



The power of control. Automated.



# Access Control Software User Guide



[www.larco.com](http://www.larco.com)

## Table of Contents

<b>Introduction .....</b>	<b>3</b>
<b>Getting started.....</b>	<b>6</b>
Hardware.....	6
Software .....	6
<b>Using the Guardian II software.....</b>	<b>11</b>
<b>Administration .....</b>	<b>12</b>
Site Rev / Locations .....	12
Holidays .....	15
Schedules .....	16
Harvesting keys from the system .....	17
Sign In Rights for the software application .....	18
Database management .....	20
Optional Fields .....	22
<b>Controllers .....</b>	<b>23</b>
Controller Properties .....	23
User Admit List.....	26
Group Lists.....	28
Dual Access (two keys required to open a lock).....	29
Passage Users (bypassing the relay timer).....	30
Program Admin key with controller information .....	30
<b>Users .....</b>	<b>31</b>
User Groups List .....	33
Controller Admission & Restriction .....	33
Program user keys .....	34
<b>Groups.....</b>	<b>34</b>
Admission / Restriction Controller Lists .....	35
<b>Keys.....</b>	<b>36</b>
View / Import, Make Admin/Export Keys .....	36
Save Export Key Records to the Database .....	38
Make Admin & Export keys .....	39
Make an Admin key that contains data for multiple controllers.....	42
<b>Reports.....</b>	<b>46</b>
Selecting & printing .....	46
<b>Guardian II controller board connections .....</b>	<b>48</b>
<b>User interface (LED colors and patterns).....</b>	<b>49</b>

## Introduction

Congratulations on purchasing the premier product in standalone electronic lock controls. The Guardian II access control system is versatile, easy to install and simple to use!

The Guardian II administration software kit is a package of software and hardware provided to support the Guardian II controllers and keys.



Please verify that you have the following components:



**G2 Programmer (1)** – This device connects to your computer’s USB port (with the included cable) and is used to program keys in the Guardian II system.

**Important:** The G2 Programmer driver must be installed on your computer in order for your G2 Programmer to operate. This driver is included on the software CD.

When you plug-in the Programmer to you computer a wizard will appear, asking you for this driver. Insert the CD into your computer and follow the directions in Driver Installation Manual (223-2323-232) PDF.



**Guardian II software (1)** supplied on CD-ROM – Allows the Guardian II system to communicate with the G2 Programmer. Used for setting up and configuring Locations, Controllers, Keys and viewing the information stored on keys. Also includes pdf files of the Software User Guide & Installation Manual.



**Admin key (1)** – The Admin key (Gray) is used to program and update the access controller(s) with information used to grant or deny user and group access.



**Export key (1)** – The Export key (Black) is used to transfer the audit trail events stored on each controller back into the computer, where the data is used for reporting purposes.



**User keys (5)** – These are the keys you program for your patrons or employees, to provide them simple access to your facilities. The keys are electrically unique and copy proof. User keys are available in the following four colors: blue (standard), green, red, and yellow.

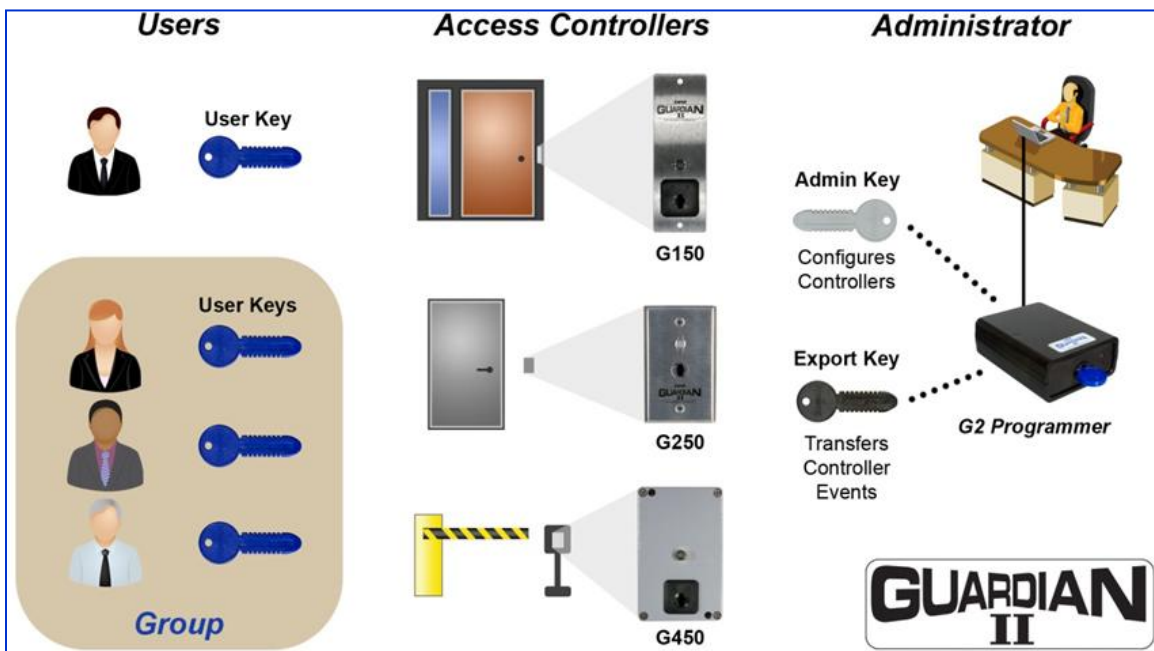
### General features

The Guardian II system consists of three major product groups: access controllers, electronic memory keys, and the administration kit (software, G2 Programmer & USB cable).

Typically, one person called the “Administrator” is tasked with setting up and operating the Guardian II system. They enter information in the software about each controller they have purchased, details regarding each user and they program the three types of electronic keys (Admin, Export & User) that are used by the system.

The diagram below gives a general overview of what a system can look like.

- Administrator - Sets up & manages the system
- GII Controllers are installed at access points
- User keys (individuals or groups of people) are admitted or restricted, when they use their programmed key.



All decisions are made by the access controller at the point of entry. Controller configurations are set up in the Guardian II software application which can be run on any Windows® PC whether or not it is connected to a network. All set-up information is transferred between the software application and the controller(s) via an admin key (programmed with the G2 Programmer). Simply turn the key and you are done!

A record of controller events (accepted or denied access with time-stamp) is also stored in the access controller's memory. When audit-trail details are desired, simply insert and turn an export key in the controller(s) and carry it back to the G2 Programmer (connected to the admin PC) for easy uploading in to the Guardian II software. The Guardian II software comes standard with a full list of available reports for audit trail evaluation as well as the ability to transfer the audit trail data to an external file.

Windows® is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Each user also carries a copy-proof user key to identify themselves to the system. Users are granted or denied access based on the set-up data written to the controllers and/or their user keys. Access can be controlled based on individual, access point, day, time, group, and more.

The graphic below shows how various keys are used to transport data throughout the system.

- Admin kit (software & G2 Programmer) is used to setup controller(s) and program all keys.
- Admin key transfers information from the software (PC) to the controller.
- Export key transfers information from the controller to the software (PC).
- Users insert & turn keys in controllers



## Getting started

### Hardware

**Controller(s)** - see the [Guardian II controller connection chart](#) (page 48) in this guide or refer to the Installation Manual (P/N: 223-0093-000) on the Guardian II CD for hardware instructions.

**G2 Programmer** - Connect the USB cable to a USB port on your computer, after the software has been installed. Once the G2Programmer has been connected to the computer, you need to load the drivers so the computer can communicate with the reader. Refer to the G2 Programmer – Driver Installation Manual (P/N: 223-0110-000) which comes on the software CD.

### Software

Insert the Guardian II software CD-ROM into your CD drive and follow the on-screen directions.

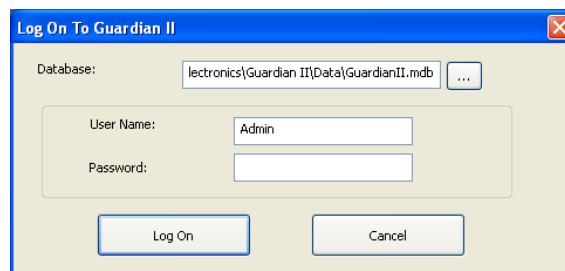
If the CD does not automatically start, do the following:

1. Select the Windows **Start** button.
2. Select **Run**.
3. Type **D:\setup.exe** in the text box and select **OK**. The installation should begin.

Once the software has been installed on your PC, go to the Windows **Start** Menu. Select **Guardian II** from the **Programs** list or double click the icon on the desktop to start the software application.

The Guardian II software can be used to set up individual doors or access points with many different configurations. The following section focuses on setting up a basic system. For additional information, refer to the detailed sections of this manual.

**Important:** Each time you start the Guardian II software application a logon screen appears. You must type Admin in the User Name field to start the application. Do not enter a password (default setting).



Once the application has been successfully started you may setup new users and associated passwords in the Administration/Guardian II Logon section of the software.

After initially logging on to the Guardian II software for the first time, you will be prompted to enter your **Site Name** (typically the name of your establishment). This Site Name will have identification numbers associated (assigned by the software) with it, that are critical to your system operation. All of your controllers and keys will use these numbers to identify themselves to each other.

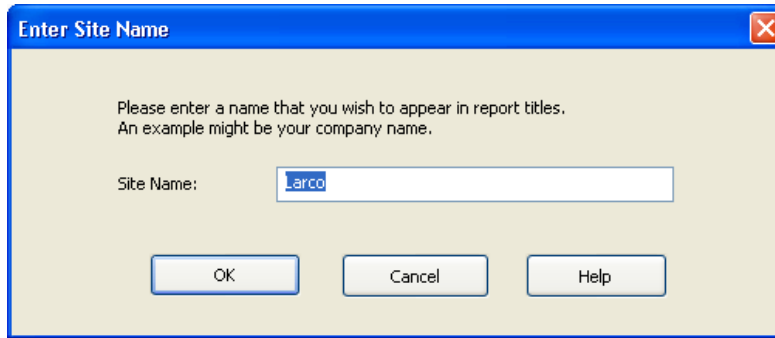


Figure 1  
Site Name Entry Window






**Important:** In order to setup the Guardian II system correctly, some basic information must be entered in the software to make it functional. Follow the steps below (1-#11) to enter the minimum required information to configure your software.

*Note: You will find detailed information pertaining to each section of the software, starting on page 14.*

1. **Enter a Site Name** to identify your specific business (i.e. XYZ Corp.). This name will be displayed on all the reports.
2. **Create (Add) at least one Location** where the controllers are to be installed (i.e. Main Office or Chicago)
  - Select the **Administration** button, then the **Site Rev / Locations** tab
  - Select the **Add Location** button
  - Enter a **Name** for each Location
  - Select the **Save** button
3. **Create (Add) a Controller** for each device that is to be installed.
  - Select the **Controllers** button, then the **Controllers Properties** tab
  - Select the **Add Controller** button
  - Choose a **Location** (from the drop-down box)
  - Name** the Controller
  - Select the **Controller Type** (**Admission** or **Restriction**)
  - Check the Set **Controller Date / Time** box and adjust for when the Admin key will actually program the controller
  - Select and enter the appropriate **Lock Settings**
  - Select the **Save** button

4. **Create (Add) and distribute User Keys** for all people that will use the system.
  - Select the **Users** button, then the **User Properties** tab
  - Select the **Add User** button
  - Enter the **Name** for the User (the next five text fields are optional)
  - Select the appropriate **Key Is Valid** button (*Always, From/To Dates or the For # of Accesses*)
  - Select and review the **Admissions** and **Restriction Controllers** tabs **Important: This is where you set who is allowed or denied access to each controller.** By default, users are not given access to controllers. You can select individuals or the entire list, and then use the arrow buttons to move to the opposite list. [See page 24](#) for detailed information on this subject.
  - Select the **Save** button and insert and turn a new User Key into the G2 Programmer and select **Make User Key**
5. **Optional - Create (Add) User Groups**. This lets you select and move individual users into groups. Groups allow you to list many users as a single entry on a controller's list, instead of entering many individual users.
  - Select the **Groups** button, then the **Group Members** tab
  - Select the **Add Group** button
  - Enter a **Group Name**
  - Move Users from the **Available Users** list to the **Selected Users** list
  - Select the **Save** button
6. **Select each main icon** (large buttons at the top of the main screen) and view each tab with its associated tabs that contain information needed to configure the settings which will be used to admit or restrict users (see more detailed information for each section, later in this manual).

Example:

-  Select the **Controller** icon from the main screen
-  Select a **Controller** from the list on the left side of the screen.
-  Select the **User Admit** or **Restrict List** tab (depending on the controller type that was chosen). When an Admin key is used later to program, all the people in the right hand list will be allowed or prohibited (depending on the controller type) by the controller when they use their key.
-  **Add or move names** from the left list to the right list (selected) or vice versa.
-  Select the **Save** button.



7. **Program (Make) an Admin Key.** Used to transfer programming information from the software to each controller in the system.
  - Select the **Keys** button, then the **Make Admin/Export Keys** tab
  - Insert and turn an **Admin key** (gray) in the G2 Programmer
  - Select a **Controller** from the list on the left of the screen
  - Select the **Make Admin Key** button
  - Type a Name** for the key
  - Select **OK**

Controllers are programmed (Administered) using two different procedures, as described below:

**1<sup>st</sup> Time an Admin key is used to program a controller** - Each controller needs to have your specific site, location and its specific information programmed into its memory, once it has been installed. **The first (initial) time you admin a controller, you must follow these specific steps in order to program it correctly.**

- Take the Admin key you created in the step above (#7) and insert it in the G2 Programmer
- Select the **Keys** button, then the **Make Admin-Export Key** tab
- Highlight the key name** from the **Admin Keys** table
- Select the controller** you want to program, from the list on the left side of the window
- The **Enable** and **Set Time** checkboxes as well as the **Program Controller 1<sup>st</sup> Time** radio button in the lower left corner of the screen are automatically checked. **Press the Clock button** to adjust the time and date [for when you will actually insert the Admin key into the controller](#). *(Example: If the controller is installed some distance from your computer, you will want to set the time into the future. Say it is 10:00AM but you need five minutes to walk to the controller. Set the time as 10:06:00 and program the Admin key. Remove the key and walk to the controller. Use a watch to see when the time reaches 10:06:00AM and then insert & turn the key in the receptacle. The LED will flash during the programming of the controller)*
- Select **Make Admin Key** button
- Insert & turn the gray Admin key into controller** to download the information to the controller

**On-going Admin key procedure** - Used to make changes in a controller(s) configuration after the initial admin procedure has been completed. The settings that are written to the Admin key in this operation are setup in the Controller section of the software. Refer to the Controller section of the software, prior to making this type of key. You can remake these types of Admin keys as many times as you wish.

- Select the **Keys** button, then the **Make Admin-Export Key** tab.
- Select the **Controller(s)** you want to program, from the list on the left side of the window.

*Note: Hold the "CTRL" key while selecting (non-adjacent) controllers on the list to select them. To select multiple items that are adjacent, click on the first item. Hold the "SHIFT" key to select all of the controllers between the first and the last selection.*

- Insert an Admin key** in the G2 Programmer (connected to your PC)
- Select an Admin key name** from the center list. *If there is no Admin key on the list, select the Make Admin Key button and enter the key name. Note: You may also select the Set Time/Date box, if you want to reset these parameters*
- Select **Make Admin Key** button
- Insert the programmed Admin Key into controller to download the information onto it

**NOTE: You can administer more than one controller at a time from this screen by selecting multiple controllers from the list on the left side of the screen.** Generally, this would be used when adding or deleting users from controllers, harvesting keys and settings that want to be applied to all controllers. If you need to change the time on many controllers, you must admin each one, individually.

8. **Insert the Admin key(s) in Controller(s) to download information into the controller.**

*The LED will flash amber 3x, then to green and the buzzer will chime 3x.*

9. **Create (Add) an Export Key.** Used to transfer audit records from controllers to the Guardian II software, for reporting purposes.

- Select the **Keys** button, then the **Make Admin-Export Key** tab
- Insert a Export key** (black) into the G2 Programmer
- Select the **Make Export Key** button
- Type a Key Name** for the export key
- Select **OK**

10. **Insert the Export key in each Controller to upload information from the controller.**

*The LED light will remain solid amber during the export cycle and then turn red when the process is complete. The buzzer will also sound.*

11. **Upload Records into the PC.**

- Insert the Export key** you created in Step 11 and insert it in the G2 Programmer
- Select the **Keys** button, then the **View/Import/Erase** tab
- Select the **View Key** button to review the keys contents
- Select the **Save Export Key Records to Database** button to move (upload) the records from the key, into the software application

The following sections of this manual will walk you through a detailed setup of your Guardian II Access Control System.

## Using the Guardian II software

This section of the manual explains in detail what each button displayed at the top of the Guardian II main screen contains and suggests different ways you may want to set your system up.



Figure 2  
Main Screen

After installing the software and entering your Site Name, begin by selecting the **Administration** button. The Administration section contains system information related to holidays, time schedules, harvest keys, locations and database management. Location information is one item that must be filled in for the system to function.

## Administration



The Administration section of the software has seven tabs that contain important system information such as **Site Names**, **Schedules**, **Holidays** and **database management** functions. When initially setting up your system, the information you enter here will be used throughout the software to configure the system.

### Site Rev / Locations

Figure 3

Site Rev / Locations setup screen

The **Site Rev/Location** tab is used to identify the physical locations where your controllers are installed (i.e. Main Office, Building 209 or Freshwater Yacht Club) and where you can modify/reset your Site information.

Location names typically identify physical locations (city) or building names (Headquarters, distribution center) that you recognize. These names will be used in the software as a primary sorting name for every controller you setup in one or more locations *Note: Initially, the Location List on the left side of the screen will be blank.*

#### Adding Locations:

1. Select the **Add Location** button.
2. Enter the name of the facility location (i.e. Main Office).
3. Click the **Save** button.

#### Editing Locations:

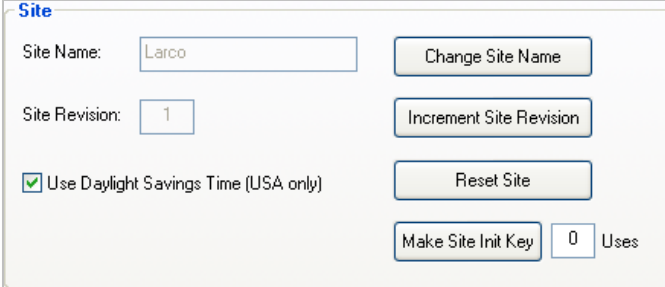
1. Select a location from the window on the left side of the screen.
2. Edit the text in the Location window.
3. Click the **Save** button.

Deleting Locations:

1. Select a location from the window on the left side of the screen.
2. Click the **Delete Location** button and then the **Yes** button in the pop-up window.

Change Site Name

**Warning: If you select this button, a window will appear asking if you want to change the Site Name. This name will appear on all the reports generated by the software.**



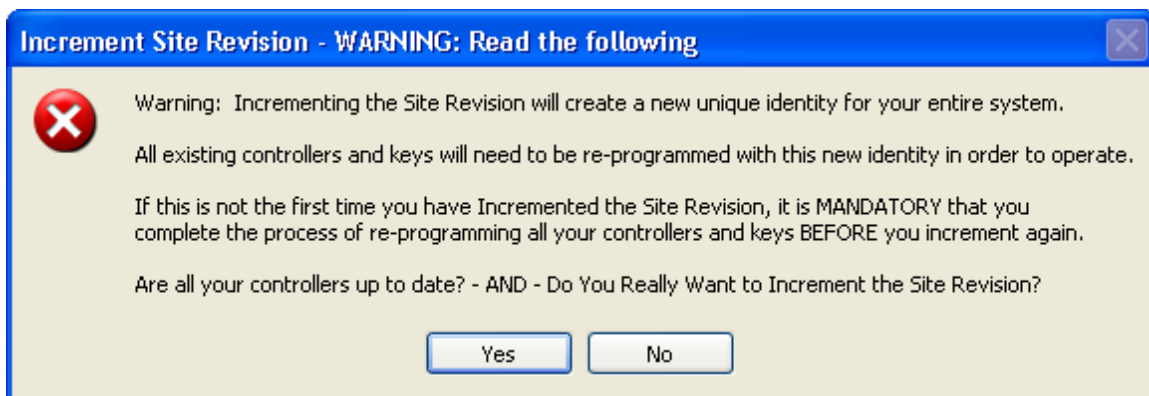
The image shows a 'Site' configuration window with the following fields and buttons:

- Site Name: Larco (text input)
- Change Site Name (button)
- Site Revision: 1 (text input)
- Increment Site Revision (button)
- Use Daylight Savings Time (USA only)
- Reset Site (button)
- Make Site Init Key (button)
- 0 (text input)
- Uses (text)

**Increment Site Revision** - When all controllers in your system have been administered and are up to date, the system allows you, if needed, to **Increment Site Revision**.

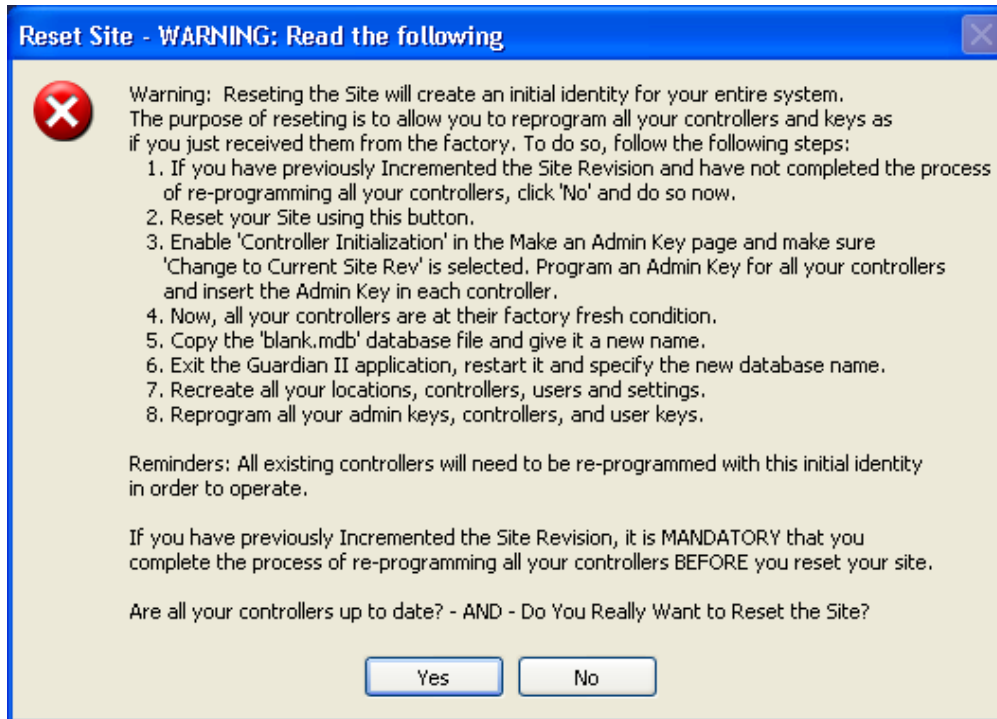
This option writes a new Site ID in the database, which will be loaded onto all your controllers and user key's. The information in the database remains (controllers & users) the same. You must then reprogram (admin key) all your controllers with this new site number and then reprogram user keys. **Once the controllers have been Admined, the user keys will not work until they have been re-programmed.**

This feature could be used in a situation where you have a high turnover of users, such as in a marina application and do not get many of your user keys back from the customer. By incrementing the site, your existing customer's information is still in the database and only their keys need reprogramming to once again operate correctly.



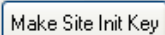
**Reset Site** – Sets your system back to the default factory site identification and start with a blank database. Once this button has been selected, all the controllers and keys must be reprogrammed with the new ID. Administrators may choose this option to simply start over with their software design and implementation of the overall system.

After pressing the  button, follow the instructions in the window below:



*Note regarding #5 (in window above) – Use Windows Explorer to make a copy of the <C:\Documents and Settings\All Users\Application Data\Larco\GuardianII\Data\blank.mdb> file.*

**Make Site Init (Initialization) Key** – This feature can be used when the administrator wants to move an existing (programmed) controller from one area to another, within your system and needs to change its identification and name. **This key erases the existing controller identification and sets it to the factory default.** Then, an Admin key is used to program a new ID, thereby giving it a new name in the software.

1. Insert a blank user key into the G2 Programmer.
2. Enter a number in the Uses box, then select the  button. Note: *Each time the key is used to set the controller to factory settings, this number will decrement.*
3. Touch the **Red/White** (REX Input #1) and **Green/White** (Ground) wires on the controller together while performing Step #4, below.
4. Insert and turn the Site Init (Initialization) key into the controllers' key receptacle. The controller is now set to the factory default settings.
5. Program an Admin key with the new controller information and insert/turn it in the controllers' key receptacle.

## Holidays

Figure 4  
Holiday Setup screen

Holidays entered in this window and used in conjunction with the scheduling portion of the software application, will restrict access in a facility on these specific dates. The Holiday list holds one year of dates. After the year has gone by, you must change the dates to reflect the next year.

*Example: If you set a standard weekday schedule of Monday - Friday, 8:00AM - 4:30 PM to allow employees in a door, they will be able to use their key anytime during this period. If you added a holiday date of 01/01/XX to this schedule, their key would not operate the lock on this day.*

#### Adding Holidays:

1. Select the **Add Holiday** button.
2. Enter a name in the **Holiday Name** box.
3. Select a **date from the calendar**. (Note: You can click on the date at the top of the calendar to quickly view different months and years).
4. Click the **Save** button.

#### Editing Holidays:

1. Select a holiday from the list on the right side of the screen.
2. Edit the text or select a different date.
3. Click the **Save** button. This will modify the existing holiday.

#### Deleting Holidays:

1. Select a holiday from the list on the right side of the screen.
2. Click the **Delete Holiday** button.
3. A warning window appears, confirming the deletion. Select **Yes** to delete, or **No** to cancel the deletion.

## Schedules

Figure 5

*Schedules Setup Screen (blue highlighted area shows First Shift time increments)*

The software can store up to 255 different time schedule periods, which are used to allow or restrict access to individual users or groups during the times shown. The default (blank) schedule throughout the program allows for 24 hours/7 days per week admittance on an admission controller.

Schedules work the best with admission controllers. **Restriction controllers that show users on the restriction list with no schedules, deny access at all times. Important: If a schedule is used for a restricted user, they will be admitted during the schedule timeframe and restricted at all other times.**

Holidays (entered on the previous tab) can be used in conjunction with any schedule. On the days designated as holidays, access will not be granted to the individuals or groups on admission controllers, with this holiday schedule.

Adding Schedules:

1. Select the **Add Schedule** button.
2. Enter the name in the **Schedule Name** box.
3. Highlight the time increment boxes at the top of the window for each half hour you would like to select. *Note: You may click (highlight) individual boxes or click-and-drag from the left or right to select a series of boxes in the same row.*
4. Select and move any applicable Holiday(s) from the available list to the selected list.
5. Click the **Save** button.



Editing Schedules:

1. Select a schedule from the window on the left side of the screen.
2. Edit the time/day box information, name or holiday text.
3. Click the **Save** button. This will modify your existing schedule.

Deleting Schedules:

1. Select a **Schedule** from the window on the left side of the screen.
2. Click the **Delete Schedule** button.
3. A warning window appears, confirming the deletion. Select **Yes** to Delete.

**Harvesting keys from the system**

Last Name	First Name
Anglin	Lawrence
<input checked="" type="checkbox"/> Blue	Vida
<input checked="" type="checkbox"/> Carter	Jimmy
<input checked="" type="checkbox"/> Couples	Fred
<input checked="" type="checkbox"/> Ford	Harrison
<input checked="" type="checkbox"/> Green	Ted
<input checked="" type="checkbox"/> Holyfield	Evander
<input checked="" type="checkbox"/> Kelly	Red

Last Name	First Name	Date
Fingers_29	Rollie	
Hunter_30	Catfish	7/21/2011

Admin Key Name
Admin 1
Export 1

Admin Key Name	Date
----------------	------

Figure 6

Harvest Key Screen

This section of the software allows the administrator to "harvest" (rouge keys that were not returned) keys from the system. After programming an Admin key with this information and inserting it in all your controllers, the next time access is attempted using that specific key, it will be erased and access will be denied to that user. The controller will record the harvested user's name as well as the time and date that access was attempted. From this point on, that specific key will not work in any controller throughout the system, rendering it useless.

One of the benefits to using this feature is that once a key has been harvested, it will not work in the system and will delete the user from active lists in the software. Reports will continue to show the user name with an underscore and key number or the name. Some competitive systems require that you keep a user on a restriction list forever, but that is not required with the Guardian II system

Hunter\_30

Figure 7

Harvest User Name format

Sign In Rights for the software application

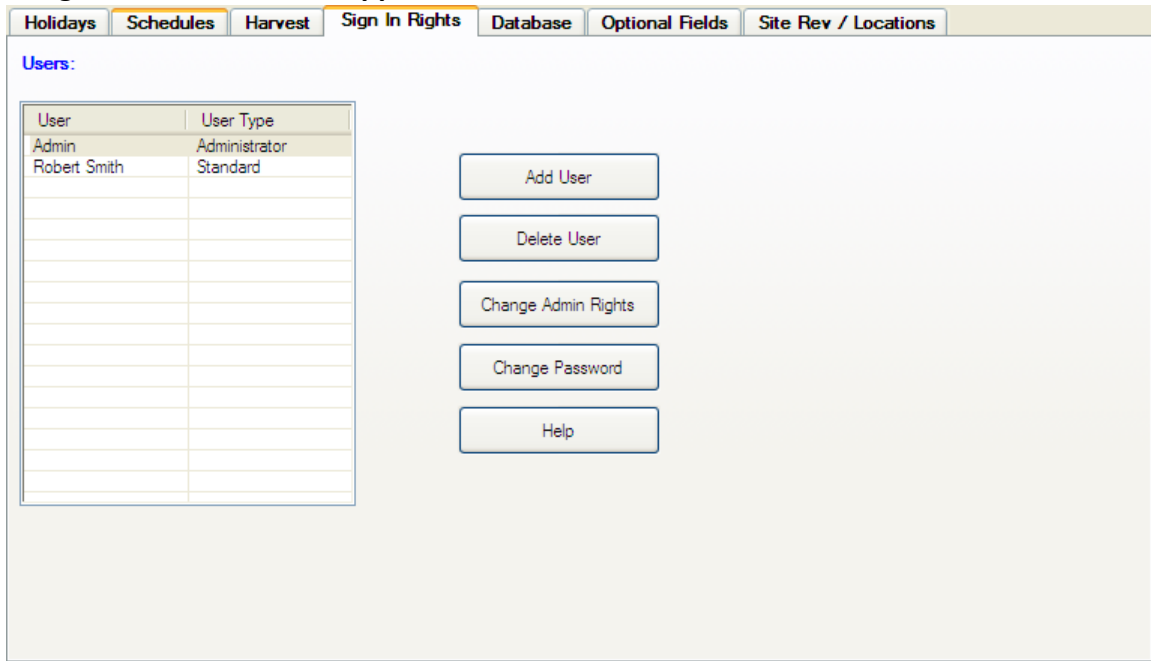


Figure 8  
Sign In Rights screen

This screen is used to set up access rights for individuals you want to be able to log into the software. You can add and delete users, change their logon passwords and change the level of rights.

There are two levels of rights that can be assigned to each person who is given rights to access the software. "**Administrator**" rights give the user unlimited access to the software, meaning they can add new users and groups to the system and allow the person to set and edit information in the Administration section. "**Standard**" users can only perform basic tasks inside the software, such as adding new users or viewing reports.

People with standard rights cannot add or delete controllers, groups or view any information inside the Administration tab.

Adding Sign In Users:

1. Select the **Add User** button.
2. Enter their name in the **User Name** box.
3. To assign the user Admin rights, **check the box** or leave blank for a Standard user.
4. (Optional) Enter a Password in the next two windows and select **OK**.

A screenshot of a dialog box titled "Site User Data". The dialog box has a blue title bar with a close button (X) in the top right corner. The main area is light beige and contains the following fields and controls:

- "User Name:" followed by a white text input box.
- An unchecked checkbox labeled "Admin User".
- "Password:" followed by a white text input box.
- "Re-Enter Password:" followed by a white text input box.
- At the bottom, three buttons: "OK", "Cancel", and "Help".

Deleting Sign In Users:

1. Select a **User** from the window on the left side of the screen.
2. Click the **Delete User** button.
3. A warning window appears, confirming the deletion. Select **Yes** to Delete.

Changing Admin Rights & Passwords:

1. Select the appropriate button (**Admin Rights** or **Passwords**).
2. Select a **User** from the window on the left side of the screen.
3. Modify the information in the window and select **OK**.

## Database management

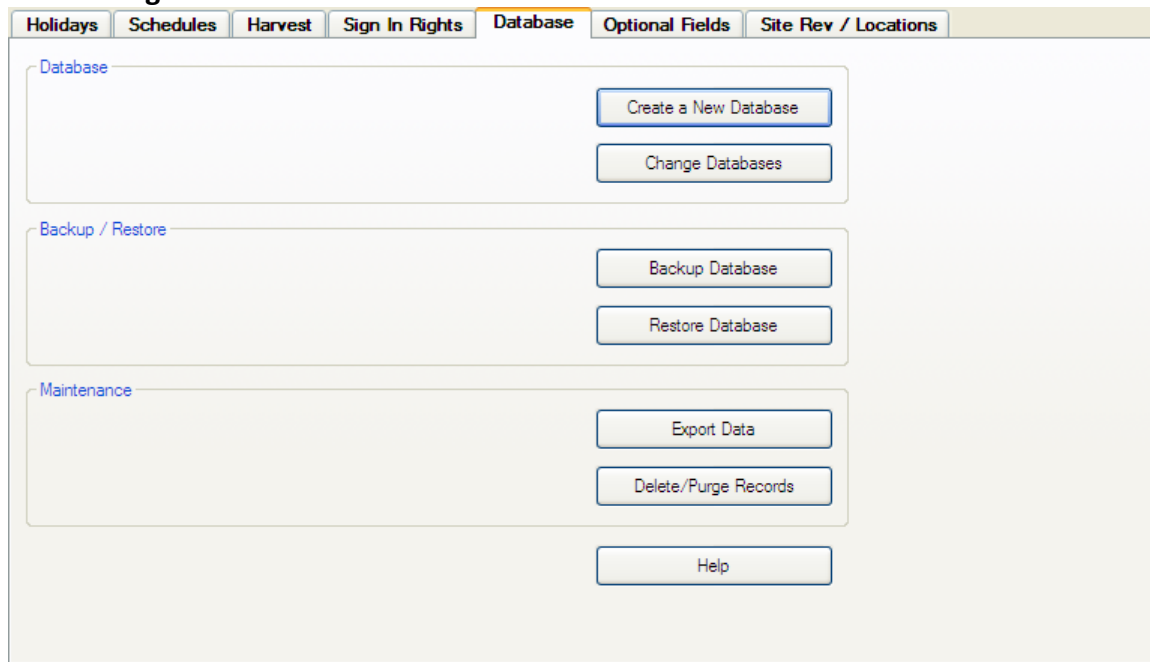



Figure 9  
Database tab screen

This window contains six database management functions that can be used to help you create and maintain your database information. The following information explains the basics of each button found on this screen.

**Create a New Database** - The Guardian II software package allows you to create multiple databases for different businesses and work with each of them, without starting additional programs. This feature is very helpful if you want to maintain multiple systems containing databases with distinct site names.

1. Select the **Create a New Database** button to open a standard window dialog box.
2. Choose a location for the new database and give it a name.
3. Select the **Open** button, to create a new database.

**Change Databases** - This button allows you to switch between different databases you have created. (Note: You can also go to File from the main menu and select/open any one of the last four databases you have worked with).

1. Select the **Change Database** button.
2. Use the browse button  to locate the database you want to use and select the **Open** button.
3. Enter your User name and password. Select the **Logon** button to open the database or the **Cancel** button to exit.

**Backup Database** - By selecting this button, a copy of your current database will be saved to a location of your choice. The software will prompt you to enter a name for the backup copy of the database and to select a location where the backup file is to be stored. In the event of a computer failure, you could use this backup file to restore your database.

1. Select the **Backup Database** button to open a standard window dialog box, where you **choose a location** to backup the existing database and **name the file** you want to backup.
2. Select the **Open** button to backup the data.
3. A message will appear to let you know the file was backed up. Select the **OK** button to finish.

**Important: Backing up your database on a regular schedule is highly recommended. As a rule of thumb, you should back up your data no less often than the amount of time you want to spend recreating the data you lose if your computer crashes, without warning!**

**Restore Database** - Allows you to restore data from a backup file in the event that your original (working) database is lost or damaged. When you select this button, a window will appear. Select the database file you want the system to replace the existing file with. **WARNING! Restoring data will overwrite the current data, so be sure this is what you want to do!**

**Export Data** - Allows you to export and save selected data files from the Guardian II database in a .csv (comma separated value) file format. This data can then be opened in other applications such as Microsoft Excel, where you can manipulate and sort the information.

Begin by selecting the **Export Data** button. A window containing the names of all created database tables will appear (Fig. 10).

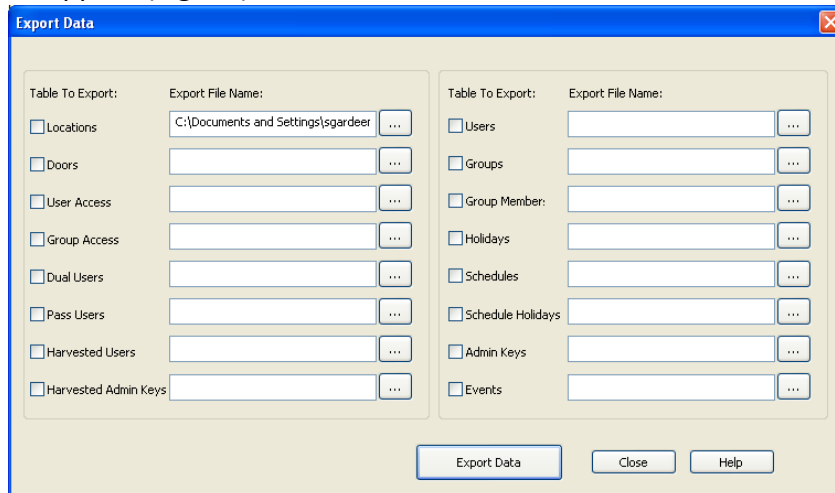



Figure 10  
Export Database Tables Screen

1. Check any of the boxes next to the table names to export them to a file location of your choice.
2. To choose the export destination for the file, select the browse  button.

3. After the window appears, choose an appropriate location of where you want the file saved, enter a name for the file and select the **Open** button. The new export destination path now shows on the Export Data window.
4. Select the **Export Data** button to complete the export process.

**Delete/Purge Records** - Allows you to delete transaction records from your database, using a date range. This will reduce the overall size of your database and speed up certain processes such as reporting and sorting of data.

1. To begin, select the **Delete/Purge Records** button.
2. Enter the **date & time range** for records that you want to delete.
3. Select the **OK** button to delete/purge all records in the range.

**WARNING: Once you delete a record from the Archive section, you will not be able to recover it. It is suggested that you make a copy of your database prior to deleting or modifying data.**

### Optional Fields

This screen is used to edit the optional field names that appear on the Locations and User Properties windows and set the time (0-30 seconds) that balloon help appears when you hover over certain areas of the software. The program does not use these fields for reporting, although you can export the data contained in these areas for reporting outside the system. Check boxes that are checked will appear on screen in the software.

Holidays Schedules Harvest Sign In Rights Database **Optional Fields** Site Rev / Locations

Optional Fields

Note: The information that is displayed in the text boxes below is what will appear in the corresponding software tabs.

Select checkbox(s) below to display the optional fields in the program and reports.

Controllers / Controller Properties	Users / User Properties
<input checked="" type="checkbox"/> Camera (Y/N)	<input checked="" type="checkbox"/> Employee SSN#
<input checked="" type="checkbox"/> Guarded (Y/N)	<input checked="" type="checkbox"/> Start Date
<input checked="" type="checkbox"/> Exported (Date)	<input checked="" type="checkbox"/> Supervisor Name
<input checked="" type="checkbox"/> Last Admin Date	<input checked="" type="checkbox"/> Department

Balloon Help Text

Display Balloon Help Text for  seconds (0 to 30) when hovering.

Save Cancel Help

Figure 11  
Optional Field screen

Controllers



Controller Properties

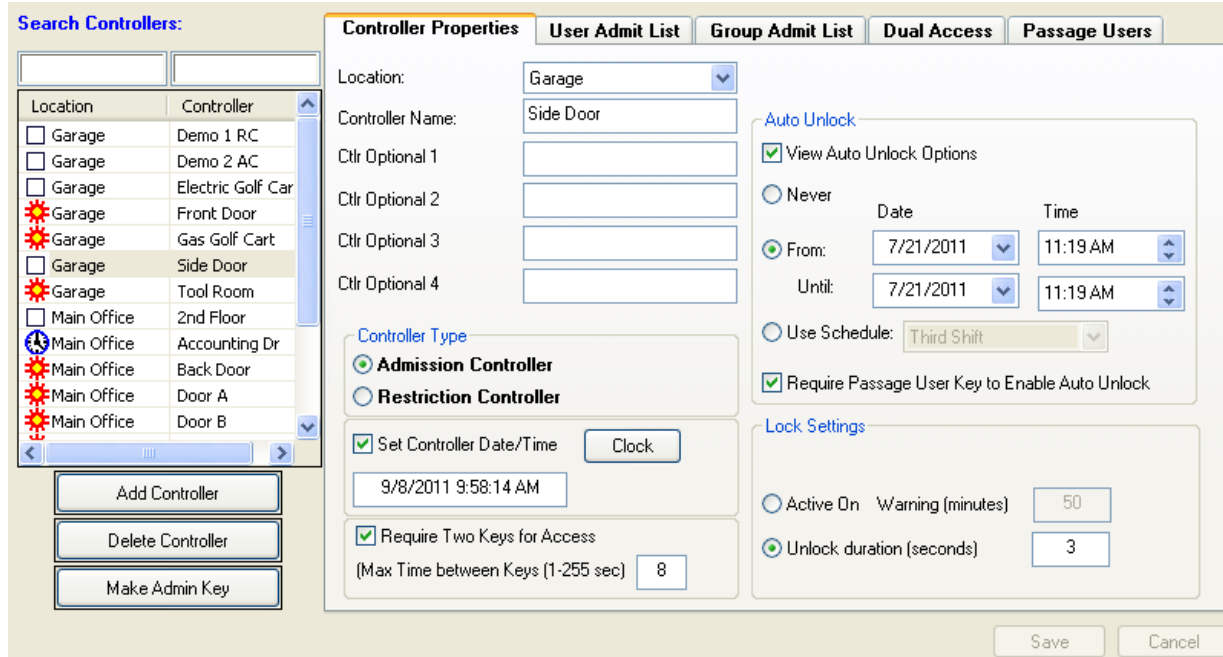


Figure 12  
Controller Properties screen (all checkboxes checked)

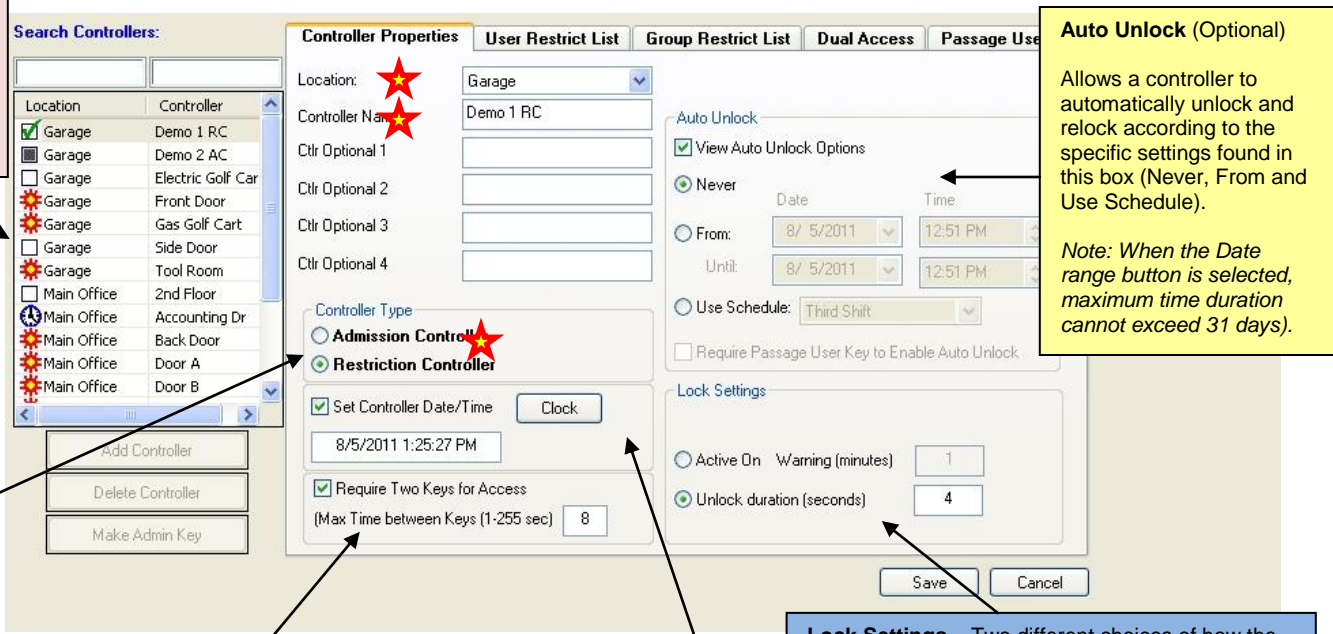
After you have entered the required information in the Administration section of the software, the Controllers section of the software is your next step in configuring all of the controllers in your system.

The controller area contains five tabs arranged with a filing folder look. The first tab, called "Controller Properties", contains fields that are used to program each controller. The remaining tabs contain lists of individual users and groups that you can admit or restrict for each individual controller. This gives you many options and a great deal of flexibility in setting up access for each controller.

*Note: The screen in Figure 12 has all of the option checkboxes selected, to show all the features available for programming a controller. As a default, when this page is normally opened, the checkboxes will be unchecked.*

**Status Icons –** Graphical interface gives you “at a glance” view of your controllers and user key status.

**Controller Type -** Sets the controller to either **Admission** or **Restriction** all listed Users & Groups on the following tabs.



**Auto Unlock (Optional)**  
Allows a controller to automatically unlock and relock according to the specific settings found in this box (Never, From and Use Schedule).  
*Note: When the Date range button is selected, maximum time duration cannot exceed 31 days.*

**Require Two Keys for Access - Dual Access tab (Optional)**  
Two user keys are required to activate the relay on the controller.  
When using this feature (by selecting the checkbox) enter the time in seconds that a controller waits before resetting, when a Dual Access User key (1<sup>st</sup> key) has been inserted and when a Dual Access Required User key (2<sup>nd</sup> key) has been inserted and turned in a receptacle.

Used to set the controllers real time clock (RTC).

**Lock Settings –** Two different choices of how the relay responds after a valid key is inserted and turned in a receptacle.  
**Unlock duration** Sets the time the on-board relay stays energized after a valid key has been inserted. An electric strike or other mechanism is wired to the relay contacts. Time can be set between 1 and 252 seconds.  
**Active On** will energize the lock for as long as a valid key is inserted and turned. The buzzer will sound continuously during the warning period, until the relay de-energizes. *This has been used in golf cart applications.*

**Location (★ required field)** - Choose from one of the locations shown in the drop-down box. The location should reflect the physical location of where the controller will be installed. *Note: The Locations available in the drop-down menu were originally entered in the Administration - Site Rev/Locations tab section of the software.*

**Controller Name (★ required field)** - Enter a name that is associated with the particular controller. This name will be used on lists and reports throughout the software.

**Optional Fields** - You may enter additional information, pertinent to your business for each controller into any or all of these four fields, if desired.



**Controller Types (★ required field)** - This is a very important choice when setting up each controller. There are two ways to configure a controller, either as an **Admission** or **Restriction** type.



**Admission Controller** - Controllers set as “Admission Controller” allow access only to those who are on the accompanying (tabs) access lists.

*Note: Typically, the setting is used for controllers that have a relatively few number of individuals or groups needing access. Again, it is easier to list the few people who should have access, rather than a larger list of those you would have to restrict.*

**Restriction Controller** - Controllers set as “Restriction Controller” will deny access only to those individual users or groups who are shown on the accompanying restriction lists (tabs). All other keys with the correct Site information will be granted access.

*Note: The restriction setting is generally used on a controller that has high traffic volume, such as a business’s front door. In these high-use areas, it is easier (shorter list) to restrict those who you don’t want to get in, such as employees who quit and didn’t give their key back to the company.*

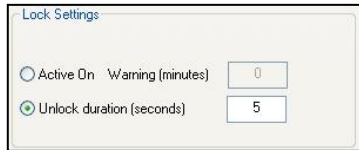
**Set Controller Date/Time** - Used to set the time clock inside each controller (using an Admin key). When you check the box for this section a Clock button appears. If you select the button, a calendar and clock time window appears. You can select the OK button to set the current time (set by the computer clock) or using the calendar and clock, set a time in the future when you will be at the controller to upload this new information.

**Require Two Keys for Access (Dual Access)** - This sets the time allowed for two users to insert each of their keys into a controller to open the lock. A typical use for Dual

Authentication entry is for narcotics cabinets, where an employee is required to have a supervisor present to authorize (validate) the opening of the cabinet.

**Auto Unlock** - Can be used to automatically unlock a controller at a predetermined time by setting a **From/To date and time** (not to exceed a 31 day period) or by **using a preset Schedule**. When the “Require Passage User Key to Enable Auto Unlock” feature is checked, the controller will not automatically open during this period, until a pre-approved user who is listed on the Passage tab, has inserted their key in the controller.

No matter which type of setting is used, at the end of the period the controller relocks. This type of setting can be used in many situations where you want a door or gate to be open without using a key to gain entrance (i.e. open houses or delivery of items through a door for an extended period of time).



**Lock Settings** – Select “*Unlock duration*” to set the length of time a valid key will activate the on-board relay, thereby allowing a lock to remain open (unlocked). You may enter a time between 1 and 252 seconds. After the expiration time, the relay will deactivate and the device will return to its original state. Typically, 3–5 seconds is sufficient for most locking actions.

The “*Active On*” setting is used to power the relay continuously, as long as a valid key is turned in a receptacle. The value entered in the white box is the time that a warning signal will activate before the user’s key runs out of time. This has been used to secure and control golf carts. When a users’ key is programmed to be valid between two periods of time, and the time period remaining on the key gets low, the warning (buzzer) beeps continuously until the time on the key runs out and the controller shuts off .

**User Admit List**

Depending on the controller type you selected on the Controller Properties screen; the User tab will read either **User Admit List** or **User Restrict List**. There are two user tables on the screen. One list contains the names of all available users **Not Admitted** or **Not Restricted**, in your system. The other list contains the names of those who are **Admitted** or **Restricted** by that specific controller. You can select and move individual users or the entire list from one side to the other, using the buttons that are located between the two lists.

The right table also contains a schedule column, that is used to set times that users admission or restriction is active. *Note: The default schedule (blank) is set for 24 hours/7 days per week.*

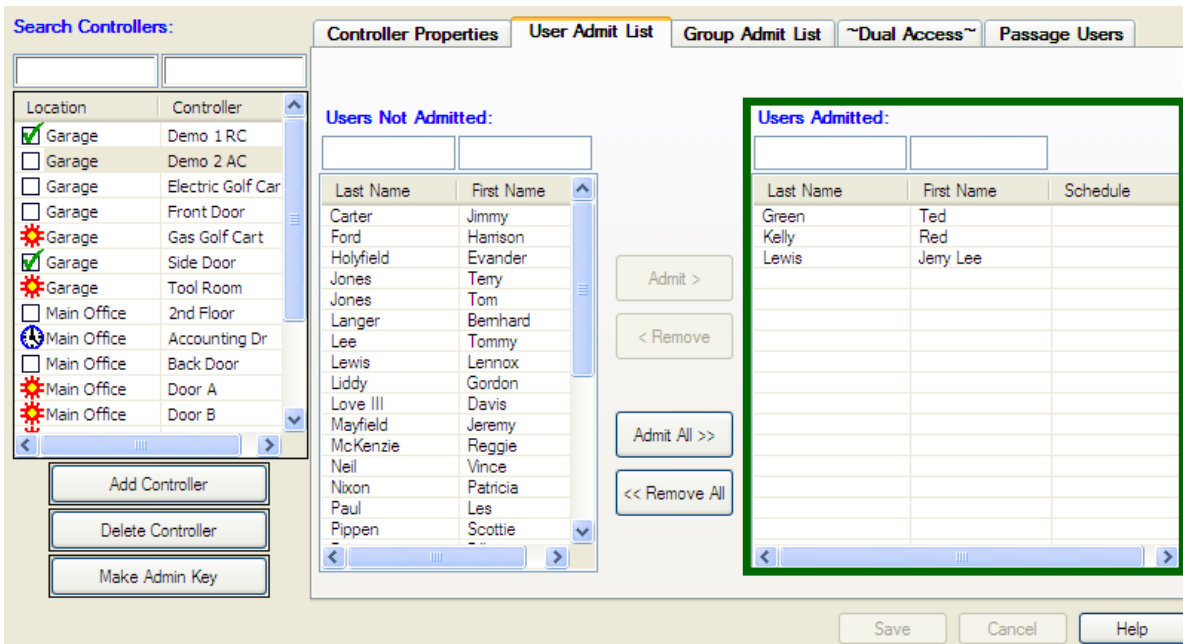


Figure 13  
Admission Controller - User Admit List screen

- For Admission type controllers, only the names that appear on the right-hand list will be granted access.
- For Restriction type controllers, the only people who will not be granted access appear on the right-hand list.

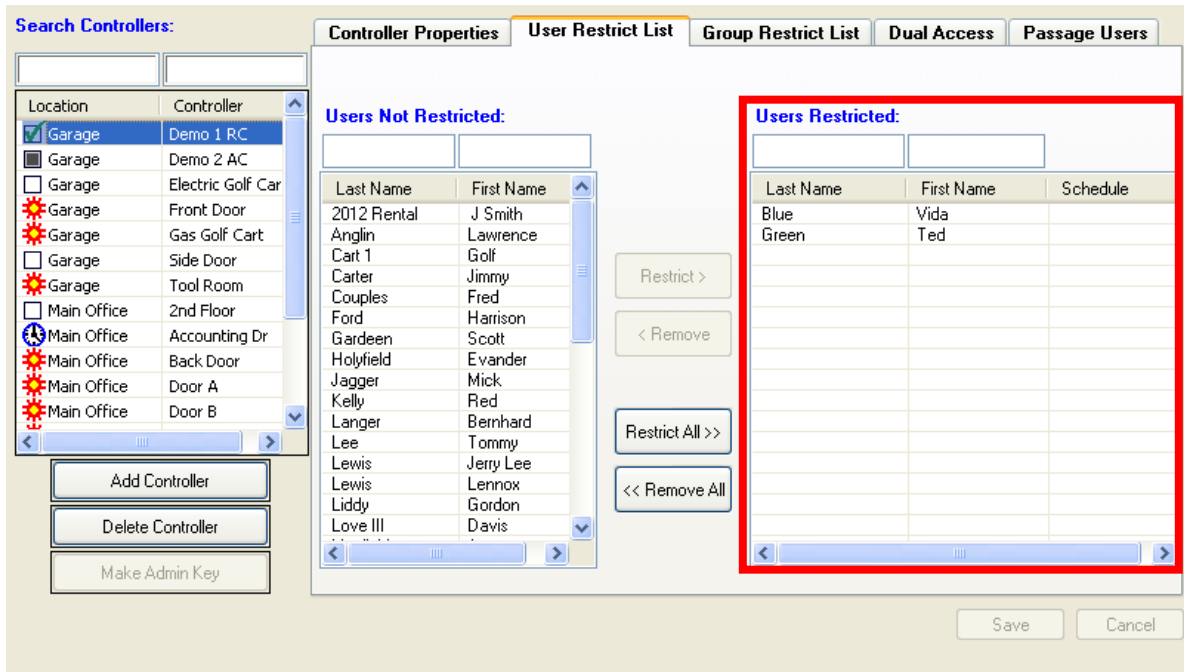



Figure 14

Restriction Controller - User Restrict List screen

Admit or restrict User(s) on each controller:

1. Select the Controllers button  at the top of the screen, and then select the **User Admit or Restrict List** tab (depending on controller type).
2. Select a **Controller** from the left hand list.
3. Select **User(s)** from the list(s) and **move them between lists**, using the buttons with arrows and select **Save**.

**Example:** For the Main Entrance of a building, many administrators choose to program the controller as a restriction type controller. This would grant all active users of your system, access to the door. Initially, no one would be restricted therefore; no names would be listed in the right hand table. If you decided that two manufacturing employees should use the Back door instead of the Front, you would move their two names from the left-hand table to the right-hand table then make an Admin key and insert it into the controller to program the door.

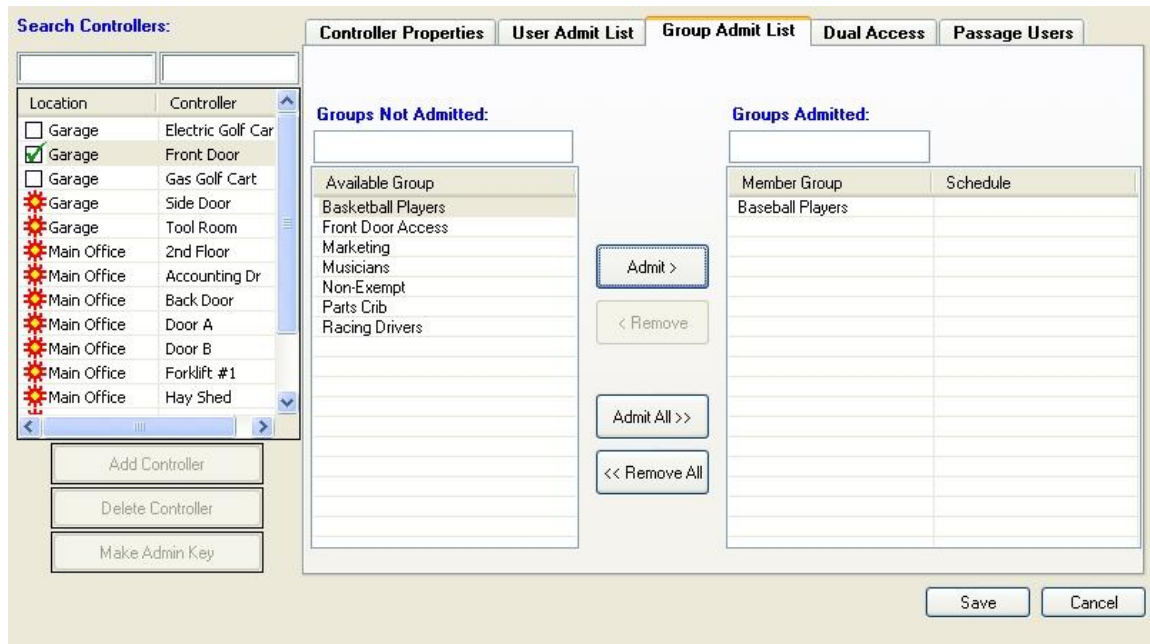
After the controller has been updated, the two employees' keys would not work in the Front Door. If at any time you wanted them to use the front door again, just move them from the right table back to the left and make an Admin key and insert it in the controller.

## Group Lists

Group lists work in the same way as the user lists. The only difference is that you can admit or restrict a group of individuals as a single entity, rather than having to list a large number of people individually.


Once a group has been added to the Group Admit List, an Admin key made and inserted/turned in the controller, new users can be added to the group (in the software), the user keys programmed and thereby, granted access without having to reprogram the controller.

Figure 15



Controllers section - Group Admit List screen

### Admit or restrict groups for each individual controller:

4. Select the Controllers button  at the top of the screen, and then select the **Group Admit or Restrict List** tab.
5. Select a **Controller** from the left hand list.
6. Select a **Group(s)** and move the group name from the left-hand list to the right-hand list, using the buttons with arrows and select **Save**.

Note: See the [Groups](#) section of the software to learn how to create Groups.

## Dual Access (two keys required to open a lock)

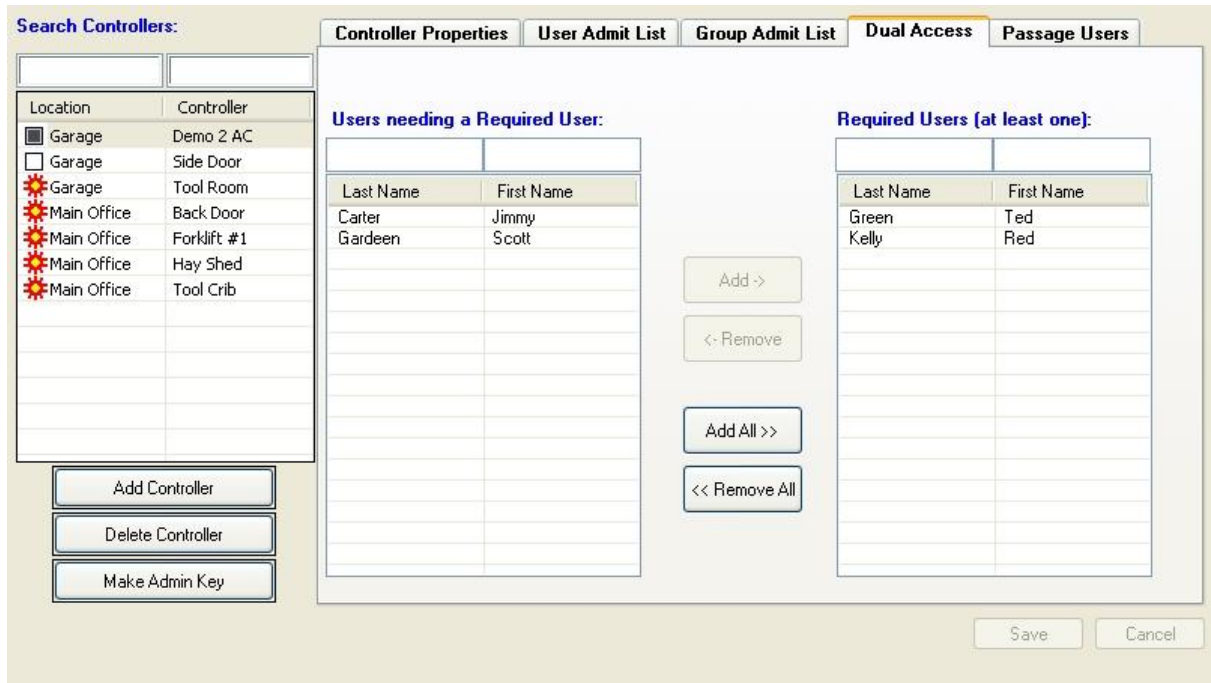


Figure 16

Controller Section - Dual Access List screen

Dual Access controllers require that two user keys must be inserted and turned in a period of time (specified on the controller properties tab), to energize the relay (open the lock).

This feature is commonly used for setting access rights to such things as narcotics cabinets. This tab is used to add individuals (not groups) who are authorized to use their keys in specific Dual Access controllers.

All dual access controllers in the system are shown in the far left window. When a controller is selected, corresponding users are shown the other two window lists.

The center list, “**Users needing a required User**” shows all users who have been given rights to use this controller (from the User Admit List tab). The list on the right “**Required Users**” shows those users whose key must be used in conjunction with others shown on this screen for the controller relay to activate.

**Important: There must be at least one user shown on the “Required Users” (right side) list and their key used, for this type of controller to work correctly.**

**Keys from either list can be used in any order when inserting and turning them in the controller receptacle.**

You can add authorized people to the “**Required Users**” list and remove them by selecting the appropriate add/remove buttons, save the data and program an Admin key to upload the information onto the controller.

### Passage Users (bypassing the relay timer)

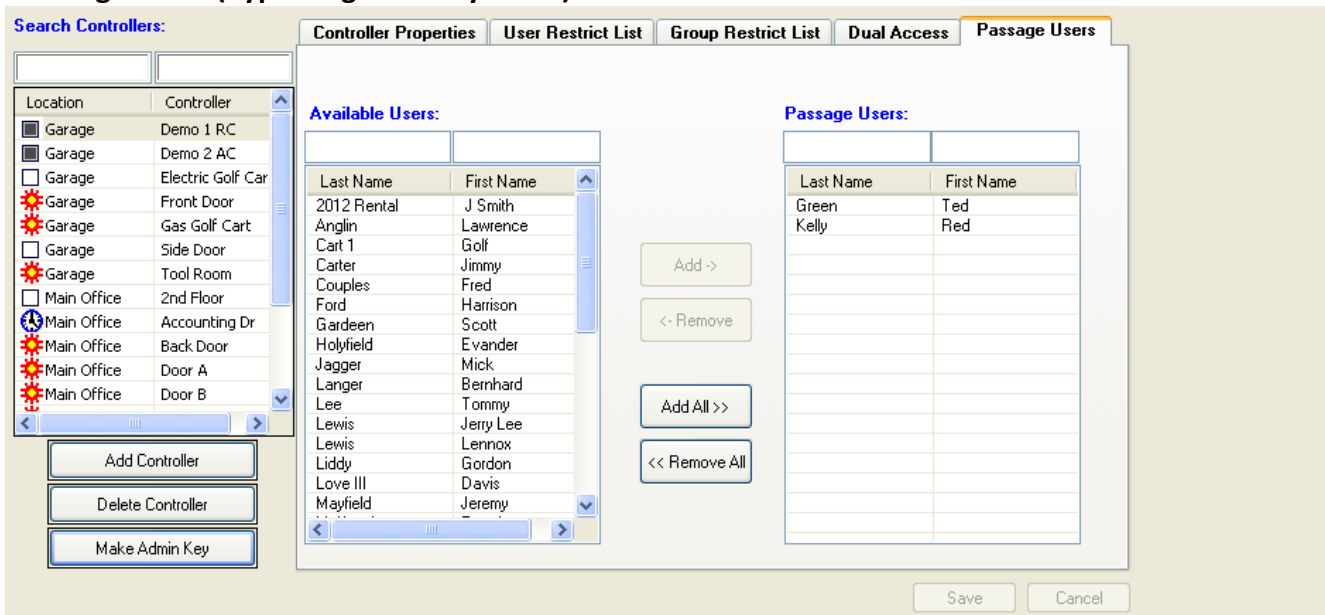


Figure 17

#### Controller Section – Passage Users screen

This tab is used to give certain users the capability of setting a controller into the passage mode. Setting a controller in the passage mode means that when a listed “**Passage User**” inserts their key and turns it twice within five seconds, the controller relay will energize (unlock) and stay that way until the passage key it is turned twice again. If the controller is using a schedule, the auto unlock will relock when the time expires.

The passage mode is typically used in the case of an unexpected delivery of goods or when a service technician needs to gain entry into your facility multiple times in a short time span. Rather than make these temporary personnel a key, a supervisor or any other person with this passage privilege can unlock and relock the controller without any special programming of keys.

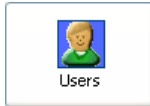
Selecting individuals you want to have passage mode capability is the same as the preceding tab. Once the names have been added to the right-hand list, the Admin key must be programmed and inserted into the corresponding controller for administration.

**Note: Any key listed on the “Passage Users” list can unlock or relock the controller. It does not have to be the same key that set the controller in this mode.**

#### Program Admin key with controller information

1. Select a **Controller** from the list.
2. Insert an Admin key into the G2 Programmer and select the **Make Admin Key** button ([see Admin section](#)). This programs the information in the software to the Admin key.
3. **Insert the Admin Key into the appropriate controller** and turn the key. The information stored on the key will be uploaded into the controllers’ on-board memory.

## Users



Search Users:

Last Name	First Name
2012 Rental	J Smith
Anglin	Lawrence
Blue	Vida
Cart 1	Golf
Carter	Jimmy
Couples	Fred
Ford	Harrison
Gardeen	Scott
Green	Ted
Holyfield	Ewander
Jagger	Mick
Kelly	Red

Add User  
Delete User  
Make User Key

**User Properties** | User Groups | Admission Controllers | Restriction Controllers

Last Name: Green  
First Name: Ted  
Middle Initial:   
User Optional 1:   
User Optional 2:   
User Optional 3:   
User Optional 4:   
Advanced  
 Instant Access Key  
 Master Key (Access to All Controllers)

Key Is Valid:  
 Always Date: 7/27/2011 Time: 10:33 AM  
 From: 7/27/2011 10:33 AM  
 To: 7/27/2011 10:33 AM  
 For: 5 # of Accesses (0-127)

Save Cancel

Figure 18

## Users Section - User Properties Screen

This section is used to enter information about each person you want using the Guardian II system. At a minimum, you must enter their name (last & first), set a valid date range for each key you make and review/set controller admission and restrictions. You may also assign an individual user to a group(s) and set the controller admission and restrictions from this section for their specific key.

Once the information has been entered and saved, a user key can be programmed. You must enter at least a First and Last Name in the appropriate boxes. User Fields 1-4 are optional. A default user key contains an "Always" valid date and time range. There are also two advanced user key types.

Advanced

Instant Access Key  
 Master Key (Access to All Controllers)

The **Advanced** area contains two additional user key types that can be set:

**Instant Access** - This key type gives the holder, access to **Admission type controllers** without the Administrator having to first upload information with an Admin key to each controller, thereby saving you time.

**Master Key** - With this key, the holder has complete access to all controllers in your system. The only way to prevent the use of this type of key, one programmed is to add it to the harvest (disable) or restriction list. If this key has been added to the harvest list and the controller has been administered with this change, the next time this key is introduced to any controller in your system, it will be rendered useless.

Key Is Valid:

Always
  From:

For:

For:






**Key is Valid** - User keys can be programmed in one of three different ways.

**Always** - Sets the valid date out to the year 2255.

**From:/To:** - Enables you to set a valid time and date for a key's life to begin and end. One such use for this type of setting would be when an outside contractor or vendor needs access to one of your facilities. You make the key ahead of time with the valid date and time; send it to the vendor for them to use at the predetermined time. The person can use the key during that period of time only. If for some reason they do not turn the key back in, it becomes invalid after the period of time you set.

**For # of Accesses** - You can set the number of accesses (1-127) that the key can be used before becoming invalid. If you want to charge a patron fee for entry into specific areas, this key will decrement the number of accesses each time it is used in the controller. Once the key reaches zero, you can re-program it for future use.

Icons appearing in the User List show the status of each User Key in the system. Here is a description for each icon:

Icon	User List Message (Description)
	User key is out of date and needs to be reprogrammed.
	User key has been programmed and is up to date.
	User key needs to be updated to current Site Revision.
	User key needs to be programmed its first time.
	User key is currently not valid.



User Groups List

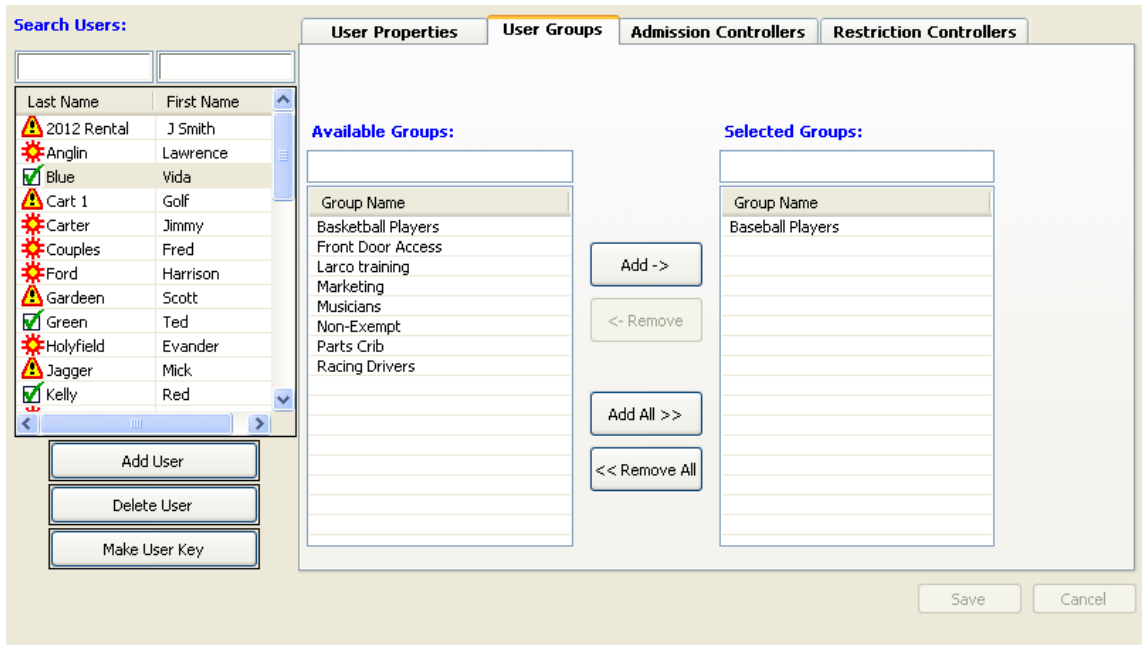


Figure 19

User Groups screen

From the User Groups tab, you can add (assign) Users to one or more groups, right from inside the User section of the software. After selecting a user from the left list, you can select one or more groups from the available list and move them to the selected group list by pressing the **Add** button.

Controller Admission & Restriction

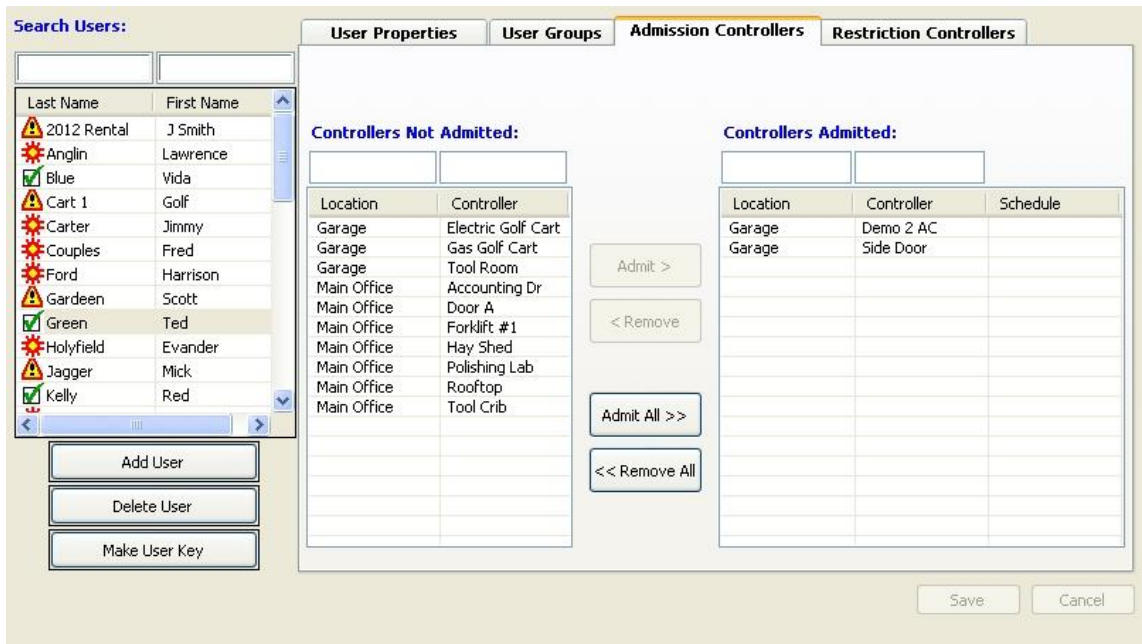


Figure 20

Users Section - Controller Admission screen

The following two tabs (Admission & Restriction Controllers) are used to add a single user to any controller in your system. All the controllers in your system are listed on one of these two lists.

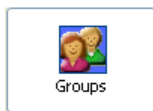
**Note:** The same admitting and restricting can be done in the Controllers section of the software.

After selecting a user from the left-hand list, choose the controllers you want them added to and select the **Add** button. Any changes made will take effect next time you program an Administration key to update the affected controller(s).

**Program user keys**

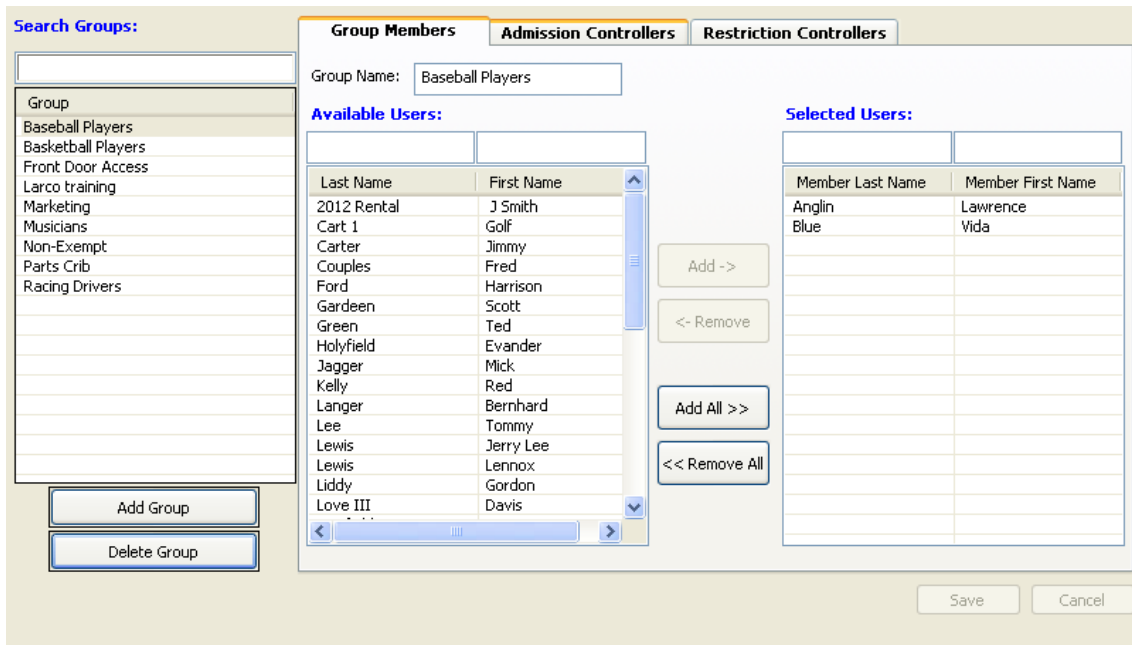
1. Select a **User** from the list.
2. Insert a **User key** into the G2 Programmer and select the **Make User Key** button. This programs the information in the software to the User key.

**Groups**



**Group members**

Select the **Groups** button from the icon area at the top of the application window. From this screen, you can assign individual users to specific groups in the software. This feature is especially helpful when you want to admit or restrict a common group of users for a particular controller,



allowing you to make one entry that affects all users in that group.

Figure 21  
Group Properties screen

Existing groups are shown in the left list. The center list shows all users not in the group (Available Users) and the right list shows who is currently in the group (Selected User).

Adding Groups:

1. Select the **Add Group** button and type the **Group Name** in the box.
2. Select **Available Users** from the list and **Add** them to the **Selected Users** list.
3. Select the **Save** button.

Deleting Groups:

1. Select a **Group** from the left Group List.
2. Click the **Delete User** button.
3. A warning window appears, confirming the deletion. Select **Yes** to Delete.

Example: Marina with main gate and three dock gates:

The main gate would be set up as a Restriction type controller (due to the high number of potential users). All programmed user keys will be granted access to the main gate, no one would be restricted.

Each of the three dock gates would be Admission type controllers and named Dock A, B and C. Three groups (Dock A Boaters, Dock B Boaters and Dock C Boaters) will be created in the software and each user key will be assigned to the group where their boat is docked.

Each controller will admit only those users with the same group name as the dock. (Dock A controller will only admit Group A users.) This makes setting up and maintaining the marina very straightforward. All boaters who have a slip at the marina will be issued a key. Each key can also be programmed with a start and stop time and date. Then, every year the boater can bring their key back to be re-programmed with a new start/stop date when they pay the next season's rental fees.

**Admission / Restriction Controller Lists**

**Search Groups:**

Group

- Baseball Players
- Basketball Players
- Front Door Access
- Larco training
- Marketing
- Musicians
- Non-Exempt
- Parts Crib
- Racing Drivers

**Group Members** | **Admission Controllers** | **Restriction Controllers**

**Controllers Not Admitted:**

Location	Controller
Garage	Electric Golf ...
Garage	Gas Golf Cart
Garage	Tool Room
Main Office	Accounting Dr
Main Office	Door A
Main Office	Forklift #1
Main Office	Hay Shed
Main Office	Polishing Lab
Main Office	Rooftop
Main Office	Tool Crib

**Controllers Admitted:**

Location	Controller	Schedule
Garage	Demo 2 AC	
Garage	Side Door	

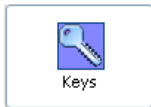
Buttons: Add Group, Delete Group, Admit >, < Remove, Admit All >>, << Remove All, Save, Cancel

Figure 22

Group Section – Admission Controllers List screen

The next two tabs in the Groups section are where you can admit or restrict any or all of your groups by individual controller. The **Admissions Controller** tab contains all of the Admission type controllers. By moving them from the left-hand list to the right, you are granting them admission to this controller. The **Restriction Controllers** list works in the same manner, only you are restricting the groups you move to the right-hand list. *Note: New users can be added to the group (in the software), the user keys programmed and thereby, granted access without having to reprogram the controller.*

## Keys



### View / Import, Make Admin/Export Keys

In the **Keys** portion of the software, you can view information contained in all three different types of keys used by the system (*Admin, Export & User keys*) and make the Admin and Export keys, which are used to program and retrieve information from the controllers in your system.

You also upload records from export keys, into the database. User keys are programmed in the [User section](#) of the software.

Use the “**View/Import**” tab to view User, Export and Admin key information. Once a key has been inserted into the G2 Programmer, press the **View Key** button to display the contents of that specific key.



### Viewing User Keys (Blue, Green, Red & Yellow)

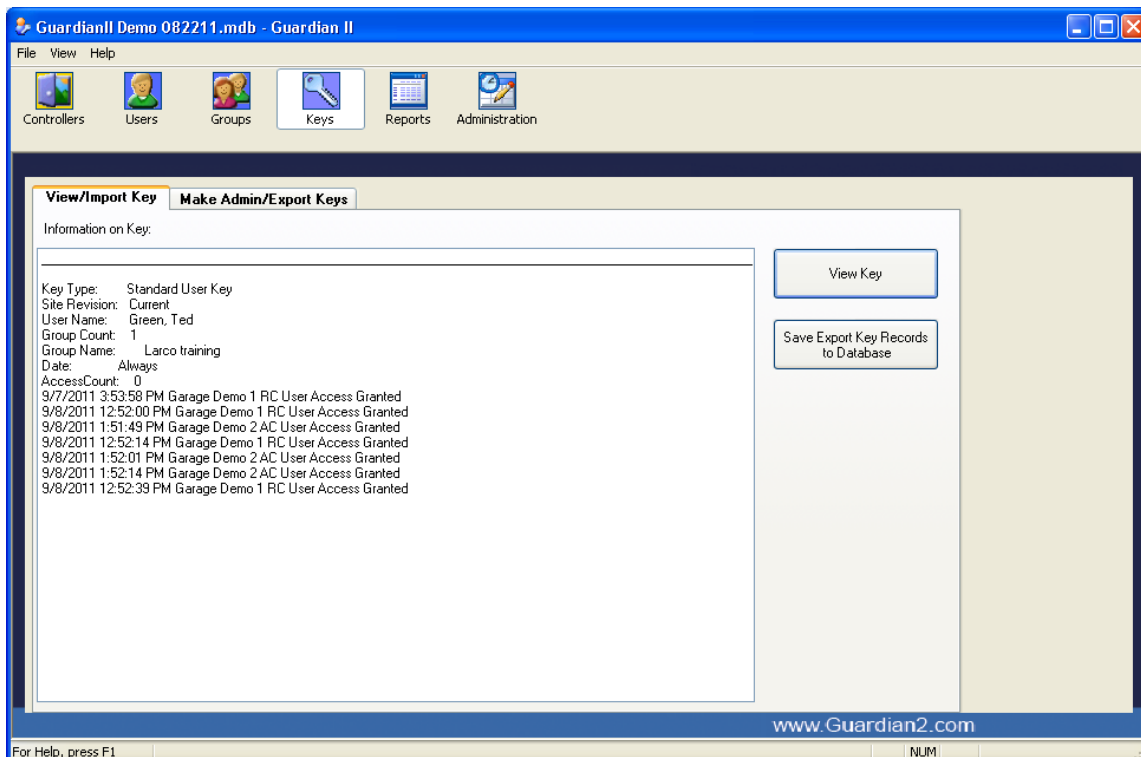


Figure 23  
Keys Section - View User Key screen

Figure 23 displays the information contained on a sample User key. Information displayed includes:

- Key type
- Site revision
- User name
- Group membership
- Dates that the key is valid
- The number of accesses allowed before the key expires
- An audit list of the last fifteen transactions performed by the user



### View the Admin key (Gray)

The screenshot shows a software window titled 'View/Import Key' with a sub-tab 'Make Admin/Export Keys'. The main area is divided into two sections: 'Information on Key:' and 'Garage Front Door Configure'. The 'Information on Key:' section contains the following text:

```
Key Type: Admin Key
Site Revision: Current
User Name: Admin 1
Controllers: 1
```

The 'Garage Front Door Configure' section contains the following text:

```
Time Delay: 5
Dual Delay: 9
Use Daylight Savings Time
Access Controller
User: Jagger, Mick P
User: Preston, Billy X
Harvest User: Holyfield_37, Evander
Harvest User: Lee_20, Tommy
Harvest User: Preston_116, Billy B
Harvest User: Preston_51, Billy
Dual User: Preston, Billy X
Passage User: Gardeen, Scott M
Auto Unlock Disabled
```

On the right side of the window, there are two buttons: 'View Key' and 'Save Export Key Records to Database'.

Figure 24

Keys Section - View (Admin) Key screen

Figure 24 displays information contained on a sample Admin key. The data written on this key will be downloaded (transferred) to the Garage - Front Door controller from the software.

Configuration data contained on the key includes:

- Key type (Admin)
- Site revision (Current)
- User name (Admin 1)
- Configuration: Time delay for the relay (lock) activation (5 sec.), Dual Access time between key insertions (9 sec.), Daylight savings time, Controller Type (Access), Names of the groups and individuals with access privileges or are on the harvest list.

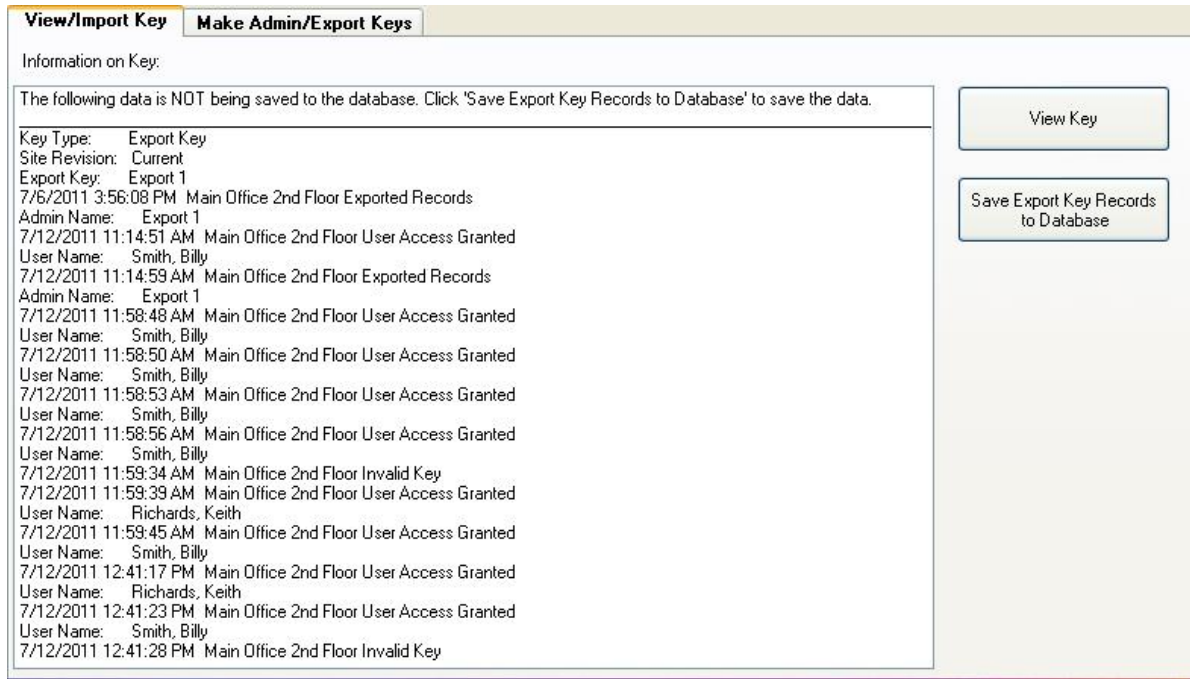

 **View the Export key (Black)**


Figure 25

**Keys section - View (Export) key screen**

Each time someone uses a key at one of your controllers, a record of the transaction is stored in the controller's memory. [The export key is used to extract this data from the controller and transfer it back to the computer.](#) Once you insert and turn the export key in the G2 Programmer, you can select the **View Key** to review the records on the key.

**Save Export Key Records to the Database**

1. **Insert a programmed Export key into your controllers** to retrieve all the transactions stored in the controller's memory.
2. Take the export key back to your computer and insert it into the G2 Programmer.
3. Select the **Keys** icon  from the top, icon menu.
4. Select the **View/Import Key** tab.
5. Select the **View Key** button to review the transaction records.
6. Select the **Save Export Key Records to Database** button to transfer the records from the key to the software. [Once the data has been uploaded into the programs database, you can then run reports from the Reports section of the software.](#)
- 7.

**Important:** Before deleting an Export Key, it is a good idea to view the contents of the key and export the records to the database. Once a key has been deleted or written over, the data is not recoverable.

## Make Admin & Export keys

This section of the software is very important. All Admin and Export keys for your system are created and programmed here.

- ❖ **Admin keys** are used to program controllers with the information that has been entered in the software application. After data has been written to the Admin key, the key needs to be inserted in the controllers' receptacle, so the data can be uploaded and stored in the controllers' memory. Each controller holds its specific data independently of all other controllers, thereby allowing or denying access to key holders on a per controller basis.
- ❖ **Export keys** are used to transfer information from each controller back into the software, where the data can be viewed and reports generated. Once an export key has been made in the software, it can be inserted in a controllers' receptacle to upload the data from the controller onto the key. The key is then taken back to the PC and inserted into the G2 Programmer and uploaded into the software.

**Important: At a minimum, you will need to create at least one Admin and one Export key in order to administer your system. A controller must first be entered in the software before and Admin key can be made.**

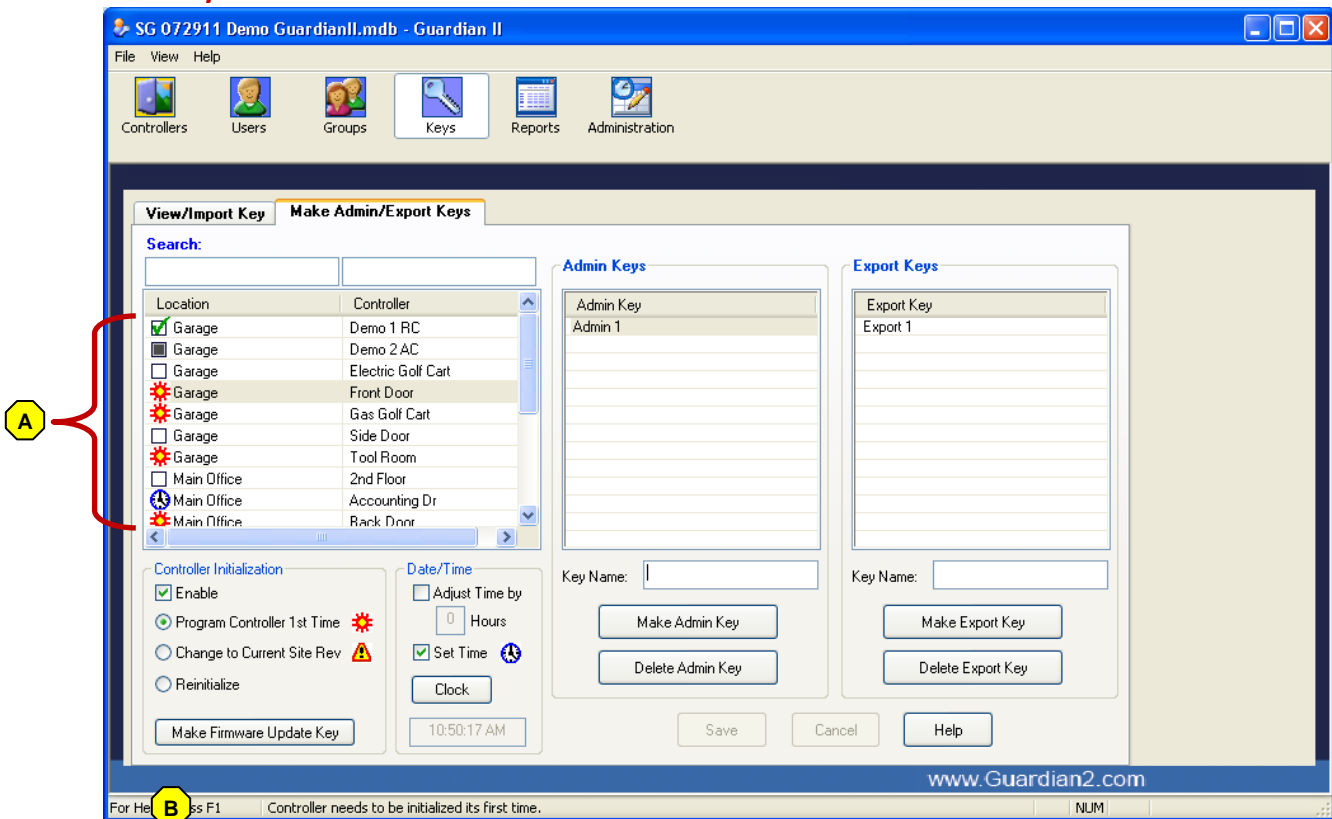


Figure 26

Keys section – Make Admin/Export Key screen

- ❖ **Icons appearing in the left list above show the administrative status of each controller in the system. Any icon that does not have the green check mark needs some action to be taken, either with an Admin or Export key.**

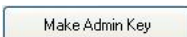
As you scroll down the controller list, different sections on this screen become activated and the message bar **B** gives a description of the controllers' administrative state.

Here is a description of each icon:

Icon	Controller List Message (Description)
	Controller needs to be initialized its first time (appears on all new controllers, not yet programmed)
	Controller is up to date
	Controller needs to be reprogrammed with an Admin Key (changes have been made in software and an Admin key needs to be programmed and inserted in this controller)
	Controller needs to export records to Export Key, and then please save its records to (controller data was written to an Admin key and should have been uploaded into the controller. The next time records are exported from controller and saved in the software, this icon will change to a green checkmark)
	Controller needs to have its Time Set (this appears if the set time checkbox was unchecked during other Admin key programming or the Daylight Savings Time box is toggled. Located in the Administration section of the software.)
	Controller needs to be initialized to current Site Revision (the Site Revision has been changed and the controller requires an Admin key be programmed and inserted/turned in the controller receptacle.)

You can choose to program a single controller or multiple controllers (page 45), using one or more Admin key(s). **When programming a controller for the first time, you can only load one controller on an Admin key at a time. Important: at least one controller must always be selected to make or program data onto an Admin key.** This screen contains various buttons that are used to Make (name & program) and Delete both Admin and Export keys. The following section describes what each is used for:



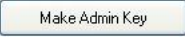
**Make Admin Key**





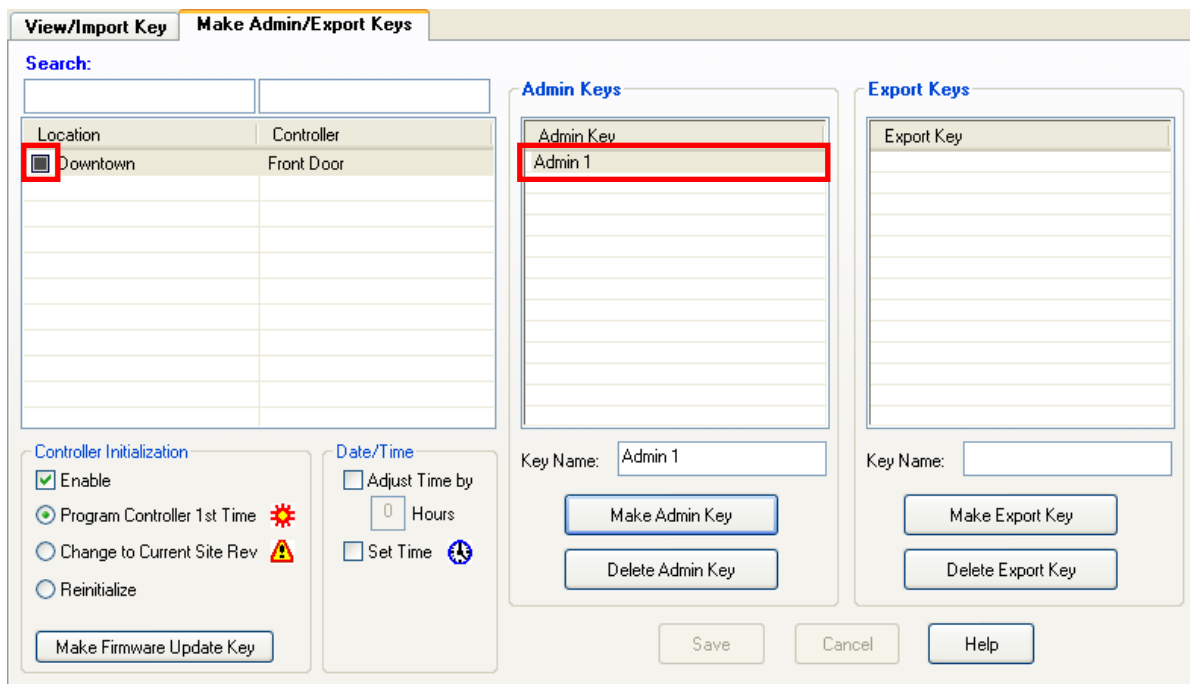
- Programs an Admin key (Gray) with its name, key type and controller data. **Important: You must have an Admin key in the G2 Programmer before you select the "Make Admin Key" button.**

The screenshot shows the 'Make Admin/Export Keys' window. On the left, a table lists controllers with checkboxes and status icons. Callout 2 points to the 'Side Door' controller which has a sun icon. Below the table are 'Controller Initialization' and 'Date/Time' sections. On the right, the 'Admin Keys' section shows a list with 'Admin 1' selected (callout 3) and a 'Key Name' field (callout 5). Below these are 'Make Admin Key' and 'Delete Admin Key' buttons. The 'Export Keys' section is empty. At the bottom are 'Save', 'Cancel', and 'Help' buttons.



1. Select the **Keys** button  at the top of the screen, and then select the **Make Admin/Export Keys** tab.
2. Select a **Controller** from the left list. *Note: The Gear icon  indicates that the controller has never been programmed and needs to have an Admin key made and inserted to initialize its memory.*
3. Select the **Admin key** from the middle list. *Note: If no Admin key has been made see #5.*
4. **Insert and turn an Admin key** into the G2 Programmer.
5. If no Admin Key appears on the list, type a name for the Admin key in the Key Name box and press the **Make Admin Key** button . A pop-up window appears, select **OK**. The data will be written to the key. As the key is being made, two windows pop-up (Key Added & Key Complete) are shown. When the windows disappear, the key has been successfully written to.
6. Insert & turn the programmed Admin key in the receptacle on the controller you want to program. **Important: All records should be exported from controllers before inserting an Admin key.**

The following screen capture example shows the new Admin key name, “Admin 1” and the change of the icon for the controller, to a gray square . This indicates that an Admin key has been programmed and needs to be inserted in that controller. Once an export key is inserted in this controller and the data has been uploaded into the software, the icon will change to a green checkmark .



**View/Import Key**   **Make Admin/Export Keys**

**Search:**

Location	Controller
<input checked="" type="checkbox"/> Downtown	Front Door

**Admin Keys**


Admin Key
Admin 1


**Export Keys**

Export Key

**Controller Initialization**

Enable

Program Controller 1st Time 


Change to Current Site Rev 

Reinitialize

**Date/Time**

Adjust Time by

Hours

Set Time 

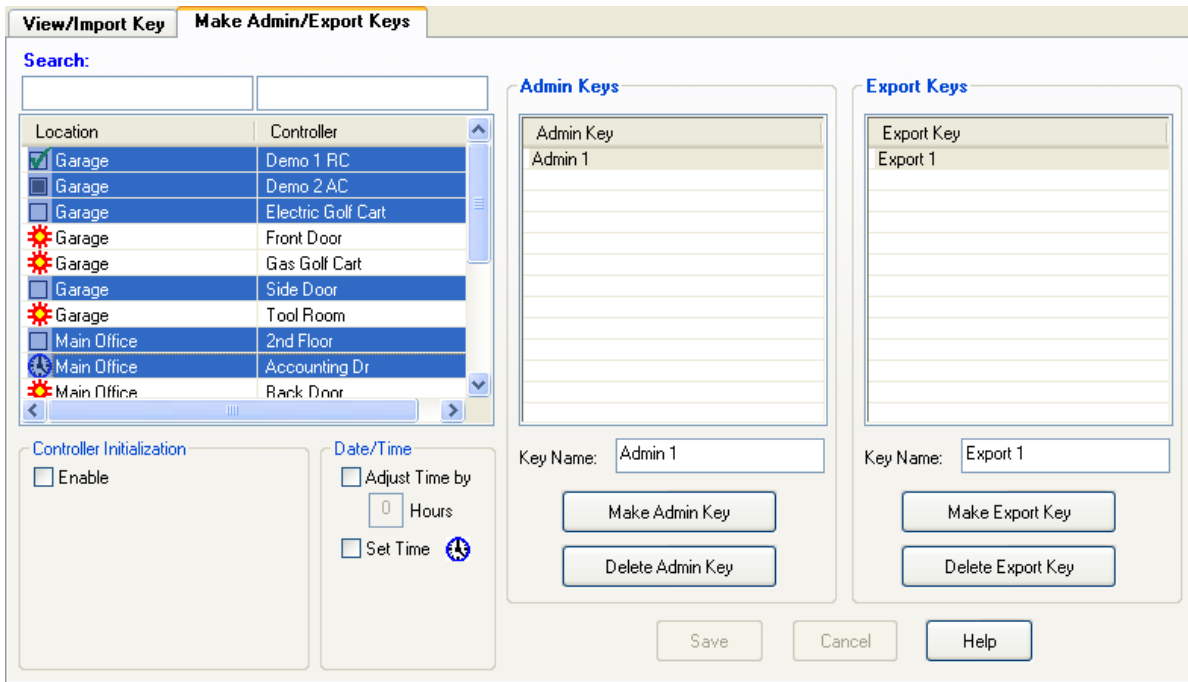
Key Name: Admin 1


Key Name:

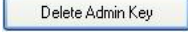
### Make an Admin key that contains data for multiple controllers

The software allows you to write data for multiple controllers on a single Admin key.

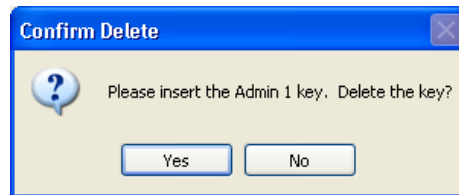
*Example:* If you added a new user in the User section of the software and gave them access rights to multiple controllers, you need to update each of those controllers with this new information.




1. Select the **Keys** button  at the top of the screen, and then select the **Make Admin/Export Keys** tab.
2. Select a multiple **Controllers** from the left list.
3. Select the **Admin key** from the middle list.
4. **Insert and turn an Admin key** into the G2 Programmer.
5. Select the **Make Admin Key** button.
6. Remove key from the G2 Programmer and insert it into each of the selected controllers. The pertinent data for each controller will be downloaded accordingly.

**Delete Admin Key**  (optional) - Deletes an Admin key from the software. **Important:** You should have the specific Admin key you want to delete in the G2 Programmer before you select “Delete Admin Key”. You can delete this type of key from the software without putting it in the Programmer, but that is strongly discouraged, due to security concerns.


1. Insert the Admin key you want to delete into the G2 Programmer.
2. Select the **Admin key** from the middle list.
3. Select the **Delete Admin Key** button. A window confirming the deletion appears, select the **OK** button.




**Make Export Key** - Programs an Export key (Black) with its name and key type. **Important:** You must have an Export key (black) in the G2 Programmer before you select the “Make Export Key” button.

1. Insert a blank Export key (black) into the G2 Programmer.
2. Type a name for the Export key in the Key Name box and press the **Make Export Key** button .
3. Select **OK** on the pop-up window.

You can now insert this programmed, export key into your controller(s) to upload records onto it, then insert the key in your G2 Programmer to transfer the records from the key, into the software application.


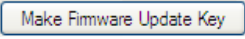
**Delete Export Key**  (optional) - Deletes an Export key from the software. **Important:** You should have the specific Export key you want to delete in the G2 Programmer before you select “Delete Export Key”. You can delete this type of key from the software without putting it in the Programmer, but that is strongly discouraged, due to security concerns.

1. Insert the Export key you want to delete into the G2 Programmer.
2. Select the **Export key** from the right hand list.
3. Select the **Delete Export Key** button. A window confirming the deletion appears, select the **OK** button.

**Controller Initialization** – This area of the screen appears when a controller with a gear icon  is selected. It lists the reason a controller needs to be programmed, initially.

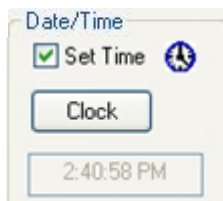


- ❖ **Program Controller 1<sup>st</sup> Time** – This programs your site specific information in the controller, as well as the properties you have selected for the controller in the other sections of the software and sets the time on the controller.
- ❖ **Change to Current Site Rev** – Occurs when you have changed the site revision, typically due to security concerns. This writes new identification information in the software and therefore all your controllers need to be re-administered.
- ❖ **Reinitialization** – Used to reset a controllers' information, if you wanted to move a controller from one area to another. You would enter a new controller in the software and select the Reinitialization radio button, program an Admin key and the controller would be seen by the software as a different controller.
- ❖ **Make Firmware Update Key** – Used to update the controllers firmware. If updates related to the operation of the hardware are needed, an electronic file can be downloaded from the manufacturer to your computer and written to an Admin key by selecting this button. To make a firmware update key:

1. Insert a gray Admin key into the G2 Programmer.
2. Select the **Keys** button  at the top of the screen, and then select the **Make Admin/Export Keys** tab.
3. Select the **Enable** checkbox (lower-left corner) and then the  button.
4. Select the appropriate file (.bin) from the Open file window, and then select the **Open** button. The key will be programmed immediately. After the key has been made, insert the key into each controller. The LED will flash a fast amber light while the firmware is being updated. Once the transfer is complete, the LED will turn to solid red.

Date/Time

- ❖ **Set Time** - Is automatically checked the first time a controller is administered after installation has occurred. Used to set the time clock inside each controller (using an Admin key). When you check the box in this section, a Clock button appears. If you select the button, a calendar and clock time window appears. You can select the “OK” button to set the current time (set by the computer clock) or, using the calendar and clock, set a time in the future when you will be at the controller to download this new information.



Reports



Selecting & printing

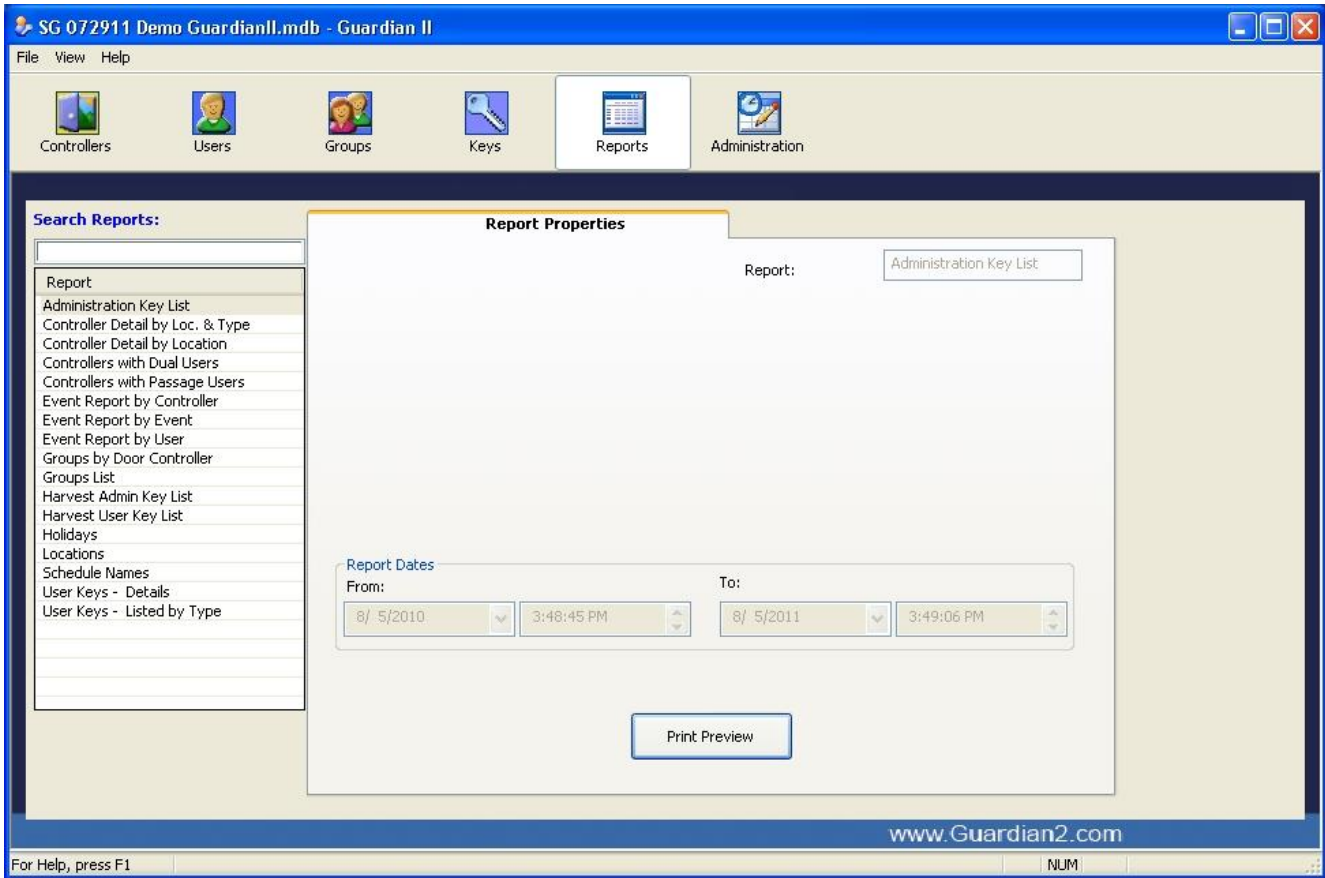


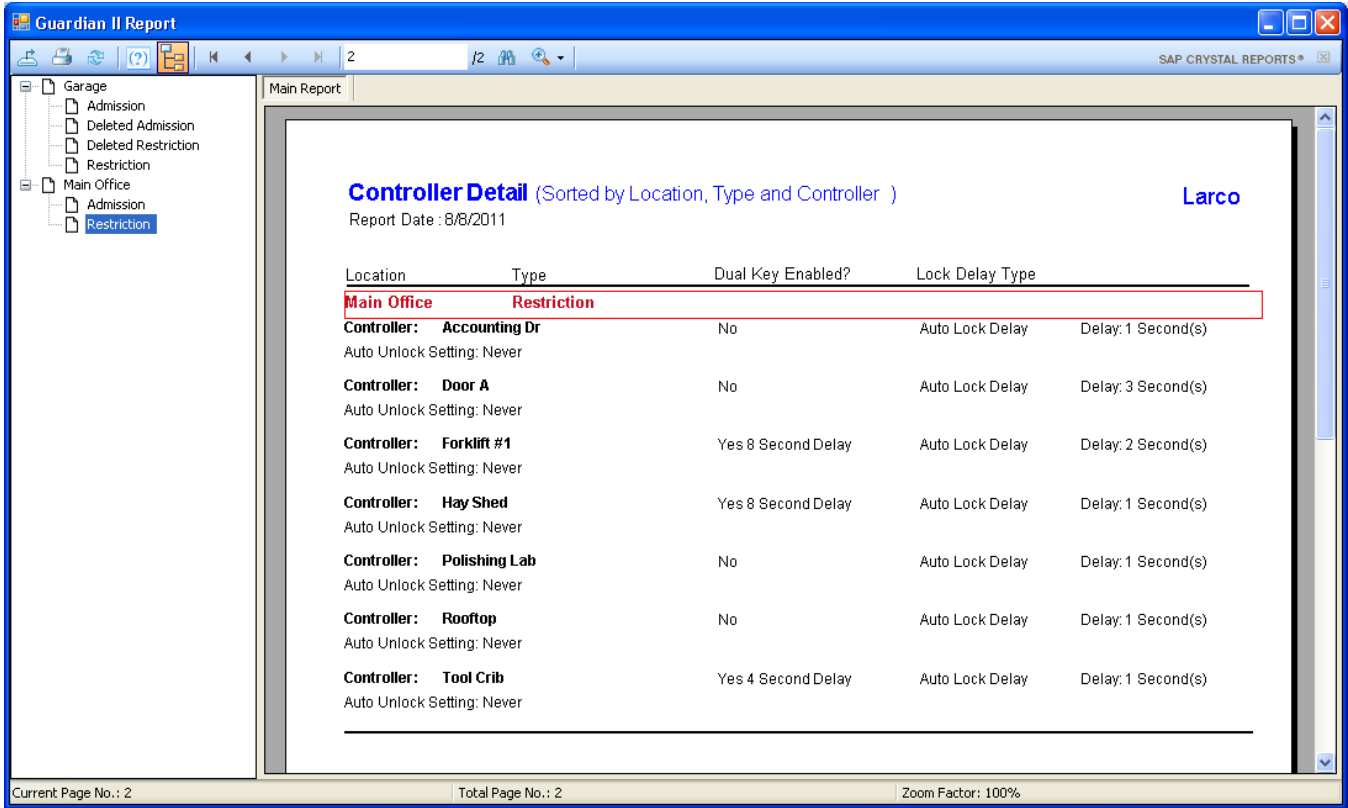
Figure 27  
Report Properties Screen

From this area, you can view and print reports related to information in your system. There are a variety of "canned" reports, containing information related to Controllers, Group Lists, User Lists and transaction data.

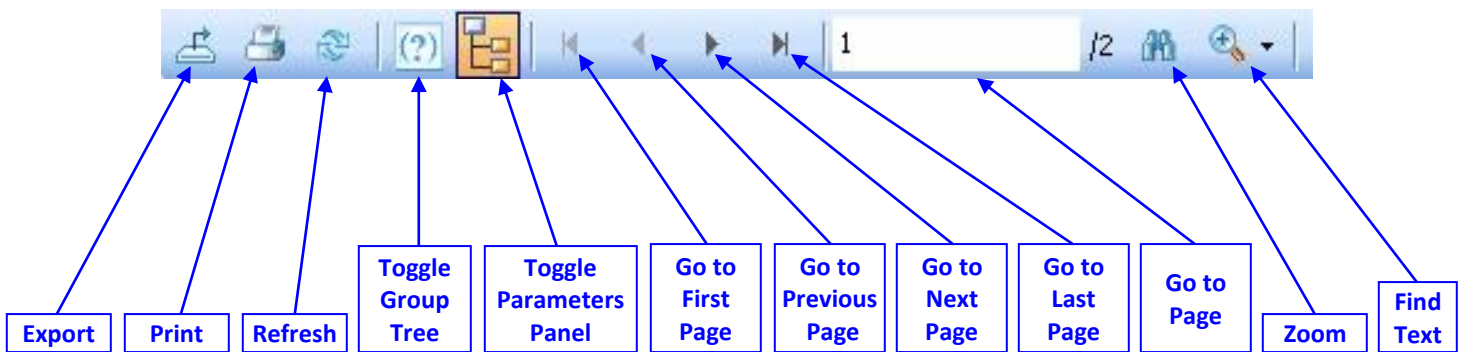
To get the latest information in your reports, you will want to upload data from all your controllers with an export key back into the software.

Select the report type from the list on the left hand side of the window. When a report contains variables, such as date ranges, you will need to enter specific dates in the pop-up window. Enter a beginning and ending date and time in each specific field and select the **Print Preview** button.

The report viewer window has a menu bar where you select the page(s) to view and print your report. Along the left side, there are expand/collapse text fields that you can select to jump to different sections of the report.



The toolbar contains various icons shown below with a description of each.



Guardian II controller board connections

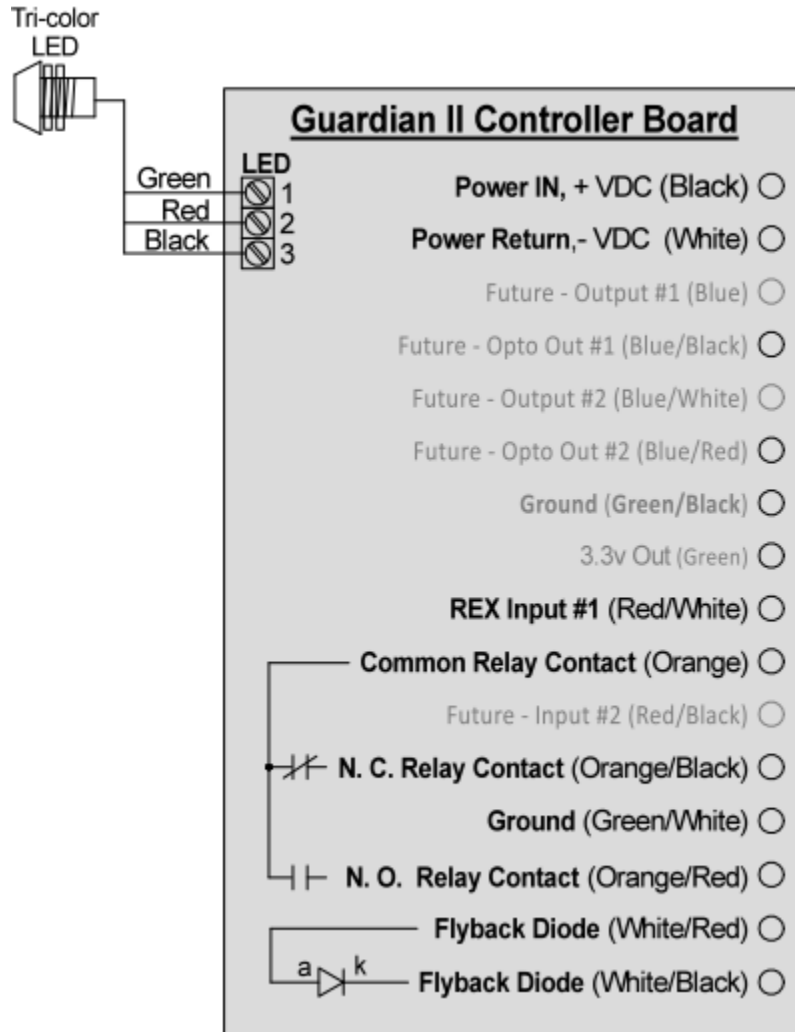
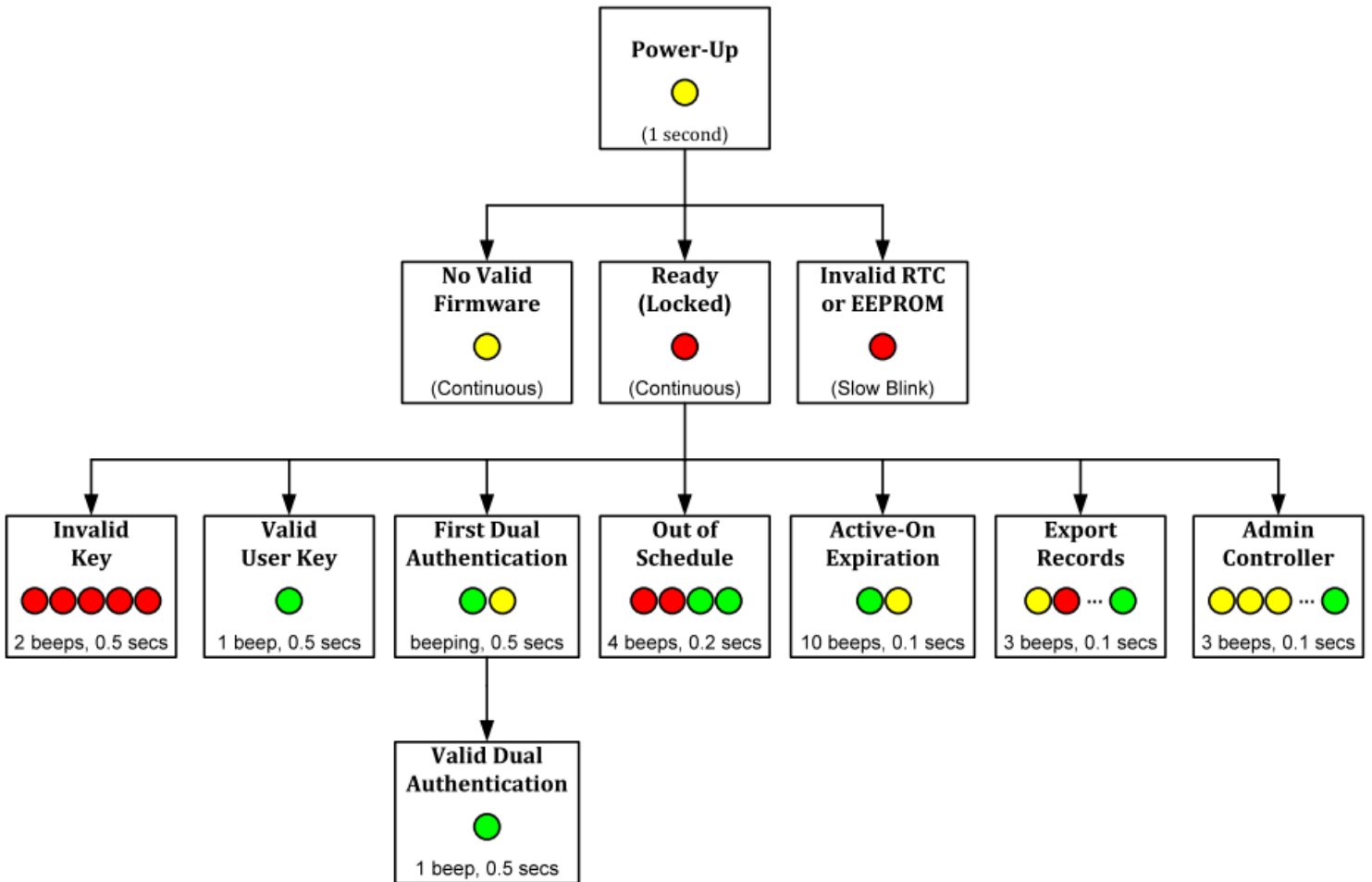


Figure 28  
Controller connections



User interface (LED colors and patterns)



Copyright notice

©2014 ATEK Access Technologies, LLC - All Rights Reserved.

No part of this manual may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of ATEK Access Technologies, LLC.

ATEK Access Technologies, LLC reserves the right to make changes in specifications at any time and without notice. The information furnished in this publication is believed to be accurate and reliable. However, no responsibility is assumed for its use nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent right of ATEK Access Technologies, LLC. Dimensions are nominal and subject to manufacturer's tolerance.

**Trademarks:** Larco® is a registered trademark of ATEK Access Technologies, LLC. Microsoft® is a registered trademark of Microsoft Corporation. Windows® XP, Windows® Vista and Windows® 7 are trademarks of Microsoft Corporation. All other brand names and product names used in this manual and associated documentation are trademarks, registered trademarks or trade names of their respective holders.



WARNING: Cancer and Reproductive Harm - www.P65Warnings.ca.gov