Crystal report formats.



The toolbar supports paging forward, backward, to the first, the last or a specific page within a report. It also supports a search function which allows users to search for a string within a report. The toolbar allows users to zoom in or out of a report with a zoom factor between 25 and 400. Additionally, the toolbar supports the ability to close or refresh a report page, print a report, and export a report.

You can change the Zoom on the report or page down to see more of the lock detail data.

Program Lock

The second option on the Locks menu is “Program Lock”. This menu item is used to initiate the program locks wizard. It should be selected to define the original lock setup data, users, and time windows for a lock.

Note: *The Program Lock operation requires a the teal programming key fob.*

If you choose the “Program the Lock” menu option from the Unicon CL Series PC software, you can define the following data in a lock:

- Lock ID
- Access Combination Requirements
- Access Mode
- Lock Operating Mode
- Sound ON/OFF
- Reporting Capabilities
- Users
- Access Schedules

Note: *The date and time in the lock will automatically be set to match the date and time of the PC when the lock is programmed with the programming key fob.*

1. Select **Program Lock**.

Program Lock - Lock Options

The **Program Lock - Lock Options** screen is displayed.

The screenshot shows the 'Program Lock Wizard' window with the 'Lock Options' tab selected. The form contains the following fields and options:

- Select or Enter New Lock Name: (dropdown menu)
- Select LockID: (text box containing '0001')
- Select Access Combination Requirement: (dropdown menu with 'User ID + PIN' selected)
- Select Access Mode: (dropdown menu with 'Single User' selected)
- Select Lock Mode: (dropdown menu with 'Independent' selected)
- Select Sound Setting: (dropdown menu with 'Sound ON' selected)
- Select Reporting Capabilities: (dropdown menu with 'All' selected)
- Lock Location: (text box)
- Lock Serial Number: (text box)
- Lock Description: (text area)

Navigation buttons at the bottom: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

1. Enter the name for a new lock or select the name of a pre-existing lock that is being reprogrammed.

Note: *To program a new lock to replace a lock that had been previously programmed and is no longer functional, simply select the old lock name from the dropdown window.*

2. If you would like to assign a lock ID to the lock, enter a four-digit number (0001-9999) for the lock ID. Otherwise, you may leave the default of "0001" for no lock ID assignment. This ID can serve to uniquely identify a lock in an audit report.
3. Select the access combination requirement. The default is User ID + PIN. The other alternative is User ID only. This decreased access requirement lessens the security of the lock and is not recommended in most situations.

Note: *The full 8-digit combination of User ID + PIN is always required for the Master User.*

4. Select the access type. The default is Single User Access.

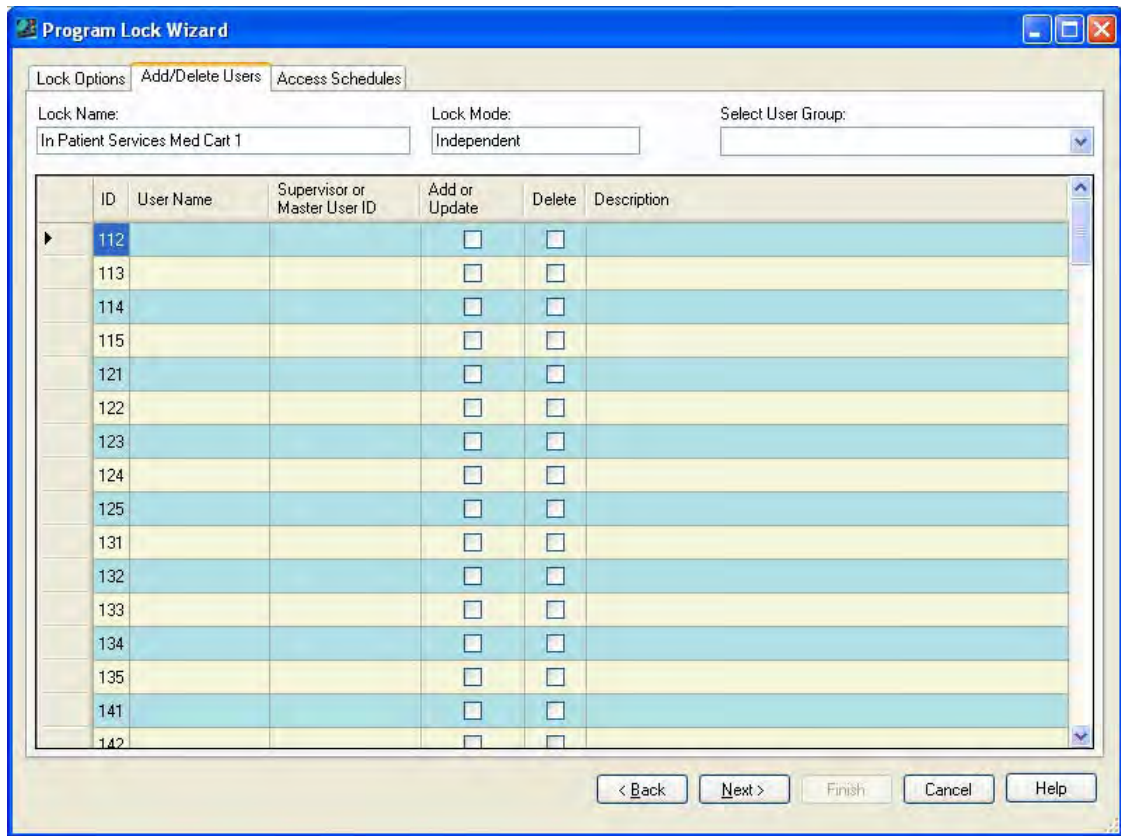
5. Select the lock mode. The default is Independent Mode.
6. Select whether you would like to have Sound turned “On or “Off” in the lock. The default value for the lock sound is “on”.
7. Select the reporting capabilities for the lock. The default is All, but you can also choose to restrict the reporting capabilities to the Master User and other designated User IDs (112, 113, 114, 115) or to only the Master User.
8. Enter a descriptive Lock Location.
9. Enter the Lock Serial Number.

Note: *The lock serial number can be found on the side of the lock chamber and also on the side of the box in which the lock was shipped.*

10. Enter a Lock Description.
11. Click on **Next** to continue.

Program Lock - Add/Delete Users

You will be prompted with the **Program Lock - Add/Delete Users** screen. You can assign users to a lock from a predefined User Group, assign users to the lock individually, or a combination of both.

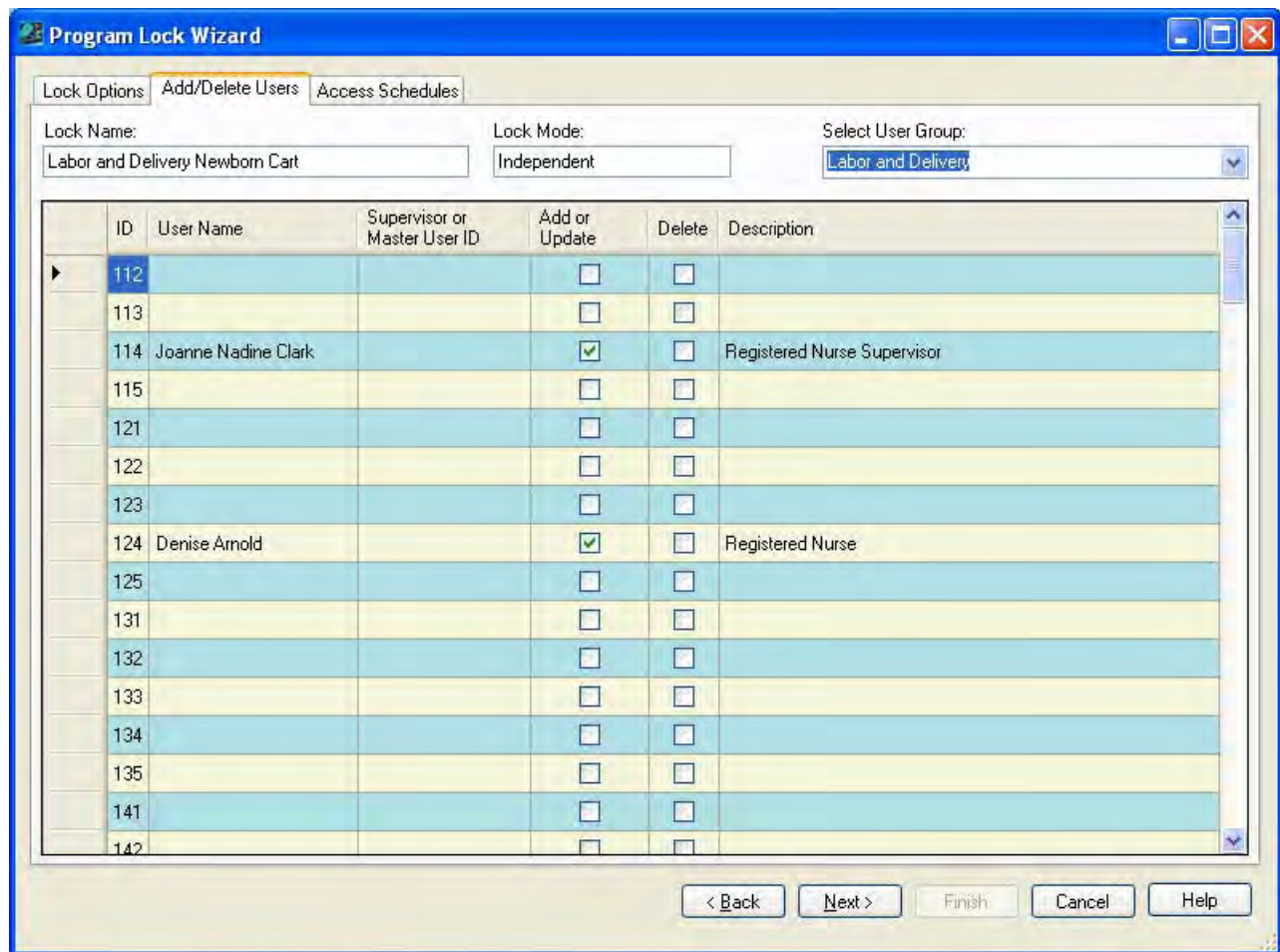


Assign Users to Lock from User Group

If you want to assign users to the lock from a predefined User Group, complete the following steps:

1. Select the User Group from the Select User Group dropdown window.

The fields will be filled with the predefined users for the User Group.



2. Click on **Next** to continue.

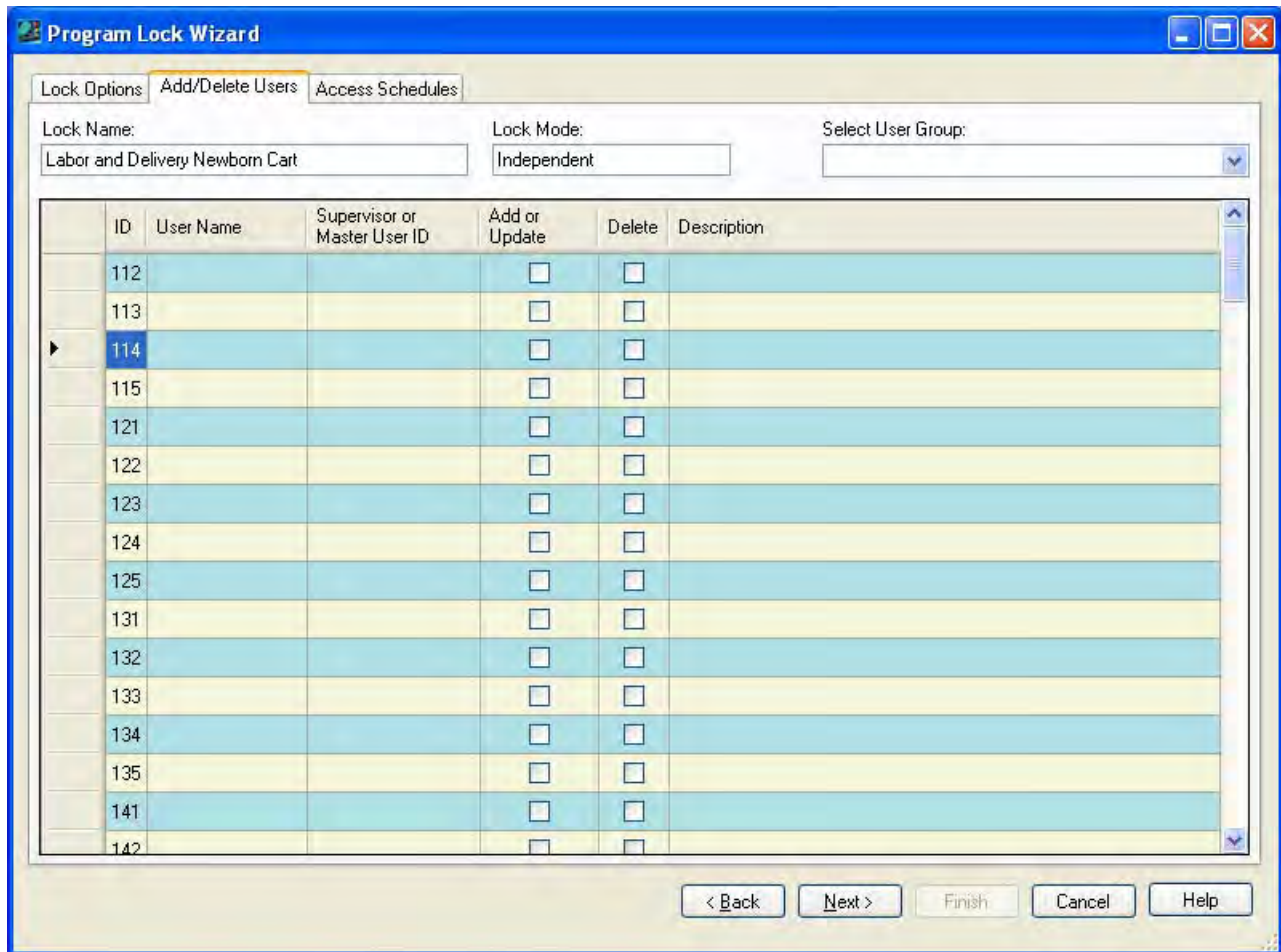
You will be prompted with the Program Lock - Access Schedules screen. Go to the section for Program Lock - Access Schedules.

Assign Users to Lock

If you want to assign users to the lock individually, complete the following steps:

Note: *In Super/Sub mode certain User IDs 112, 113, 114, and 115 are reserved for Supervisors. These are also considered to be managerial User IDs when reporting restrictions have been defined for the lock.*

1. Select the User ID to which you want to assign a user for the lock.

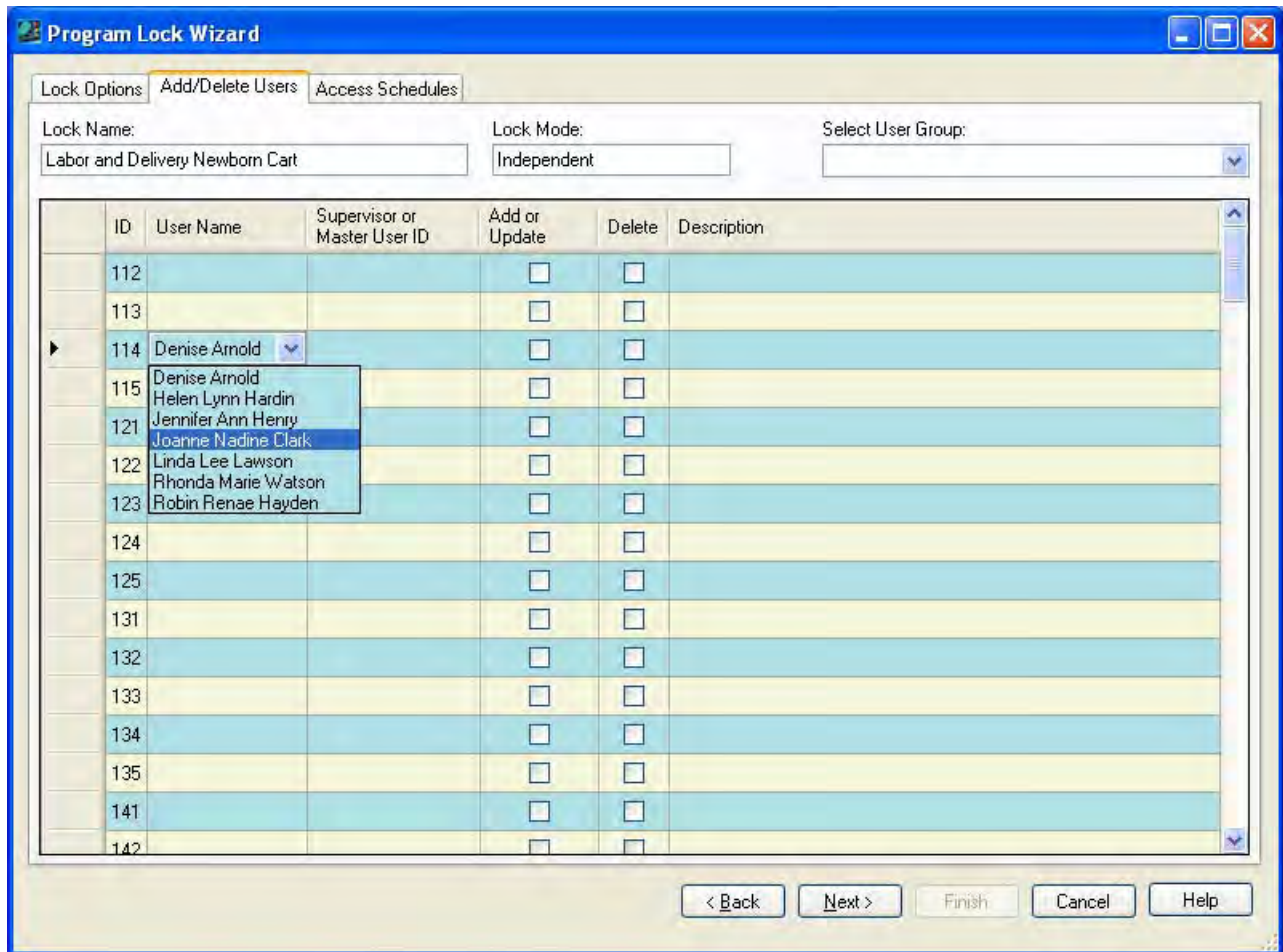


2. Click on the User Name field in the same line as the selected User ID.

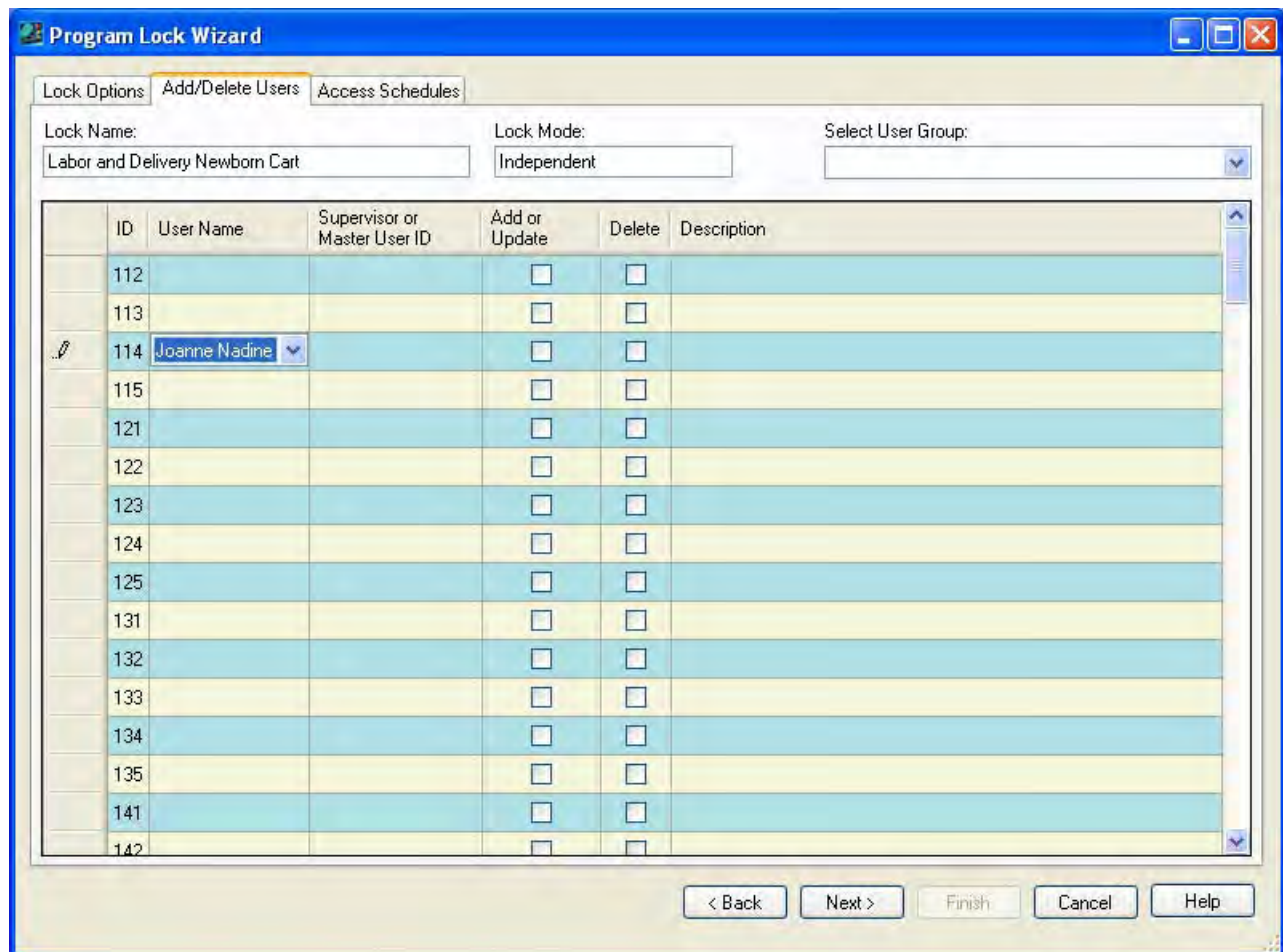
A dropdown box arrow will appear on the right hand side of the field.

3. Select a user name from the dropdown selection box.

Helpful Hint: *You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.*



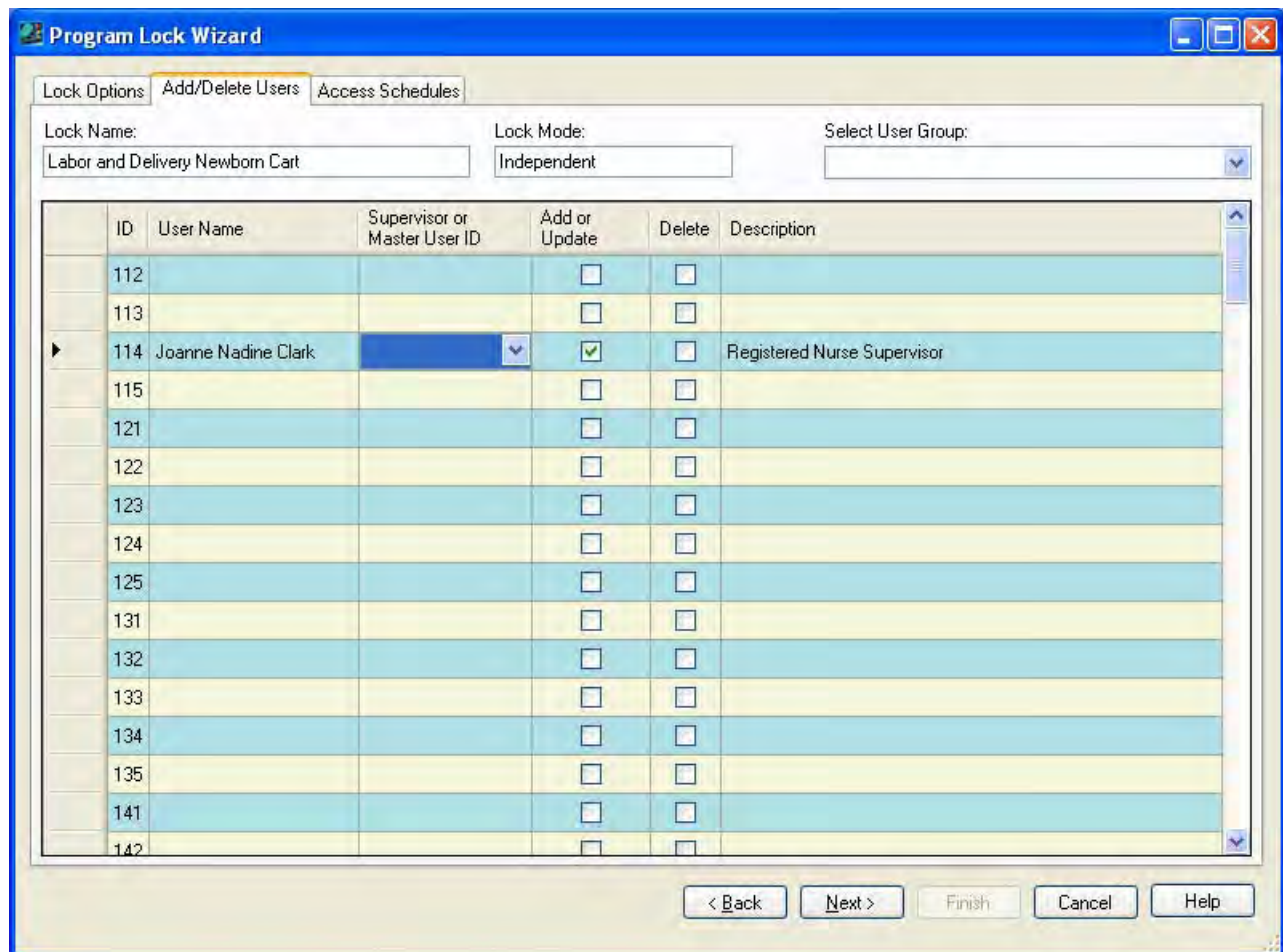
The selected name will fill the window.



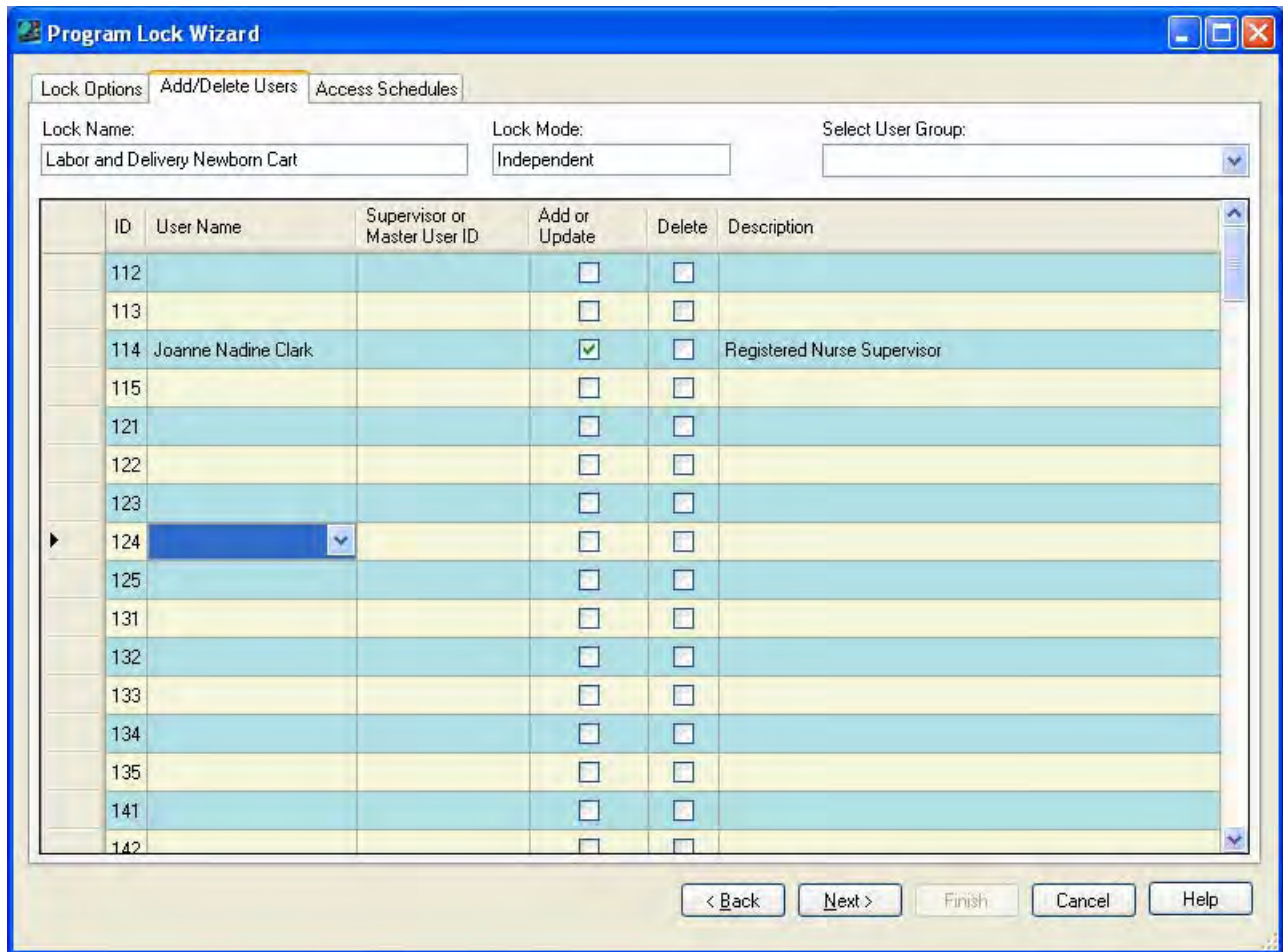
Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to “Clear Name”. Click on the “Clear Name” tab.*

4. If you are operating the lock in Supervisor/Subordinate Mode , a Supervisor or a Master User must be assigned to the user. Click on the Supervisor or Master User ID field and type in the Supervisor or Master User ID, or you can make a selection from the dropdown box.

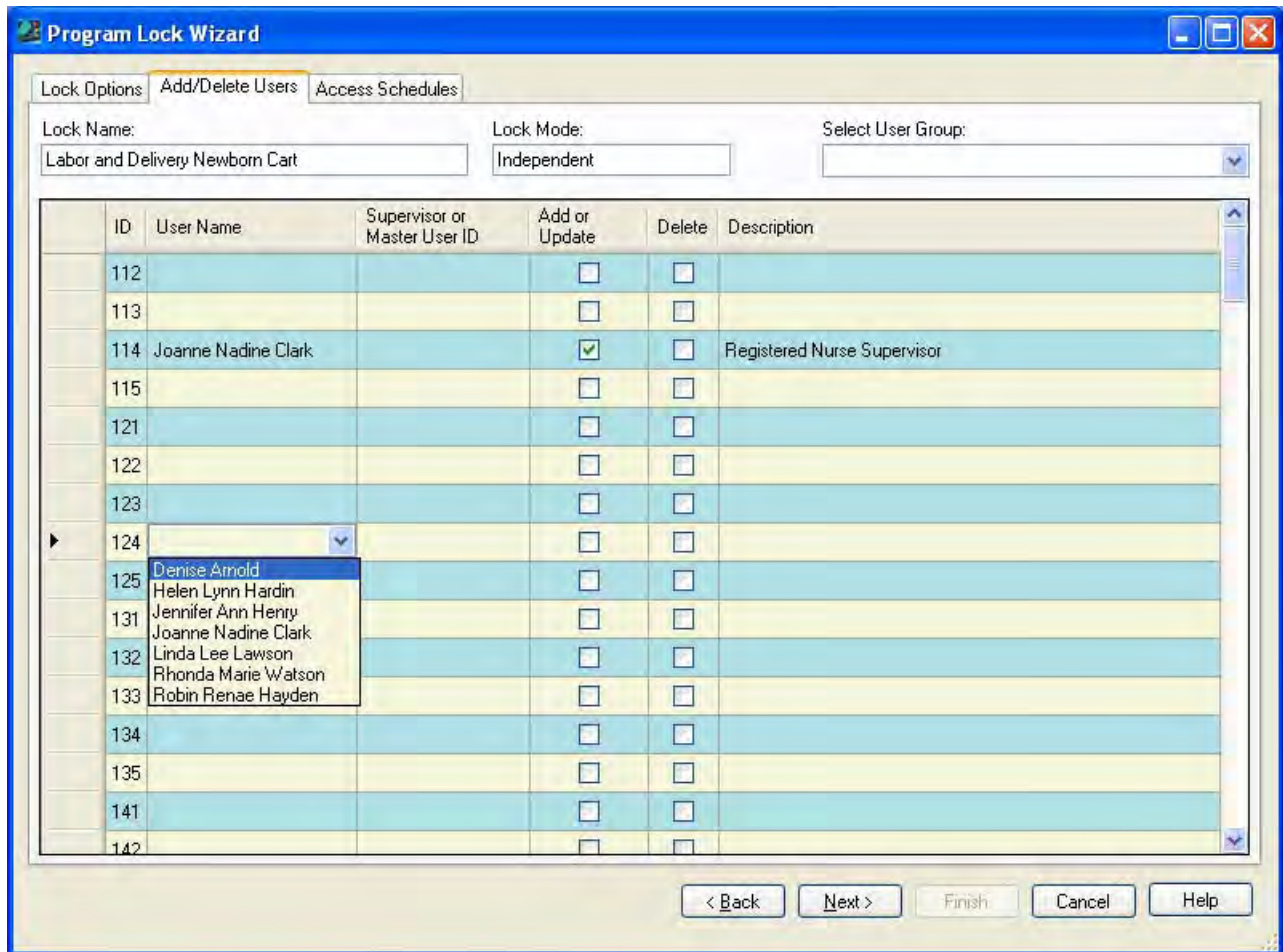
Note: *For a designated Supervisor ID (i.e., 112, 113, 114, 115), the only selection choice is the Master User ID of 111. For all other User IDs, the choices are limited to the designated Supervisor IDs of 112, 113, 114, and 115.*



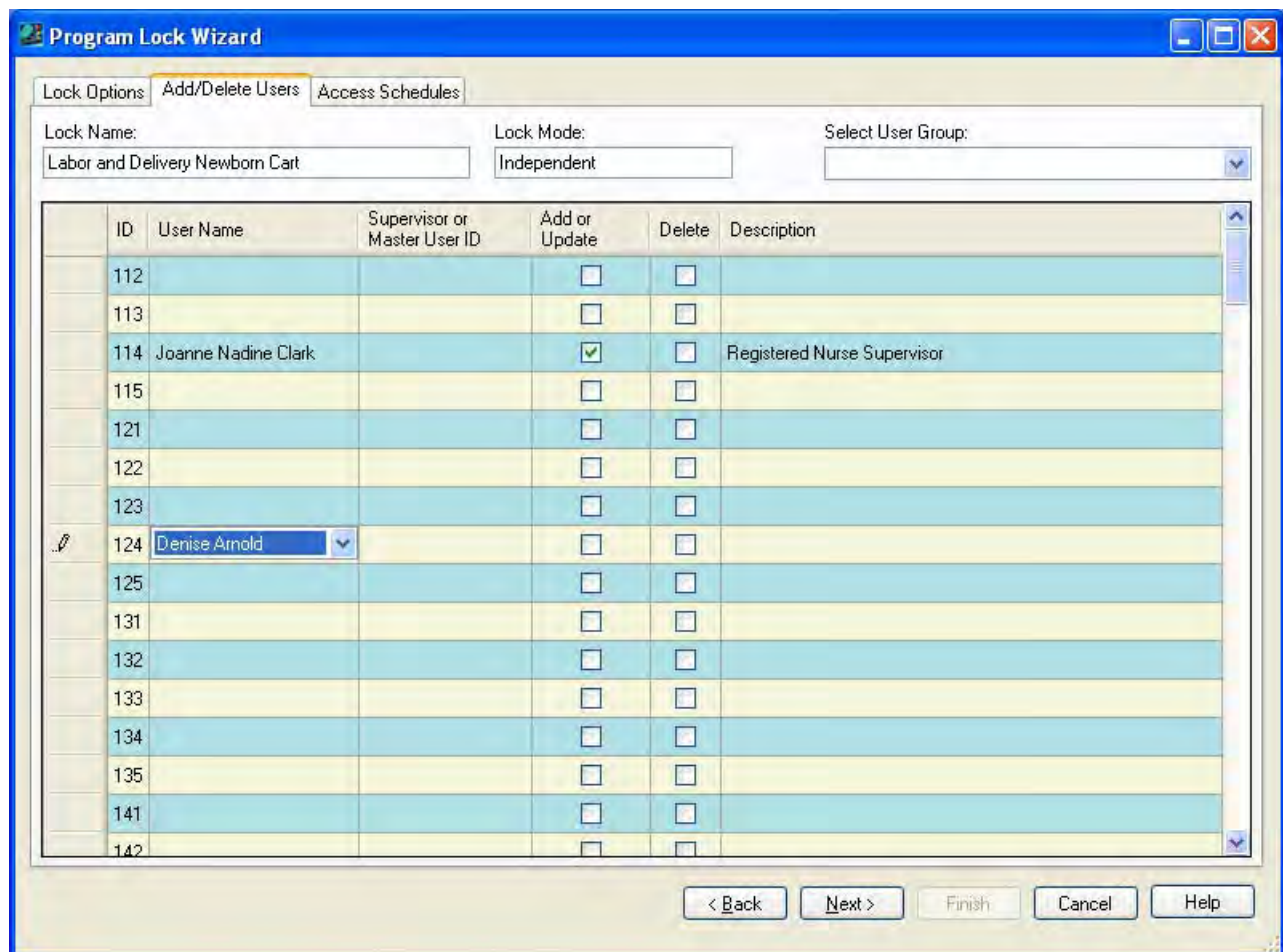
5. Select the next User ID you want to assign to a user for this user group.
6. Click on the User Name field in the same line as the selected User ID.
A dropdown box arrow will appear on the right hand side of the field.



7. Select a user name from the dropdown selection box.



The selected name will fill the window.

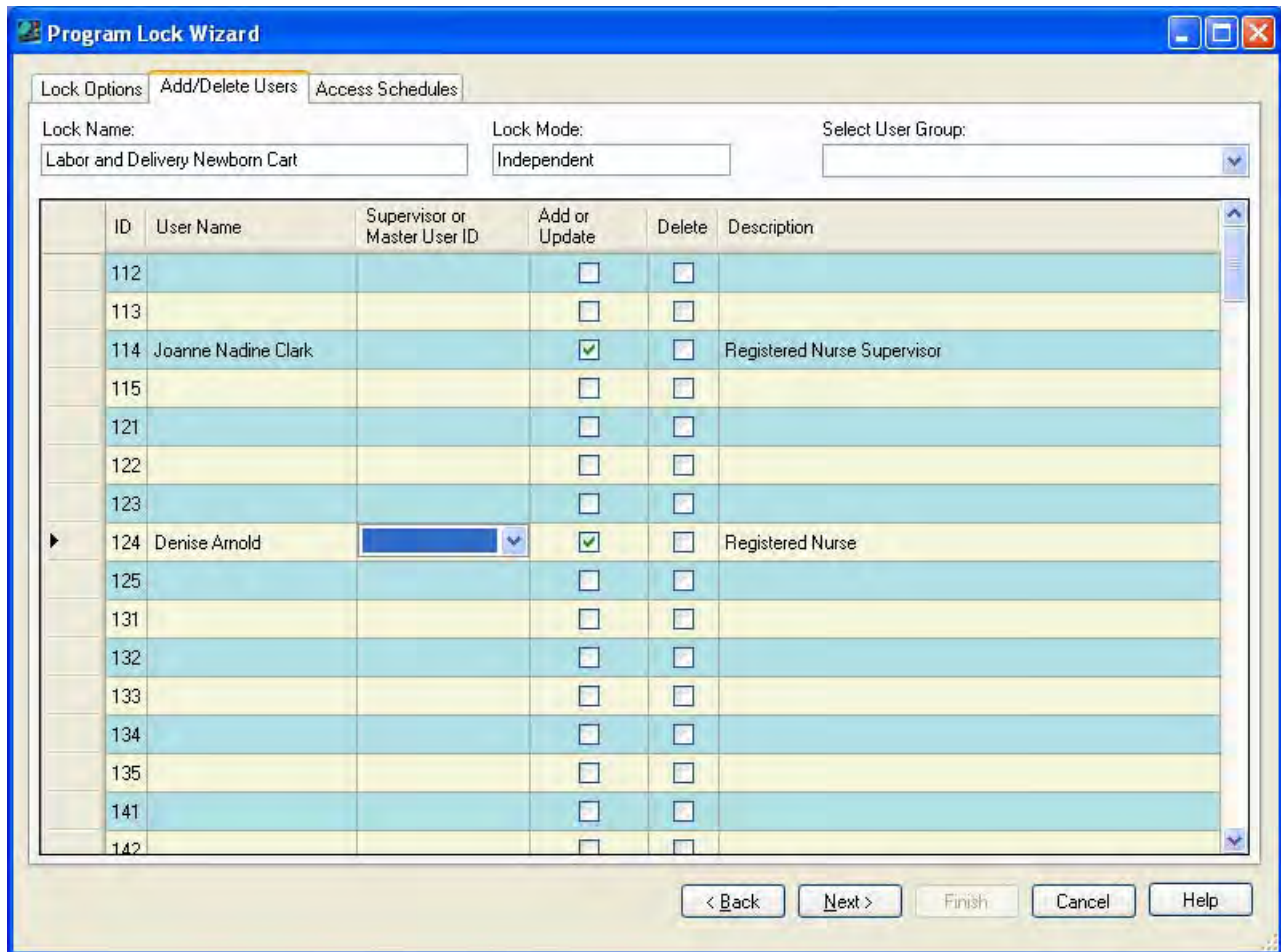


8. Click on the User ID field for the user just added.

The **Add or Update** column should now be checked for the user to be added to the lock.

9. If you are operating the lock in Supervisor/Subordinate Mode, a Supervisor or a Master User must be assigned to the user. Click on the Supervisor or Master User ID field and type in the Supervisor or Master User ID, or you can make a selection from the dropdown box.

Note: For a designated Supervisor ID (i.e., 112, 113, 114, 115), the only selection choice is the Master User ID of 111. For all other User IDs, the choices are limited to the designated Supervisor IDs of 112, 113, 114, and 115.



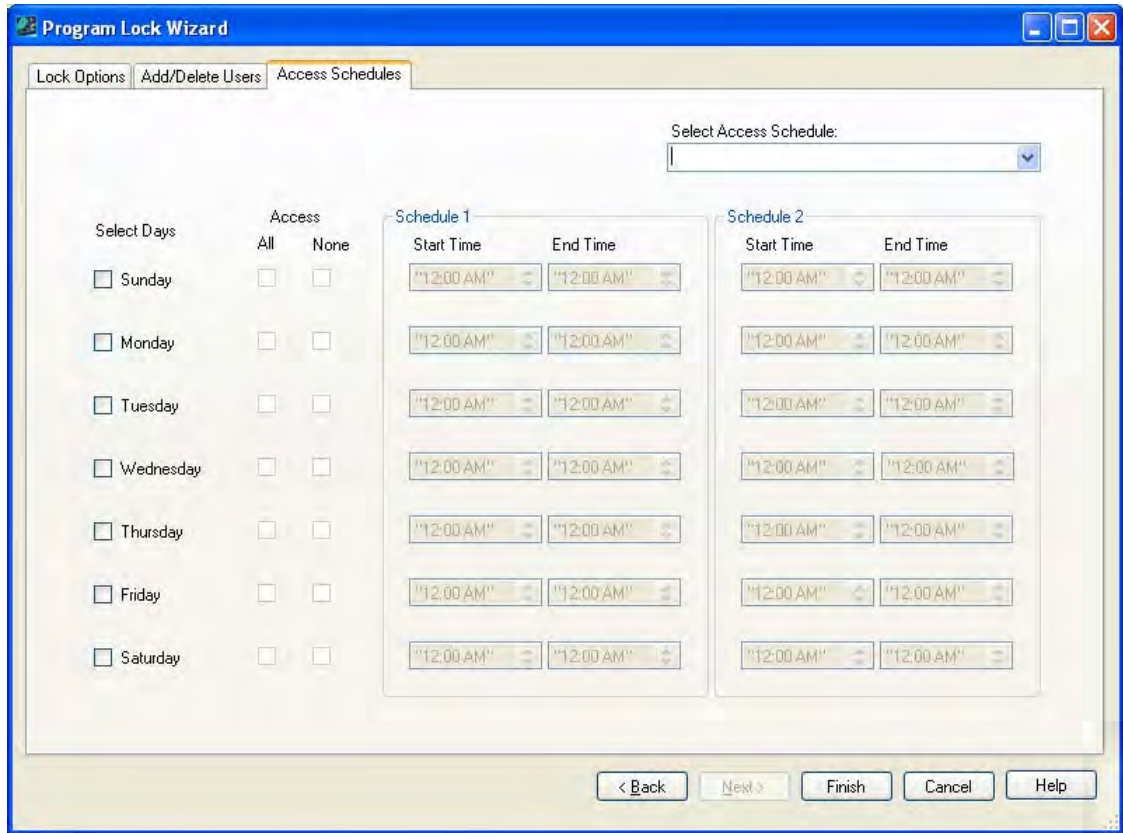
10. Continue repeating the steps to add another user to the user group until the user group members have all been defined.

11. Once all user assignments are defined, ensure that the appropriate columns are checked for the users to be added to the lock and click on **Next** to continue.

You will be prompted with the Program Lock - Access Schedules screen. Go to the section for Program Lock - Access Schedules.

Program Lock - Access Schedules

You will be prompted with the **Program Lock - Access Schedules** screen. You can assign an access schedule to a lock from a predefined access schedule template or define a unique access schedule for the lock from this screen.

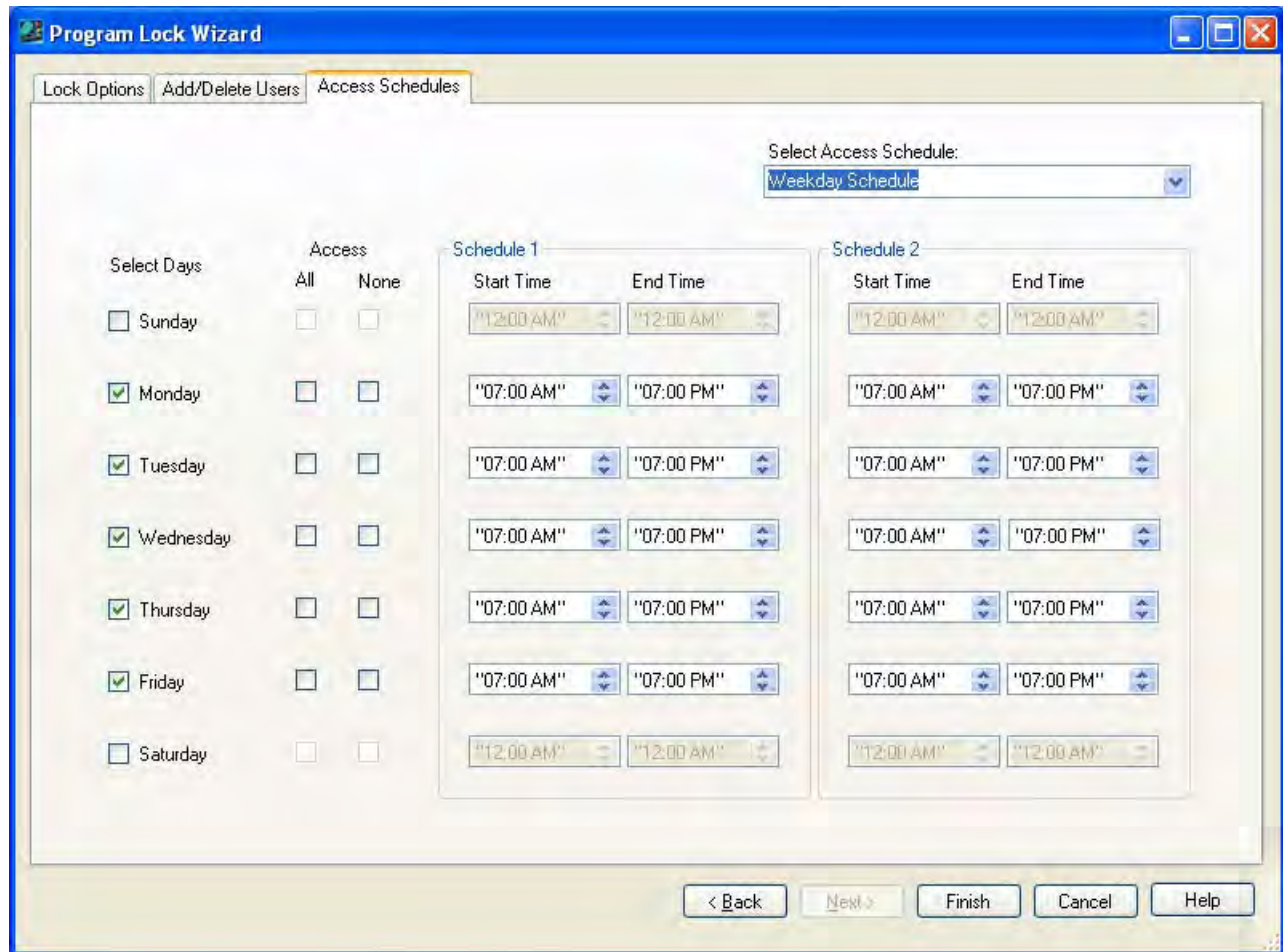


Assign Access Schedules to Lock from Access Schedule Template

If you want to assign the access schedules for the lock from a predefined Access Schedule template, complete the following steps:

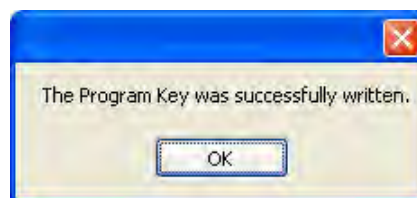
1. Select the Access Schedule from the Select Access Schedule dropdown window.

The fields will be filled with the predefined access schedule values.



2. Ensure that a programming key fob has been attached to the Unicon data cable and click on **Finish**.

The following message window is displayed to indicate that the Program Key was written successfully.



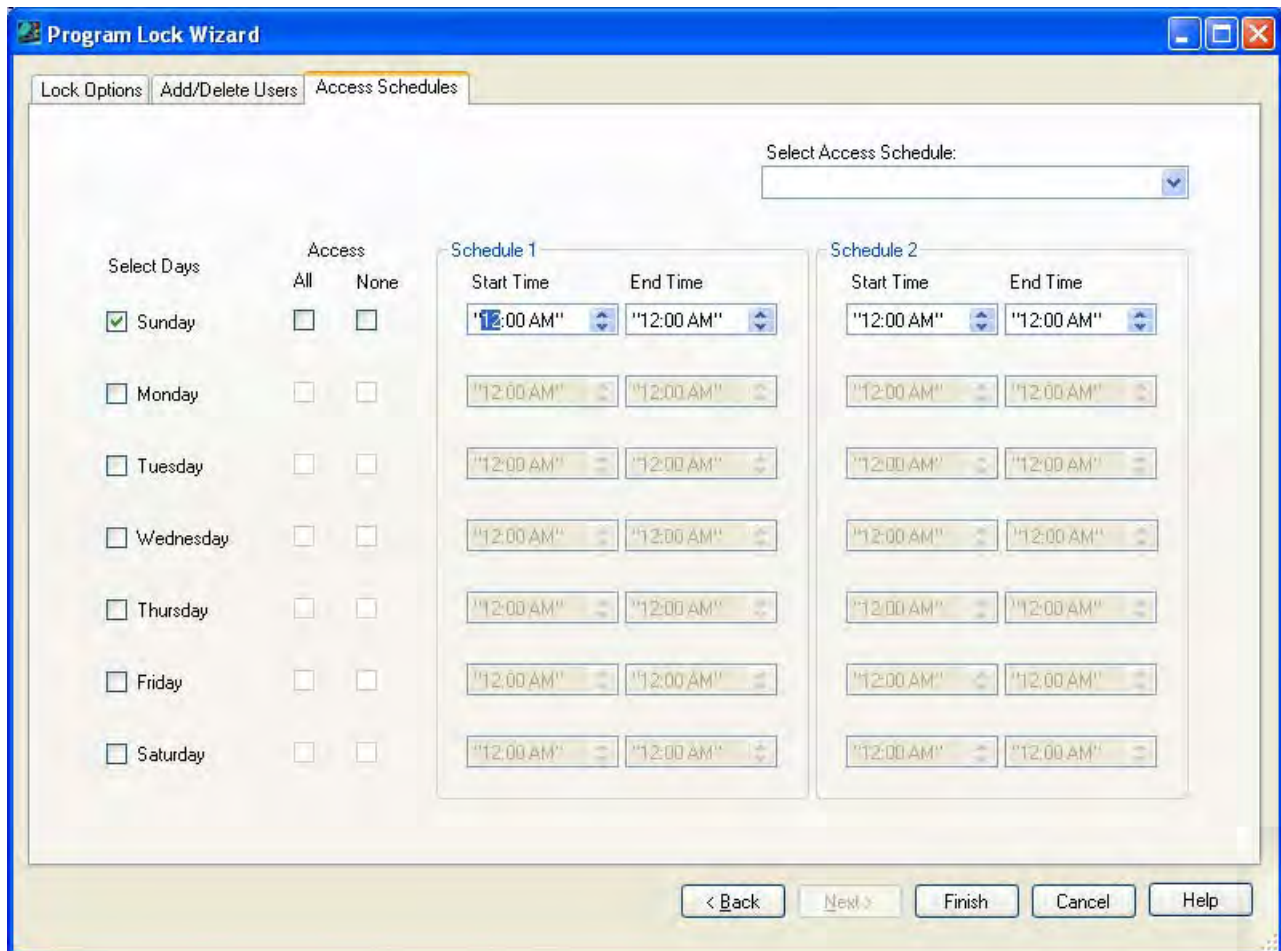
Assign Access Schedules to Lock

If you want to define the access schedules for the lock individually, complete the following steps:

1. To change the access schedule settings for a given day, click on the Select Days box for that day. If the box is not checked, the lock window settings will not be affected for that day and will remain set to whatever values are currently set at the lock.

Note: *The access schedule settings will default to “all access” at the lock unless defined otherwise via manual programming at the lock or via data upload to the lock from the software.*

Once the Select Days box has been selected for a specific day, the other input fields for that day will become enabled for data entry.



- 2a. If you want No Access Restriction (24 hour access) for the selected day, select the appropriate box for “All Access”. All other input fields will become unavailable for that day.

- 2b. If you want no lock access allowed for the selected day, select the “None” box. All other input fields will become unavailable for that day.
- 2c. If you want to limit access to a certain time period of the selected day, define an access time window by entering a Start Time and End Time under the Schedule 1 section of the screen. Specify all times in HH:MM format. Enter times as they would be set at the lock.

Note: *When data is entered for Schedule 1, the same Start and End Time will automatically be filled in for Schedule 2 once you click into the second window.*

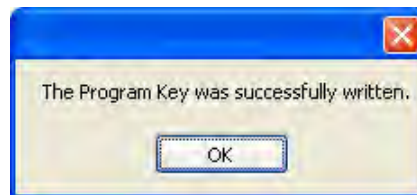
3. Tab to the Start Time in Schedule 2. If you want to define a second access time window for the selected day, update the Start Time and End Time under the Schedule 2 section of the screen to the values for the second window.

Note: *If you do not choose to define a second window, the second window will default to the same time period as the first window.*

Repeat steps 2 and 3 for each day that you would like to define lock access.

4. Once you are finished with the Access Schedules screen, ensure that a programming key fob has been attached to the data cable and click on **Finish**.

The following message window is displayed to indicate that the Program Key was written successfully.



5. Click on **OK**.
6. The programming key fob should now be taken to the lock to program the lock data.

Note: *Previous to uploading any data to a lock, the Master User PIN must be “set” in the lock. The default PIN assigned to the Master User is “12345”. The default PIN assigned to a new User or Supervisor ID is “55255”. A user must change this default PIN before any lock operations can be performed. See the **Unicon CL20 Operating Instructions** for further detail.*

Program Lock Users

This option is used to add and/or delete users to or from a lock using a Programming Key Fob. The option should be selected only to add or delete users to a lock that has already been programmed.

Note: *If the lock is operating in Supervisor/Subordinate Mode, Supervisors cannot be added or deleted using this option.*

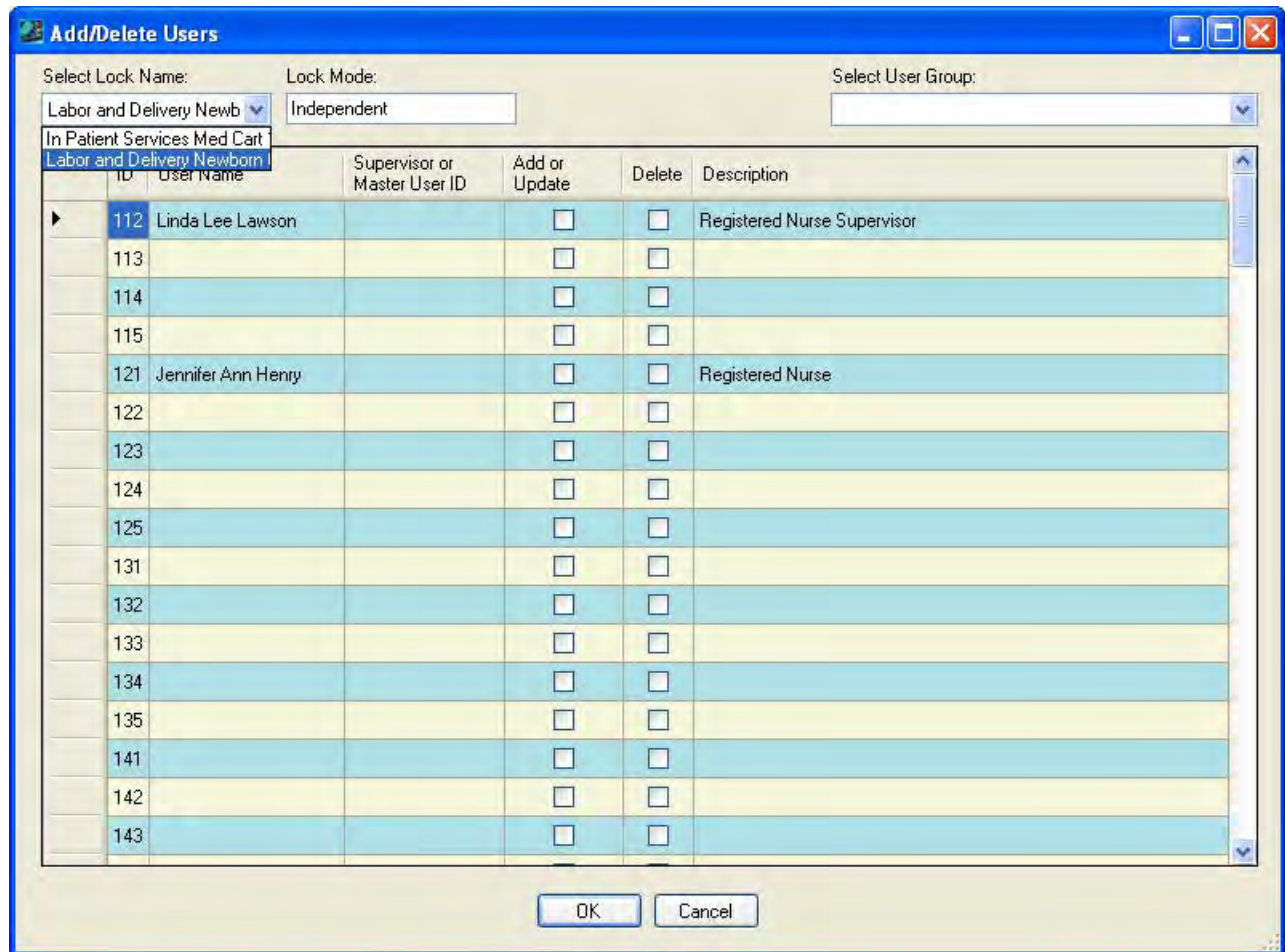
1. Select **Program Lock Users**.

The “Add/Delete Users” screen is displayed.

Note: *The first lock (in alphabetical order) is shown as the default.*

ID	User Name	Supervisor or Master User ID	Add or Update	Delete	Description
112	Linda Lee Lawson		<input type="checkbox"/>	<input type="checkbox"/>	Registered Nurse Supervisor
113			<input type="checkbox"/>	<input type="checkbox"/>	
114			<input type="checkbox"/>	<input type="checkbox"/>	
115			<input type="checkbox"/>	<input type="checkbox"/>	
121	Jennifer Ann Henry		<input type="checkbox"/>	<input type="checkbox"/>	Registered Nurse
122			<input type="checkbox"/>	<input type="checkbox"/>	
123			<input type="checkbox"/>	<input type="checkbox"/>	
124			<input type="checkbox"/>	<input type="checkbox"/>	
125			<input type="checkbox"/>	<input type="checkbox"/>	
131			<input type="checkbox"/>	<input type="checkbox"/>	
132			<input type="checkbox"/>	<input type="checkbox"/>	
133			<input type="checkbox"/>	<input type="checkbox"/>	
134			<input type="checkbox"/>	<input type="checkbox"/>	
135			<input type="checkbox"/>	<input type="checkbox"/>	
141			<input type="checkbox"/>	<input type="checkbox"/>	
142			<input type="checkbox"/>	<input type="checkbox"/>	
143			<input type="checkbox"/>	<input type="checkbox"/>	

2. Select the name of the lock to which you want to add/delete users.



Once the lock is selected, the lock mode will be displayed along with the users currently assigned to the lock.

ID	User Name	Supervisor or Master User ID	Add or Update	Delete	Description
112			<input type="checkbox"/>	<input type="checkbox"/>	
113			<input type="checkbox"/>	<input type="checkbox"/>	
114	Joanne Nadine Clark		<input type="checkbox"/>	<input type="checkbox"/>	Registered Nurse Supervisor
115			<input type="checkbox"/>	<input type="checkbox"/>	
121			<input type="checkbox"/>	<input type="checkbox"/>	
122			<input type="checkbox"/>	<input type="checkbox"/>	
123			<input type="checkbox"/>	<input type="checkbox"/>	
124	Denise Arnold		<input type="checkbox"/>	<input type="checkbox"/>	Registered Nurse
125			<input type="checkbox"/>	<input type="checkbox"/>	
131			<input type="checkbox"/>	<input type="checkbox"/>	
132			<input type="checkbox"/>	<input type="checkbox"/>	
133			<input type="checkbox"/>	<input type="checkbox"/>	
134			<input type="checkbox"/>	<input type="checkbox"/>	
135			<input type="checkbox"/>	<input type="checkbox"/>	
141			<input type="checkbox"/>	<input type="checkbox"/>	
142			<input type="checkbox"/>	<input type="checkbox"/>	
143			<input type="checkbox"/>	<input type="checkbox"/>	

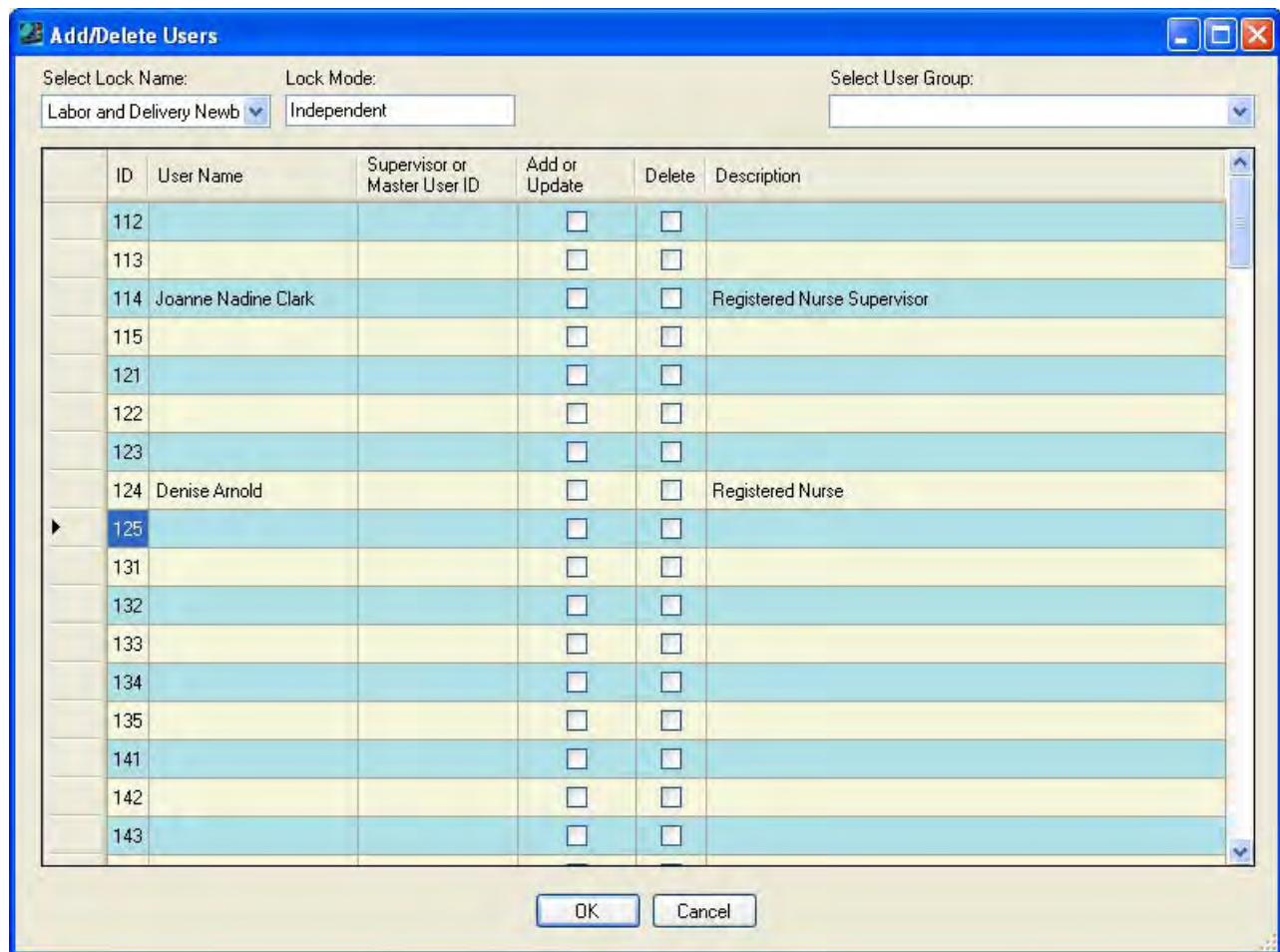
Caution: Do not click on **OK** until you have completed **all** user changes for the lock. Clicking on **OK** will actually write the add/update/delete user information to the database and to the Programming Key Fob.

Add Users to the Lock

If you want to add new users to the lock, complete the following steps for each user to be added:

Note: In Super/Sub mode certain User IDs 112, 113, 114, and 115 are reserved for Supervisors. When operating in Independent Mode, these User IDs are also considered to be managerial /administrative User IDs. Reporting restrictions can be defined for the lock allowing these users to retrieve data from the lock for reporting purposes.

3a. Select the User ID to which you want to assign a new user for the lock.

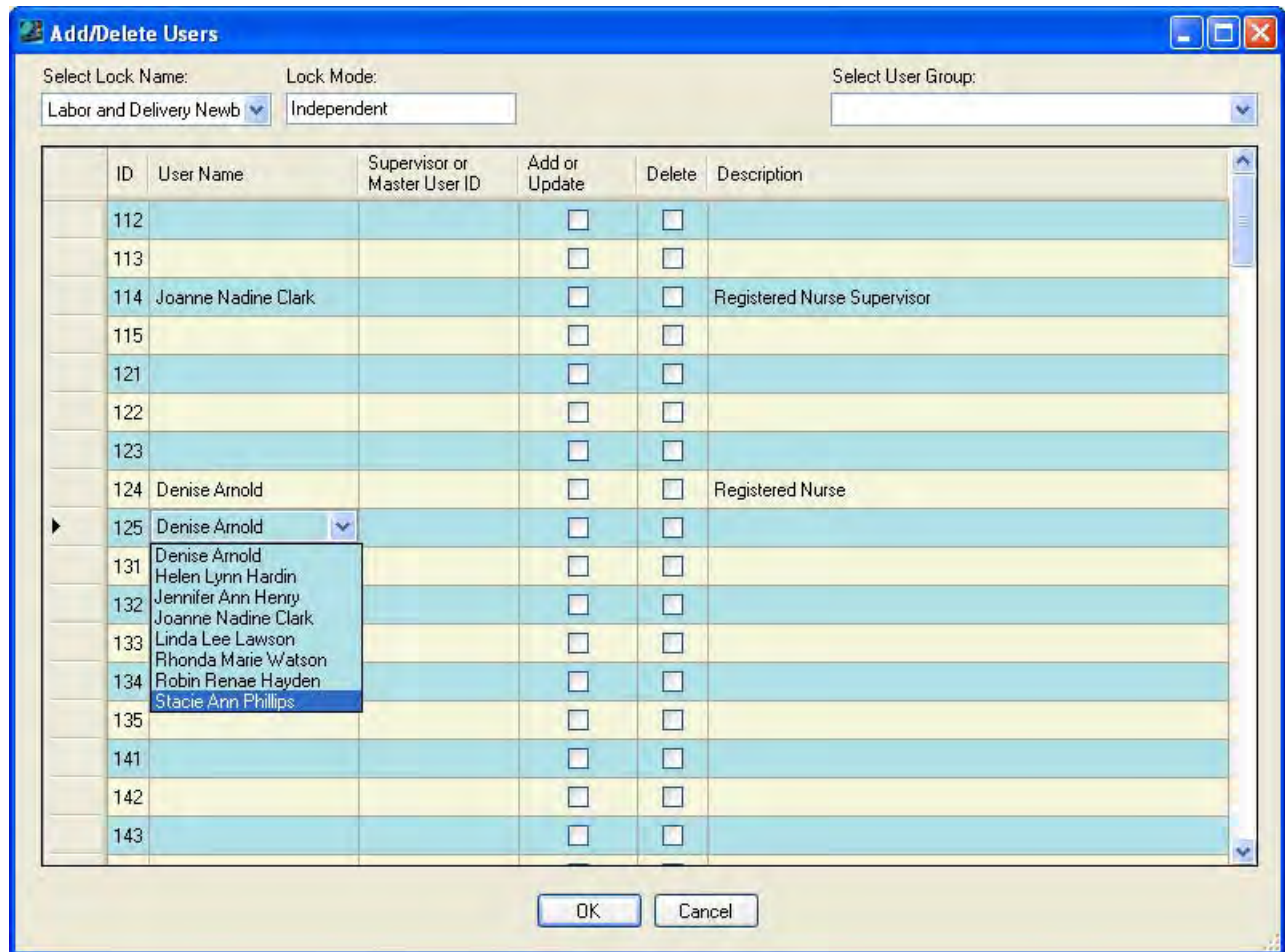


3b. Click on the User Name field in the same line as the selected User ID.

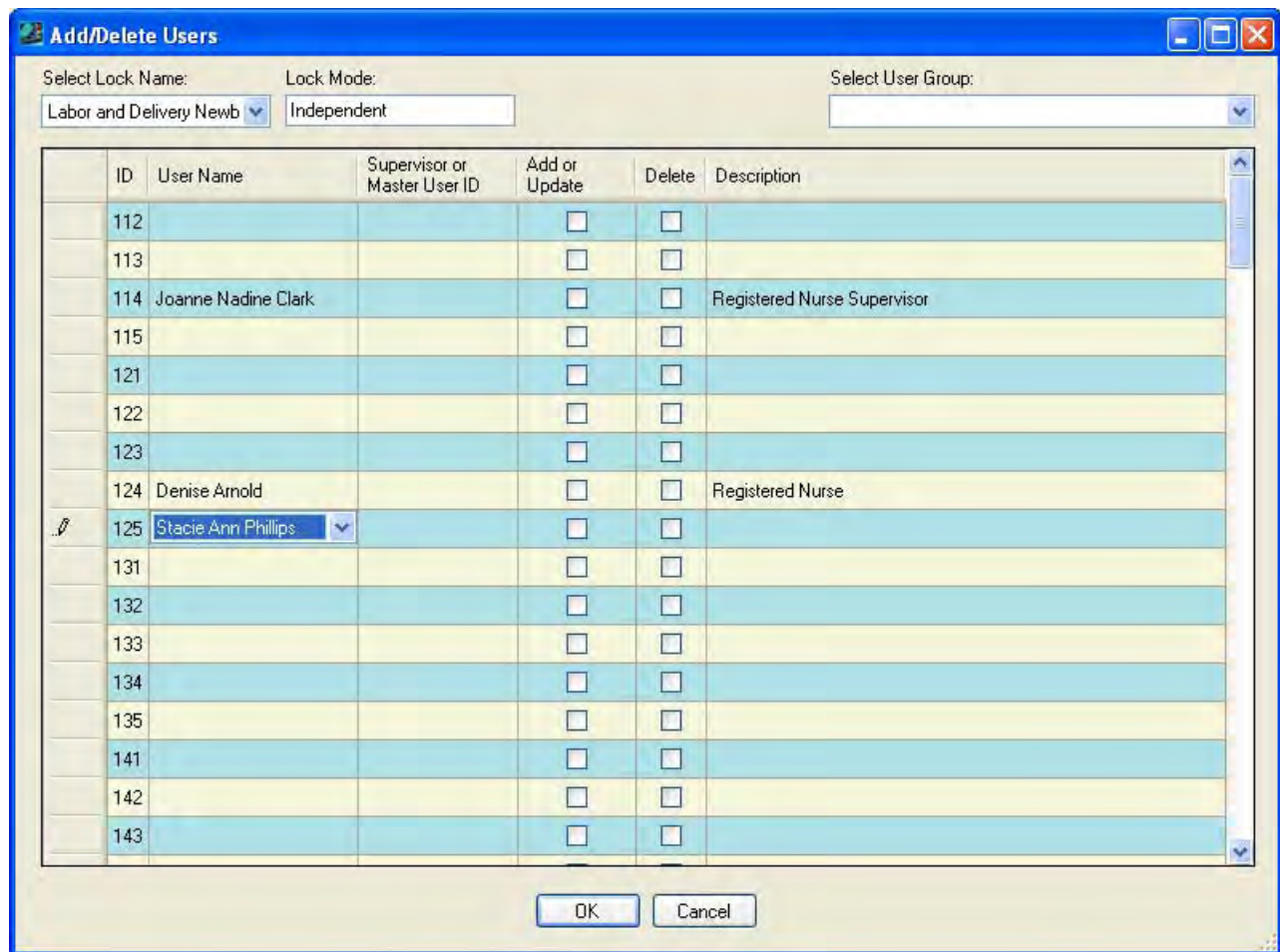
A dropdown box arrow will appear on the right hand side of the field.

3c. Select a user name from the dropdown selection box.

Helpful Hint: You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.



The selected name will fill the window.



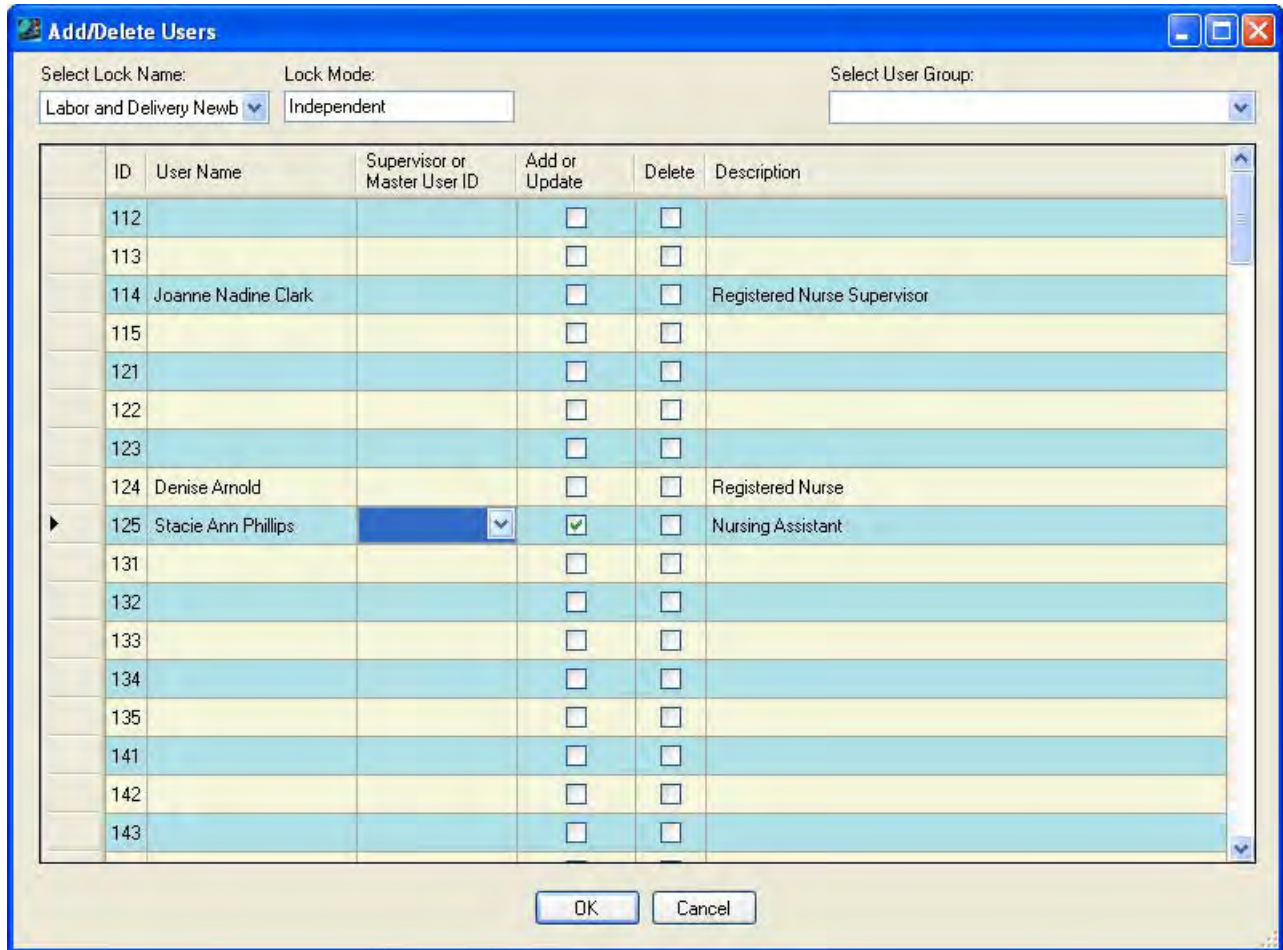
Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name and then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

3d. Click on the User ID field for the user just added.

The **Add or Update** column should now be checked for the user to be added to the lock.

3e. If you are operating the lock in Supervisor/Subordinate Mode, a Supervisor or a Master User ID must be assigned to the user. Click on the Supervisor or Master User ID field and type in the Supervisor or Master User ID, or you can make a selection from the dropdown box.

Note: For a designated Supervisor ID (i.e., 112, 113, 114, 115), the only selection choice is the Master User ID of 111. For all other User IDs, the choices are limited to the designated Supervisor IDs of 112, 113, 114, and 115.

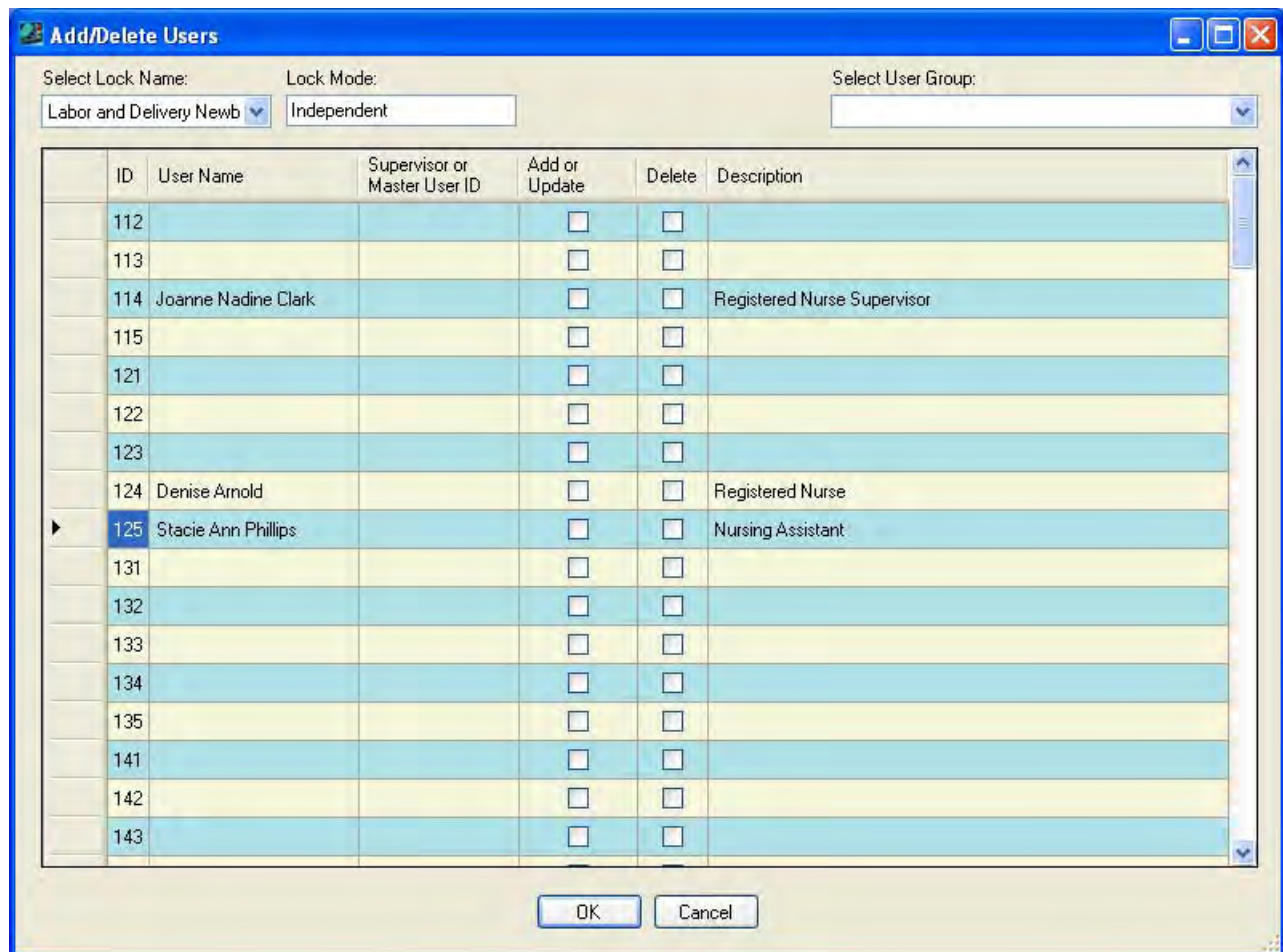


Change User ID Assignment

If you want to change the user who is currently assigned to a User ID, complete the following steps for each User ID assignment to be changed:

Note: In Super/Sub mode certain User IDs 112, 113, 114, and 115 are reserved for Supervisors. These are also considered to be managerial User IDs in Independent mode when reporting restrictions have been defined for the lock.

3a. Select the User ID to which you want to assign a different user for the lock.

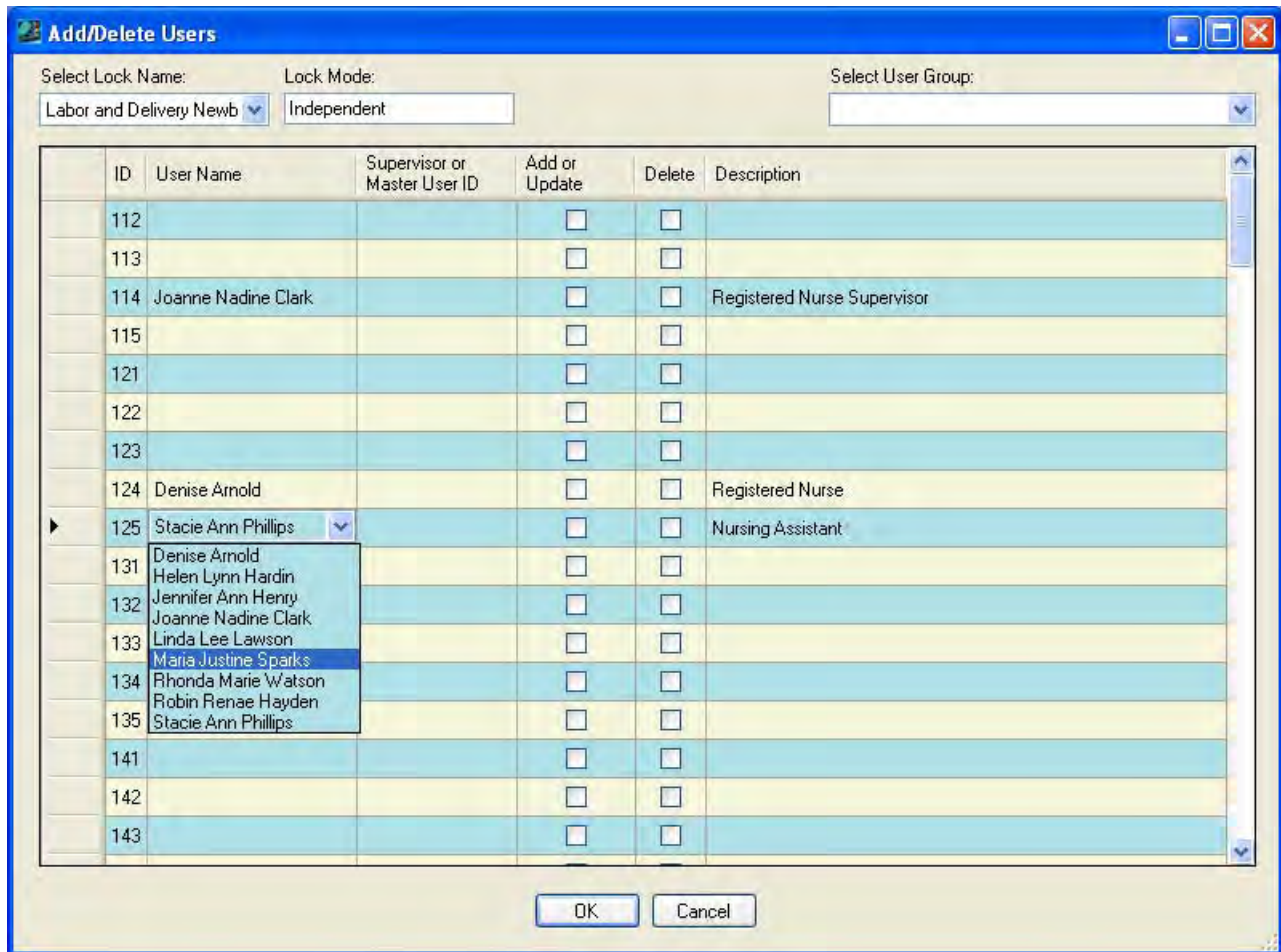


3b. Click on the User Name field in the same line as the selected User ID.

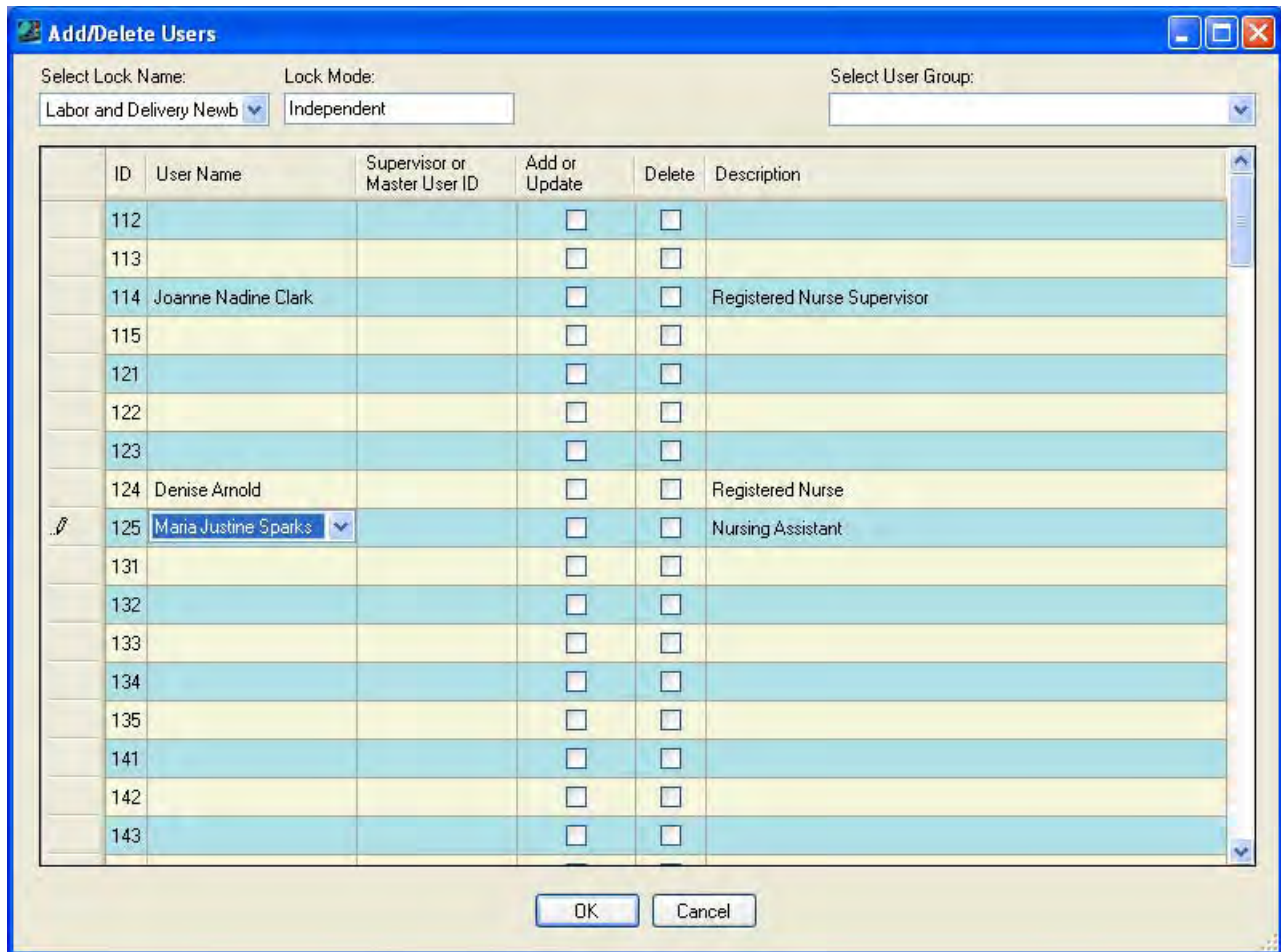
A dropdown box arrow will appear on the right hand side of the field.

3c. Select a different user name from the dropdown selection box.

Helpful Hint: You can also type the first letter of the user name that you want to select in the User Name field. The field will automatically be filled with the user name that is closest to that letter (in alphabetical order.) If you access the dropdown selection box at this point, the pointer will be sitting at that name in the selection list.



The selected name will fill the window.



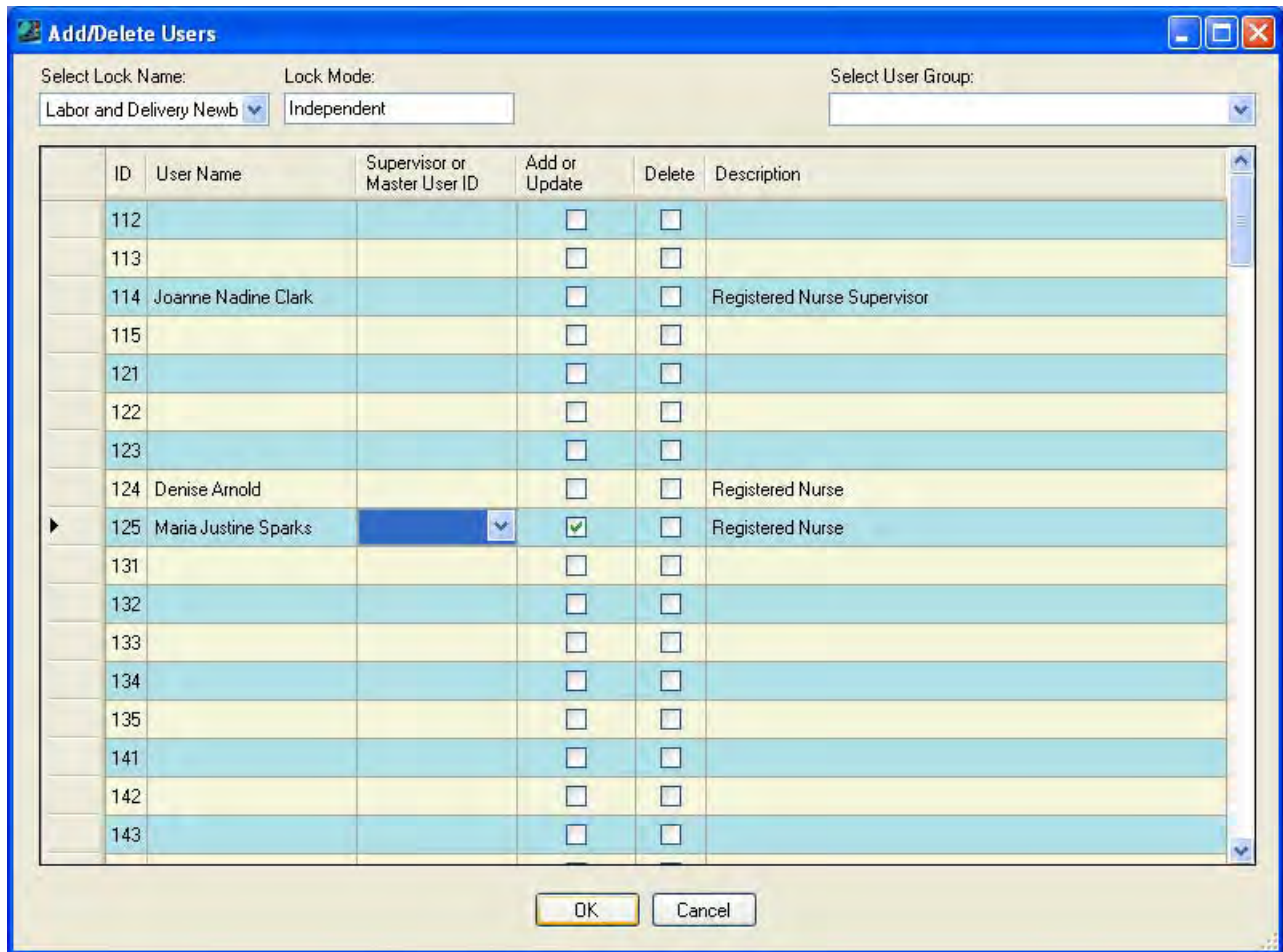
Note: *If you make an incorrect name selection, you can change your selection by returning to the dropdown selection box. If you incorrectly assigned a user to a User ID that you did not intend to use, you can clear the name from that User ID. Simply click on a field other than User Name and then return to the User Name field. Once you have clicked on the User Name field again, you can right click. A tab is displayed to "Clear Name". Click on the "Clear Name" tab.*

3d. Click on the User ID field for the user just updated.

The **Add or Update** column should now be checked for the user to be updated in the lock.

3e. If you are operating the lock in Supervisor/Subordinate Mode, a Supervisor or a Master User ID must be assigned to the user. Click on the Supervisor or Master User ID field and type in the Supervisor or Master User ID, or you can make a selection from the dropdown box.

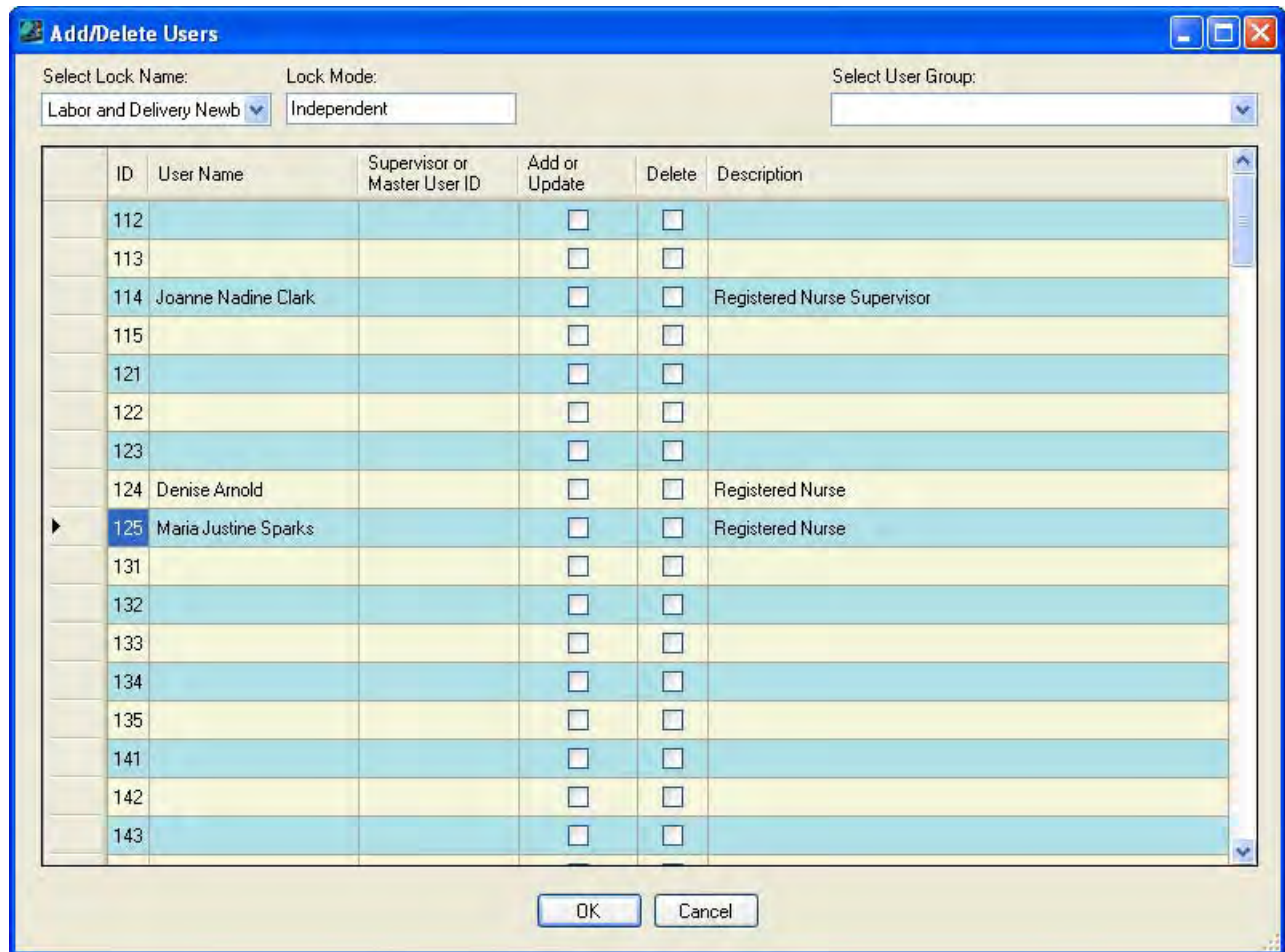
Note: For a designated Supervisor ID (i.e., 112, 113, 114, 115), the only selection choice is the Master User ID of 111. For all other User IDs, the choices are limited to the designated Supervisor IDs of 112, 113, 114, and 115.



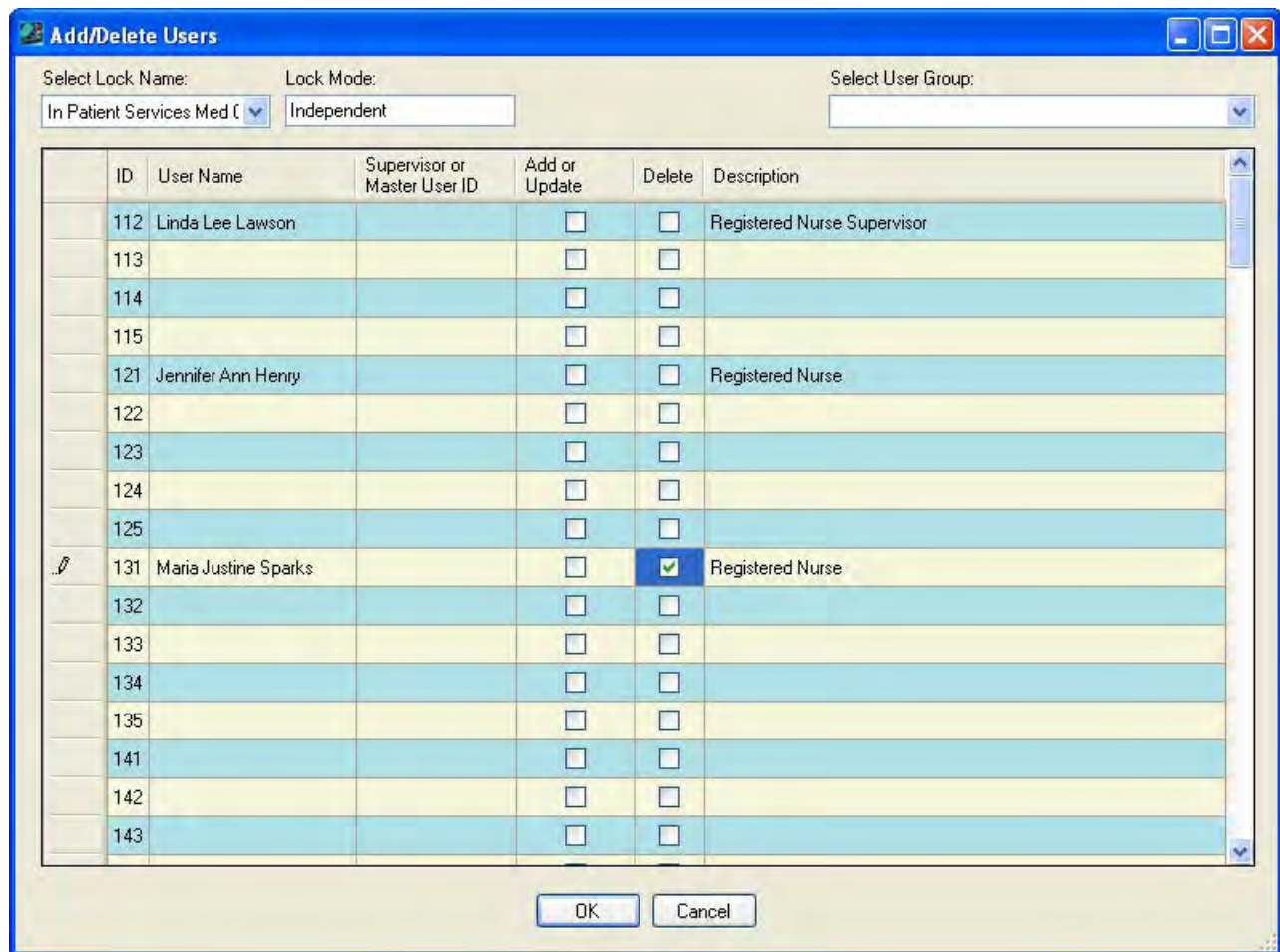
Delete Users from Lock

If you want to delete users from the lock, complete the following steps for each user to be deleted:

- 3a. Select the User ID that you want to delete from the lock.



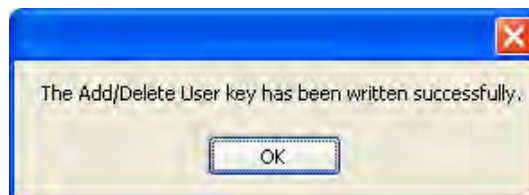
3b. Click on the Delete box for the User ID that you want to delete from the lock.



Write to the Key

- When all settings are complete and all desired users have been added/deleted appropriately, ensure that the Programming Key Fob has been attached to the Unicon data cable and click on the **OK** button.

A message window will be displayed indicating that the Add/Delete key was written successfully.



- Click on **OK** to return to the Lock Options screen.
- The key should now be taken to the lock to add/delete users to/from the lock.

Note: *Previous to uploading any data to a lock, the Master User PIN must be “set” in the lock. The default PIN assigned to the Master User is “12345”. The default PIN assigned to a new User or Supervisor ID is “55255”. A user must change this default PIN before any lock operations can be performed. See the **Unicon CL20 Operating Instructions** for further detail.*

Program Lock Access Schedules

By default, the lock is set to have no access schedule restriction for all seven days. This means that users can open the lock at any time during any day. This option allows access schedules to be programmed at the PC and then uploaded to the lock.

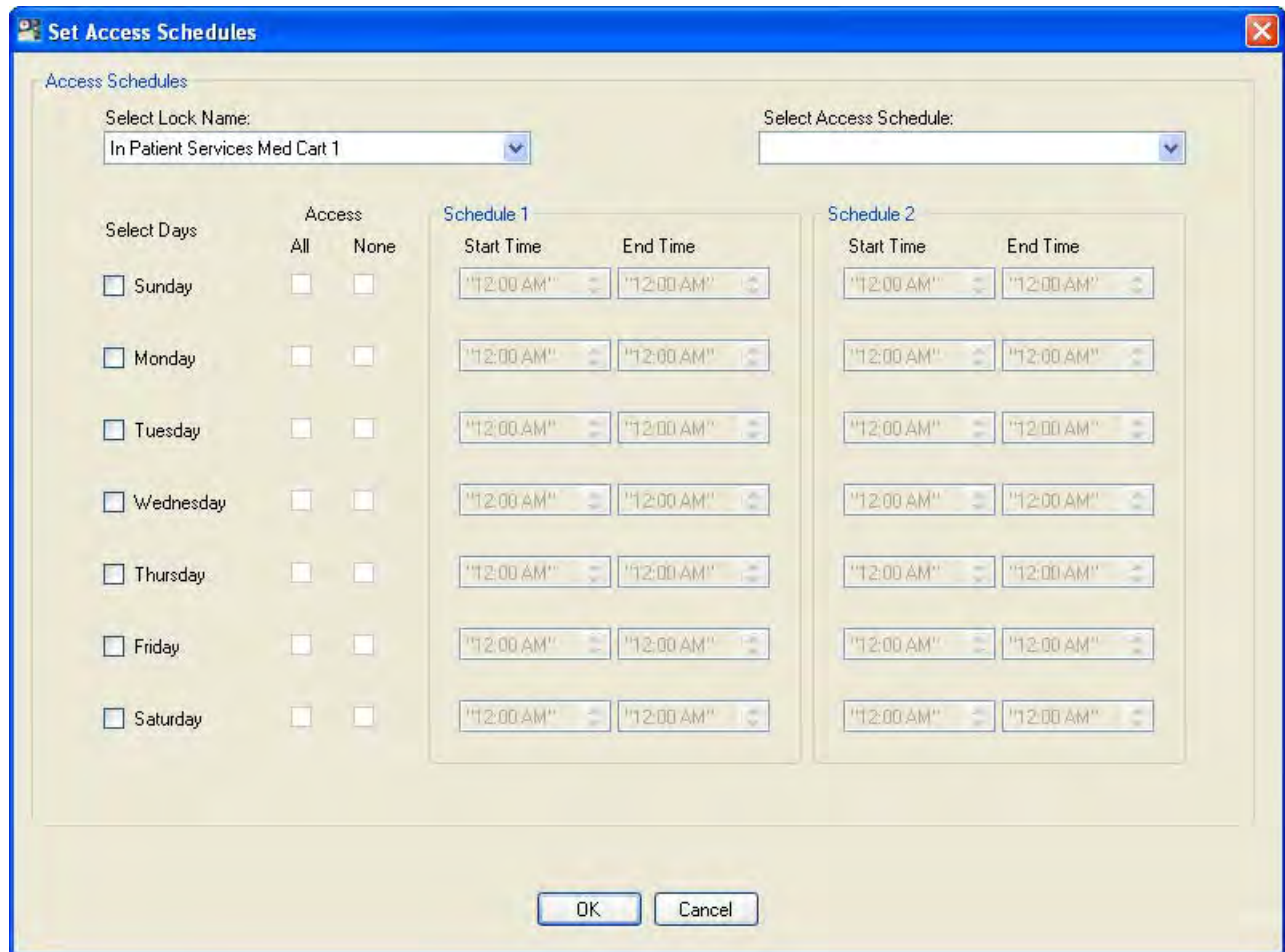
Note: *The access schedule settings will default to “all access” at the lock unless defined otherwise via manual programming at the lock or via data upload to the lock from the software.*

From the Locks menu:

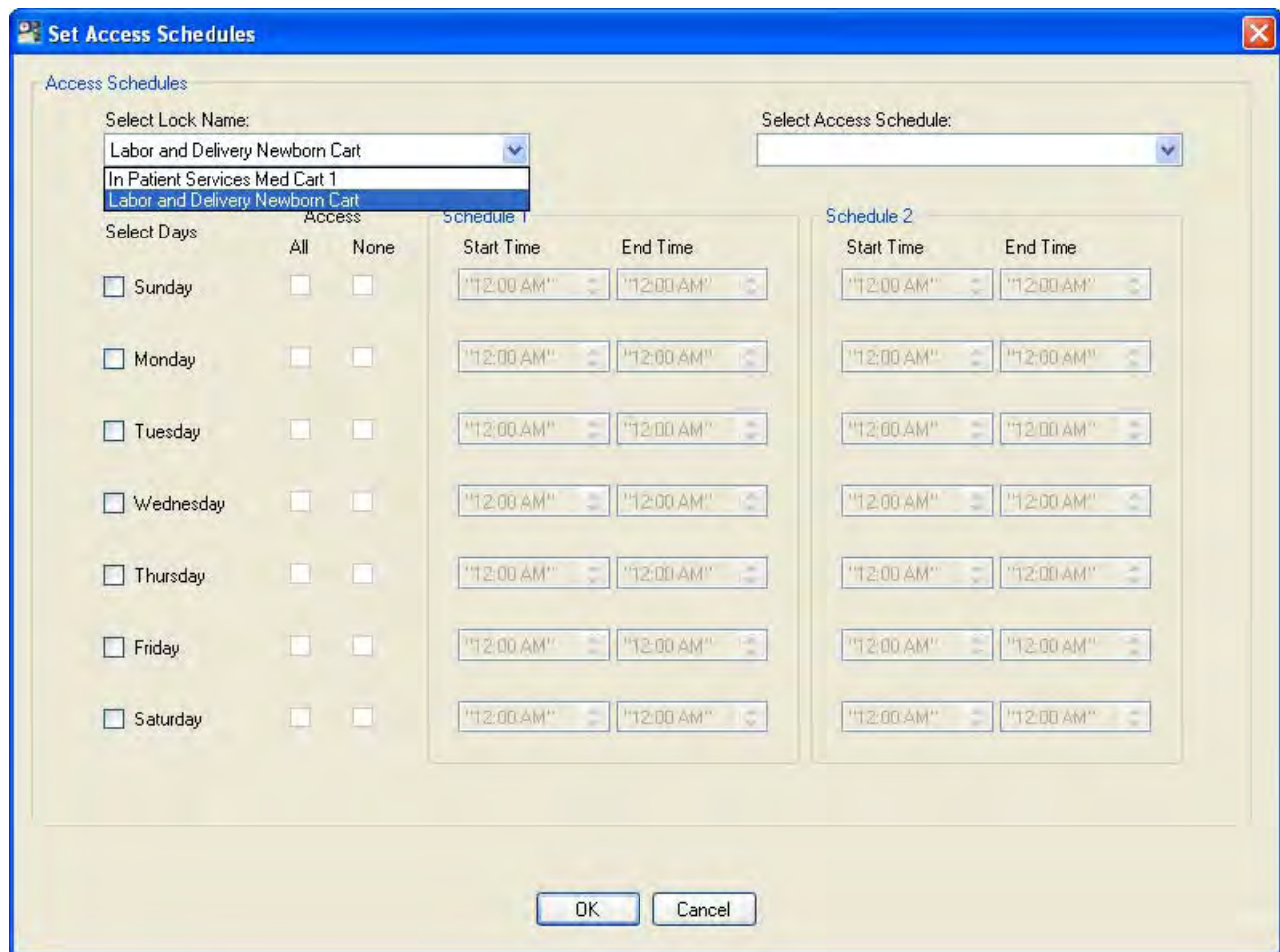
1. Select **Program Lock Access Schedules**.

The “Set Access Schedules” screen is displayed.

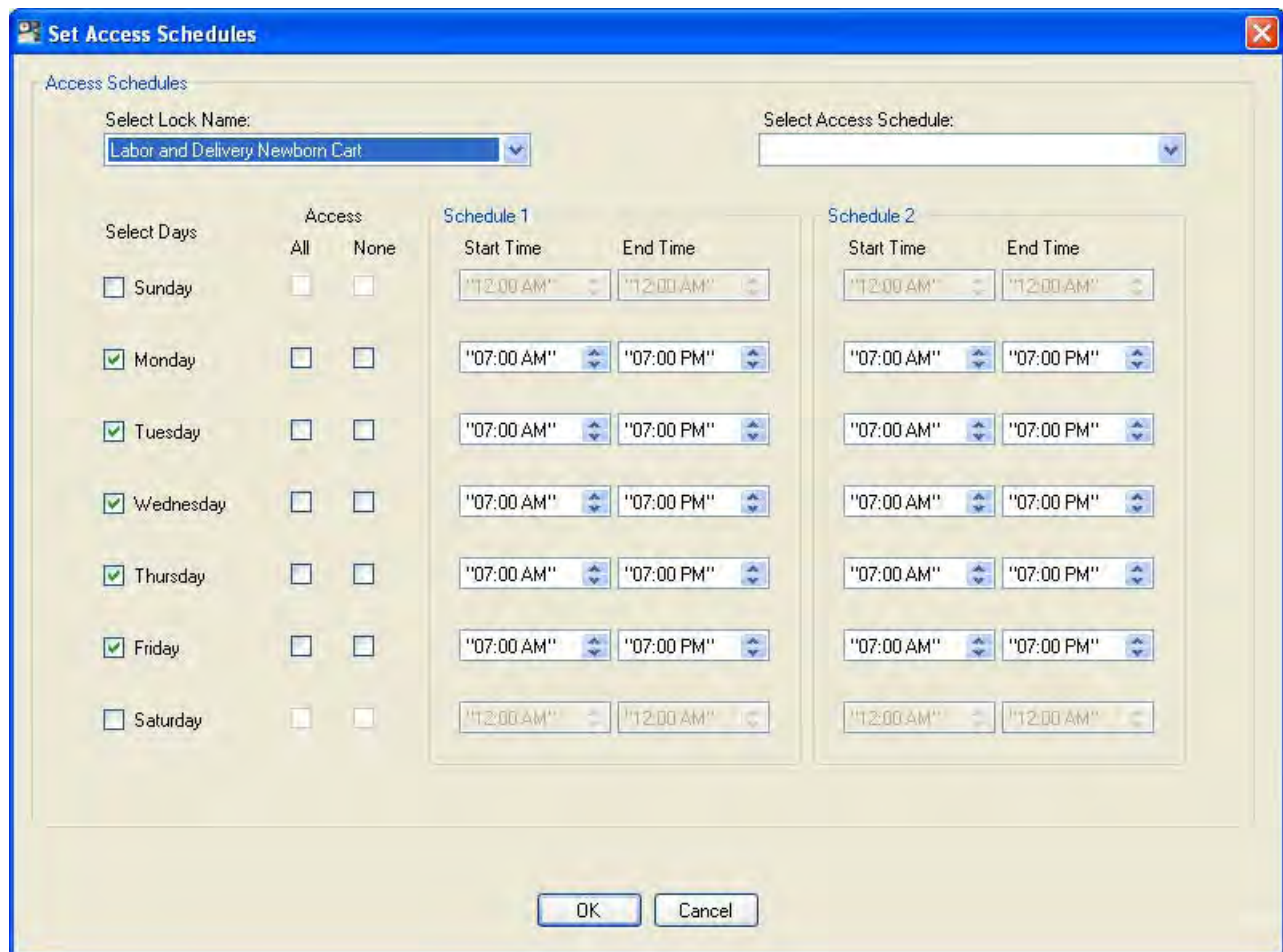
Note: *The first lock (in alphabetical order) is shown as the default.*



2. Select the name of the lock whose access schedules you wish to update.



Once the lock is selected, the current access schedules defined for the lock will be displayed.

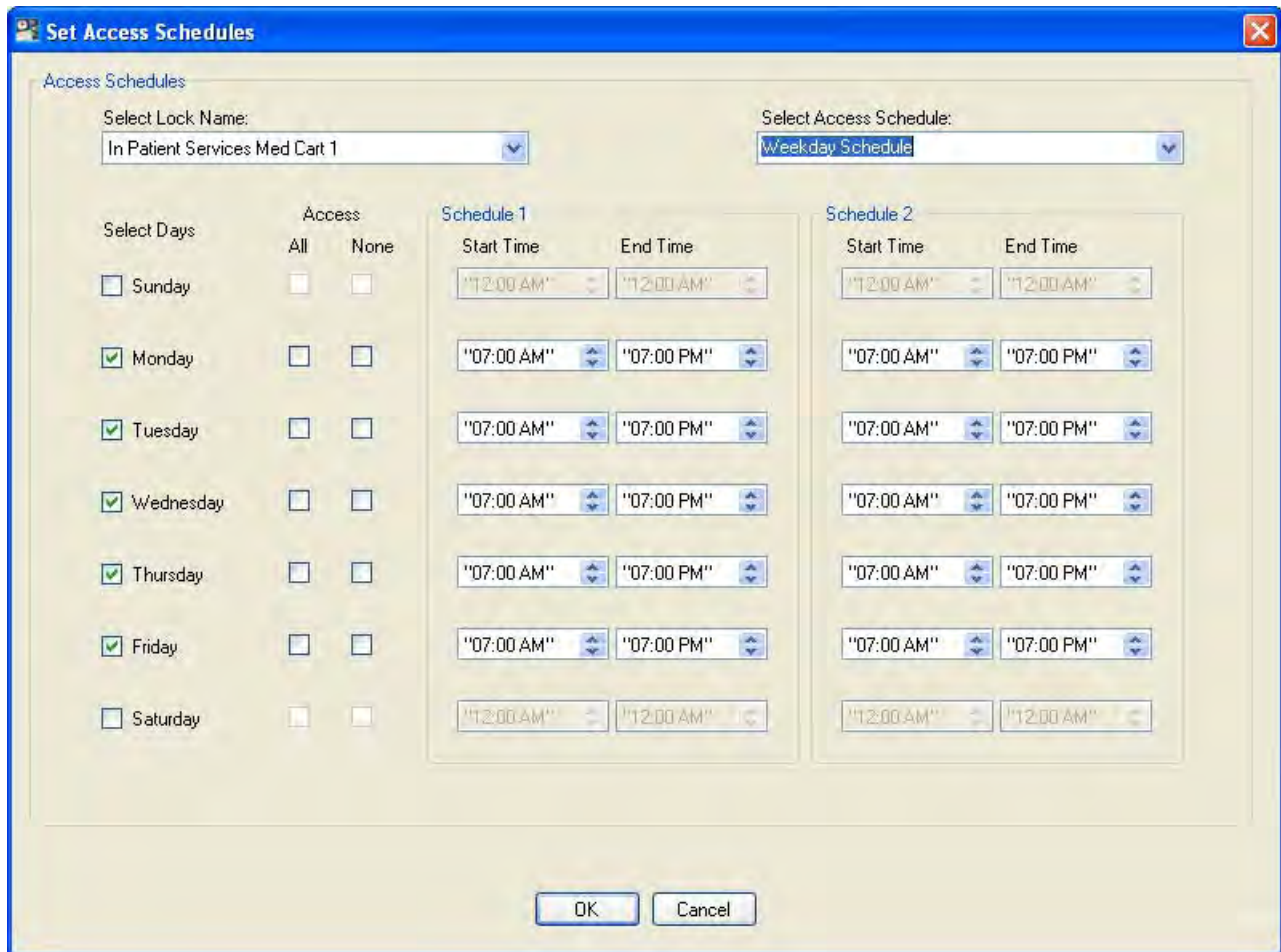


Assign Access Schedules to Lock from Access Schedule Template

If you want to assign the access schedules for the lock from a predefined Access Schedule template, complete the following steps:

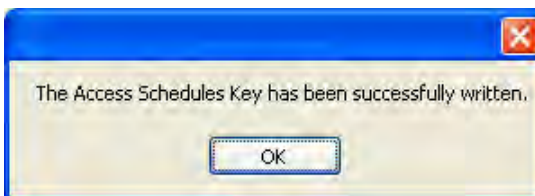
1. Select the Access Schedule from the Select Access Schedule dropdown window.

The fields will be filled with the predefined access schedule values.



2. Ensure that a programming key fob has been attached to the Unicon data cable and click on **OK**.

The following message window is displayed to indicate that the Access Schedules key was written successfully.



Assign Access Schedules to Lock

If you want to define the access schedules for the lock individually, complete the following steps:

1. To change the access schedule settings for a given day, click on the Select Days box for that day. If the box is not checked, the lock window settings will not be affected for that day and will remain set to whatever values are currently set at the lock.

Note: *The access schedule settings will default to “all access” at the lock unless defined otherwise via manual programming at the lock or via data upload to the lock from the software.*

Once the Select Days box has been selected for a specific day, the other input fields for that day will become enabled for data entry.

The screenshot shows the 'Set Access Schedules' dialog box. At the top, there are two dropdown menus: 'Select Lock Name:' with 'Labor and Delivery Newborn Cart' selected, and 'Select Access Schedule:' which is empty. Below these are two columns of settings. The first column, 'Select Days', lists days from Sunday to Saturday with checkboxes. Monday through Friday are checked. The second column, 'Access', has 'All' and 'None' options. The third and fourth columns, 'Schedule 1' and 'Schedule 2', each have 'Start Time' and 'End Time' dropdown menus. For Monday through Friday, the start times are '07:00 AM' and end times are '07:00 PM'. For Saturday and Sunday, both start and end times are '12:00 AM'. At the bottom are 'OK' and 'Cancel' buttons.

- 2a. If you want No Access Restriction (24 hour access) for the selected day, select the appropriate box for “All Access”. All other input fields will become unavailable for that day.

2b. If you want no lock access allowed for the selected day, select the “None” box. All other input fields will become unavailable for that day.

2c. If you want to limit access to a certain time period of the selected day, define an access time window by entering a Start Time and End Time under the Schedule 1 section of the screen. Specify all times in HH:MM format. Enter times as they would be set at the lock.

Note: *When data is entered for Schedule 1, the same Start and End Time will automatically be filled in for Schedule 2 once you click into the second window.*

If you want to define a second access time window for the selected day, update the Start Time and End Time under the Schedule 2 section of the screen to the values for the second window.

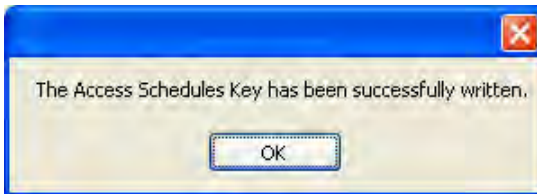
3. Tab to the Start Time in Schedule 2. If you want to define a second access time window for the selected day, update the Start Time and End Time under the Schedule 2 section of the screen to the values for the second window.

Note: *If you do not choose to define a second window, the second window will default to the same time period as the first window.*

Repeat steps 2 and 3 for each day that you would like to define lock access.

4. Once you are finished with the Access Schedules screen, ensure that a programming key fob has been attached to the data cable and click on **OK**.

The following message window is displayed to indicate that the Access Schedules Key was written successfully.



5. Click on **OK**.
6. The programming key fob should now be taken to the lock to update access schedule data in the lock.

Note: *Previous to uploading any data to a lock, the Master User PIN must be "set" in the lock. The default PIN assigned to the Master User is "12345". See the **Unicon CL20 Operating Instructions** for further detail.*

Program Lock Date & Time

This option allows the current date and time to be uploaded to the lock.

Time in the Unicon locks does not automatically adjust for Daylight Savings Time so must be adjusted via manual programming at the lock or via a Programming Key Fob programmed at the software.

If you change the batteries in the lock, you might also need to reset the date and time in the lock.

From the Locks menu:

1. Ensure that a programming key fob has been attached to the Unicon data cable and select **Program Lock Time**.

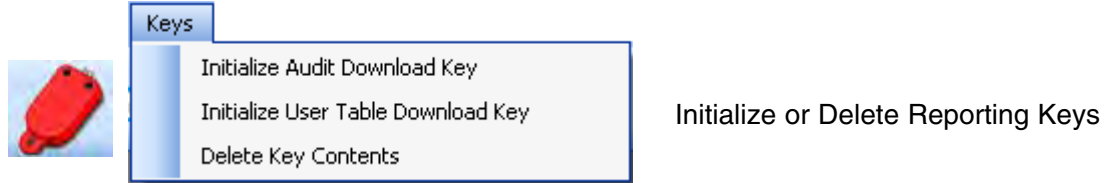
The following message window is displayed to indicate that the key to set the date and time was written successfully.



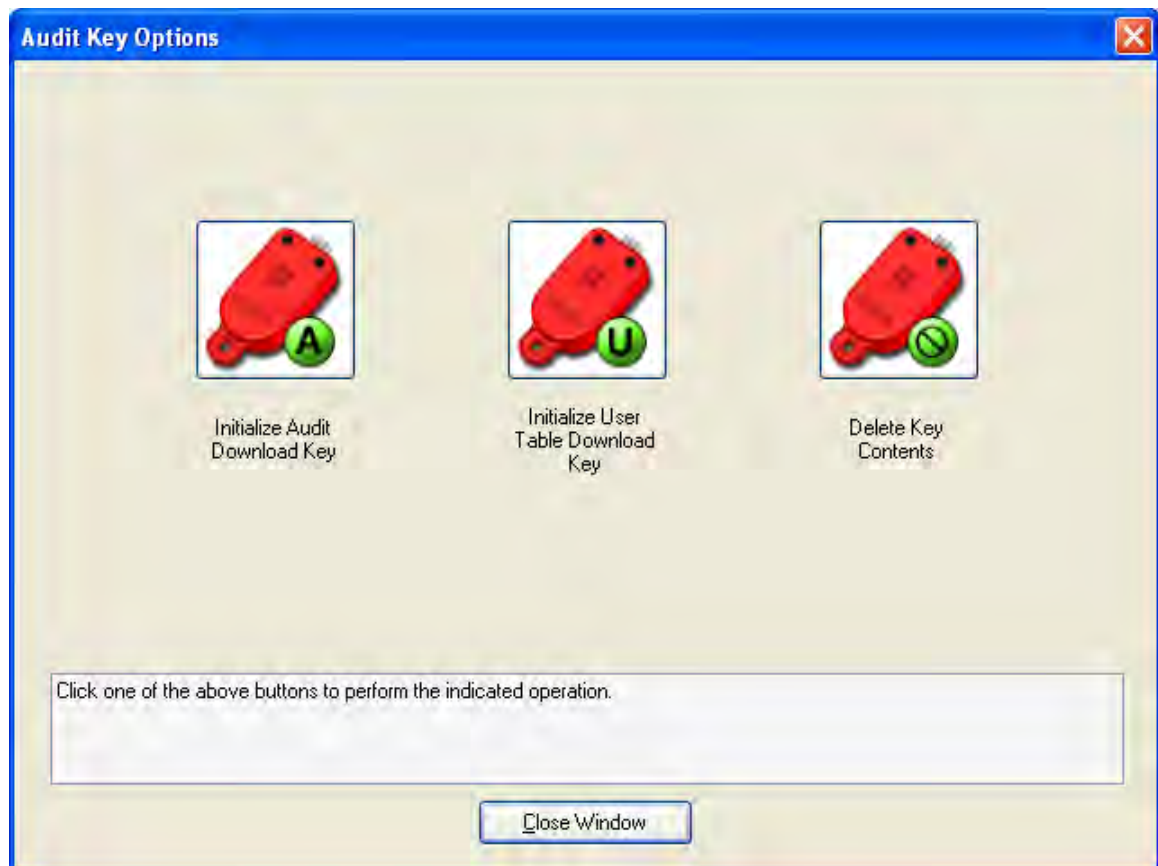
2. Click on **OK**.
3. The programming key fob should now be taken to the lock to program the lock date and time.

Note: *Previous to uploading any data to a lock, the Master User PIN must be "set" in the lock. The default PIN assigned to the Master User is "12345". See the **Unicon CL20 Operating Instructions** for further detail.*


Keys



The fifth menu option on the Main Menu is “Keys”. The reporting key fob is used to transfer data between the Unicon CL Series Software program and the locks. The reporting key fob is programmed by the Unicon CL Series program for a specific function and can only be used for that function until reprogrammed. The Keys menu options can also be accessed by selecting the Keys icon from the Toolbar.



From the Main menu:

1. Select the **Keys Menu** or the  toolbar icon.

Initialize Audit Download Key

The first option on the Keys menu is “Initialize Audit Download Key.” This function is used to initialize a Supervisor Audit key so that it can be taken to a lock to obtain an audit download from a lock’s memory. The key is then returned to this system so that the data can be retrieved from the key. From the Keys menu:

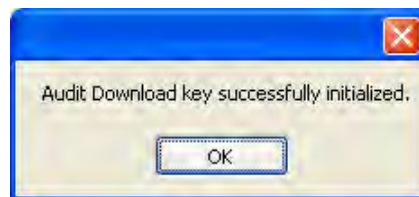
1. Select **Initialize Audit Download Key**.

If a reporting key fob has not been attached to the Unicon data cable, the following message will be displayed.



Ensure that there is a reporting key fob attached to the data cable and click on the **OK** button to proceed.

The reporting key fob will be initialized for the lock audit download and the following confirmation message will be displayed.



Note: *If you get a message window indicating a TMEX error, contact Kaba Mas Customer Support.*

3. Click on the **OK** button to close the window.
4. Take the reporting key fob to the lock to retrieve the audit data. Return the key to the PC to report on the audit data.

Initialize User Table Download Key

This option is used to initialize a reporting key fob so that it can be used to download the user table from a lock. From the Keys menu:

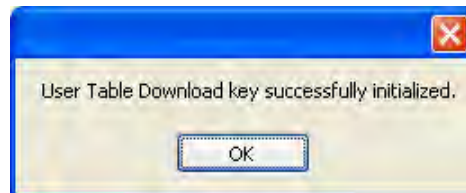
1. Select **Initialize User Table Download Key**.

If a reporting key fob has not been attached to the Unicon data cable, the following message will be displayed.



Ensure that there is a reporting key fob attached to the data cable and click on the **OK** button to proceed.

The reporting key fob will be initialized for the user table download and the following confirmation message will be displayed.



Note: *If you get a message window indicating a TMEX error, contact Kaba Mas Customer Support.*

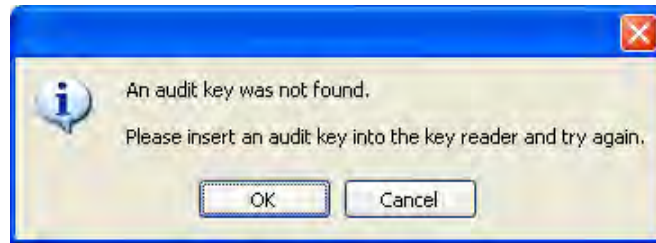
3. Click on the **OK** button to close the window.
4. Take the reporting key fob to the lock to retrieve the user table data. Return the key to the PC to report on the user data.

Delete Key Contents

The next option on the SA Keys menu is “Delete SA Key”. This option is used to delete the contents of a Supervisor Audit key after data has been retrieved from a lock. Once data has been retrieved from a lock and the data has been viewed, printed or saved through a Report option, you may want to delete the data from the key for security purposes. From the SA Keys menu:

1. Select **Delete Key Contents**.

If a reporting key fob has not been attached to the Unicon data cable, the following message will be displayed.



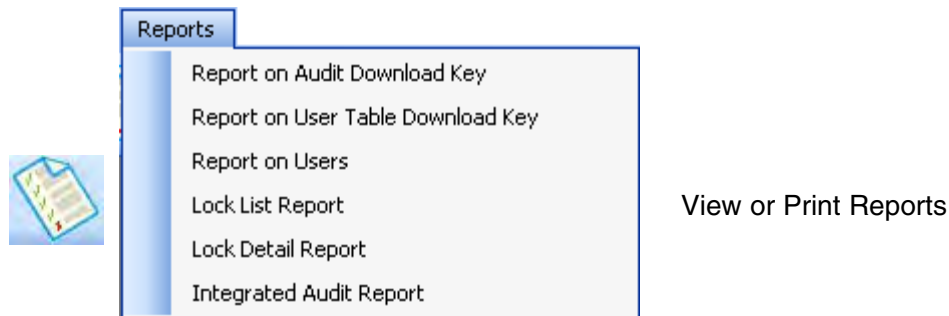
Ensure that there is a reporting key fob attached to the data cable and click on the **OK** button to proceed.

The contents of the reporting key fob will be deleted and the following confirmation message will be displayed.



3. Click on the **OK** button to close the window.

Reports



The Reports Menu option allows the operator to generate Crystal Reports from system data in addition to data that has been retrieved from the lock(s). The Reports menu options can also be accessed by selecting the Reports icon from the Toolbar.

Sort criteria is identified at the top of each report screen. You can change the sort criteria at any time by making your sort selections from the dropdown windows and then clicking on the **Submit** button.

There are standard functions available from the toolbar in all of the Crystal reports.

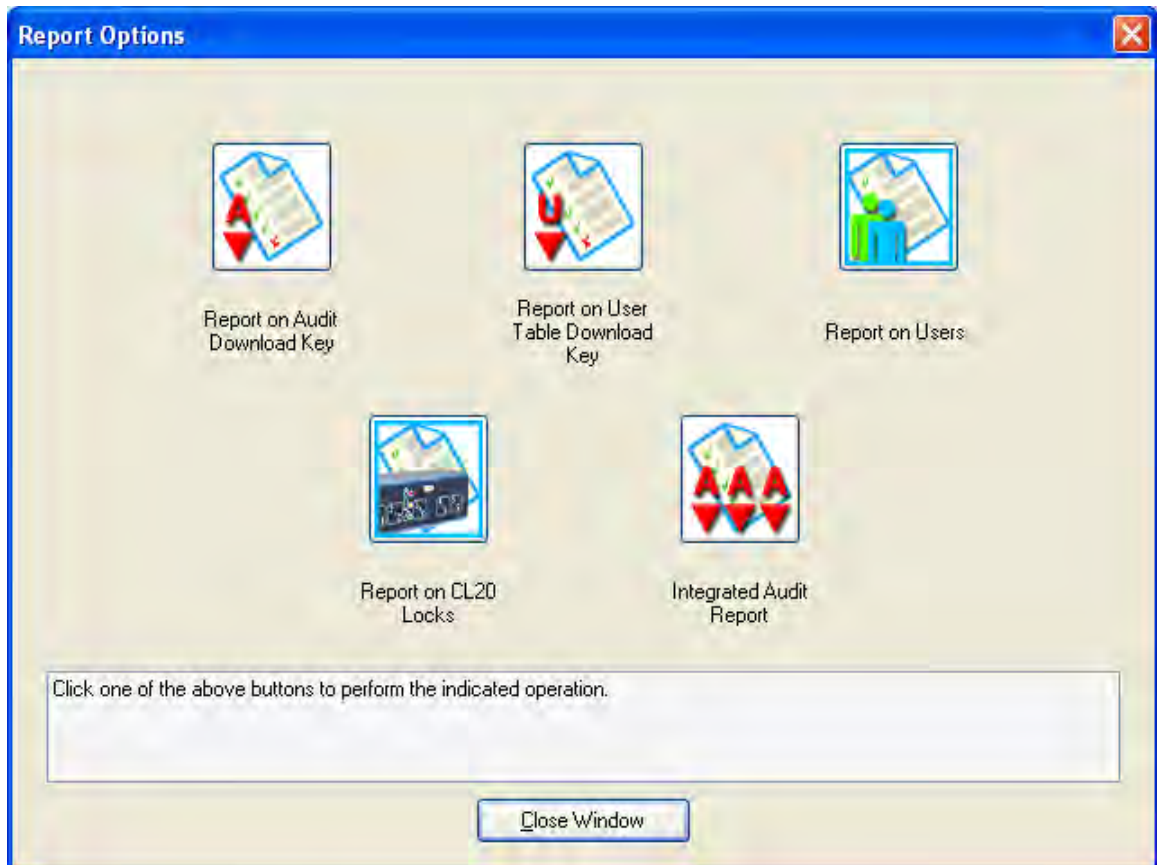


The toolbar supports paging forward, backward, to the first, the last or a specific page within a report. It also supports a search function which allows users to search for a string within a report. The toolbar allows users to zoom in or out of a report with a zoom factor between 25 and 400. Additionally, the toolbar supports the ability to close or refresh a report page, print a report, and export a report.

Caution: *When exporting a report to a file, you should only choose file types that are supported by third party software that is installed on your system.*

From the Main Menu:

1. Select the **Reports Menu** or the  tool bar icon.



Report on Audit Download Key

This option allows you to display a report on the contents of a Reporting Key Fob. This option will only report on a key that was initialized and used for an Audit Download from a lock and cannot be used for a user table report.

1. Select **Report on Audit Download Key**.

The reporting key reminder message will be displayed.



2. Make sure that the Reporting Key Fob with audit data is attached to the Unicon data cable.

3. Click on the **OK** button to close the window and display the audit data.

Some variations occur in the Audit Data Report depending on whether the audit data has been retrieved from a CL10 lock or a CL20. In both types of reports the report heading will be followed by the individual audit records.

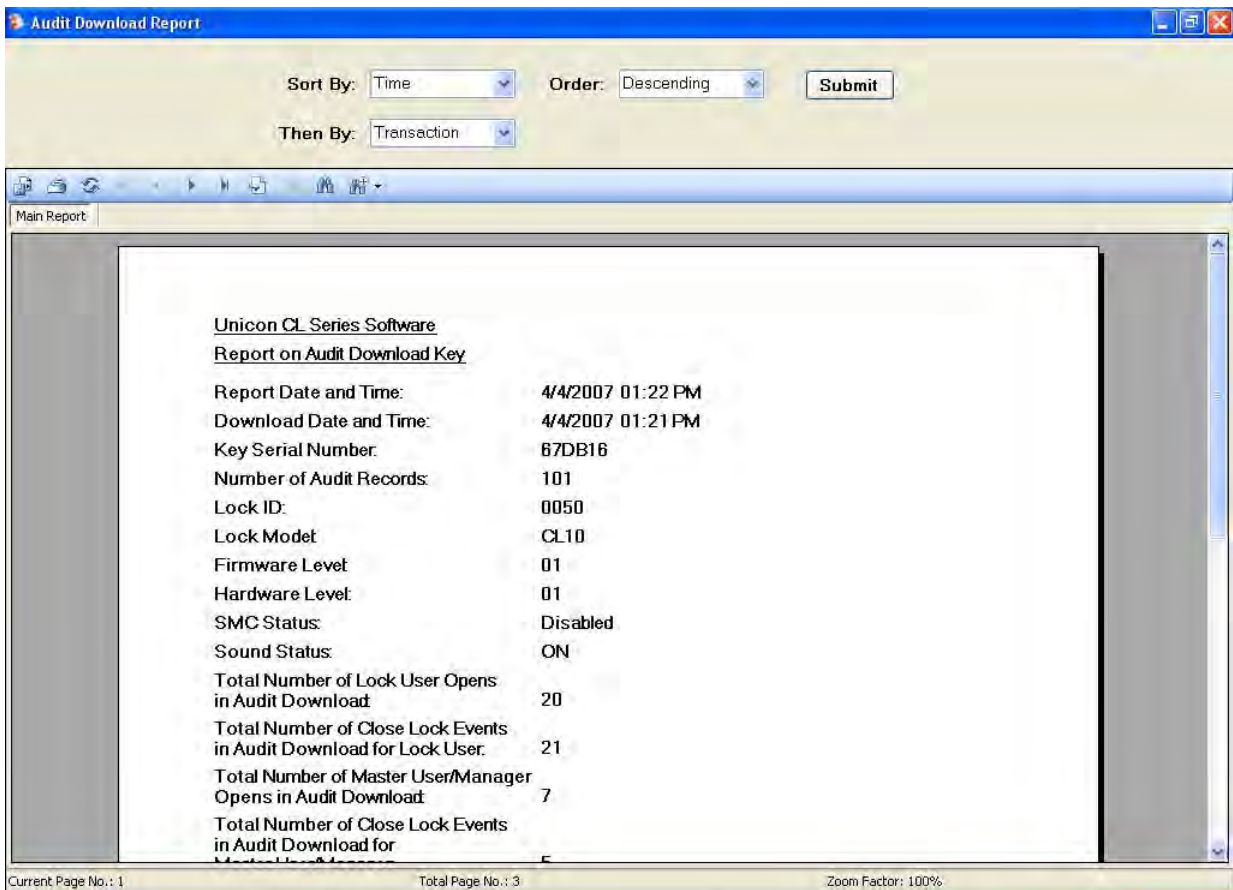
The User field on each audit record indicates the User ID of the person who performed that action.

A default date of 1/1/2070 and default time of 12:00 AM are initialized in the lock when it is programmed at the factory. Until the date & time in the lock are programmed from the PC, the default date & time stamp in the audit will reflect the factory initialized date & time.

Refer to the following sections for detailed information about each of the report types and the types of audit transactions found in the reports.

Model CL10 Audit Data Report

For audit data from a Model CL10 lock, the following screen is displayed.



You can change the Zoom on the report or page down to see the audit records.

Audit Download Report

Sort By: Time Order: Descending Submit

Then By: Transaction

Main Report:

in Audit Download for Master User/Manager. 5


Total Number of Key Override Opens in Audit Download 0

Transaction	User	Date & Time
Audit Download	111	4/4/2007 01:21 PM
Close Lock	200	4/4/2007 01:20 PM
Combination Locked State	200	4/4/2007 01:20 PM
Open Lock	200	4/4/2007 01:20 PM
Close Lock	200	4/4/2007 01:20 PM
Lock User Changed PIN	200	4/4/2007 01:20 PM
Combination Locked State	200	4/4/2007 01:20 PM
Open Lock	111	4/4/2007 01:20 PM
Close Lock	111	4/4/2007 01:20 PM
Combination Locked State	111	4/4/2007 01:20 PM
Program Lock Operation	111	4/4/2007 01:20 PM
Open Lock	111	2/13/2070 02:37 AM
Close Lock	111	2/13/2070 02:37 AM
Combination Locked State	111	2/13/2070 02:37 AM
Open Lock	111	2/12/2070 07:55 AM
Close Lock	111	2/12/2070 07:55 AM
Combination Locked State	111	2/12/2070 07:55 AM
Open Lock	200	1/24/2070 04:22 AM
Close Lock	200	1/24/2070 04:21 AM
Lock User Changed PIN	200	1/24/2070 04:21 AM
Combination Locked State	200	1/24/2070 04:21 AM

Page 1 of 3

Current Page No.: 1 Total Page No.: 3 Zoom Factor: 100%

To sort the report differently, select a “Sort By” field, a “Then By” field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

Click on the red X Close button  in the upper right hand corner to close the report and return to the Reports Menu.

CL10 Audit Transaction Types and Definition: (in alphabetical order)

Activate/Change PIN

The PIN has been set or changed for the indicated User ID.

Add User

A user has been added to the lock either manually or using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Audit Download

The indicated User retrieved Audit data from the lock via a Reporting Key Fob.

Close Lock

The lock is in a “combination locked state” and the knob has been turned to the locked position to physically lock the lock. The User ID is that of the user who entered the combination to put the lock in a “combination locked state”.

Combination Locked State

The lock has been put into a “locked” state by a user. The Master User or a Manager User may have pressed the shift (arrow) key followed by a valid combination, or the Lock User may have entered a valid combination followed by the shift (arrow) key, to place the lock in this state. If the bolt is also extended, the lock is also “physically” locked. The User ID is that of the user entering the combination to lock the lock.

Delete User

A user has been deleted from the lock either manually or using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Disable SMC

The Super Master User Combination has been permanently disabled. The User ID is always 111 indicating action by the Super Master or Master User.

End DST (-1 hour)

The time in the lock has been set back by one hour to change over to Standard Time. The User ID is always 111 since only the Master User can perform this operation.

Key Override Open

The lock was opened via the physical Key Override. The User ID is always “—” since no specific user can be associated with this physical action.

Key Override Close

The bolt was extended back to the locked position after the physical Key Override open occurred. The User ID is always “—” since no specific user can be associated with this physical action.

Lock POR

The lock power has been reset. The User ID is always “—” for Lock POR operations since this transaction is not associated with a specific user.

Lock User Changed PIN

A new Lock User 4-7 digit combination has been set. The User ID is always 200 to indicate the temporary Lock User.

Master Shelve

The lock was “shelved” using the Master User combination. The User ID will always be 111 to indicate the Master User.

Open Lock

This transaction is generated after a valid combination has been successfully entered to access the lock. The User ID is that of the user who entered the combination. (The Lock User will be identified as User 200.)

Program Lock Operation

The lock has been programmed with data from the PC via the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Restrict Audit Access

Audit access (retrieval of data from the lock) has been restricted. The User ID is always 111 since only the Master User can perform this operation.

Set Lock ID

The Lock ID has been defined for the lock either manually at the lock or via the Programming Key Fob. User ID is always 111 since only the Master User can perform this operation.

Set Lock Time

User 111 has set the date & time in the lock using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Start DST (+1 hour)

The time in the lock has been set forward by one hour to change over to DST (Day light Savings Time). The User ID is always 111 since only the Master User can perform this operation.

Super Master Changed PIN

The Super Master PIN has been set or changed. The User ID is always 111 to indicate the Super Master.

Super Master Shelve

The lock was “shelved” using the Super Master User combination. The User ID is always 111 to indicate the Super Master.

User Table Download

The indicated User retrieved User Table data from the lock via a Reporting Key Fob.

Wrong Try Penalty

Three invalid attempts were made and generated a wrong try penalty lockout of 3 minutes. Any successive invalid attempts would generate an additional penalty. The User ID is always “—” since this is the result of invalid attempts and does not have a specific user associated with the result.

Model CL20 Audit Data Report

For audit data from a Model CL20 lock, the following screen is displayed.

The screenshot shows a web browser window titled "Audit Download Report". At the top, there are two dropdown menus labeled "Sort By:" and "Order:", followed by a "Submit" button. Below this is a navigation bar with a "Main Report" tab. The main content area displays the following information:

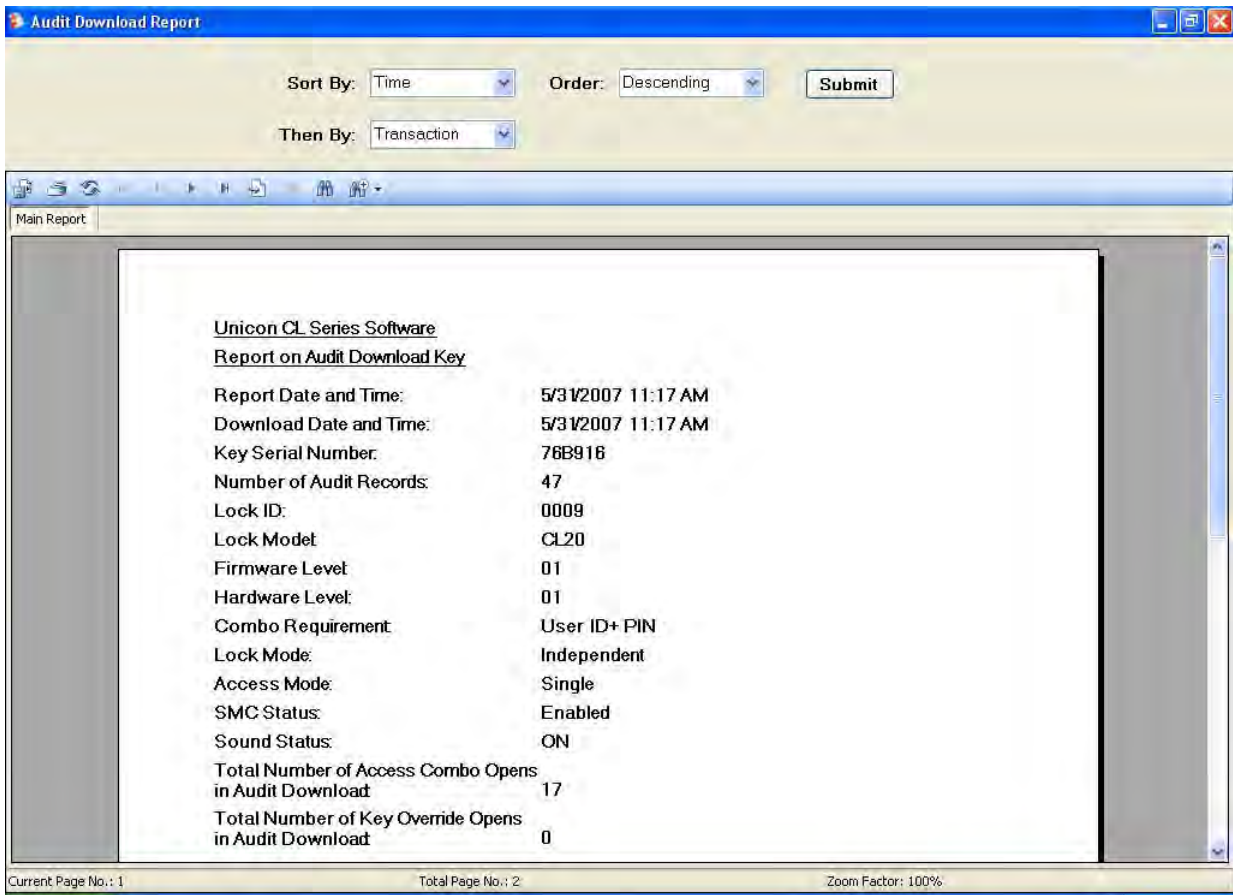
Unicon CL Series Software
Report on Audit Download Key

Report Date and Time:	8/30/2006 04:50 PM
Download Date and Time:	2/18/2070 11:21 PM
Key Serial Number:	DDFB14
Number of Audit Records:	171
Lock ID:	5555
Lock Model:	CL20
Firmware Level:	01
Hardware Level:	01
Combo Requirement:	User ID+ PIN
Lock Mode:	Independent
Access Mode:	Single
SMC Status:	Enabled
Sound Status:	ON
Total Number of Access Combo Opens in Audit Download:	22
Total Number of Key Override Opens in Audit Download:	61

[CLICK HERE TO VIEW ACCESS SCHEDULES](#)

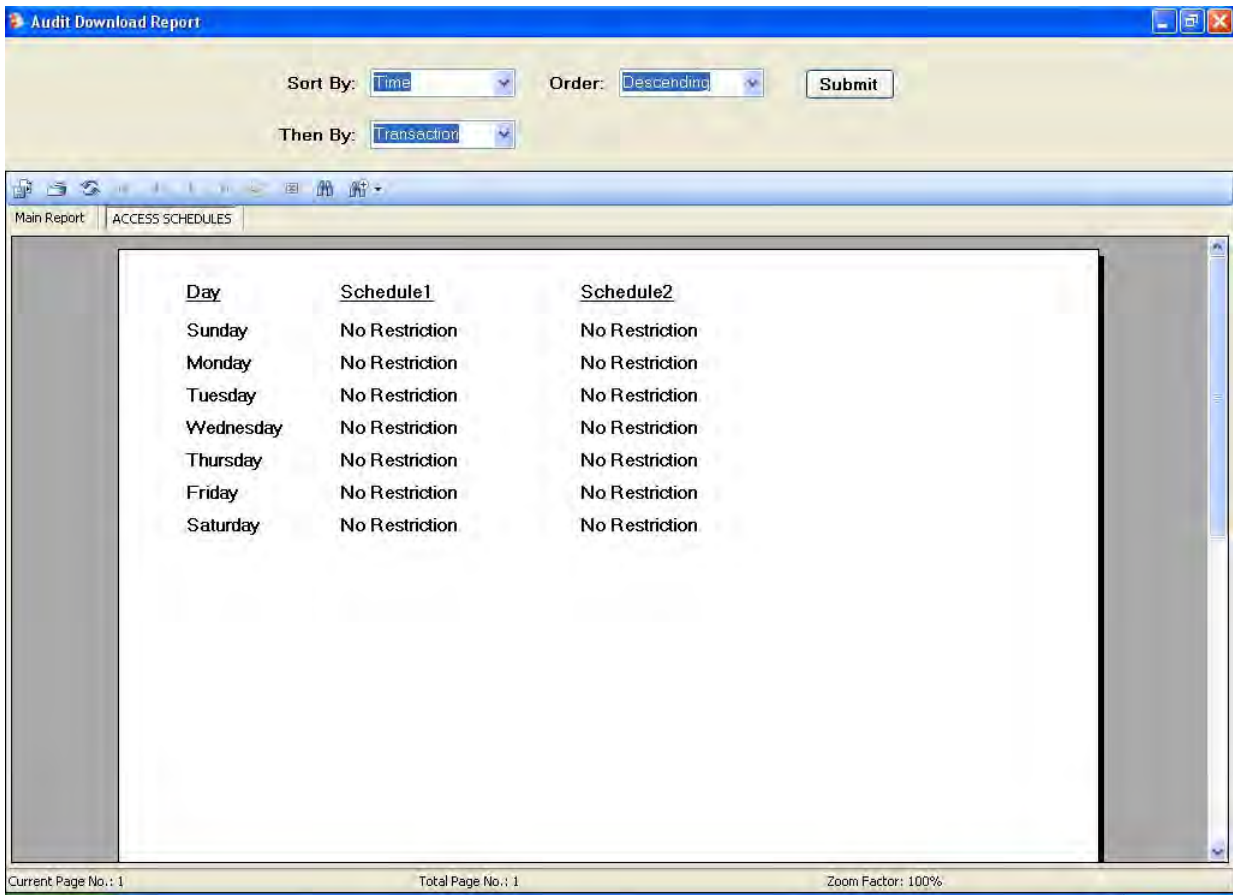
At the bottom of the window, there is a status bar with the following information: "Current Page No.: 1", "Total Page No.: 5", and "Zoom Factor: 100%".

You can change the Zoom on the report or page down to see the audit records.




To sort the report differently, select a “Sort By” field, a “Then By” field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

If you would like to view the access schedules defined in the lock, you can click on the report link for [CLICK HERE TO VIEW ACCESS SCHEDULES](#). A sub-report is displayed showing the Access Schedules.



To return to the Main Report, click on Main Report.

Click on the red X Close button  in the upper right hand corner to close the report and return to the Reports Menu.

CL20 Audit Transaction Types and Definition: (in alphabetical order)

Activate/Change PIN

The PIN has been set or changed for the indicated User ID.

Add User

A user has been added to the lock either manually or using the Programming Key Fob. The User ID is usually the Master User, or it could also be a Supervisor's ID if operating in Supervisor Subordinate Mode and the user added is a Subordinate.

Audit Download

The indicated User retrieved Audit data from the lock via a Reporting Key Fob.

Change to User ID only mode

The lock access requirement has been changed to only require a valid 3-digit User ID for access instead of the full 8-digit combination. User ID is always 111 since only the Master User can perform this operation

Change to User ID + PIN mode

The lock access requirement has been changed back to require the full 8-digit combination for access instead of only a valid 3-digit User ID. User ID is always 111 since only the Master User can perform this operation.

Close Lock

The lock is in a locked state because the “time to open lock” period knockoff has occurred and the knob has been turned to the locked position to physically lock the lock. The User ID is that of the user who previously entered the combination to open the lock.

Delete User

A user has been deleted from the lock either manually or using the Programming Key Fob. The User ID is the Master User or It could also be a Supervisor’s ID if operating in Supervisor Subordinate Mode and the user deleted is a Subordinate.

Disable SMC

The Super Master User Combination has been permanently disabled. The User ID is always 111 indicating action by the Super Master or Master User.

Disable Subordinate Users

A supervisor’s group of Subordinate Users has been disabled for lock access. The User ID is that of the supervisor disabling his own or another supervisor’s Subordinates.

Enable Subordinate Users

A supervisor’s group of Subordinate Users has been enabled for lock access. The User ID is that of the supervisor enabling his own or another supervisor’s Subordinates.

End DST (-1 hour)

The time in the lock has been set back by one hour to change over to Standard Time. The User ID is always 111 since only the Master User can perform this operation.

First User Entered PIN

When operating in Dual Access mode, this transaction is generated when the first valid user combination (User ID + PIN) is entered. The User ID is that of the user who entered the combination.

Key Override Open

The lock was opened via the physical Key Override. The User ID is always “—” since no specific user can be associated with this physical action.

Key Override Close

The bolt was extended back to the locked position after the physical Key Override open occurred. The User ID is always “—” since no specific user can be associated with this physical action.

Lock POR

The lock power has been reset. The User ID is always “—” for Lock POR operations since this transaction is not associated with a specific user.

Master Shelve

The lock was “shelved” using the Master User combination. The User ID will always be 111 to indicate the Master User.

Open Lock

This transaction is generated after a valid combination (or combinations if operating in Dual Access mode) has been successfully entered to access the lock. The User ID is that of the user who entered the combination or the user who entered the second combination if operating in dual mode.

Program Lock Operation

The indicated User has programmed the lock with data from the PC via the Programming Key Fob. The User ID is always 111 for the Master User unless the lock is operating in Supervisory/Subordinate mode, in which case a Supervisor is allowed to add and delete users via the Programming Key Fob.

Restrict Audit Access

Audit access (retrieval of data from the lock) has been restricted. The User ID is always 111 since only the Master User can perform this operation.

Set Access Schedules

Access schedules in the lock have been defined or modified via the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Set Lock ID

The Lock ID has been defined for the lock either manually at the lock or via the Programming Key Fob. User ID is always 111 since only the Master User can perform this operation.

Set Lock Time

User 111 has set the date & time in the lock using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Start DST (+1 hour)

The time in the lock has been set forward by one hour to change over to DST (Daylight Savings Time). The User ID is always 111 since only the Master User can perform this operation.

Super Master Changed PIN

The Super Master PIN has been set or changed. The User ID is always 111 for the Super Master.

Super Master Shelve

The lock was “shelved” using the Super Master User combination. The User ID is always 111 to indicate the Super Master.

User Table Download

The indicated User retrieved User Table data from the lock via a Reporting Key Fob.

Wrong Try Penalty

Five invalid attempts were made and generated a wrong try penalty lockout of 3 minutes. Any successive invalid attempts would generate an additional penalty. The User ID is always “—” since this is the result of invalid attempts and does not have a specific user associated with the result.

Report on User Table Download Key

This option allows you to display a report on the contents of a Reporting Key Fob. This option will only report on a key that was initialized and used for a User Table Download from a lock and cannot be used for an audit report.

1. Select **Report on User Table Download Key**.

The reporting key reminder message will be displayed.



2. Make sure that the Reporting Key Fob with User Table data is attached to the Unicon data cable.
3. Click on the **OK** button to close the window and display the lock’s user data.

Model CL10 User Table Report

For a user table from a Model CL10 lock, the following screen is displayed.

User Table Download Report

Sort By: Order:

Unicon CL Series Software
Report on User Table Download Key


Report Date and Time: 4/4/2007 02:12 PM
Download Date and Time: 4/4/2007 02:12 PM
Key Serial Number: 88EB16
Lock ID: 0050
Lock Model: CL10
Firmware Level: 01
Hardware Level: 01
SMC Status: Disabled
Sound Status: ON

<u>User ID</u>	<u>Status</u>
111	Added
112	Not Added
113	Not Added
114	Not Added
115	Added
121	Not Added
122	Not Added
123	Not Added
124	Not Added
125	Not Added

Current Page No.: 1 Total Page No.: 3 Zoom Factor: 100%

You can change the Zoom on the report or page down to see all of the user records.

To sort the report differently, select a “Sort By” field and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

Click on the red X Close button  in the upper right hand corner to close the report and return to the Reports Menu.

Model CL20 User Table Report

For a user table from a Model CL20 lock, the following screen is displayed.

Unicon CL Series Software
Report on User Table Download Key

Report Date and Time: 5/30/2007 11:46 AM
Download Date and Time: 7/17/2008 01:11 AM
Key Serial Number: 76B916
Lock ID: 0000
Lock Model: CL20
Firmware Level: 01
Hardware Level: 01
Combo Requirement: User ID+ PIN
Lock Mode: Independent
Access Mode: Single
SMC Status: Enabled
Sound Status: ON

[CLICK HERE TO VIEW ACCESS SCHEDULES](#)

User ID	ID 2	Status
111	111	Added
112	—	Not Added
113	—	Not Added

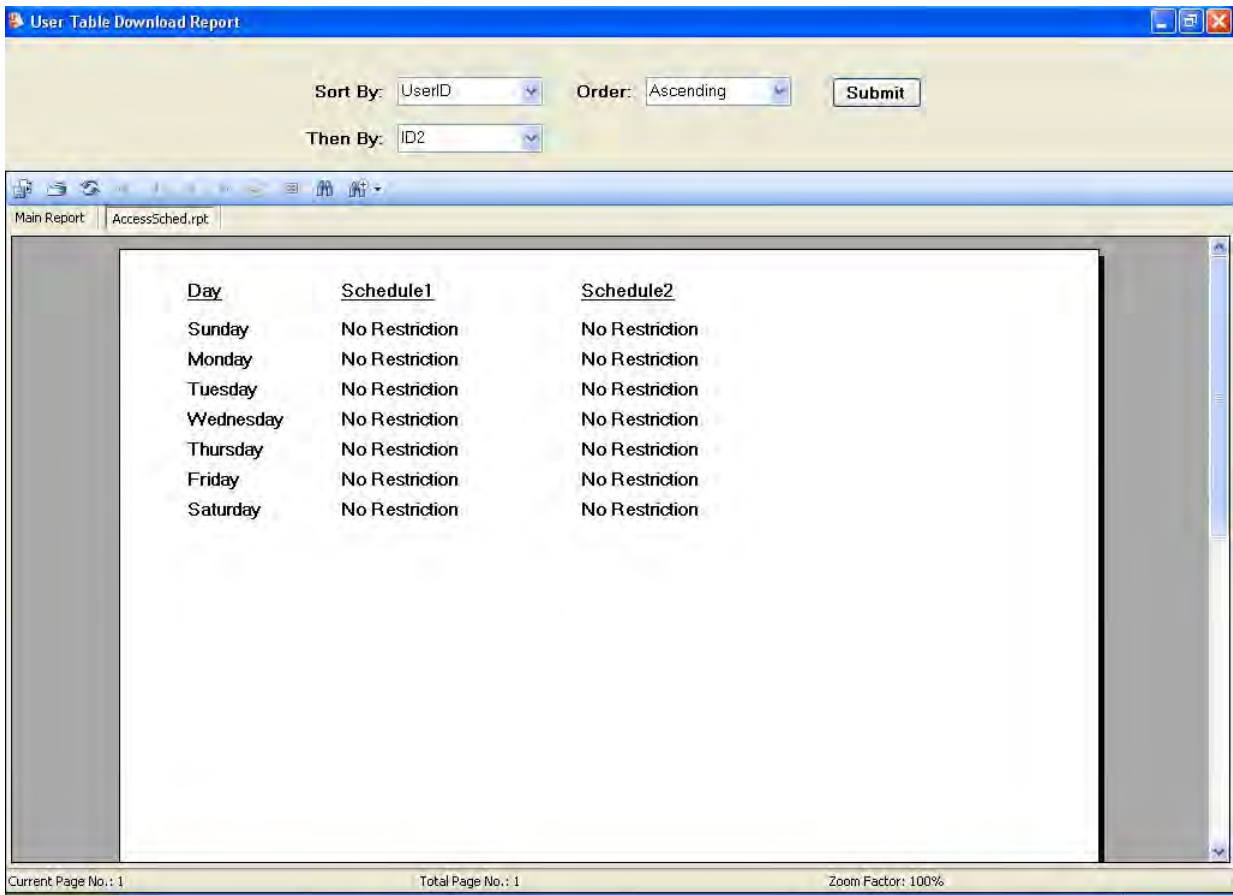
Current Page No.: 1 Total Page No.: 4 Zoom Factor: 100%

You can change the Zoom on the report or page down to see all of the user records.


The ID 2 field on each user table record indicates the User ID of the person who added the User.

To sort the report differently, select a “Sort By” field, a “Then By” field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

If you would like to view the access schedules defined in the lock, you can click on the report link for [CLICK HERE TO VIEW ACCESS SCHEDULES](#). A sub-report is displayed showing the Access Schedules.



To return to the Main Report, click on Main Report.

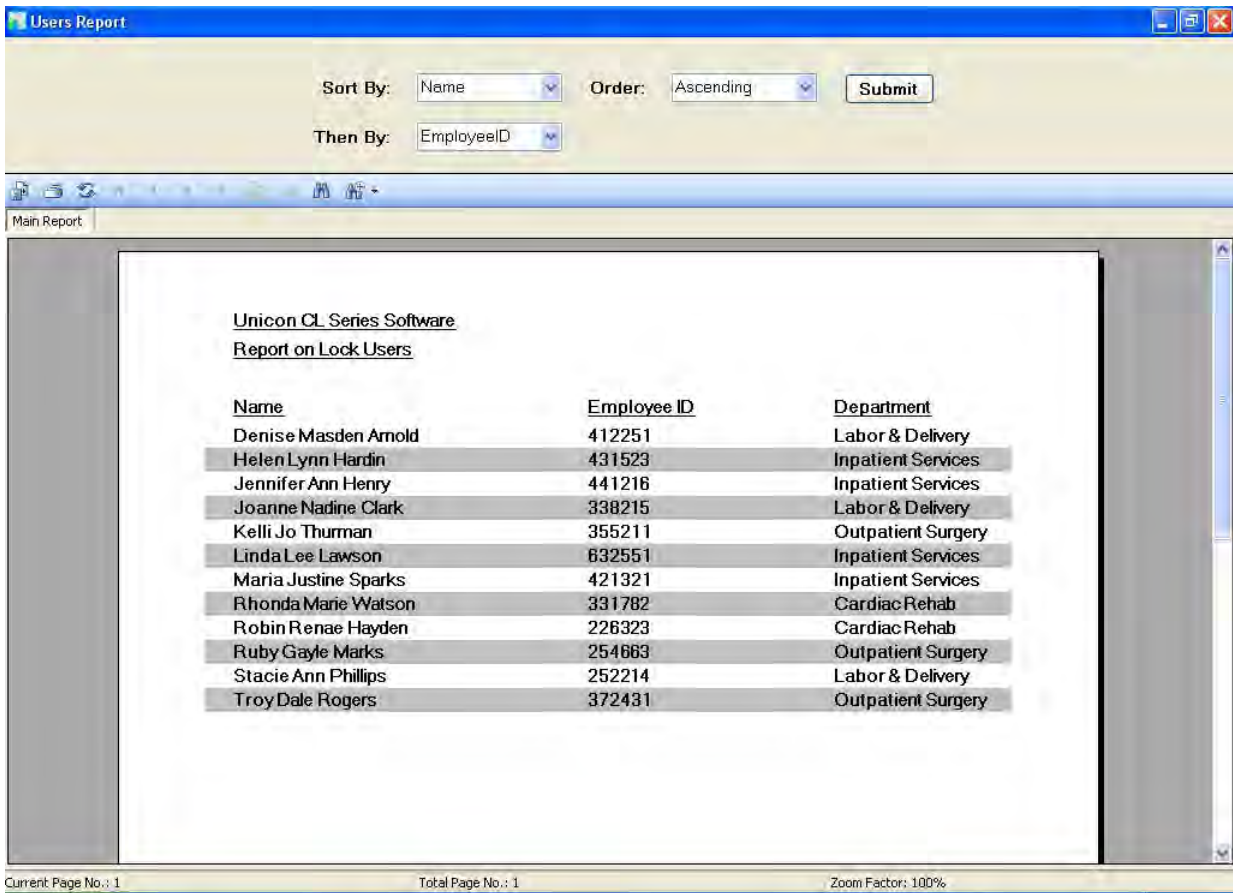
Click on the red X Close button  in the upper right hand corner to close the report and return to the Reports Menu.

Report on Users

This option allows you to display a report on the users defined at the PC in the Unicon database.


1. Select **Report on Users**.

The user data defined in the Unicon database at the PC is displayed.



You can change the Zoom on the report or page down to see all of the user records.

To sort the report differently, select a “Sort By” field, a “Then By” field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

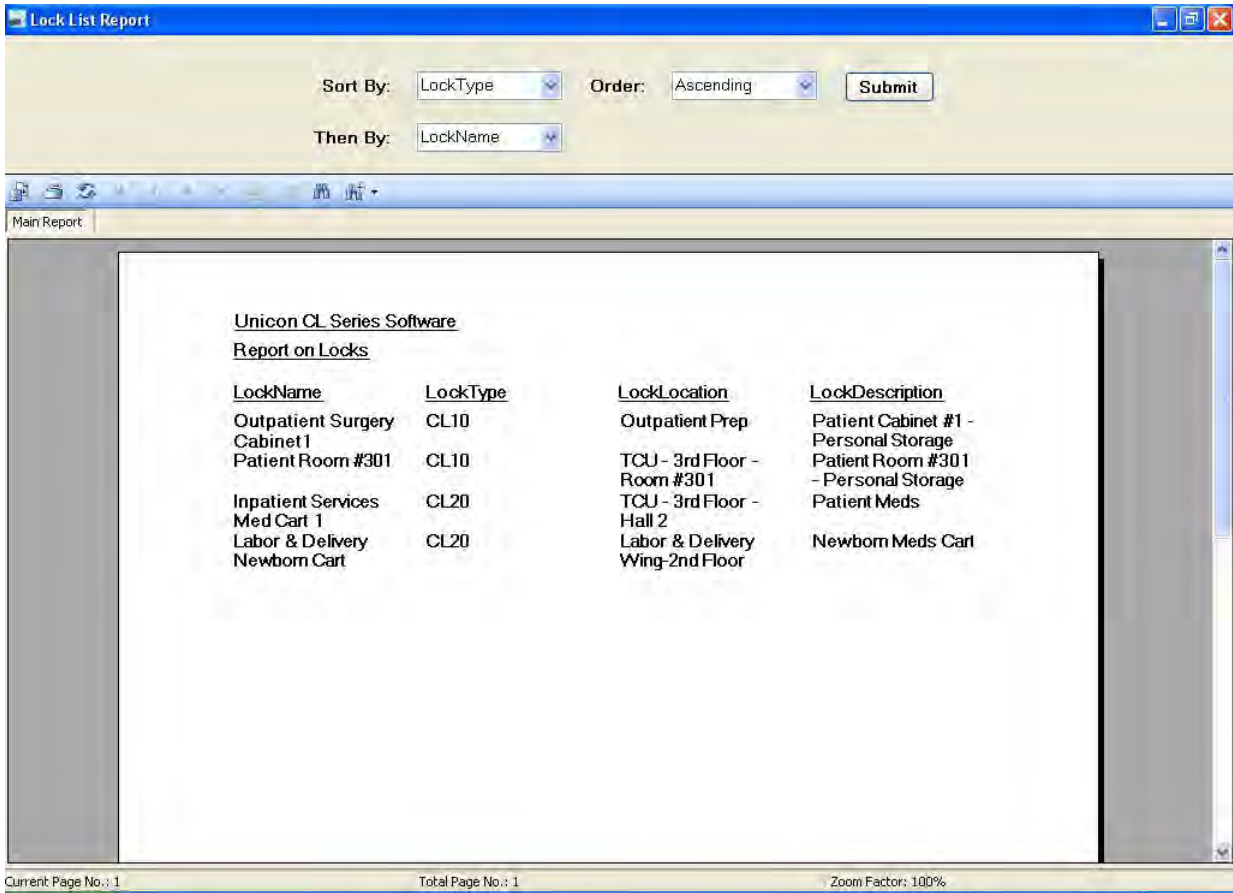
Click on the red X Close button  in the upper right hand corner to return to the Reports Menu.

Lock List Report

This option allows you to display a report for all of the locks (CL10 and CL20) defined at the PC in the Unicon database.


1. Select **Lock List Report**.

The locks defined in the Unicon database at the PC are displayed.



You can change the Zoom on the report or page down to see all of the user records for the first lock in the report. To view the remaining locks defined in the system, page forward.

To sort the report differently, select a “Sort By” field, a “Then By” field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

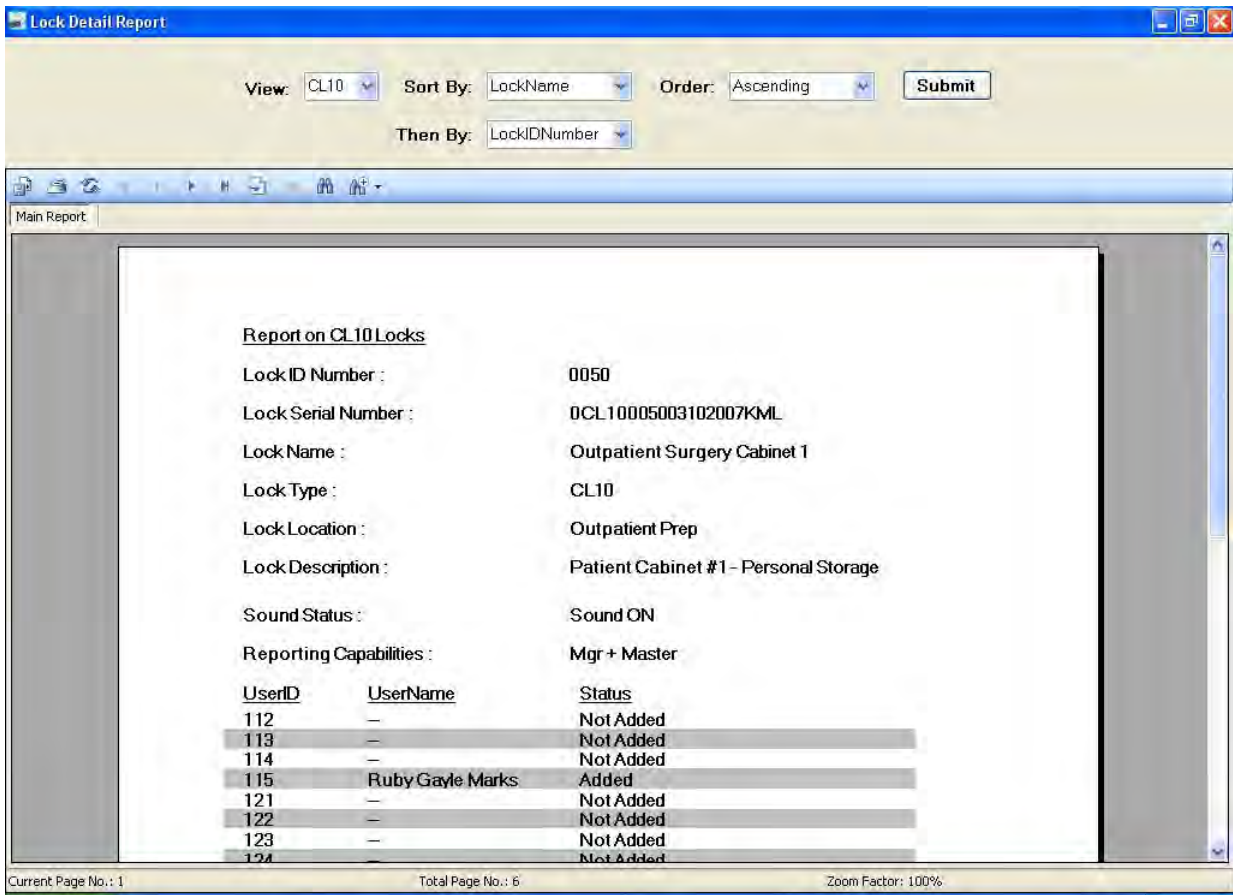
Click on the red X Close button  in the upper right hand corner to return to the Reports Menu.

Lock Detail Report

This option allows you to display a detail report on the locks defined at the PC in the Unicon database.

1. Select **Lock Detail Report**.


The locks defined in the Unicon database at the PC are displayed.



Note: *The report defaults to displaying only the locks for the current lock interface. You can change the lock selection by clicking on the **View** dropdown window.*

You can change the Zoom on the report or page down to see all of the user records for the first lock in the report. To view the remaining locks in the report, page forward.

To sort the report differently, select a “Sort By” field, a “Then By” field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the “Submit” button.

Click on the red X Close button  in the upper right hand corner to return to the Reports Menu.

Integrated Audit Report

This option allows you to integrate the contents of multiple audit report keys (CL10 and CL20) into one report. This option will only report on a keys that were initialized and used for Audit Downloads from a lock and cannot be used for a user table report.

Note: It is important to have assigned unique Lock IDs if you will be using this reporting capability.

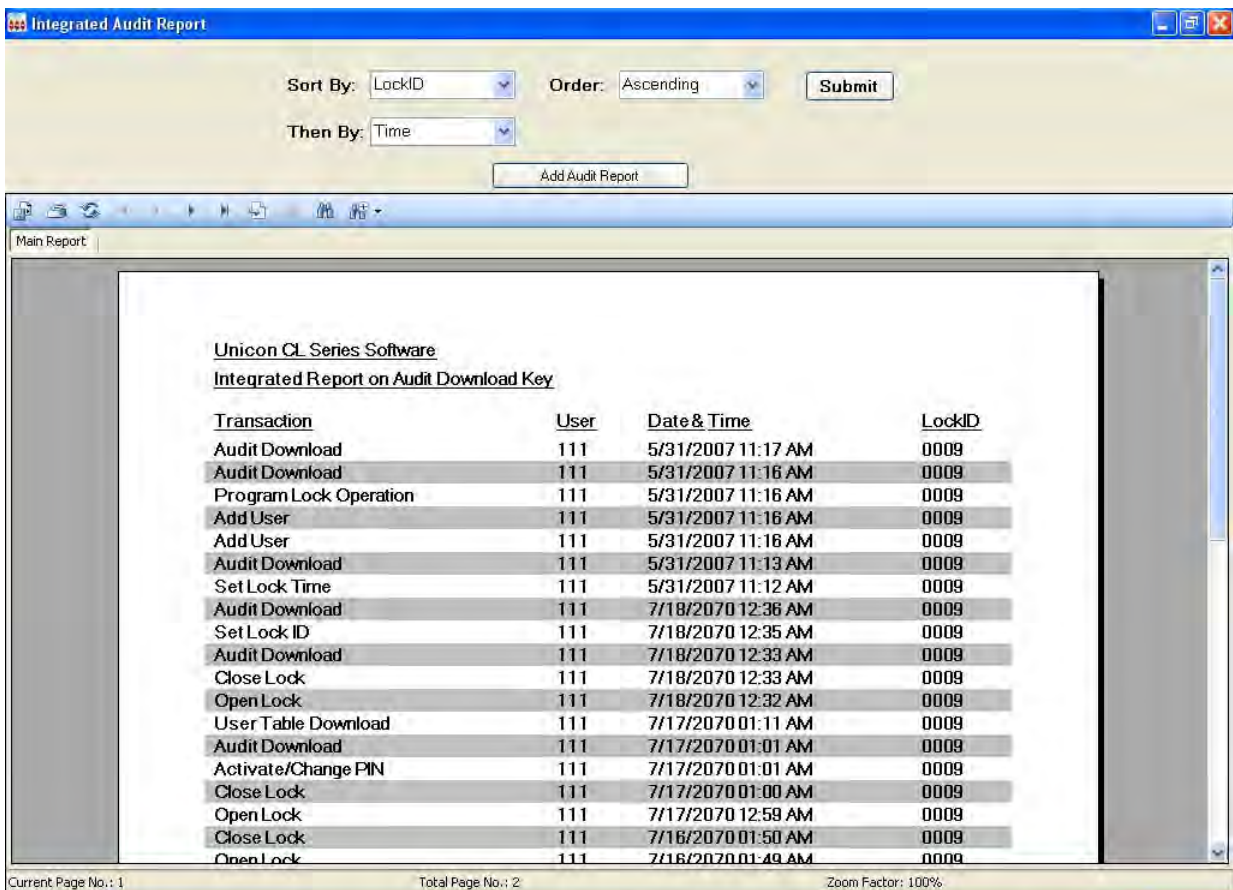
1. Select **Integrate Audit Report**.

The reporting key reminder message will be displayed.



2. Make sure that the Reporting Key Fob with audit data is attached to the Unicon data cable.

3. Click on the **OK** button to close the window and display the audit data.



4. To integrate the contents of another audit key into the report, attach a different Reporting Key to the Unicon data cable and click on the **Add Audit Report** tab.

The new key's audit data will be added to the report and the screen will be refreshed.

Sort By: LockID Order: Ascending Submit

Then By: Time Add Audit Report

Main Report:

Unicon CL Series Software
Integrated Report on Audit Download Key

Transaction	User	Date & Time	LockID
Audit Download	111	2/14/2070 11:58 PM	0000
Close Lock	111	2/14/2070 11:58 PM	0000
Open Lock	111	2/14/2070 11:58 PM	0000
Close Lock	111	2/9/2070 02:49 AM	0000
Open Lock	111	2/9/2070 02:49 AM	0000
Close Lock	111	2/9/2070 02:48 AM	0000
Open Lock	111	2/9/2070 02:48 AM	0000
Close Lock	111	2/9/2070 02:48 AM	0000
Open Lock	111	2/9/2070 02:48 AM	0000
Close Lock	111	2/9/2070 02:48 AM	0000
Open Lock	111	2/9/2070 02:48 AM	0000
Close Lock	111	2/9/2070 02:48 AM	0000
Open Lock	111	2/9/2070 02:48 AM	0000
Close Lock	111	2/9/2070 02:47 AM	0000
Open Lock	111	2/9/2070 02:47 AM	0000
Close Lock	111	2/9/2070 02:46 AM	0000
Open Lock	111	2/9/2070 02:46 AM	0000
Close Lock	111	2/9/2070 02:46 AM	0000
Open Lock	111	2/9/2070 02:45 AM	0000
Close Lock	111	2/9/2070 02:45 AM	0000
Open Lock	111	2/9/2070 02:45 AM	0000


Current Page No.: 1 Total Page No.: 6 Zoom Factor: 100%

5. Repeat Step 4 for as many audit reporting keys as you have to be included in the report.

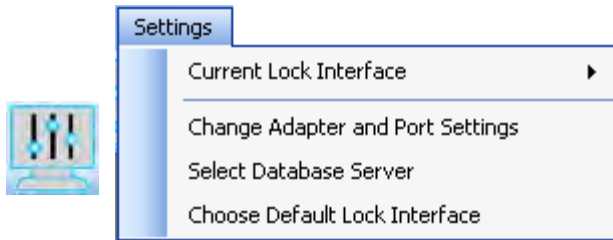
You can change the Zoom on the report or page down to see more of the audit records.

To sort the report differently, select a "Sort By" field, a "Then By" field (for secondary sort), and select the order in which you want it sorted (i.e., ascending or descending.) Then hit the "Submit" button.

Once you have integrated all of the data into the displayed report, you can save it out to a file by selecting the Export Report option from the Reports tool bar.

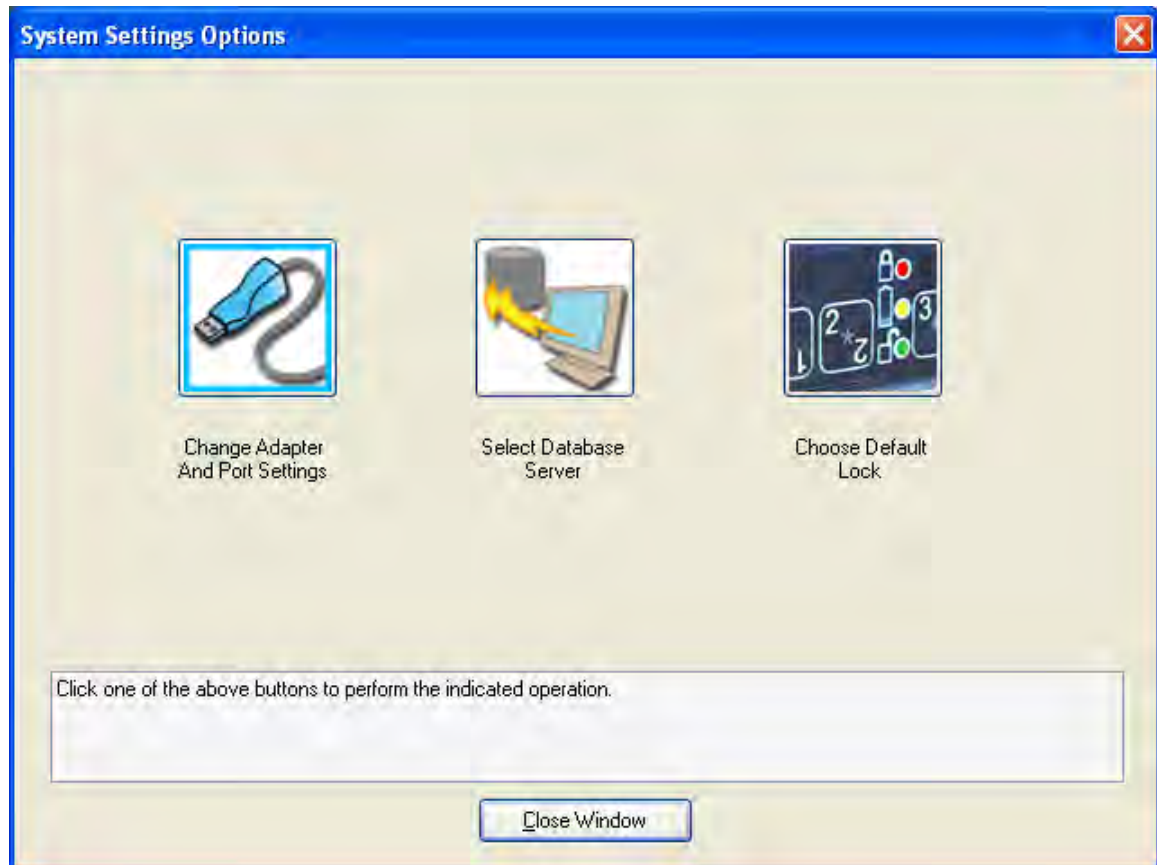
When you have finished with the report, click on the red X Close button  in the upper right hand corner to close the report and return to the Reports Menu.

Settings



Define or Maintain System Settings & Data

These menu options allow you to perform system maintenance functions. System Settings should be addressed at System startup but can also be maintained from this menu. The Settings menu options (other than Current Lock Interface) can also be accessed by selecting the Settings icon from the Toolbar.



From the Main menu:

1. Select the **Settings Menu** or the  toolbar icon.

Current Lock Interface

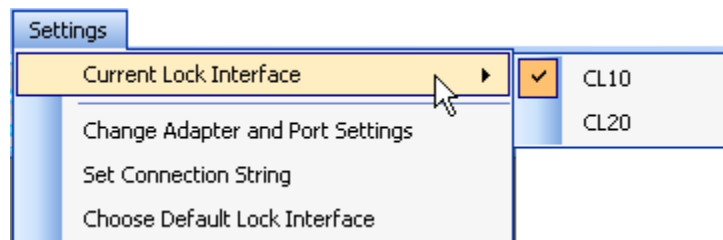
The Current Lock Interface setting indicates whether the CL10 or the CL20 lock interface for the software is currently presented. This menu option is used to determine the current lock interface setting and change it if desired.

At program startup this setting defaults to the Default Lock Interface setting as defined in the user profile for the user who is logged on to the PC.

The current lock interface can easily be toggled at anytime during operation of the software for customer applications where both types of locks are installed. From the Settings menu:

1. Select **Current Lock Interface**.

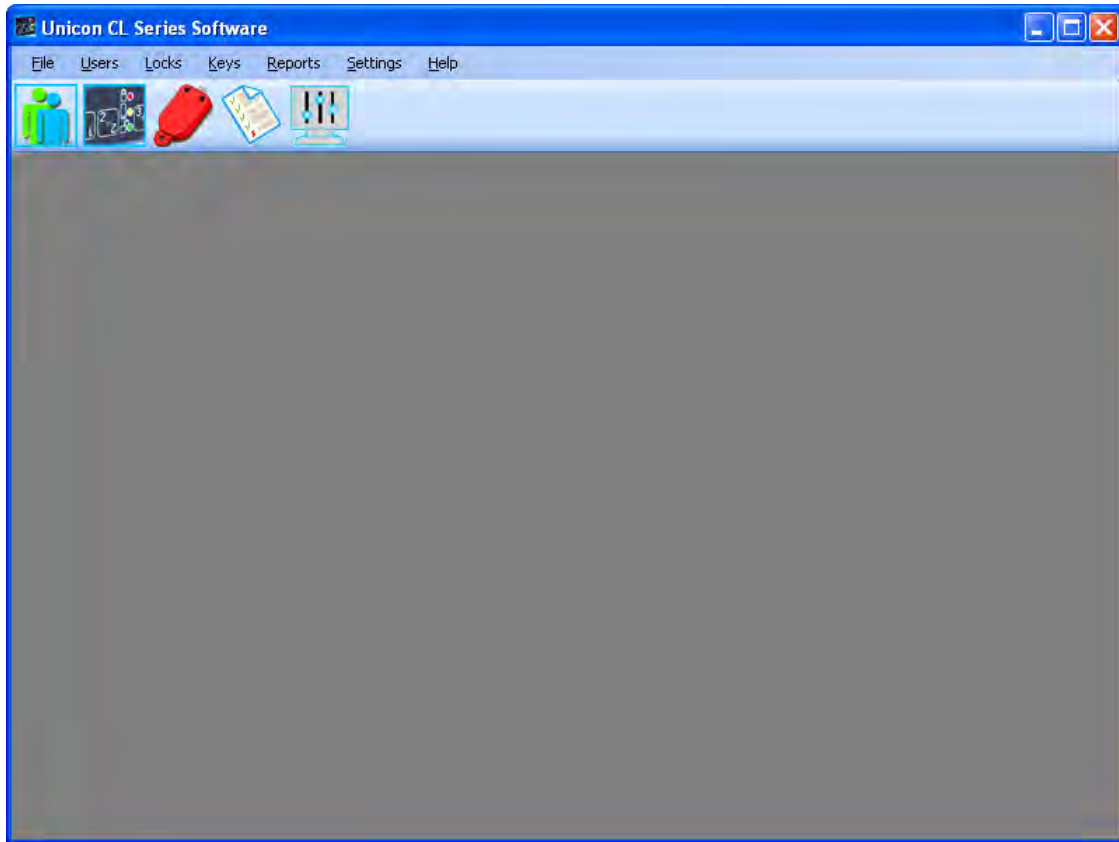
A second dropdown menu will appear indicating the Current Lock Interface.



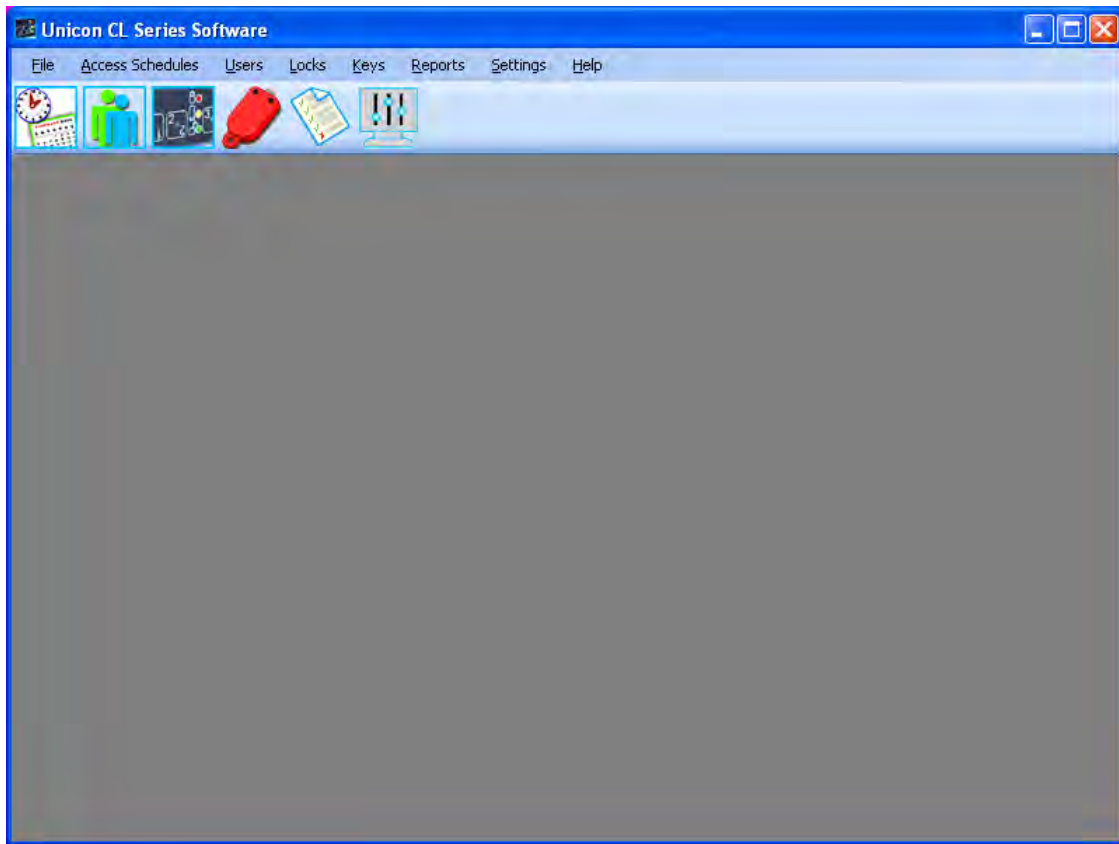
2. If you wish to switch to the alternate lock mode for your **Current Lock Interface**, click on the appropriate lock model in the menu.

The software interface for the chosen lock model will appear.

If the Model CL10 is selected for the Current Lock Interface, the following screen is displayed.



If the Model CL20 is selected for the Current Lock Interface, the following screen is displayed.

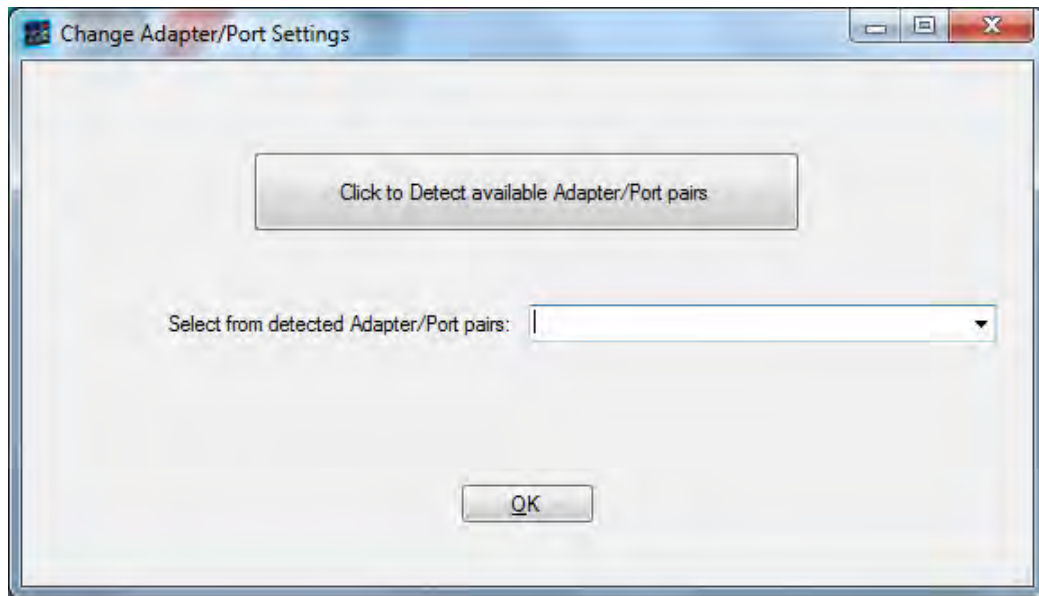


Change Adapter and Port Settings

This option is used to change the adapter and port settings in case the adapter type is changed or the adapter has to be moved to a different port. From the Settings menu:

1. Select **Change Adapter and Port Settings**.

The **Change Adapter/Port Settings** screen is displayed. This window prompts you to select what type of data cable adapter you have and where it is installed.



2. Click on the bar to "**Detect available Adapter/Port pairs**". Select the tab for the **Adapter Type** that you have installed with your system. The **default value** for the Adapter Type is the **DS9490 USB Adapter**. If the Adapter Type is different from the default, change it at this time.
2. Select the tab for the **Adapter Type** that you have installed with your system. The **default value** for the Adapter Type is the **DS9490 USB Adapter**. If the Adapter Type is different from the default, change it at this time.
3. If you are using a Serial Adapter, select the Com Port number where the key reader was installed. The **default value** for the Serial Port is **Com1**. If the Serial Port that you are using for the key reader is anything other than Com 1, change it at this time.

4. If you have updated the adapter and port settings, click on the **OK** button to save the changes.

Select Database Server

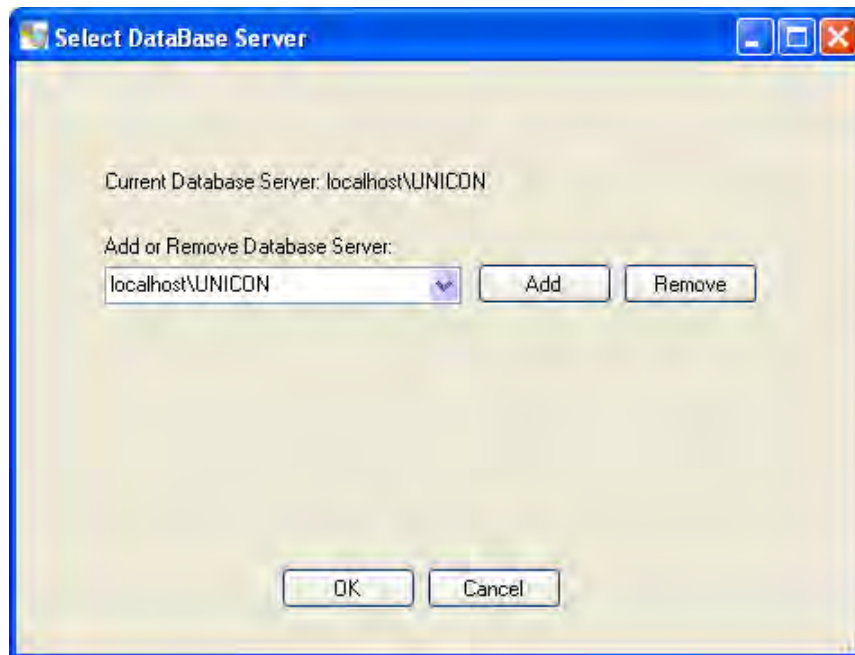
This option allows you to change the database server for this software application.

Note: *The default value is the local host instance of the Unicon database (localhost\UNICON).*

From the Settings menu:

1. Select **Select Database Server**.

The Select Database Server screen will be displayed.



2. If you wish to select a different database server, click on the drop down arrow to view available servers for selection.

Note: *If the required database server is not shown in the list, type in the database server name (Computer Name\UNICON) and click on the **Add** button.*

3. Select the database server name from the list.

- Click on the **OK** button to process the selection.

Choose Default Lock Interface

This option is used to change the Default Lock Interface setting for the current user.

The Unicon CL Series Software allows programming and reporting for both Model CL10 and Model CL20 locks. When you first load the Unicon CL Series Program, you will be prompted to select the default lock model for your activity. This setting determines whether the CL10 or the CL20 lock interface for the software will be presented when you start the program. This default setting will be associated with your User profile as it is known to the Windows operating system. This setting will determine the lock interface that is presented for you when the software is loaded.

From the Settings menu:

- Select **Choose Default Lock Interface**.

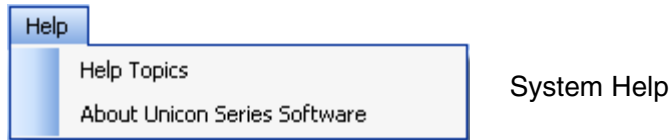
The **Choose Unicon Lock** screen is displayed. This window prompts you to specify which Unicon CL lock software interface you would like to have as a default on program startup.



- Select your personal Default Lock Interface setting for the Unicon CL Series Software and click on Save.

Note: *The Default Lock Interface setting can be changed at any time after the software is loaded. The Current Lock Interface setting can also be toggled during usage of the software.*

Help



From this menu, you can: 1) Access the online system help information, or 2) Display the Unicon CL Series Software version number and copyright information.

From the Main Menu:

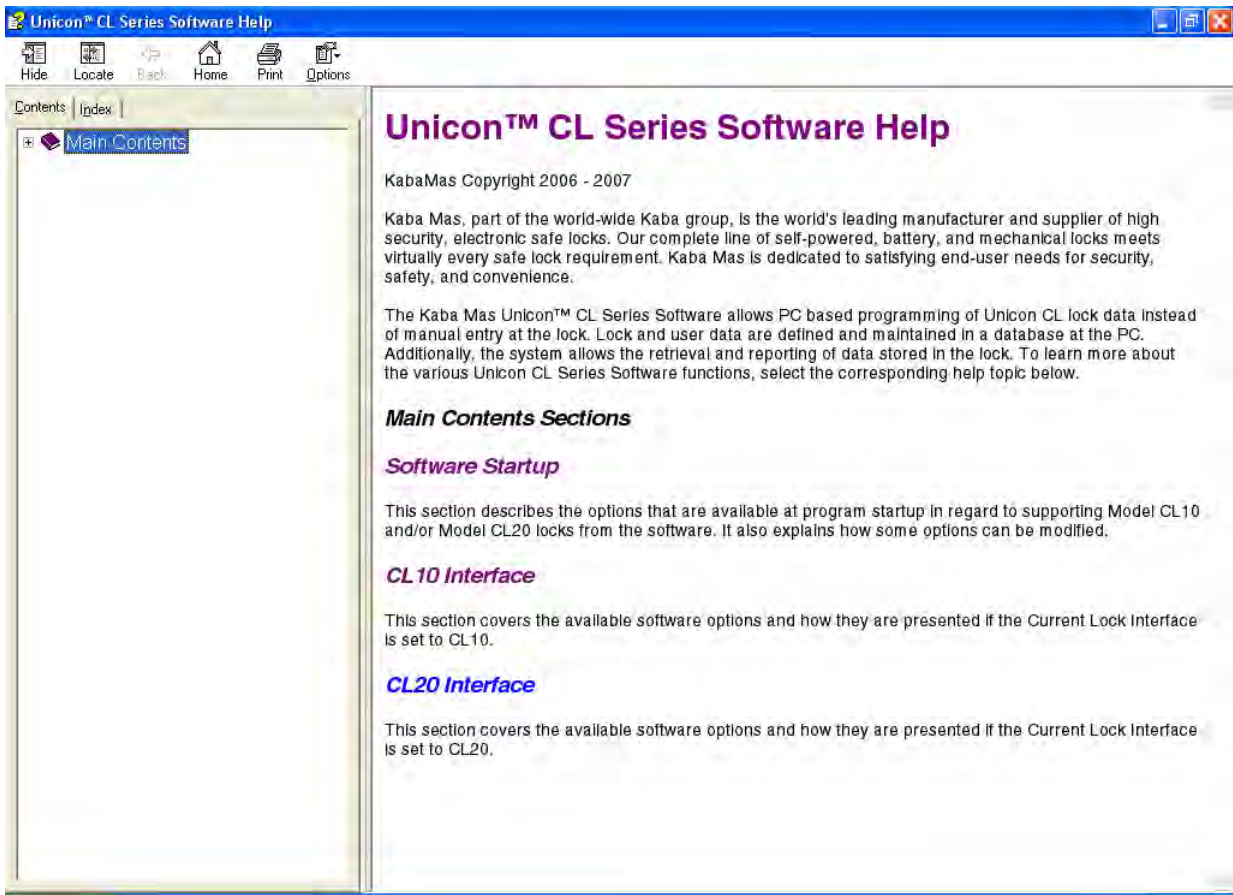
1. Select **Help**.


Help Topics

The Unicon CL Series Software has extensive Help screens available which cover all portions of the operation of the Unicon CL Series Software. The Help Topics option displays the main Help window. From the Help menu:

1. Select **Help Topics**.

The Unicon CL Series Software Help window is displayed.

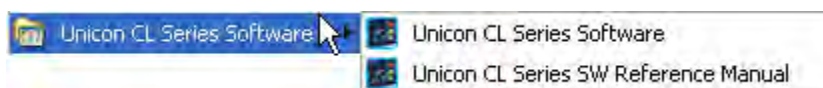


From this window, you may obtain help on the Unicon CL Series Software functions by clicking on the name of the function. The detailed help screen for the selected function is displayed. If the Help data is longer than one screen, use the scroll bars to move through the data. The taskbar commands at the top of the screen may be used to move through the help screen for the different functions. Click on the red X Close button  in the upper right hand corner to close the Help functions.

The Unicon CL Series Software Reference Manual is also available online. The Unicon CL Series Software Reference Manual is also available in PDF format from the Unicon CL Series Software Menu for printing or for online assistance.

From the Programs Menu:

1. Select the **Start** icon from the Windows task bar.
2. Select the **Programs** menu item.
3. Select the **Unicon CL Series Software** menu item.



4. Select the **Unicon CL Series SW Reference Manual** icon.



About Unicon CL Series Software

The About Unicon CL Series Software option displays data about the Unicon CL Series Software program. From the Help menu:

1. Select **About Unicon CL Series Software**.

The About Unicon Series window is displayed.



2. Click on the **OK** button to close the window.

AUDIT TRANSACTION RECORDS - CL10

CL10 Audit Transaction Records and Definition: (in alphabetical order)

The User ID field on each audit record indicates the User ID of the person who performed that action. If the User ID for a specific transaction type will always be the same, you will see that User ID indicated in the record layout below. If the User ID can vary, it will be indicated by an “xxx” in the record layout. In an actual audit record of that type, the User ID of the person who performed that action will be shown. If a transaction record is generated by the lock system, there will be no user associated with that record that the User ID will be indicated as “—”.

111 = Super Master or Master User

200 = Temporary Lock User

xxx = Variable User ID

— = No User ID (System generated)

Transaction Type	User ID	Date	Time
Activate/Change PIN	xxx	mm/dd/yyyy	hh:mm AM/PM
The PIN has been set or changed for the indicated User ID.			
Add User	111	mm/dd/yyyy	hh:mm AM/PM
A user has been added to the lock either manually or using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.			
Audit Download	xxx	mm/dd/yyyy	hh:mm AM/PM
The indicated User retrieved Audit data from the lock via a Reporting Key Fob.			
Close Lock	xxx	mm/dd/yyyy	hh:mm AM/PM
The lock is in a “combination locked state” and the knob has been turned to the locked position to physically lock the lock. The User ID is that of the user who entered the combination to put the lock in a “combination locked state”.			
Combination Locked State	xxx	mm/dd/yyyy	hh:mm AM/PM
The lock has been put into a “locked” state by a user. The Master User or a Manager User may have pressed the shift (arrow) key followed by a valid combination, or the Lock User may have entered a valid combination followed by the shift (arrow) key, to place the lock in this state. If the bolt is also extended, the lock is also “physically” locked. The User ID is that of the user entering the combination to lock the lock.			

Delete User **111** **mm/dd/yyyy hh:mm AM/PM**

A user has been deleted from the lock either manually or using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Disable SMC **111** **mm/dd/yyyy hh:mm AM/PM**

The Super Master User Combination has been permanently disabled. The User ID is always 111 indicating action by the Super Master or Master User.

End DST (-1 hour) **111** **mm/dd/yyyy hh:mm AM/PM**

The time in the lock has been set back by one hour to change over to Standard Time. The User ID is always 111 since only the Master User can perform this operation.

Key Override Open — **mm/dd/yyyy hh:mm AM/PM**

The lock was opened via the physical Key Override. The User ID is always “—” since no specific user can be associated with this physical action.

Key Override Close — **mm/dd/yyyy hh:mm AM/PM**

The bolt was extended back to the locked position after the physical Key Override open occurred. The User ID is always “—” since no specific user can be associated with this physical action.

Lock POR — **mm/dd/yyyy hh:mm AM/PM**

The lock power has been reset. The User ID is always “—” for Lock POR operations since this transaction is not associated with a specific user.

Lock User Changed PIN **200** **mm/dd/yyyy hh:mm AM/PM**

A new Lock User 4-7 digit combination has been set. The User ID is always 200 to indicate the temporary Lock User.

Master Shelve **111** **mm/dd/yyyy hh:mm AM/PM**

The lock was “shelved” using the Master User combination. The User ID will always be 111 to indicate the Master User.

Open Lock **xxx** **mm/dd/yyyy hh:mm AM/PM**

This transaction is generated after a valid combination has been successfully entered to access the lock. The User ID is that of the user who entered the combination. (The Lock User will be identified as User 200.)

Program Lock Operation **111** **mm/dd/yyyy hh:mm AM/PM**

The lock has been programmed with data from the PC via the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Restrict Audit Access **111** **mm/dd/yyyy hh:mm AM/PM**

Audit access (retrieval of data from the lock) has been restricted. The User ID is always 111 since only the Master User can perform this operation.

Set Lock ID **111** **mm/dd/yyyy hh:mm AM/PM**

The Lock ID has been defined for the lock either manually at the lock or via the Programming Key Fob. User ID is always 111 since only the Master User can perform this operation.

Set Lock Time **111** **mm/dd/yyyy hh:mm AM/PM**

User 111 has set the date & time in the lock using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Start DST (+1 hour) **111** **mm/dd/yyyy hh:mm AM/PM**

The time in the lock has been set forward by one hour to change over to DST (Day light Savings Time). The User ID is always 111 since only the Master User can perform this operation.

Super Master Changed PIN **111** **mm/dd/yyyy hh:mm AM/PM**

The Super Master PIN has been set or changed. The User ID is always 111 to indicate the Super Master.

Super Master Shelve **111** **mm/dd/yyyy hh:mm AM/PM**

The lock was “shelved” using the Super Master User combination. The User ID is always 111 to indicate the Super Master.

User Table Download **xxx** **mm/dd/yyyy hh:mm AM/PM**

The indicated User retrieved User Table data from the lock via a Reporting Key Fob.

Wrong Try Penalty **—** **mm/dd/yyyy hh:mm AM/PM**

Three invalid attempts were made and generated a wrong try penalty lockout of 3 minutes. Any successive invalid attempts would generate an additional penalty. The User ID is always “—” since this is the result of invalid attempts and does not have a specific user associated with the result.

AUDIT TRANSACTION RECORDS - CL20

CL20 Audit Transaction Records and Definition: (in alphabetical order)

The User ID field on each audit record indicates the User ID of the person who performed that action. If the User ID for a specific transaction type will always be the same, you will see that User ID indicated in the record layout below. If the User ID can vary, it will be indicated by an “xxx” in the record layout. In an actual audit record of that type, the User ID of the person who performed that action will be shown. If a transaction record is generated by the lock system, there will be no user associated with that record that the User ID will be indicated as “—”.

111 = Super Master or Master User

xxx = Variable User ID

— = No User ID (System generated)

Transaction Type	User ID	Date	Time
Activate/Change PIN	xxx	mm/dd/yyyy	hh:mm AM/PM
The PIN has been set or changed for the indicated User ID.			
Add User	xxx	mm/dd/yyyy	hh:mm AM/PM
A user has been added to the lock either manually or using the Programming Key Fob. The User ID is usually the Master User, or it could also be a Supervisor’s ID if operating in Supervisor Subordinate Mode and the user added is a Subordinate.			
Audit Download	xxx	mm/dd/yyyy	hh:mm AM/PM
The indicated User retrieved Audit data from the lock via a Reporting Key Fob.			
Change to User ID only mode	111	mm/dd/yyyy	hh:mm AM/PM
The lock access requirement has been changed to only require a valid 3-digit User ID for access instead of the full 8-digit combination. User ID is always 111 since only the Master User can perform this operation			
Change to User ID + PIN mode	111	mm/dd/yyyy	hh:mm AM/PM
The lock access requirement has been changed back to require the full 8-digit combination for access instead of only a valid 3-digit User ID. User ID is always 111 since only the Master User can perform this operation.			
Close Lock	xxx	mm/dd/yyyy	hh:mm AM/PM
The lock is in a locked state because the “time to open lock” period knockoff has occurred and the knob has been turned to the locked position to physically lock the lock. The User ID is that of the user who previously entered the combination to open the lock.			

Delete User **xxx** **mm/dd/yyyy hh:mm AM/PM**

A user has been deleted from the lock either manually or using the Programming Key Fob. The User ID is the Master User or It could also be a Supervisor's ID if operating in Supervisor Subordinate Mode and the user deleted is a Subordinate.

Disable SMC **111** **mm/dd/yyyy hh:mm AM/PM**

The Super Master User Combination has been permanently disabled. The User ID is always 111 indicating action by the Super Master or Master User.

Disable Subordinate Users **xxx** **mm/dd/yyyy hh:mm AM/PM**

A supervisor's group of Subordinate Users has been disabled for lock access. The User ID is that of the supervisor disabling his own or another supervisor's Subordinates.

Enable Subordinate Users **xxx** **mm/dd/yyyy hh:mm AM/PM**

A supervisor's group of Subordinate Users has been enabled for lock access. The User ID is that of the supervisor enabling his own or another supervisor's Subordinates.

End DST (-1 hour) **111** **mm/dd/yyyy hh:mm AM/PM**

The time in the lock has been set back by one hour to change over to Standard Time. The User ID is always 111 since only the Master User can perform this operation.

First User Entered PIN **xxx** **mm/dd/yyyy hh:mm AM/PM**

When operating in Dual Access mode, this transaction is generated when the first valid user combination (User ID + PIN) is entered. The User ID is that of the user who entered the combination.

Key Override Open **—** **mm/dd/yyyy hh:mm AM/PM**

The lock was opened via the physical Key Override. The User ID is always "—" since no specific user can be associated with this physical action.

Key Override Close **—** **mm/dd/yyyy hh:mm AM/PM**

The bolt was extended back to the locked position after the physical Key Override open occurred. The User ID is always "—" since no specific user can be associated with this physical action.

Lock POR **—** **mm/dd/yyyy hh:mm AM/PM**

The lock power has been reset. The User ID is always "—" for Lock POR operations since this transaction is not associated with a specific user.

Master Shelve **111** **mm/dd/yyyy hh:mm AM/PM**

The lock was "shelved" using the Master User combination. The User ID will always be 111 to indicate the Master User.

Open Lock **xxx** **mm/dd/yyyy hh:mm AM/PM**

This transaction is generated after a valid combination (or combinations if operating in Dual Access mode) has been successfully entered to access the lock. The User ID is that of the user who entered the combination or the user who entered the second combination if operating in dual mode.

Program Lock Operation xxx mm/dd/yyyy hh:mm AM/PM

The indicated User has programmed the lock with data from the PC via the Programming Key Fob. The User ID is always 111 for the Master User unless the lock is operating in Supervisory/Subordinate mode, in which case a Supervisor is allowed to add and delete users via the Programming Key Fob.

Restrict Audit Access 111 mm/dd/yyyy hh:mm AM/PM

Audit access (retrieval of data from the lock) has been restricted. The User ID is always 111 since only the Master User can perform this operation.

Set Access Schedules 111 mm/dd/yyyy hh:mm AM/PM

Access schedules in the lock have been defined or modified via the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Set Lock ID 111 mm/dd/yyyy hh:mm AM/PM

The Lock ID has been defined for the lock either manually at the lock or via the Programming Key Fob. User ID is always 111 since only the Master User can perform this operation.

Set Lock Time 111 mm/dd/yyyy hh:mm AM/PM

User 111 has set the date & time in the lock using the Programming Key Fob. The User ID is always 111 since only the Master User can perform this operation.

Start DST (+1 hour) 111 mm/dd/yyyy hh:mm AM/PM

The time in the lock has been set forward by one hour to change over to DST (Day light Savings Time). The User ID is always 111 since only the Master User can perform this operation.

Super Master Changed PIN 111 mm/dd/yyyy hh:mm AM/PM

The Super Master PIN has been set or changed. The User ID is always 111 to indicate the Super Master.

Super Master Shelve 111 mm/dd/yyyy hh:mm AM/PM

The lock was "shelved" using the Super Master User combination. The User ID is always 111 to indicate the Super Master.

User Table Download xxx mm/dd/yyyy hh:mm AM/PM

The indicated User retrieved User Table data from the lock via a Reporting Key Fob.

Wrong Try Penalty — mm/dd/yyyy hh:mm AM/PM

Five invalid attempts were made and generated a wrong try penalty lockout of 3 minutes. Any successive invalid attempts would generate an additional penalty. The User ID is always "—" since this is the result of invalid attempts and does not have a specific user associated with the result.

Document Number 3076.026
Rev. C - 10/10



Kaba Mas LLC
749 W. Short Street, Lexington, KY 40508 USA
Phone: (859) 253-4744 FAX: (859) 255-2655
Customer Service: (800) 950-4744
www.kaba-mas.com