Operator's Manual

Quantum 1.7

by INTELLIKEY® CORPORATION

100760 Rev 5

Technical Support

For technical support for your INTELLIKEY products, contact your local INTELLIKEY dealer, or contact INTELLIKEY directly:

Phone: (321) 724-5595
Fax: (321) 724-5695
email: techsupport@intellikey.com
Internet: www.intellikey.com

Contents

Introduction

Quantum

This manual is a User's Guide for operation of the INTELLIKEY® Quantum™ software. Quantum provides the functions necessary to implement a key and access control system based on the INTELLIKEY Electronic Keys and Controllers.

With its easy-to-use, Microsoft® Windows™ based interface, Quantum simplifies the task of defining the parameters of your access control system. The Quantum software then allows you to program the access information into your controllers and keys, and keeps track of how each item has been programmed. As your system grows, Quantum tracks the relationships between keys, keyholders, and controllers, and provides you with up-to-date reports on the status of your INTELLIKEY system.

Don't be put off by the number of chapters in this manual. Although the Quantum software performs a lot of functions, it is really very easy to use. Each of the operations you can do with Quantum is described in a separate section. The material in this manual is organized for a new Quantum user. If you read the manual in order, you will quickly acquire a working knowledge of the Quantum functions.

Quantum Versions

The Quantum software is available in two versions, the *End-User* version and the *Dealer* version. The End-User version is for a single site which has all of the programming equipment necessary to perform all functions associated with an INTELLIKEY-based access control system. The Dealer version has additional functions which allow an INTELLIKEY dealer to support several smaller sites with one copy of the Quantum software, and one set of programming equipment.

Most operations are identical between the two versions. The few that are different are pointed out at the appropriate places in this manual. The chapter on "The Dealer Version" describes the extra functions provided for dealers.

Requirements for Using Quantum

Hardware Requirements

Operation of the Quantum software requires an IBM-PC compatible 486 or higher computer with the following:

Microsoft® Windows® 98, NT, 2000, or XP

64 Megabytes of memory

Hard disk with 10 Megabytes of free space

CD-ROM or floppy disk drive for installation and file backup

At least one dedicated serial port (COM1 – COM9)

Windows Skills Required

This manual assumes that you are already familiar with using Windows. You should at least know the following Windows operations:

Use menus and dialog boxes to choose options and preferences

Use the mouse to click, drag, and double-click

Minimize and maximize windows and icons

Look for on-line Help

The person responsible for managing the Quantum system will need to be able to perform certain disk and file related operations, using the Windows File Manager or equivalent program. You should refer to the Windows manual which accompanied your PC to learn how to:

Format a floppy disk

Copy a disk

Appearance of Screens

The pictures of Quantum screens used in this manual were taken from Windows 98. The screens may appear slightly different under other versions of Windows, but the functionality is the same.

Software License Agreement

The Quantum software programs ("Software") are copyrighted by INTELLIKEY® Corporation ("INTELLIKEY"). You should carefully read the following terms and conditions before using the Software. Using the Software indicates your agreement to the terms of the following LICENSE STATEMENT and DISCLAIMER OF WARRANTY.

LICENSE STATEMENT

This software is licensed for the exclusive use of the original purchaser ("YOU"). A single copy of the Software may be executed from a common disk shared by multiple CPUs, subject to the maximum number of concurrent users imposed by the Software itself.

This software is not copy protected. INTELLIKEY authorizes YOU to make backup copies of the software for YOUR archives only for the sole purpose of protecting your investment from loss.

YOU are free to move this software from one computer location (or common disk) to another, so long as there is no possibility of it being used at one location while it is being used at another. Just like a book that cannot be read by two different people at two different locations at the same time (unless, of course, INTELLIKEY's copyright has been violated).

DISCLAIMER OF WARRANTY

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. INTELLIKEY SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO DEFECTS IN THE DISKETTES, DOCUMENTATION, SOFTWARE, AND THE LICENSE GRANTED HEREIN. IN NO EVENT SHALL INTELLIKEY BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGE, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES.

Additional Disclaimer

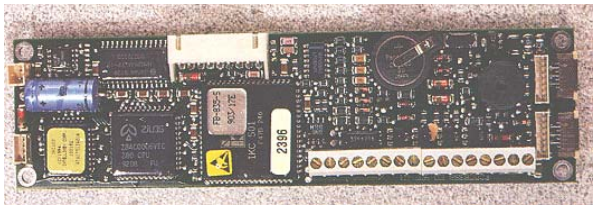
All of the company and institution names used in the examples in this manual are, as far as we know, fictional. If we have used any real names (other than friends and relatives who either said it was okay or who will never read the manual), it was unintentional.

System Overview

Hardware

The Lock Controller

The INTELLIKEY Electronic Controller controls access to doors. The INTELLIKEY controller consists of an electronic cylinder attached to an electronics assembly. The controller communicates through an infrared link with the INTELLIKEY key to exchange access control information. Based on this information, the controller decides whether or not the key should be allowed to operate it.



Throughout this manual, we will refer to the key *operating* the controller, rather than unlocking or opening it. Since INTELLIKEY controllers can be used in a variety of control applications, as well as standard locking mechanisms, operate is a more appropriate term. You can think of operate as meaning "had this been a mechanical lock, the person using the key would have been able to rotate the key after inserting it". Also, since the controllers are controlling access to locks and doors, I will use the terms "controller", "lock", and "door" interchangeably throughout the manual.

INTELLIKEY controllers are available in two configurations: fixed cylinder and rotating cylinder. Fixed cylinders function as reader devices only -- when you insert your key into the cylinder, the controller reads the key's information and activates an output signal which causes an external locking mechanism to function. This type of cylinder would be used in conjunction with an electric strike or magnet, for example. Rotating cylinders fit into standard locking mechanisms. When you insert your key, the controller releases the cylinder, allowing you to turn the key and activate the

mechanical locking mechanism. This type of cylinder fits into existing mortise and rim cylinder applications.

The Electronic Key

The INTELLIKEY Electronic Key allows each keyholder access to a specific set of controllers. Each key has a special feature memory which may be programmed with the keyholder's access control information. The key has an infrared communications system which allows it to transmit this access control information to an INTELLIKEY controller.

The Key Processing Unit

The KPU is the device by which the electronic keys are programmed with features and access codes. The KPU is also used to query (interrogate) programmed keys to determine their contents. The KPU connects to a standard personal computer and is controlled by the Quantum software.

The Controller Programming Unit

The Controller Programming Unit (CPU) is the device by which the electronic controllers are initially programmed with features and access codes. The CPU may also be used to update and query (interrogate) controllers. The CPU connects to a standard personal computer and is also controlled by the Quantum software.

The Restricted Authorization Key

The Restricted Authorization Key (RAK) is a hand-held programming device for modifying and interrogating the electronic controllers. There is a separate *RAK User's Manual* which describes operation of the RAK in more detail.

Site Codes

Each INTELLIKEY site (end customer) is assigned a site code which uniquely identifies all controllers and keys associated with that site. The site code programmed into an INTELLIKEY key must match that of the controller into which it is inserted before the controller will allow the key to operate it. INTELLIKEY Corporation has set up a site code distribution system which guarantees that no two sites will ever have the same site code.

The 'SiteCode Key™' is the mechanism by which site codes are distributed to the end user. A SiteCode Key is a specially programmed INTELLIKEY key which contains your unique site code. The Quantum Installation program reads the site code from the SiteCode Key, and records it for insertion into each of your controllers and keys.

Data Flow

The Quantum software's main function is as a key control system. Quantum maintains records of what feature and access information is programmed into each electronic controller and key in your system. Quantum also keeps track of which keys have been issued to keyholders. By maintaining the relationships between keys, controllers, and keyholders, Quantum allows you to instantly determine such things as which controllers a lost key would operate, and which keyholders would be able to operate a specific controller.

In order to maintain accurate records of the access control information programmed into each component of your system, Quantum must keep up-to-date database files. To do this, Quantum forces you to follow a strict sequence for defining and programming access control information:

1. Enter the information into the Quantum database.
2. Program the information into the controller or key.
3. Update the information in the database to reflect and changes to be made to the key or controller programming.
4. Reprogram the controller or key with the new information from the database.

Steps 3 and 4 may be repeated (in sequence) as often as necessary. By requiring that you always update your database before reprogramming your controllers and keys, Quantum will always have an accurate record of what information your system components contain.

Identifying the Components

In order to maintain the proper relationships between the elements of the INTELLIKEY system, each component (key, controller, and keyholder) must be uniquely identified. The easiest method of identifying parts is by each one a meaningful name. Thus, each user has a first and last name, each controller has a building and door name, and so forth.

The concept of meaningful names carries over into all Quantum components. For example, time zones are given names such as "First Shift" or "Office Hours". Groups of users can be identified by department ("Marketing") or title ("Engineers").

User Identification

Users (persons having keys) are identified in the Quantum database by name. Each user has a first and last name ("John" "Smith"), each 25 characters long. A user may have just a first name, or just a last name, but at least one must be specified. The names may consist of letters, numbers, and symbols (!@#$%). Each user may also given an optional identification code, such as an employee number or Social Security number.

Controller Identification

Controllers in your system are identified by a building and door name. This allows you to identify doors by logical names, such as "Research 104B". All reports and data entry screens which refer to your controllers will use these names. You must assign both the building and the door name for each controller. You may use the same building name or the same door name for a number of controllers, but the combination of Building+Door must be unique for each controller. You may have, for example, controllers "Admin 205" and "Admin 206", but you may not have two controllers identified as "Admin 206".

Extra Data Fields

Quantum provides four optional data fields for both users and controllers. These fields are 15 characters long, and may contain information specific to a site. For example, the user fields might contain such things as the user's title, department, or phone number. The controller fields may contain the type of lock or the date of the next battery change. The data in these fields may be used to select specific users and controllers when generating reports. For example, if one of the user's fields is designated as the user's department, you could print a report listing only users from the "Maintenance" department.

Key and Controller Numbers

Quantum assigns each key and each controller in your system a unique number. These key and controller numbers are used to relate the keys and controllers to the users. For example, when a key is issued to a user, the key ID number of the key is stored in the database along with the user's name. Thus, the controller needs only store the key number to identify which user used the door; the Quantum software can match the key number with the user's name. Quantum assigns each user a key number when the user is added to the system. The user retains the same key number until he loses the key, or is deleted from the system. In a similar fashion, Quantum assigns lock numbers as you add controllers to the database.

Other Components

In addition to the physical components (users and controllers) of your INTELLIKEY system, Quantum supports names for other commonly used items. In fact, just about everything you use in setting up your system can be given a meaningful name. For example, you can give time zones names describing the period they cover such as "Office Hours" or "Weekend".

With the exception of user names, all items within a particular category must be unique. This means you can't have two time zones named "First Shift" or two controller default configurations named "Front Doors". This restriction only applies to similar items. It is possible to have a user access group and a controller access group both named "Security Department". The user group would contain a list of users who work in the Security Department; the controller group would contain a list of doors belonging to the Security Department.

Defaults

To simplify the process of data entry when adding users and controllers, Quantum allows you to enter and store common data ahead of time. This data, know as the **default** data, will be added to a new user or controller's database information when the user or controller is first added to the system. For example, if everyone in the Cleaning Department will have the same access rights (e.g. the ability to enter the front door of any building during second shift), you can define a default configuration known as "Cleaning Dept" which contains these settings. When you add a new user, you can specify to Quantum that the person belongs to the Cleaning Department, and the user will automatically be authorized for the front doors.

You can customize the settings for each user after selecting the defaults. For example, the shift supervisor might need access to other doors besides just the front doors. You identify the shift supervisor as belonging to the Cleaning Dept group to give her access to the front doors, then add access to the specific additional doors.

The Quantum User and Controller menus have options for creating and updating default information.

Access Groups

It is sometimes convenient to be able to refer to several users or controllers as a group. For example, when granting access to a user, it is much easier to specify "All doors in the Administration Building", rather than "Administration Building, Front Door", "Administration Building, Conference Room", and so on. **Access Groups** allow you to group users and controllers in logical groupings: "All front doors", "All Security Personnel", etc. A user or controller may belong to any number of groups.

The Quantum User and Controller menus have options for creating and updating access group information.

User Activity Log

Quantum maintains a file of information known as the User Activity Log. This file contains a list of dates and times users have accessed controllers. Information may be added to the log from several sources - reading the audit information from users' keys, reading Controller Audit Keys, and querying controllers directly. Quantum supplies a report option for displaying the information from this file.

Security

Since the information maintained by Quantum is potentially very sensitive, the Quantum software supplies a number of security features.

Operators

Like most secure systems, Quantum requires that each person operating the software be authorized. Quantum allows the establishment of **operators** who are allowed to perform the access control functions necessary to maintain your site.

Each operator may be authorized for specific Quantum operations. This allows you to have, for example, clerks who may enter keyholder and controller information, but not actually issue keys. Quantum's menus automatically adjust for the operator's security rights. If an operator is not allowed to perform a specific function (Issuing a Key, for example) he will not be able to select that function from the Quantum menu

Each operator is assigned an operator identification code and password, which he must supply to Quantum before being allowed to operate the software. This process is known as **logging on**.

The Operator identification code consists of 1-9 characters. These would typically be the user's initials, but any combination of letters, numbers, and symbols is allowed. The operator's password consists of 1-6 characters. This also can be any combination of letters, numbers, and symbols. Operators can easily change their passwords at any time. Chapter 14 describes the procedure for doing this.

Quantum initially creates an operator with the name **System Manager.** The system manager is authorized for all Quantum functions, including adding other operators. The first time you use Quantum, you log on using the System Manager's ID and password (both "1234"). You should now add the appropriate operators for your site, each with his or her own ID and password, and specific authorizations.

Operator Activity Log

The Quantum software maintains an activity log file, or "audit trail" of all significant operator activity. Quantum records the Operator ID, date, and time for each of the following events:

Issue key
Update key
Return key
Delete key
Program controller
Update controller

The System Manager may view or print the contents of the activity log, and may delete the contents when the log file gets too large or out of date.

Operating on a LAN

You may configure Quantum to work on a Local Area Network. This allows you to have two or more operators simultaneously entering data or programming keys from different PC's connected to the LAN.

In this configuration, Quantum performs the functions necessary to guarantee that two operators aren't trying to change the same information. For example, if two operators both try to modify the feature information for a controller, one of them will be informed that the other is already using the information. The second operator will

not be allowed to make any changes to the information until the first operator has finished.

For the most part, using Quantum on a LAN is no different than using it on a single PC. The only differences you will likely see are the occasional conflict when two operators try to modify the same database information, or when printing reports. Quantum will take longer to print reports when running on a LAN, since it must verify that nobody is trying to change each piece of information before it prints it.

There are also certain Quantum functions which may not be performed when more than one operator is logged on the system. These are typically functions which affect several files at one time, and are only available to the Quantum System Manager. These functions include Backup and restore, and purging the Quantum activity log. If you attempt to perform these functions while other operators are active on the system, Quantum will inform you that you cannot do so.

Features

What the INTELLIKEY System Can Do

This chapter describes the operational features and capabilities of your INTELLIKEY controllers and keys. Feature information is stored in special memory devices in the controller and key. The controller reads the feature information from the key's memory and from its own memory and determines whether the key is allowed to operate the controller.

You use your Quantum software to specify the feature information for each component in your system. This information is stored in your Quantum database files. Quantum in turn uses your KPUand Controller Programming Unit to transfer the feature information from your Quantum database files to your controllers and keys. The procedures for specifying feature information and transferring it to your controllers and keys are described in later chapters.

Controlling Access

The fundamental purpose of any access control system is to control who is allowed to enter specific areas. Under Quantum, the person setting up the access control system selects from a list of users and controllers, using a simple "point-and-click" method of selecting which users are authorized for each controller.

Features

Activation and Expiration date

Each key may be programmed with dates to determine the "lifetime" of the key - a time frame during which the key will be allowed to operate. The activation date may be used, for example, to program and issue keys before they are supposed to be used. The keys will not operate until the specified activation date. The expiration date might be used for construction keying, or in a hotel, where it is desirable to have the key cease functioning after a specific date if it is not returned.

Time Zones

Both the controller and key contain Time Zone tables. These tables define 'windows' during which the controller or key is allowed to operate. Each table contains seven windows. A window may cover only a few hours, such as a normal work shift, or may cover several days.

Holidays

Each key may be programmed for up to 16 periods during which it will not operate. These may be holidays or days during which the keyholder's place of employment is closed. Each controller may also be programmed for 16 periods during which features such as Automatic Unlock are disabled.

Controller Configurations

The controller may be programmed to operate with two basic types of lock mechanism. The correct choice is dependent on the INTELLIKEY controller hardware.

Rotating cylinder

In the rotating cylinder configuration, the controller electronics unlocks the cam on the cylinder, allowing the cylinder to be rotated. The cam, in turn, throws a latch or deadbolt mechanism to unlock a door when the key is turned.

A rotating cylinder controller may be programmed to function in two modes:

Single turn - In this mode, the controller unlocks the cylinder long enough to allow it to be turned once. As soon as the key is rotated in the cylinder, the controller releases the locking mechanism. When the key is rotated back to the original insertion position again, the cylinder will be locked, requiring that you remove and reinsert the key to operate the lock again.

Multi-turn - In this mode, the controller holds the cylinder unlocked for a fixed period of time, allowing the key to be rotated more than once in the cylinder. Certain types of locks require more than one turn to be completely unlocked. This mode may also be used when the controller is first installed, since it allows users the opportunity to rotate their key in both directions, assuming they turned the key the wrong way the first time.

Fixed cylinder

In the fixed cylinder configuration, the controller functions as a data reader, reading information from the key, and activating some type of latching mechanism. The key is inserted into the controller, but not turned. This configuration is used with locking devices such as electric strikes and magnetic locks.

A fixed cylinder controller may be programmed to function in two modes:

Relock - In this mode, the controller unlocks itself for a specified period of time, then automatically relocks. This mode would be used for hotel guest rooms, or high security areas which should normally remain locked.

Toggle - In this mode, the controller alternates between the locked and unlocked states each time it is activated by a key.

Daylight Savings Time adjustment

The controller may be programmed to automatically adjust its clock by one hour at the beginning and ending of Daylight Savings Time. The beginning and ending dates and times may be programmed for up to 3 years in advance.

Automatic Unlock/Relock

The controller may be programmed to automatically unlock itself at a specified time, then automatically relock itself at a later time. This feature is useful for the front door of a building to which a large number of people would have access. There are seven programmable windows which, like time zones, may span any length of time during the week. This feature is available only on doors configured for Fixed cylinder operation, and having an external power source.

Audit Trail in Controller

The controller may be programmed to record key accesses, and thus provide an audit trail of keyholders who have used the door. The data to be recorded is selectable, and includes legal accesses, illegal accesses, or both.

Audit Trail in Key

The key may also be programmed to record a list of controllers in which the key has been used. The data to be recorded is selectable, and includes legal accesses, illegal accesses, or both.

Dual-key operation

INTELLIKEY controllers may be programmed for dual-key operation. In this configuration, you must insert two specific keys into the controller within a 15 second period in order to open the controller. This operation is similar to a safety-deposit box which requires both a bank manager's key and the box owner's key.

Anti-Passback

The Anti-Passback feature prevents you from using a key twice in a row in the same door. This feature can be used, for example, in a parking garage. After the keyholder uses his key to open the entrance gate, he must use it to open the exit gate before it will open the entrance gate again. This prevents the keyholder from opening the entrance, then "passing back" the key to someone else to open the entrance illegally.

AREST®

The Automatic Restraint System feature is intended for use in high security areas. Both the controller and key may be programmed to keep track of how many illegal (unauthorized) access attempts it has been involved in. Each unit maintains a separate count. The key tracks how many times it has been inserted into controllers to which it does not have access. The controller tracks how many unauthorized keys have been inserted into it. Each unit also has a programmable limit. When the unit reaches its limit for illegal accesses, the controller will take protective action. This action is also programmable and includes disabling either the key or controller or both. The controller also records the keystamp number, date, and time in its memory,

and the lockstamp number, date and time in the key's memory. These values can be read using the Quantum software. A disabled key must be either updated or reset using the Key Processing Unit before it can be used in a controller. A disabled controller must be reset using a Restricted Authorization Key before it can be operated with a normal key.

Authorizing Keys in Controllers

The most difficult part of maintaining any electronic access control system is updating the authorization information in the various components. As new users are added to the system, the controllers must know which ones are authorized. As controllers are added, the existing users' keys must be updated to operate the new controllers. The INTELLIKEY system provides several authorization techniques which simplify the process of maintaining your access control system:

Grandmaster Keys

"Grandmaster Keys" are keys which are automatically authorized in all controllers. Quantum allows you to specify at installation time how many Grandmaster Keys your system will contain. Grandmaster Keys have a selectable limited lifetime which eventually automatically disables a lost key.

Authorizing Keys at Controller Programming Time

When a new controller is added to the system, its memory can be pre-programmed with a list of authorized users. This allows you to add controllers without having to recall and reprogram keys.

Automatic Key Enable

INTELLIKEY keys may be programmed to automatically authorize themselves in controllers the first time they are used. This eliminates the need to go to each door to manually enable new keys. The keys have a programmable cutoff date after which the automatic enable feature will no longer work.

With the Quantum Software

The Quantum software itself can be used to update the authorization lists in controllers. If Quantum is run on a laptop computer, the computer can be carried door-to-door to perform any necessary updates to the controller programming, and will maintain a log of all changes made.

Disabler Keys

Disabler Keys (described below) provide a simple method of disabling lost or stolen keys.

Special Key Functions

INTELLIKEY keys may be programmed to perform special functions apart from their normal access control functions. All of these functions may be performed by standard INTELLIKEY keys. See "Creating Special Function Keys" for information on programming and using these special purpose keys.

Key	Description
Shutout	When a Shutout key is inserted in a controller, all standard keys are prevented from operating the controller until the Shutout key is inserted again. This function may be used when a room must be temporarily secured. For example, a room containing dangerous materials may be temporarily sealed to all users.
Disabler	A Disabler key may be used to disable a user's key in several controllers. This key is used when someone loses a key with wide access privileges.
Guard Tour	A Guard Tour key records the lockstamp number and date and time of each insertion into a controller. This function can be used to verify that a guard or maintenance person visited each door or station. The Quantum software can read and display the tour information.
Emergency Key	An Emergency key overrides several controller security features, allowing it to operate a controller in an emergency situation. An Emergency key overrides any time-related features, such as time zones and holidays, and other features such as Display/Shutout.
Controller Audit Key	A Controller Audit key reads the audit trail information from a controller and stores it in the key's memory. The Quantum software can read and display the information.
Controller Update Key	A Controller Update key can be used for reprogramming an INTELLIKEY Controller.

Setting Up Your Access Control System

Getting Started

The INTELLIKEY system offers many features and options. It is very important that you understand these features, and carefully plan your access control system before you start using your Quantum software. The more time you spend defining your requirements ahead of time, the less time you'll spend reconfiguring your system later.

If you haven't done so already, read the chapters on "Features" and "Access Control". These chapters describe the features of the INTELLIKEY system. When you are thoroughly comfortable with how the controller and key features interact with each other, you will be ready to start designing your system.

If you are using the Dealer version of Quantum, you will need to perform the following steps for each site you support.

Setting Up Your System

The steps to follow for each are:

1. Design your keying system

   Your main goal is to establish a method for controlling which users will be allowed to open specific doors. Your keying system design should be independent of any other INTELLIKEY features. Features such as time zones add flexibility to a keying system, but you shouldn't count on them to fill holes in a weak keying system. In fact, if your keying system is designed properly, you will frequently find that you don't need to use many of the other features.

2. Determine the programming information for each controller

   Write down the keying and feature information for each INTELLIKEY controller in your system.

3. Determine the programming information for the users

Determine what access and feature information is appropriate for each user.

4. Determine how you want to authorize keys in controllers.

   When first setting up a site, you will be able to enter all of the initial access information before programming any controllers or keys. Thus, at least initially, all keys will carry the proper access information. But the system will expand -- as you add users to the system, their keys will probably need access to existing doors; as you add doors, some existing keys will probably need access to them. Plan to use the automatic enable feature to allow new keys to authorize themselves in existing doors. Program new doors to accept existing keys. This will save a lot of time and effort in recalling keys and reprogramming locks when your access requirements change.

5. Transfer the information to the Quantum database

   The chapters on "Managing Your Controllers" and "Managing Users and Keys" describe the procedures for entering your controller and user information into Quantum. You may enter the information in whatever order is most convenient - controllers first, then users, or vice versa

   Take advantage of the default settings for both controllers and users. The defaults allow you to enter just once feature information that will be common to most controllers or users. This saves time and prevents errors when entering the specific information later.

6. Use the Access reports to verify your masterkeying

   The key and controller access reports help you verify your keying. These reports show to which controllers a user has access, and which users have access to a specific controller. Depending on the number of controllers and users in your system, you will want to either list all combinations, or just a representative sample.

7. Program your controllers

   "Managing Controllers" describes the procedure for programming controllers. You can program your controllers and keys in any order, but it's usually easier to test your system if the controllers are all programmed first.

8. Program (issue) your keys

   "Managing Users and Keys" describes the procedure for issuing keys. If you still have your programmed controllers handy, you can test each key as it is programmed.

Maintaining Your System

Although Quantum is designed to simplify your initial system setup, its primary function is as a key control system. The various Quantum functions allow you to easily issue and return keys, update user and controller information, and track access.

The Quantum database keeps tracks of key possession. Once you have issued a key to a user, you cannot issue a duplicate key until you have accounted for the first one.

When you return a key, Quantum records the fact that the user no longer has the key, and disables the key so that it may not be used until it has been reprogrammed.

Running Quantum

Starting and Leaving Quantum

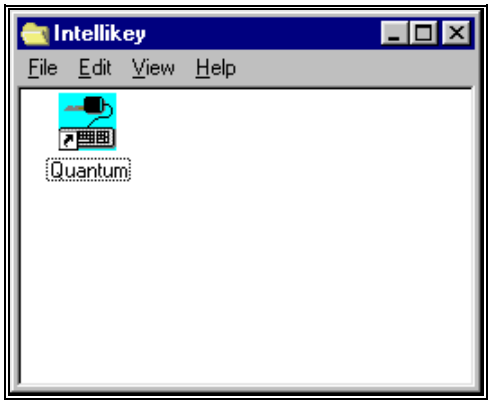
Installing Quantum

Before running Quantum, you must install it on your hard drive or network drive. If you have not done so already, refer to Appendix B for installation instructions.

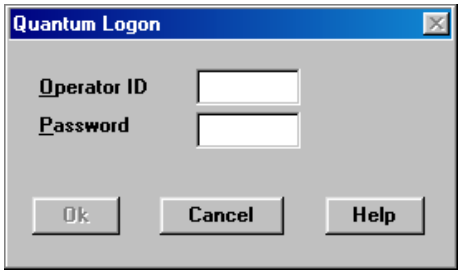
Starting Quantum

Before you may use the Quantum software, you must have a valid Operator Identification code and password. The Quantum System Manager assigns ID codes, passwords, and adds Quantum operators. This person should be the one to provide you with this information.

Start Quantum from the Windows Program Manager or desktop by double-clicking its icon:



Before you use the Quantum software, you must **log on**. Logging on means to enter your Operator ID and password for Quantum to verify. Quantum first presents you with the logon screen:



*When running Quantum for the first time, use **1234** for both the Operator ID and password.*

The cursor should be positioned in the text field following the label Operator ID. If it isn't, press the **TAB** key until it is. Enter your Operator Identification code, then press **TAB**. The cursor next jumps to the field following Password.

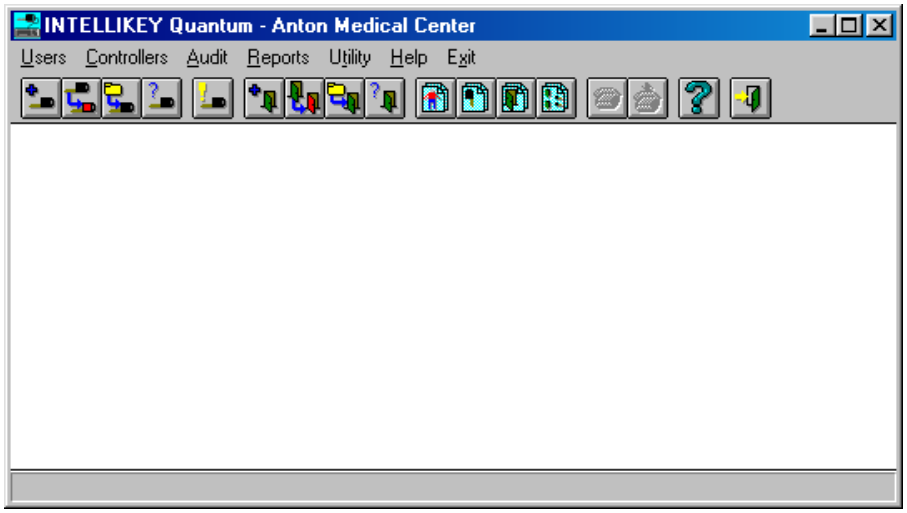
Enter your password exactly as given to you by the System Manager. As you type your password, the characters will appear as "*****". This prevents someone looking over your shoulder from learning your password.

After you have entered your password, press **ENTER** or click on the ***OK*** button. If you have entered your ID and password correctly, the logon box will disappear, leaving you with the Quantum main menu. If you made a mistake, Quantum displays a warning message asking you to reenter your codes.

If you don't want to use Quantum, simply select the ***Cancel*** button from the logon box. You can do this by pressing the **TAB** key until ***Cancel*** is highlighted, then pressing **ENTER**, by selecting the ***Cancel*** button with your mouse, or by pressing the **ESC** key.

The Quantum Main Menu

The Quantum Main Menu bar displays the top level options available to you:



Each of these options is explained in detail in a separate chapter:

Choice	Chapter	Function

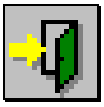
Dealer	The Dealer Version	This menu option appears only if you are using the Quantum Dealer version. It allows you to select a site to work on, add sites, delete sites, and reconfigure programming equipment.
Users	Managing Users and Keys	Add new users; update user information; Issue keys to users; Return, Query, Update, and Delete keys.
Controllers	Managing Controllers	Controller database and programming.
Audit	Audit Operations	Read and report on various audit data.
Reports	Reports	Generate reports for Controller, Key, and User information.
Utility	Utilities	Maintenance functions: add and delete Quantum operators, make changes to the way the Quantum software has been installed on your computer, backup your database files, etc.
Exit	below	Leave the Quantum program or allow another operator to use the system

The Quantum menus are arranged for convenient operation of an established system. The operations which you perform most often are the first choices on the menus. The descriptions given in the following chapters, however, are arranged for the novice Quantum operator. Each chapter describes operations in the order in which they would be used when setting up a new keying system for a site.

The "toolbar" immediately below the main menu provides quick access to the most commonly used Quantum functions. Clicking the mouse on one of the buttons in the toolbar is equivalent to selecting the corresponding operation from the menu. For example, clicking the Add Controller button

is the same as selecting **Controllers** from the main menu, then selecting **Add** from the Controller pop-up menu. Whenever a toolbar button can be used in place of a menu selection, the button will be shown in the left margin of the manual, as shown in the next section.

Leaving Quantum



The Exit menu allows you to tell the Quantum software that you will no longer be using the system. If you select the **Exit** option, the Quantum program will terminate and return to Windows. If you select the **New Operator** option, the logon screen will appear, requiring the next operator to enter a valid ID and password before the system may be used again.

Getting Help

Getting Help for Using Quantum

The **Help | Contents** function activates the Quantum on-line help system. In addition, most data entry screens have a ***Help*** button which may be selected to provide information about the fields on the screen.

Getting Help for Using Help

The **Help | Using Help** function activates the on-line manual for the Windows Help system.

Determining Quantum Version Number

The **Help | About** function displays the version number of your Quantum software.

Data Entry Screens

Standard Data Entry Screens

To simplify the operator interface, Quantum uses the same data entry screens throughout its various functions. For example, the same Time Zone Screen is used whenever viewing or modifying time zone information, whether for the system time zone settings, a user's key or a controller's automatic unlock function. This consistent use of screens makes learning to use the Quantum software much easier, since the operator sees a consistent interface whenever the same type of information is presented.

This chapter presents a description of each data screen, and how it is used. Later chapters describe how and when each screen is used.

Each screen contains an ***Ok***, ***Close, Cancel,*** or ***Help*** button. Selecting the ***Ok*** or ***Close*** button saves any changes you have made to the data in the screen, closes the screen, and returns you to the previous menu or screen. If you select the ***Cancel*** button (or press the ESC key), Quantum will close the screen but will not keep any changes you have made to the screen data. The ***Help*** button will take you to the on-line Quantum Operator's Guide.

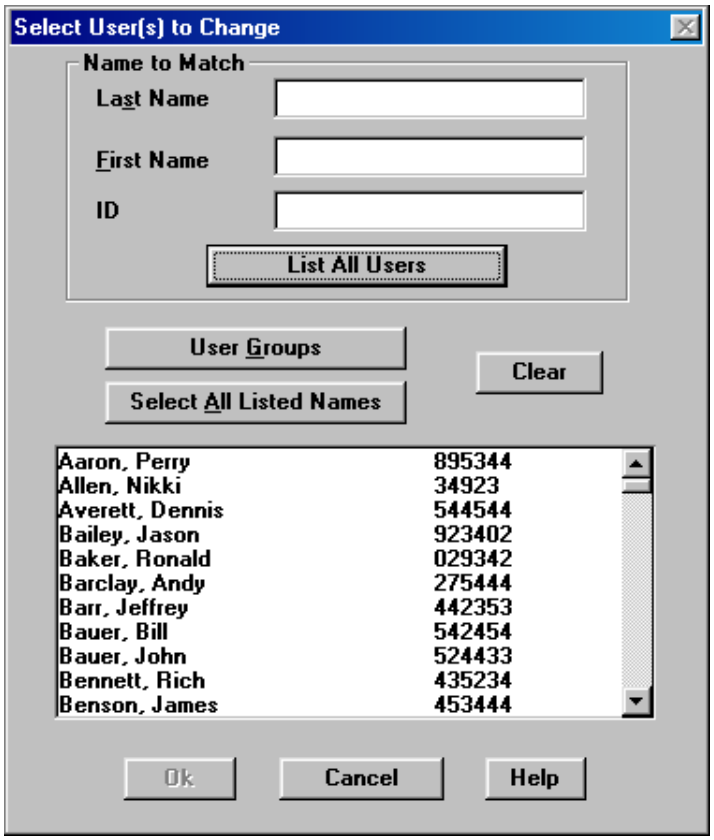
Some of the features and functions shown on the screens are simply on or off - the feature is active or it isn't. Some features are simply numeric values. And some features are a combination of the two -- when the feature is turned on, it requires additional data.

The screens allow you to set all of the types of parameters. For example, features which may be turned off and on are shown with a checkbox beside them. If the box is checked, the feature is turned on, otherwise it is turned off. If a feature has numeric or text data associated with it, the data is shown next to the description of the feature, and may be modified. If the feature is turned off, Quantum will retain the data setting, but will not use it.

User/Key Screens

Selecting Users

Many user and key operations require that you select one or more users to perform the operation on. Quantum uses a standard screen for selecting users:



The title bar at the top of the screen indicates what the users are to be selected for - changing, issuing keys, etc. The top section of the screen contains text fields for entering user names, and a selection button initially labeled ***List all Users***. The lower section of the screen contains a list box which will contain the names of selected users. Selecting a user or users for a particular operation involves getting their names listed in the list box, selecting them from the list, and pressing ***OK***.

To list all of the users in your system, select ***List All Users***. Quantum will fill the list box with the names of all users appropriate for the current function. This can take awhile if you have a large system.

To pick users from a defined access group, select the ***User Groups*** button. When you select one or more groups, Quantum adds the names from those groups to the listbox. Note that only names which fit the current function (keys to be issued, etc.) are selected from the groups.

The text fields at the top allow you to specify a particular user, or group of users. You can enter the full name (first and last) or a partial name (just the first, or just the last). As you start entering data in either field, the label on the button changes from ***List all Users*** to ***List Matching Names***. After entering the user's name, select ***List Matching Names***. Quantum will fill the list box with the names of users matching the information you have supplied. Quantum will match partial names and similar spellings, also. For example, if you enter "Smith" for the last name, Quantum will also be able to find names with the spelling "Smith".

When the list is complete, select the specific user or users you want to work on by highlighting them in the list or choose the entire list by selecting ***Select All Listed Names***. When you have the appropriate users highlighted, select ***OK***. Quantum will perform the indicated operation on each selected user in turn.

If you want to work on a single user, and know the exact spelling of his or her name, you can enter the full name, then select ***OK*** without listing matching names. If Quantum cannot find the name you entered, it will provide a list of similar names for you to select from.

To return to the main menu without performing any operation, select ***Cancel***.

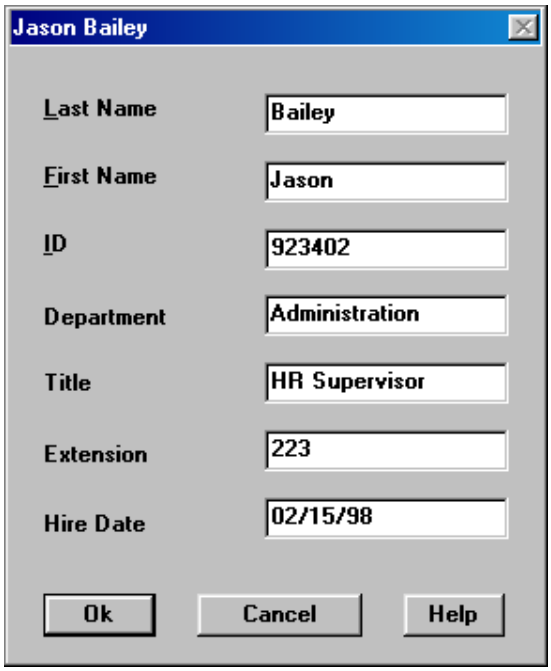
User/Key Main Screen

All User and Key data entry operations begin from the User/Key Main Screen:

Depending on the user or key function you are currently performing, some of the choices may be disabled. As you select each button, Quantum activates a secondary screen to allow you to enter the appropriate data for the selected features or functions:

Button	Function
User Description	Change descriptive information about the user. See "User/Key Description Screen"
Group Name	Change the name of a user default group. See "User/Key Defaults Name Screen"
User Features	Change feature settings for the user. See "User/Key Features Screen"
User Access	Change user's access rights. See "User/Key Access Screen - Horizontal System " and "User/Key Access Screen - Vertical System"
User Groups	Select which access groups this user is a member of. See "User Access Groups Screen"
Audit Key	During the Query Key function, this button allows you to read and display audit information from the key. This button will be disabled if the user's key is not programmed for the audit function.

User/Key Description Screen



This screen allows you to change the descriptive information about the key user.

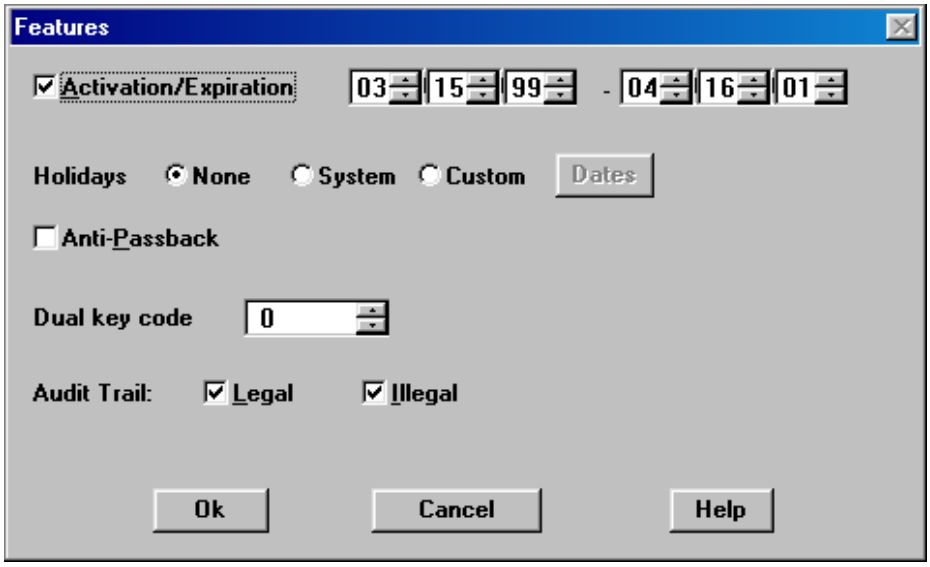
Field	Function
Last Name	The user's last name
First Name	The user's first name
ID	The user's identification code. This code will be site dependent.
Field 1 **Field 2** **Field 3** **Field 4**	The actual names displayed for these fields will depend on your site setup. The data in fields 1 through 4 may be used to sort user entries when creating reports. For example, if Field 1 is used to list the user's department, you can create a report for all users in a specific department.

User/Key Defaults Name Screen

The Group Name Screen allows you to change the name of a user default configuration. Simply type in the new name for the group. Note that the name must be unique - you can't give a group a new name which matches the name of another existing group.

User/Key Features Screen

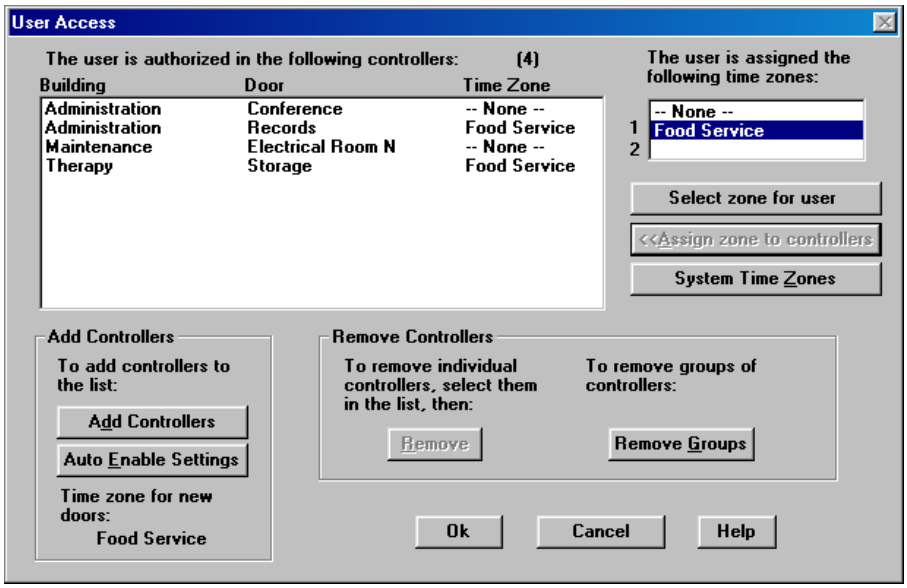
The Features Screen controls many of the basic key features.



Field	Function
Activation/Expiration	Enables Activation date and Expiration Date features. If this feature is turned on, you must also enter the date range during which the key will be active. Note that the Expiration date is the first date for which the key will not work. For example, if you enter the date range as March 1, 1995 through June 1, 1995, the key will actually work from 12:00 AM on March 1 to 12:00 AM on June 1.
Holidays	Enables the Holidays feature. If you select the ***Dates*** button associated with Holidays, Quantum presents the Holiday Screen to allow you to change the holidays for this key.
non-standard dates	If checked, indicates that the holidays for this key do not match the standard dates set for the site. When this key is updated, the dates will not automatically be set to the latest system dates.
Anti-passback	Enables the Anti-Passback feature. When this feature is enabled, and the key is inserted in a controller which also has Anti-Passback enabled, the key must then be inserted in a different controller before it will be allowed to operate the first controller again.
Dual key code	Identifies the key as one of two which must be inserted into a controller programmed for Dual-key mode. This value will have no effect when the key is inserted in other controllers
Audit Trail	Enables the audit trail function for the key. When this key is inserted in a controller which supports the key audit function, the controller will record its identification number and the date and time in the key's memory. You may elect to record just **Legal** insertions, just **Illegal** insertions, or both.

User/Key Access Screen

The User Access screen allows you to specify which doors (controllers) the user is authorized for, and the time zones associated with them.



The main list box shows the doors for which the user is authorized, and the time zone associated with each door. If the phrase -- *None* -- appears in the Time Zone column, the user may access the door at any time. If the name of a system time zone appears in the column, the user may only access that door during the hours specified by the time zone. The smaller list box in the upper right hand corner lists the time zones assigned to the user. In the Horizontal system, a user may have 2 time zones assigned. Each controller may be restricted to the times specified in one of the 2 time zones, or have no time restrictions at all.

You may add and remove controllers and time zones as much as you like. The list that appears in the main list box when you select ***Ok*** is what will be assigned to the user.

Authorizing a User in a Door

Authorizing a user in a door involves specifying a door, and, optionally, a time zone for the door. If you want the user restricted by time, select the appropriate time zone from the user's list. If the desired time zone is not in the list, insert it into the list first, as described below in "Assigning a Time Zone to a User". If you want the user to be able to access the door at any time, select --*None*-- in the user's time zone list.

Next, select the door or doors for the user. Select ***Add Controllers*** to add individual controllers or groups of controllers. As a shortcut, you may also select a controller group whose contents nearly match the user's requirements, then add and remove individual doors from the list.

In either case, the selected controllers will now appear in the user's list box, along with the selected time zone. You may repeat this procedure as many times as necessary, optionally changing the time zone with each new controller selection, to define the user's access information.

Denying a User Access to a Door

To remove one or more doors from the user's list, simply select the appropriate doors (by either single-clicking on the controller name, or by tabbing to the controller name and pressing the space bar), then select the ***Remove*** button. You can remove any number of controllers from the list in one step. To remove all controllers belonging to one or more of your controller access groups, select ***Remove Groups***, and specify the group or groups whose member controllers you want to remove from the user's authorized list.

Assigning a Time Zone to a User

A time zone must be defined before it can be assigned to a user. If you want to assign a new time zone (a short work week, for example), select the ***System Time Zones*** button. This will bring up a menu which allows you to create or modify the Quantum time zone definitions. See "Adding a Time Zone" for details on creating new time zones.

To change one of the time zone assignments for the user, select one of the numbered slots in the time zone list box. Next, select the ***Select zone for user*** button under the list box. Quantum will display a list of the defined time zones for you to choose from. Select the appropriate time zone from the list. It will be inserted into the user's time zone list.

Similarly, you can remove a time zone from the user's list by selecting one of the numbered slots, selecting ***Select zone for user***, then selecting --*None*-- from the list of time zones.

Changing Time Zones for Doors

To change or remove the time zone associated with one or more doors in the user's list, first select the appropriate doors by either single-clicking on the controller name, or by tabbing to the controller name and pressing the space bar. Next, select the new time zone by either double-clicking on the time zone name in the user's time zone list, or by highlighting the time zone name in the user's list and selecting the ***Assign zone to controllers*** button. The new time zone name will appear next to each of the selected controllers in the *Time Zone* column in the main list box.

To authorize the user to access the door at any time, select the doors as described above, then select --*None*-- from the user's time zone list.

Setting the Automatic Enable Period

INTELLIKEY keys can be programmed to automatically enable themselves the first time they are used in a controller. This allows you to add new users (and their keys) to the system without having to update the controllers to which the new keys should have access. As a security precaution, this automatic enabling feature is limited to a short period of time. You can specify the automatic enable period in one of two ways - by a specific date, or by a number of days (up to 90) after the key is issued.

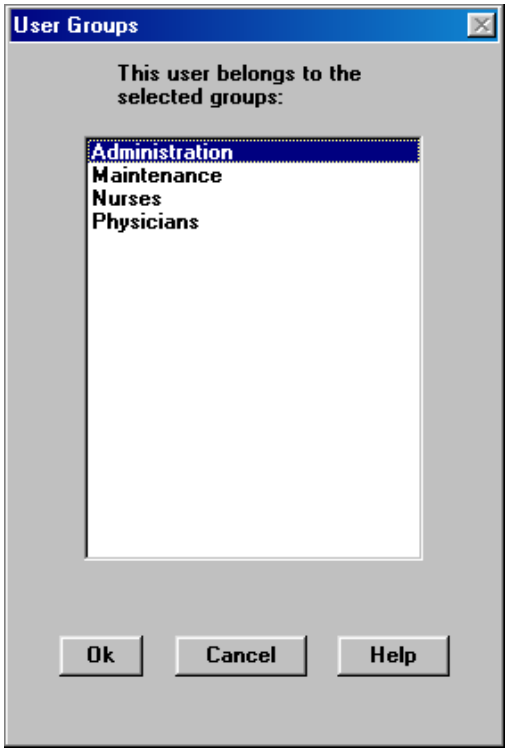
Specifying a number of days is the normal method. Typically you would issue a key to a new user and tell them that they have 7 days (or whatever number you select) in which to use the key in all of the doors to which they have access. You might use the specific date method if you are creating several keys which will be issued to the users, but which shouldn't be active immediately. For example, a university might pre-issue the keys for the fall students during the summer, when things are slower. The keys could be set with an activation date of September 1, and an automatic authorization cutoff date of September 7. With these settings, the keys could be

mailed to the students ahead of time, but wouldn't start working until the 1st of September.

Select ***Auto Enable Settings*** to adjust the automatic enable period for the user:

Select the radio button by the date control and enter a specific date, or select the radio button by the number control and select a specific number of days after the key is issued.

User Access Groups Screen



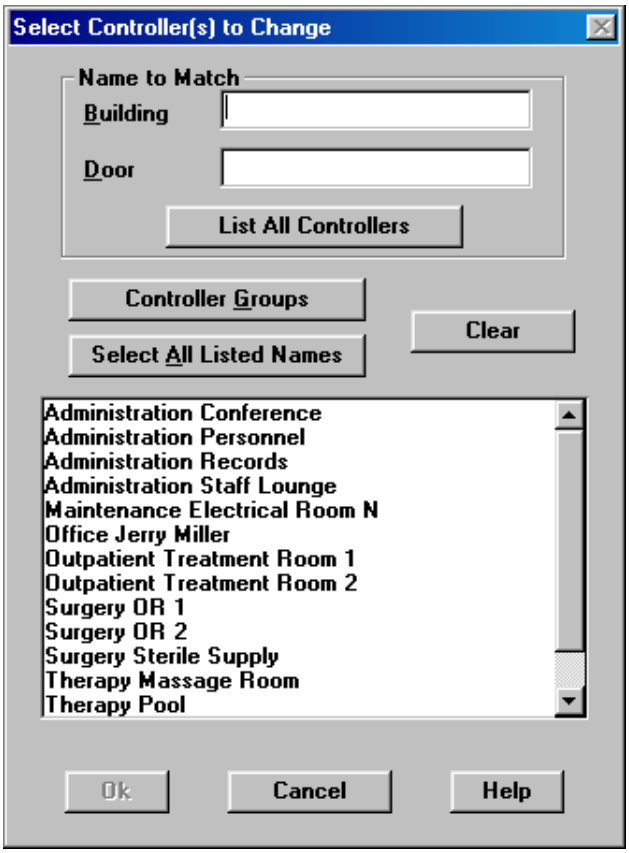
This screen allows you to select to which User Groups the user belongs. The list box contains the names of all user groups defined for the site. If the user is a member

of a group, the group name appears highlighted. Each time you select a group name - by clicking on it with the mouse, or tabbing to it and pressing the space bar - the status changes between the user belonging to the group and not belonging.

Controller Screens

Selecting Controllers

Many controller operations require that you select one or more controllers to perform the operation on. Quantum uses a standard screen for selecting controllers:



The title bar at the top of the screen indicates what the controllers are to be selected for - changing, programming, etc. Quantum will only display controllers which fit the category. For example, if you select the Program Controllers functions, Quantum will only display controllers which are not already programmed.

The top section of the screen contains text fields for entering building and door names, and a selection button initially labeled ***List all Controllers***. The lower section of the screen contains a list box which will contain the names of selected controllers. Selecting a controller or controllers for a particular operation involves

getting their names listed in the list box, selecting them from the list, and pressing ***OK***.

To list all of the controllers in your system, select ***List All Controllers***. Quantum will fill the list box with the names of the controllers appropriate for the operation to be performed. This can take awhile if you have a large system.

When the list is complete, select the specific controller or controllers you want to work on by highlighting them in the list, or choose the entire list by selecting ***Select All Listed Names***. When you have the appropriate controllers highlighted, select OK. Quantum will perform the indicated operation on each selected controller in turn.

To pick controllers from a defined access group, select the ***Controller Groups*** button. When you select one or more groups, Quantum adds the names from those groups to the listbox. Note that only names which fit the current function (controllers to be programmed etc.) are selected from the groups.

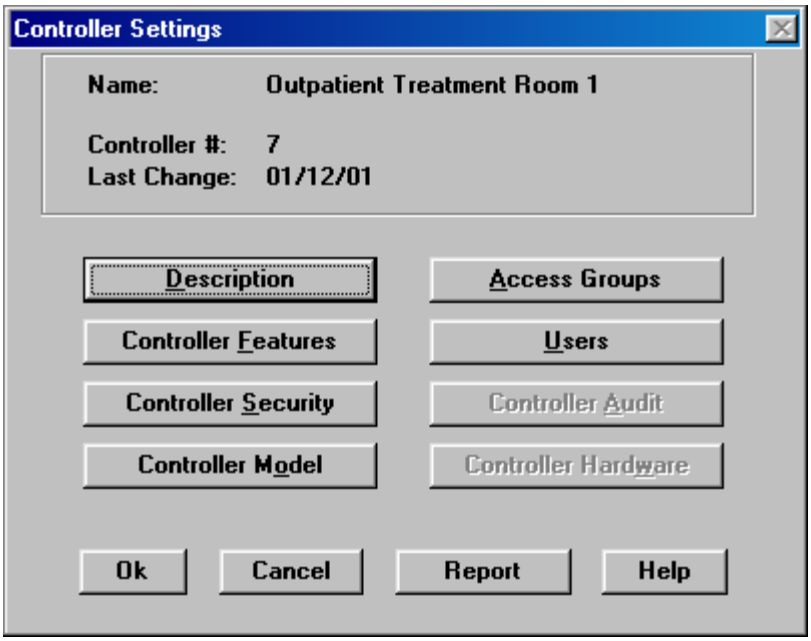
The text fields at the top allow you to specify a particular controller, or group of controllers. You can enter the full name (building and door) or a partial name (just the building, or just the door). As you start entering data in either field, the label on the button changes from ***List all Controllers*** to ***List Matching Controllers***. After entering the building and door information for the controller, select ***List Matching Controllers***. Quantum will fill the list box with the names of controllers matching the information you have supplied. Quantum will also match partial names. For example, you may abbreviate "Administration" as "Admin". When the list is complete, select the specific controller or controllers you want to work on by highlighting them in the list or choose the entire list by selecting ***Select All Listed Names***. When you have the appropriate controllers highlighted, select ***OK***. Quantum will perform the indicated operation on each selected controller in turn.

If you want to work on a single controller, and know the exact spelling of its name, you can enter the building and door information, then select ***OK*** without listing matching names. If Quantum cannot find the name you entered, it will provide a list of similar names for you to select from.

To return to the main menu without performing any operation, select ***Cancel***.

Controller Main Screen

All Controller data entry operations begin from the Controller Main Screen:

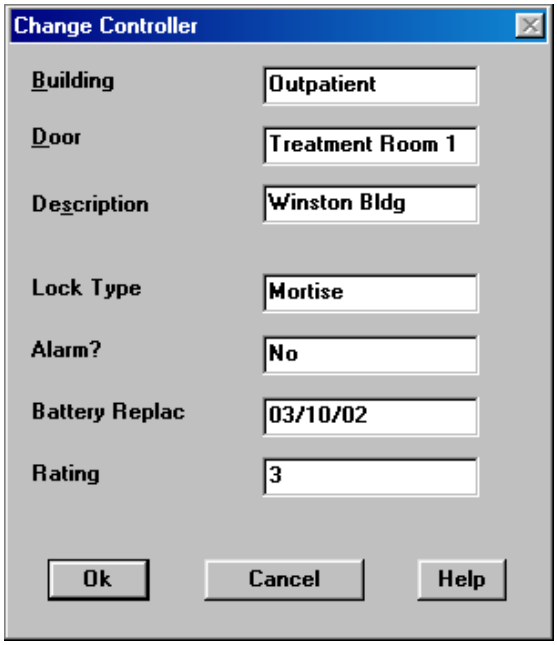


Depending on the controller function you are currently performing, some of the choices may be disabled. As you select each button, Quantum activates a secondary screen to allow you to enter the appropriate data for the selected features or functions.

Button	Function
Description	Change lock name, description, etc. See “Controller Description Screen”
Group Name	Change name of controller default configuration. See “Controller Defaults Name Screen”
Controller Features	Configure basic settings for controller. See “Controller Features Screen”
Controller Security	Configure security settings for controller. See "Controller Security Screen”
Controller Model	Configure controller hardware. “See Controller Model Screen"
Event Reporting	Allows for the enabling of certain events to be reported to the central computer. This function is only enabled if the on-line box has been checked, and it has been disabled if the off-line box has been checked.
Users	Identify users who are authorized to access the controller (Horizontal System). See “Controller Users Screen"
Keying	Set keying information for controller (Vertical System). See “Controller Keying Screen"
Copy Numbers	Select enabled copy numbers (Vertical System). See “Controller Copy Numbers Screen"
Access Groups	Select which controller groups of which this controller is a member. See “Controller Access Groups Screen"
Controller Audit	Read audit trail information while querying controller. See "Querying a Controller"
Controller Hardware	Read and set time, read audit information, etc., while querying controller. See "Querying a Controller"
Remote Site	If the online controller is located at a site other than the current location, this function allows you to specify the remote site.

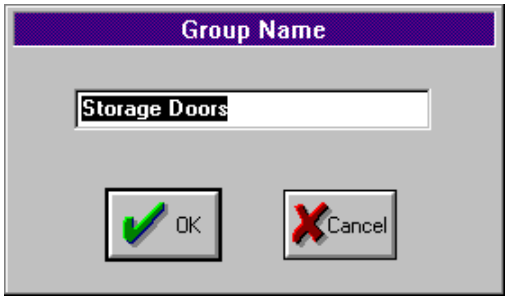
Controller Description Screen

The Description screen allows you to enter descriptive information for the controller:



Field	Purpose
Building	The building in which the controller is located (required)
Door	The door number or identifier (required)
Description	Description of door (optional)
Field 1 **Field 2** **Field 3** **Field 4**	Field 1 through Field are site-dependent. The names of the fields may be changed from the Site Setup Screen. The data in these fields may be used to sort entries when creating reports. For example, if Field 2 is used to list the type of lock hardware, you can create a report for all controllers on doors with deadbolts.

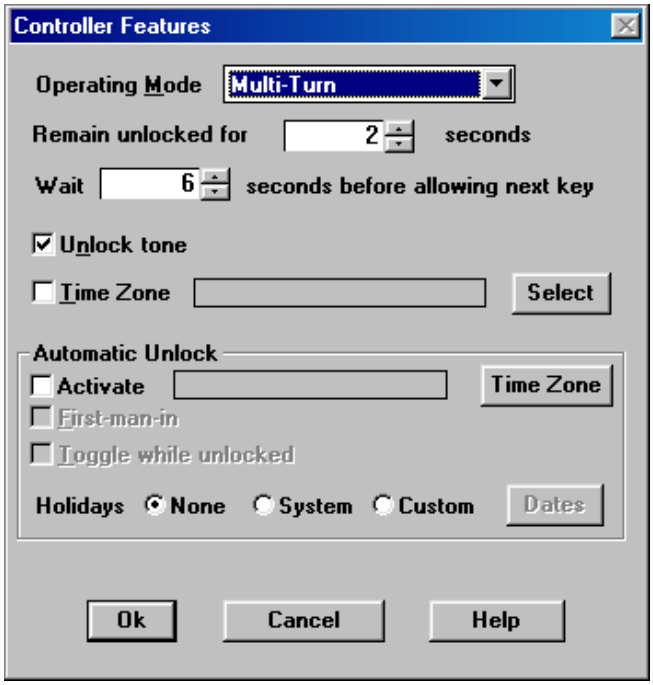
Controller Defaults Name Screen



The Group Name Screen allows you to change the name of a controller default configuration. Simply type in the new name for the group. Note that the name must be unique - you can not assign a new name to a group which matches the name of an existing group.

Controller Features Screen

The Features screen controls the settings for many of the controller's basic features:

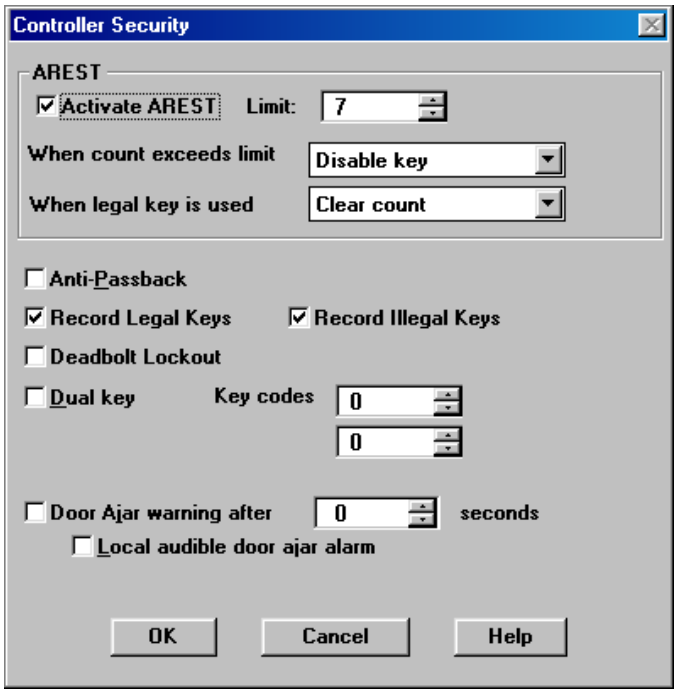


Field	Function
Operating mode	Specifies the unlocking sequence to be used by the controller: **Multi-turn**: Leaves rotating cylinder controller unlocked for the time specified in *Remain unlocked for...* field. This is the standard rotating cylinder mode, but is only available on Model 4 controllers. **Single turn**: Unlocks rotating cylinder, then relocks it as soon as key is turned. Requires that key be removed and reinserted before controller will unlock again. **Toggle**: Fixed cylinder controller alternates between locked and unlocked each time a key is inserted. **Relock:** Fixed cylinder controller remains unlocked for period specified in *Remain unlocked for ...* field, then relocks.
Remain unlocked for ... seconds	The number of seconds the door will remain unlocked while in Relock and Rotating Cylinder modes.
Wait ... seconds before allowing next key	Indicates number of seconds controller ignores keys between insertions. For rotating cylinders, this gives the user a chance to turn the key to unlock the door, then return the key to the insertion position for removal, without the controller treating this as a second insertion.
Unlock tone	Enables the single 'beep' to indicate when the controller is unlocked. All other warning beeps are always enabled.
Time Zone	Enables the Time Zone feature for the controller. When this function is enabled, users are only authorized in the controller during the specified time zone period. Select the ***Select*** button to change the time zone.

Automatic Unlock	Enables the Automatic unlock/lock feature. Select the ***Time Zone*** button associated with the Auto Unlock feature to change the lock/unlock times. Note that if you enable this function, Quantum will automatically configure the **Operating mode** as *Toggle*, to cause the controller to operate correctly. This change will not be visible until you leave the Controller Features Screen, then reselect it.
Time Zone	Select the time zone that defines the times during which the controller will automatically be unlocked.
First-man-in	Activates the First-man-in function. When this option is enabled, a legal user must have accessed the controller before it will automatically unlock on any given day.
Toggle while unlocked	For Model 4 controllers, the Automatic Unlock function may work two different ways. If *Toggle while unlocked* is enabled, each legal key insertion will toggle the controller between locked and unlocked. If *Toggle while unlocked* is not enabled, the controller will ignore key insertions while unlocked, and remain unlocked. **Note: There is no way to lock a controller during its Automatic Unlock period if this function is not enabled.**
Holidays	Selects dates for which the controller's automatic unlock function will not work. Select *None* if the automatic unlock function is always active; select *System* if the standard holidays entered under Utility -> Dates -> Holidays should be used; select *Custom* and the **Dates** button to enter dates that apply only to this controller.

Controller Security Screen

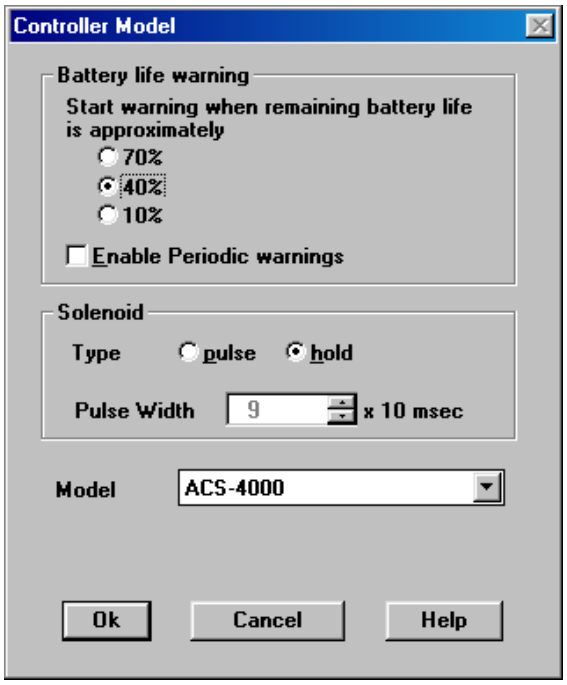
The Security dialog box controls the settings for controller features related to higher security functions:



Field	Function
Activate AREST	Enables the AREST function for the controller. If this feature is enabled, you must set the Limit to a value between 1 and 15.
Limit	Maximum number of illegal key insertions allowed. When the controller records this number of illegal insertions, it takes the action specified under *When count exceeds limit*.
Current	This field appears only when querying the controller, and shows the number of unauthorized key insertions the controller has recorded.
When count exceeds limit	Specifies what action the controller is to take when either the key's or controller's Illegal limit is reached; AREST must be enabled in the controller before the controller will take this action.
When legal key is used	Specifies how the controller is to update its illegal insertion count when an authorized key is inserted.
Anti-Passback	Activates the Anti-Passback function in the controller.
Record Legal/Illegal keys	Determines what audit trail information is recorded by the controller: ***Legal*** and/or ***Illegal*** key accesses.
Deadbolt Lockout	The Deadbolt lockout feature allows the controller to exclude any key except an Emergency key when the deadbolt is thrown. This feature requires a deadbolt sensing switch connected to the controller electronics.
Dual key	Enables Dual-key operation, and specifies which two keys must be inserted to operate the controller; the 1st and 2nd key values may be entered even if Dual-key operation is not enabled
Door Ajar Warning	Enables the warning generated when a door is left ajar (open). This feature requires a door position sensing switch connected to the controller electronics. The numeric field specifies the number of seconds the door can remain open before a warning is generated.
Local audible door ajar alarm	When a controller is connected in an on-line configuration, it might be desirable to have the controller send a warning to the central computer without having the local warning sound when a door is ajar. If this box is not checked, the controller will not generate an audible door ajar alarm.

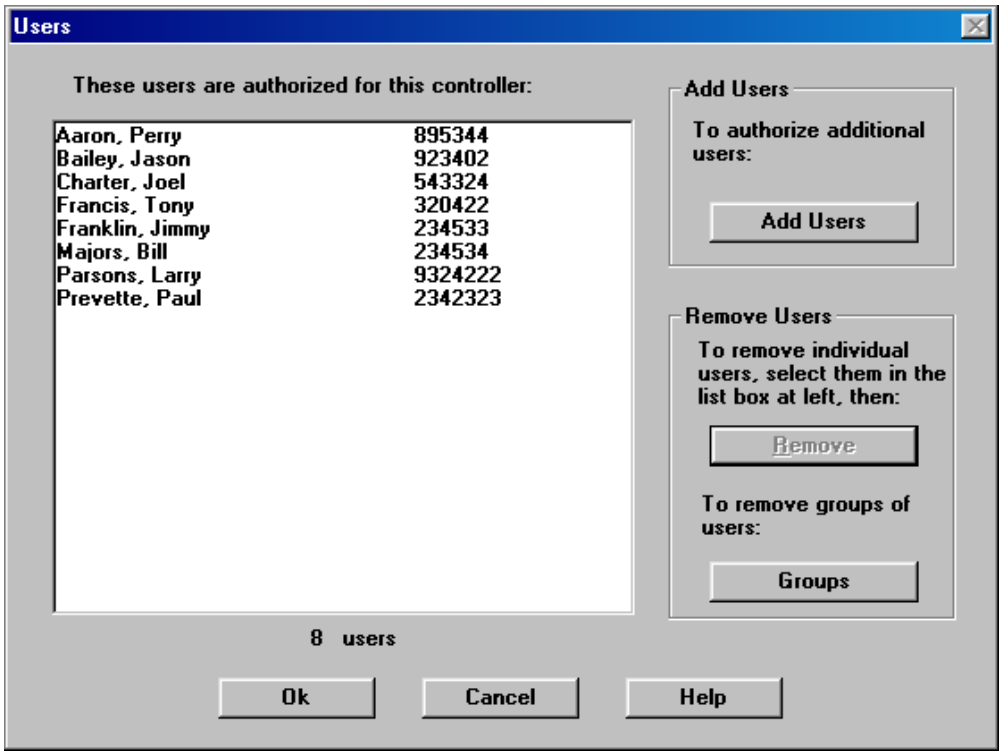
Controller Model Screen

The Controller Model screen allows you to specify settings which are dependent on the electronic hardware in the controller This information should be only be modified by someone very familiar with the controller system. In fact, selecting invalid configurations can result in incorrect controller operation. This option is provided mainly to provide a method for configuring new controller models which might become available between releases of the Quantum software. Contact INTELLIKEY for information on changing any settings other than Memory Size.



Button	Function
Start warning when ...	Indicates how early to start warning of low battery level. The actual values will vary, depending on usage and temperature, but the settings correspond roughly to the following : 70%: 2-3 months 40%: 1 month 10%: 2 weeks
Enable Periodic warnings	If this box is checked, the controller will beep periodically when the battery level has dropped to the 10% level (similar to a smoke detector).
Solenoid	Indicates what type of locking hardware the controller is connected to. Quantum sets these values automatically based on the lock operating mode. You should not change these values unless instructed to do so by INTELLIKEY personnel.
Model	Quantum normally prompts you to identify the controller model when adding a controller (unless you have specified that you have only one type of controller -- see Site Setup Screen. Quantum verifies the controller model when it programs the controller. This function allows you to change the controller model if you change the hardware later.

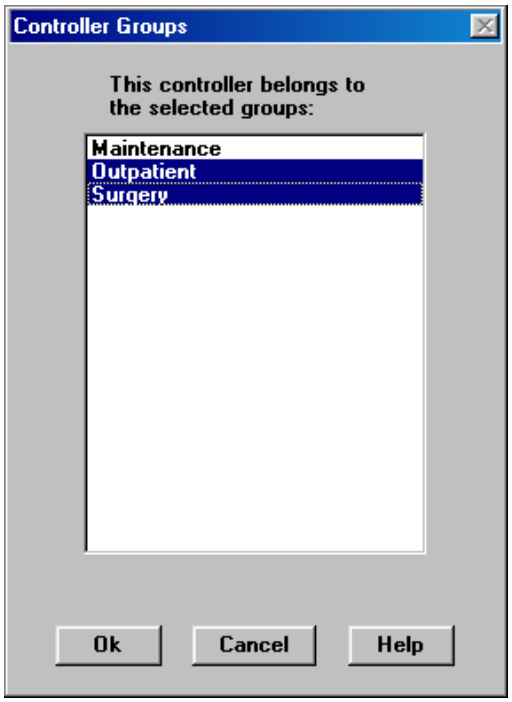
Controller Users Screen



This screen allows you to select which users will be authorized for the controller. The list box contains the names of all users authorized to operate the controller. To authorize additional users, select ***Add Users***. Quantum will prompt you to select users to add the controller's list. You may add individual users, or entire user access groups. To remove individual users from the controller, select their names in the list box, then select ***Remove***. To remove entire access groups, select ***Groups***, then specify the user access group(s) whose members are to be removed.

Controller Access Groups Screen

This screen allows you to select to which Controller Groups the controller belongs. The list box contains the names of all Controller groups defined for the site. If the controller is a member of a group, the group name appears highlighted. Each time you select a group name - by clicking on it with the mouse, or tabbing to it and pressing the space bar - the status changes between the controller belonging to the group and not belonging.

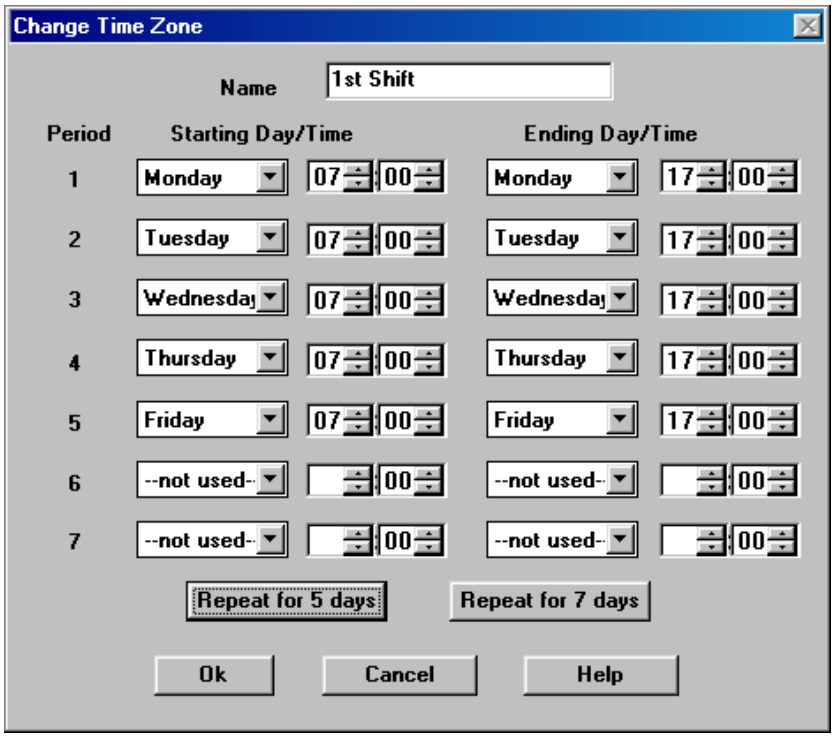


Date and Time Screens

Time Zone Screen

The Time Zone Screen lets you create or modify a time zone definition. Quantum defines a time zone as a group of 7 periods, each specified by a starting day and time and an ending day and time. The Time Zone screen displays these 7 periods, with list boxes for selecting the starting and ending days, and time controls for selecting the starting and ending times. Note that the times are displayed in 24-hour format, where 1:00 pm is 13:00 and 11:45 pm is 23:45.

As an example, consider a time zone named "First Shift" which covers Monday through Friday, 8:00 am to 5:00 pm (17:00). The screen for this time zone would look like this:

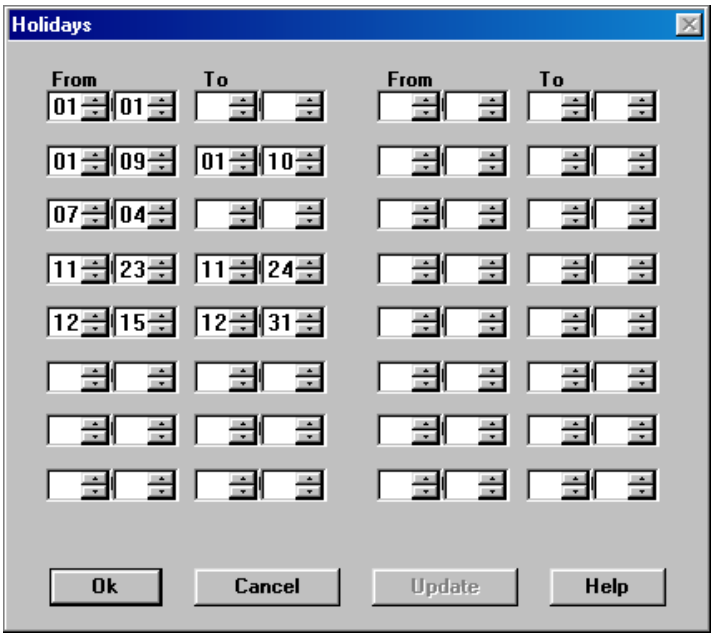


Note that this time zone uses only 5 of the available 7 periods, the remaining two are marked as *-not used-*. You can adjust the days or times for any of the 7 periods by changing the data in the appropriate controls. The time zone screen will automatically sort the periods into chronological order as you make the changes.

If the periods in your time zone fit into a pattern, such as the same starting and ending times over a period of days, you can simplify your data entry by using the ***Repeat for 5 days*** or ***Repeat for 7 days*** buttons. Enter the data for the first period on the top line (Monday 8:00 until Monday 17:00, in the case of "First Shift"), then select the appropriate ***Repeat*** button. Quantum will fill in the rest of the time zone information for you.

Holiday Screen

The Holiday Screen lets you configure the holiday settings for keys and controllers. The controllers and keys recognize up to 16 holiday periods, each up to 120 days long. Holidays in keys can be used to specify dates during which the key will not be allowed access to controllers. Holidays in controllers specify dates during which the automatic unlock function will not operate.



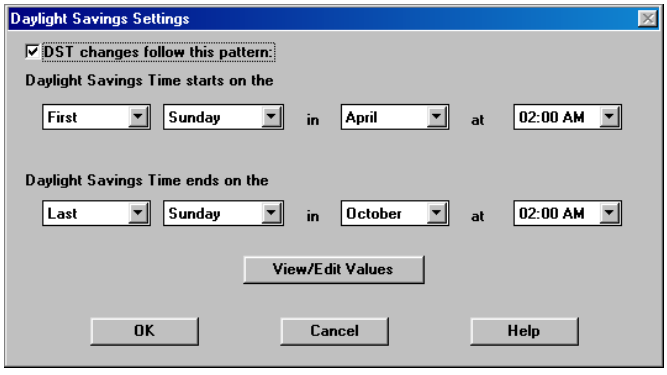
The screen shows 16 date ranges, each specified by a starting and an ending date. The dates are shown in either MM/DD or DD/MM format, depending on which date format you have chosen for you site.

Fill in the appropriate dates for each range. For single dates, you only need to set the starting date. Don't worry about putting the dates in order, Quantum will sort them chronologically when you select ***Ok.*** The ***Update*** button copies the current system-wide dates into a user or controller data record.

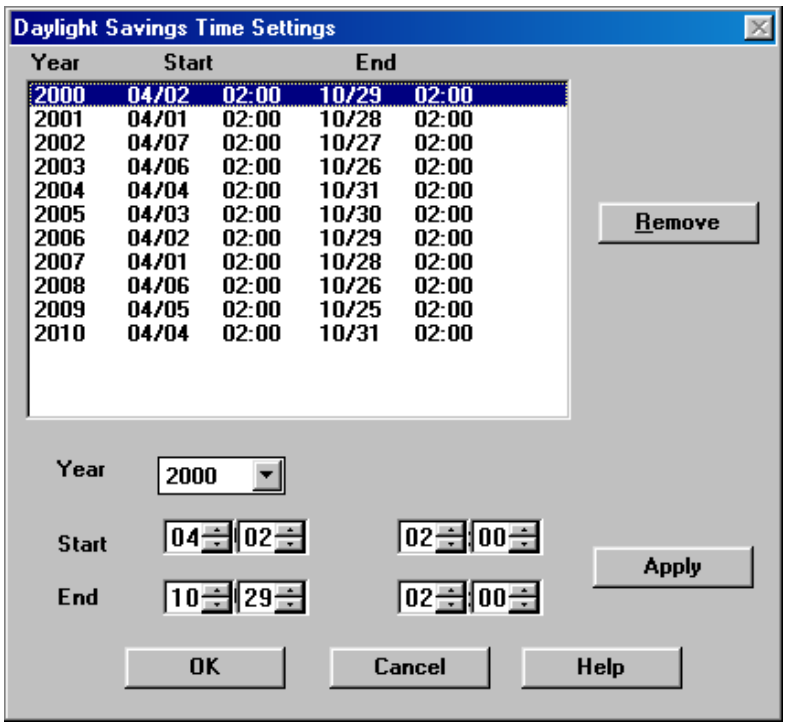
Note that a holiday range may not exceed December 31. If you need a holiday range which extends from, say, December 20 to January 2, you must create two holiday ranges, one from December 20 to December 31, and the other from January 1 to January 2.

Daylight Savings Time Screen

The Daylight Savings Time Screen lets you specify the Spring and Fall adjustment dates and times for Daylight Savings Time:



The dates are shown in the date format you have selected for your site.


Daylight Savings Time Settings
Year Start End
2000 04/02 02:00 10/29 02:00
2001 04/01 02:00 10/28 02:00
2002 04/07 02:00 10/27 02:00
2003 04/06 02:00 10/26 02:00
2004 04/04 02:00 10/31 02:00
2005 04/03 02:00 10/30 02:00
2006 04/02 02:00 10/29 02:00
2007 04/01 02:00 10/28 02:00
2008 04/06 02:00 10/26 02:00
2009 04/05 02:00 10/25 02:00
2010 04/04 02:00 10/31 02:00
Remove
Year
2000
Start
04 02 02 00
End
10 29 02 00
Apply
OK
Cancel
Help

Managing Controllers

Controller Names

Controllers in your system are identified by a Building name and a Door name. This allows you to identify doors by logical names, such as "Research 104B". All reports and data entry screens which refer to your controllers will use these names. You must assign both the building and door names for each controller

You may use the same building name or the same door name for a number of controllers, but the combination of Building+Door code must be unique for each controller. You may have, for example, controllers "Admin 205" and "Admin 206" or "Admin Front" and "Research Front", but you may not have two controllers identified as "Admin 206". If you try to enter a duplicate controller, Quantum will display an error message and ask you to enter new values.

Another thing to keep in mind is that Quantum always treats the information in the Building and Door fields as characters, even if they contain numbers. This can cause some unexpected results when you look at an alphabetized listing of your controllers. For example, if you enter ten controllers, all in the "Admin" building, with door numbers of "1", "2", "3", "4", "5", "6", "7", "8", "9", and "10", Quantum will display them alphabetically as

Admin 1
Admin 10
Admin 2
Admin 3
Admin 4
Admin 5
Admin 6
Admin 7
Admin 8
Admin 9

This happens because Quantum (like most computer programs) alphabetizes the information based on the first character it sees in a description. Thus, the "1" in "10" causes the "10" to appear before "2" or "3", instead of after the "9", as you would expect. If you had doors 11 - 19, they would appear alphabetically between "10" and "2". Similarly, doors 21 - 29 would appear between "2" and "3".

It's very simple to keep your listings in the correct order. All you have to do is put enough characters in front of the digits to make all of your number descriptions the same length. For example, if you know that your largest door number will be 100, you should make sure that all descriptions contain 3 characters. You could enter door number 1 as either " 1" (two blanks, followed by a 1) or "001". If you enter

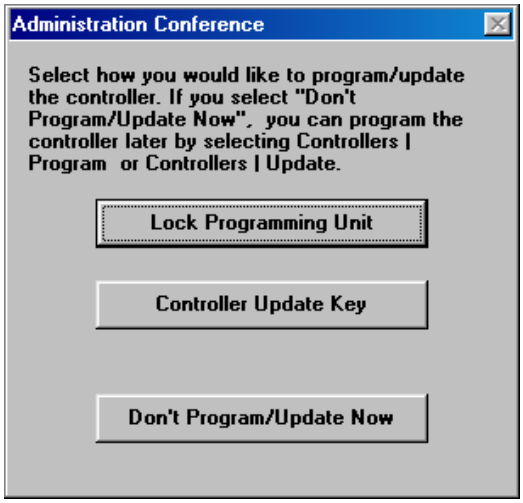
any numeric building or door descriptions in this manner, they will always appear in the correct order in any Quantum reports.

Communicating With The Controller

Communication with the controller is necessary when programming and updating feature information. Communication will also allow you to interrogate the controller for audit information. There are several methods of communication with a controller. The method of communication that is utilized is determined by whether your site has been setup as a standalone system or a network system, as well as what controller model the site has been equipped with.

Selecting Communication Methods

In order to communicate with a controller, the appropriate method of communication must first be selected from the Program/Update dialogue box that is shown below.



Quantum will only allow you to select that method(s) of communication that is compatible to the controller you've selected i.e., ***Use Network*** will only work with a controller 4 that is hooked up to the network.

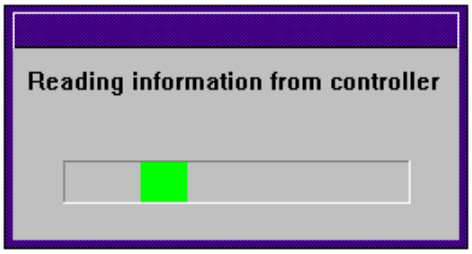
Using Your Controller Programming Unit

The Controller Programming Unit (CPU) can be utilized to directly interrogate and/or program any controller. Quantum will utilize this method of communication when you select ***Use Controller Programming Unit*** from the Program /Update dialogue box. This method of communication requires you to physically go to the controller and insert the CPU into the controller.

In order to establish a communication link, you must have your Controller Programming Unit connected to the serial channel specified in your Operator setup.

Quantum will then prompt you to insert the CPU into the cylinder connected to the controller.

Insert the key portion of the CPU into the keyway of the controller. Quantum will automatically begin communication with the controller. While Quantum is communicating with the controller, it displays a status box.



You should leave the CPU inserted in the controller until Quantum prompts you to remove it. Most operations require several transfers of information between the PC and the controller, which must not be interrupted. If Quantum should ever appear to "freeze up" for more than a few seconds, you should try to clear the communications link between the PC and the controller by pressing CTRL-C (press the Ctrl and C keys at the same time). Quantum should display a message such as "*Unable to communicate with CPU. Retry?*". Select ***Yes*** to have Quantum attempt to reestablish communications with the controller.

If for any reason the communications link between the PC and controller is completely lost, remove the CPU, press **ESC** repeatedly until you are returned to the Controller menu, then restart the controller operation.

To return to the controller menu without inserting the CPU, select the ***Cancel*** button in the prompt box, or press the **ESC** key. Since Quantum is monitoring both the CPU and the PC, you may have to press **ESC** more than once to cancel the prompt.

Communication with the Controller via Special Function Keys

A Controller Update Key and a Controller Audit Key can be used to communicate with Model 4 controllers. The Controller Update Key can be used to transfer new feature and access information to the controller. And, a Controller Audit Key can be used to read audit trail information from the controller. Refer to "Key Operations - Controller Update Key" and "Key Operations - Controller Audit Key" for details on creating and utilizing these special function keys. Quantum will utilize this method of communication when you select ***Make Controller Update Key*** from the Program/Update dialogue box. This method of communication does require you to physically go to the controller and then insert the key into the controller.

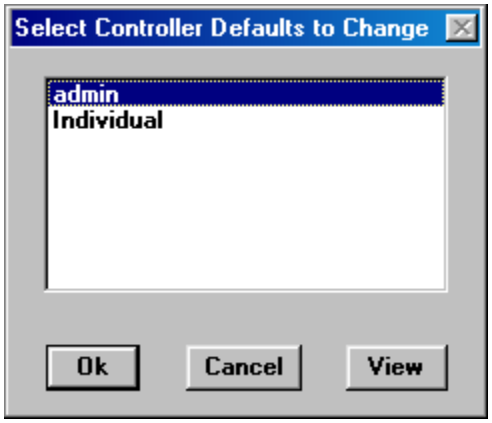
.

Controller Defaults

The controller Defaults option allows you to enter default values which will be used in programming new controllers. Each time you add a new controller to your database, its feature settings will be initialized to the values specified by the controller defaults. You may then set specific features for the controller before it is added to the database.

Selecting a Controller Default Configuration

For all operations which require you to select a controller configuration, Quantum displays a selection screen.

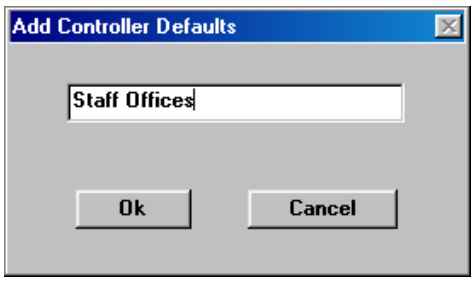


You may select the appropriate default configuration by double-clicking on its name, or by highlighting it in the list, then selecting ***Ok***. To see what the settings are in a default configuration without selecting it, single-click on its name, then select ***View***. Quantum will display the Controller Main Screen to allow you to view the settings. You will not be able to change any settings.

When Quantum is first installed, it creates one controller default configuration, named "Individual". Until you add more configurations, Quantum will automatically select this configuration, rather than prompt you to select one.

Adding Controller Defaults

To add a controller default configuration, select **Controllers | Defaults | Add**. Quantum will first prompt you for a name for the configuration.



You should give the configuration a meaningful name, such as "Front Doors", or "Admin Building". Once you have entered the name, select ***OK***. You may not have two controller configurations with the same name.

Quantum then presents the Controller Main Screen to allow you to specify the settings for the group. Enter feature, security, and other configuration information which applies to all or most controllers that will be added with the specified configuration. For example, if you want all doors in the Administration Building to have the anti-passback function enabled, check the appropriate boxes in the Controller Security Screen. You may change the name of the group using the ***Group Name*** button, but the name must still be unique - it cannot be the same as another group. Once you have completed the configuration from the Controller Main Screen, select ***OK***. At this point, you can either enter the name of the next configuration you wish to establish or you can select ***Cancel*** to close the Group Name window.

If the configuration you are creating is similar to an existing group, you may copy the existing group and change only the appropriate information for the new group. See "Copying Controller Defaults" below.

Changing Controller Defaults

You may change the settings for a controller default configuration by selecting **Controller | Defaults | Change**. Quantum prompts you to select the group to change, then presents you with the Controller Main Screen to allow you to set the default values for the group. You may change any of the settings here, including the name of the configuration. Once you have made your changes, select ***OK***. If you wish to change the defaults for another controller, select it from the list box and make your changes. Otherwise, select ***Cancel*** to close the window.

You may modify the controller defaults at any time. For example, if you use the Daylight Savings Time adjustment feature, you will want to adjust the start and end times each year to reflect the current settings. Changing the default settings will not affect any controller information already stored in the database, only new controllers added to the system.

Note that if you are using the Holidays or Daylight Savings Time features, and change the system level settings each year you do not have to change the default settings. Each time you update a controller, Quantum updates the controller's holiday and Daylight Savings Time information from the system level settings.

Copying Controller Defaults

If you want to create a controller configuration which is similar to an existing group, you may copy the existing group and change only the appropriate information for the new group. Select **Controllers | Defaults | Copy**, select the existing group, and then enter a name for the new group. Quantum then presents the Controller Main Screen to allow you to make the changes necessary for the new group. Select ***OK***

once you have completed your selections from the Controller Main Screen. Then select the next controller defaults to copy from the list box and select ***OK***. If you have completed your selections of controller defaults to copy, select ***Cancel*** to close the window.

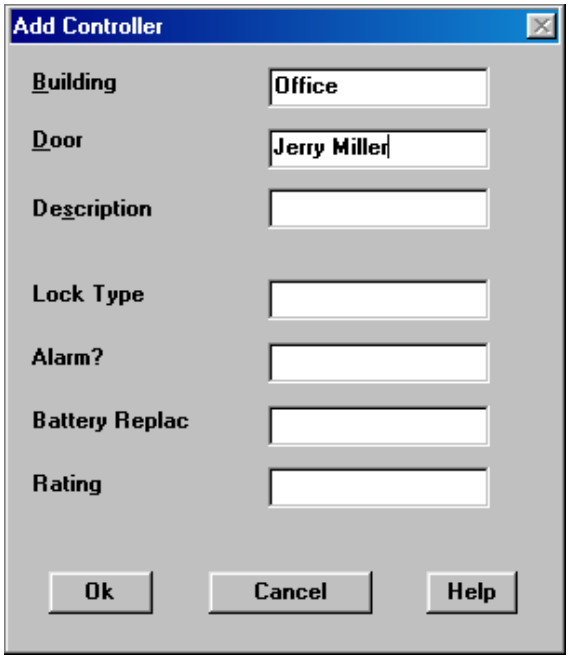
Deleting Controller Defaults

To delete a controller configuration, select **Controllers | Defaults | Delete**. Next, select the group to be deleted and select ***OK***. If you wish to delete another controller defaults, select it from the list box and complete the deletion process as previously described. Otherwise, select ***Cancel*** to close the window.

Controller Operations

Adding a controller to your system

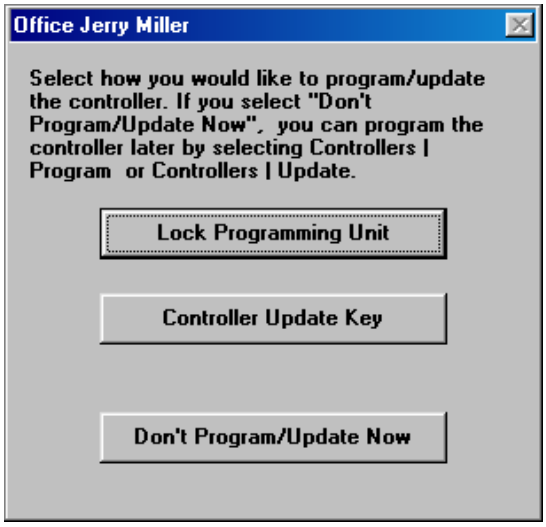
Adding a controller sets up a new database record with information to be used in programming a controller. To add a new controller, select **Controllers | Add** from the Main Menu. Quantum will present the Controller Description screen for you to enter the descriptive information for the new controller.



Fill in the appropriate values, then select ***Ok*** to continue. You must fill in the Building and Door fields, the rest of the information is optional. The section on "Controller Names" describes the requirements for naming a controller.

If you have more than one controller default configuration defined, Quantum will next ask you to select a configuration for the new controller. Select the appropriate configuration as described in Selecting a Controller Default Configuration. Quantum creates a new controller whose settings match those of the default configuration you chose.

Next, Quantum displays the Controller Main Screen. You should modify the settings unique to the new controller. These will typically include the access control information. When you have finished making your changes, select ***Ok*** from the Controller Main Screen. Quantum will next ask you how to program the controller.



If you are ready to program the controller now, select the appropriate method of communication from the programming dialogue box (see " Selecting Communication Methods"). Otherwise, select ***Don't Program/Update Now***. You will be able to program the controller later as described under Programming a Controller.

Quantum will then prompt you for the description of the next controller to add. Quantum will automatically set the Building identifier from the previous controller's information. This is done to save keystrokes based on the premise that, when adding controllers, you will typically add several from the same building at the same time. To add another controller, enter the description information, then select ***Ok***. To return to the main menu without adding another controller, select ***Cancel***.

Changing a Controller's Settings

This function allows you to modify the database information for an existing controller. You may edit the information before the controller is programmed, in which case the new information is what will be programmed into the controller. You may also edit the information after a controller has been programmed, then transfer the new information to the controller using the **Controllers | Update** option.

Activate the Edit Controller function from the Main Menu by selecting **Controllers | Change**. Enter the Building and Door information for the controller(s) to be edited. For each controller you selected, Quantum reads the information for the selected controller from the database, and displays the Controller Main Screen. Make any changes desired for the controller, then select ***Ok*** from the Controller Parameters menu to update the settings. Select ***Cancel*** to leave the original settings unchanged.

If more than one controller was selected from the list box, Quantum will prompt for the next controller to be edited. To edit another controller, enter the description,

then select ***Ok***. To return to the Controller menu without editing another controller, select ***Cancel***.

Programming a Controller

The Program Controller operation transfers information from the database to a new controller. You may program each controller only once. After you have programmed a controller, you may not program the same database information into another controller unless you first Cancel the controller (see " Canceling a Controller"). This guarantees that Quantum has an accurate record of the information programmed into each controller.

Activate the controller programming operation by selecting **Controllers | Program** from the Main Menu. Quantum prompts you to select the controller(s) for programming (see ""). Quantum will only list the controllers which haven't already been programmed.

For each controller to be programmed, Quantum prompts you to select the appropriate method of communication from the programming dialogue box. The methods of communication are ***Use Controller Programming Unit, Make Controller Update Key***, and ***Don't Program/Update Now***.

If you select the ***Use Controller Programming Unit*** method, Quantum will request that you insert your CPU into the controller. Quantum then verifies that the controller is not programmed and will transfer the programming information from the database to the controller. After the controller is programmed, Quantum will then prompt you to remove the CPU.

If you select the ***Make Controller Update Key*** method, Quantum will request that you insert the key into the KPU. Quantum will then program the key with database information for the controller. Once, the key is programmed it will request that you remove the key. To use the key, simply insert it into the Model 4 controller which it is programmed to update. The controller beeps once, then emits a series of "chirps" while it transfers the programming information to its memory. When the controller is finished, it beeps twice. You may then remove the key. If you insert the key into a controller other than the one for which it is intended, the controller will beep twice, and will not read the information from the key.

If you don't want to program the controller at this time, you can select ***Don't Program/Update Now.*** This selection acts as a cancellation function and returns you to the main screen. You will still have the ability to program the controller at a later time.

Updating a Controller

The Update Controller operation transfers updated programming information from the database to a controller. This option is used to keep the information in the controller database synchronized with the information programmed in the controller.

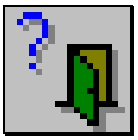
The Update Controller operation can be activated by selecting **Controllers | Update** from the Main Menu.

Quantum will prompt you to insert the CPU into the lock to be updated. Quantum then reads the controller ID number from the controller to identify it. Then Quantum reads the controller's programming information from the database. If the database information does not match the information read from the controller, Quantum reprograms the controller with the new database information.

When Quantum finishes the update operation, it prompts you to first remove the CPU from the current controller, and then to insert the CPU into another controller. To update another controller, insert the CPU into it. To return to the Controller Main menu, select ***Cancel***.

Querying a Controller

The Query Controller operation allows you to read and display the current settings of a controller, but not to modify them.



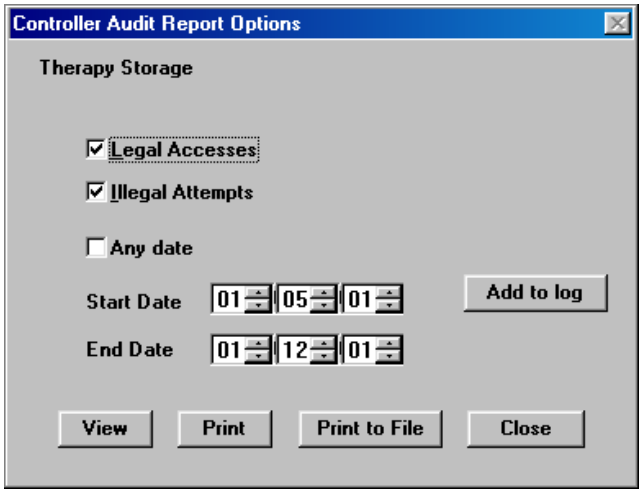
When you select **Controllers | Query,** Quantum prompts you to insert the CPU into the controller to be read. Quantum reads the programming information from the controller, and displays the Controller Main Screen to allow you to view the individual settings. You will not be able to change any of the settings. When you have finished viewing the controller data, select ***Ok*** from the Controller Main Screen.

Note: You must leave the CPU inserted in the controller the entire time. The Query operation requires several transfers of information between Quantum and the controller.

Quantum then prompts you to remove the CPU from the current controller, and to insert it into another controller. To read another controller, insert the CPU into it. To return to the Controller menu, select ***Cancel***.

Reporting the Controller's Audit Information

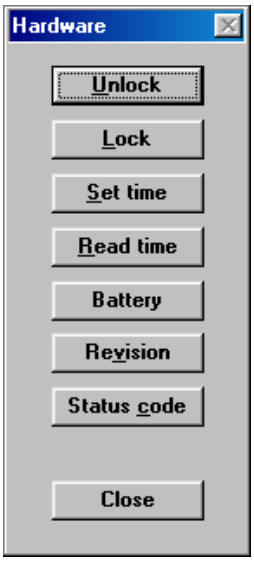
While you are querying a controller, you may display its audit trail information by selecting the ***Controller Audit*** button. Quantum reads the audit information, then asks you to select how the information should be reported.



Select the type of records to be reported (***legal*** and/or ***illegal***), and the date range of interest. Select ***View*** to see the report on your screen; select ***Print*** to print the report on the currently selected Windows printer; Select ***Print to File*** to save the report as an ASCII file. The report shows the date and time (if recorded) for each access, whether the access was Legal (authorized) or Illegal (unauthorized), and the name of the person to whom the key was issued. Select ***Add to Log*** to add the information to Quantum's User Activity log. Select ***Cancel*** when you are finished viewing the data.

Checking the Controller's Hardware

While you are querying a controller, you may test and examine some of its hardware functions. Select ***Controller Hardware*** for a list of options. The functions you may select are:



Button	Function
Unlock	Instructs the controller to perform its normal unlock sequence.
Lock	Instructs the controller to perform its normal lock sequence; note that this function will typically produce obvious results only following an uncontroller command to a controller programmed for Fixed Cylinder, Toggle mode; controllers programmed for other modes will normally be in a locked state.
Set time	Sets the controller's clock to match the PC running the Quantum software.
Read time	Display the current setting of the controller's clock.
Battery	Displays controller's battery level. The controller reports three levels -- high, medium, and low -- corresponding to the three battery warning levels (see "Controller Model Screen").
Revision	Display the revision (model) number of the controller electronics. Some controller features function differently, depending on the revision number.
Status code	Displays a message indicating why the controller considered the most recent unauthorized key access to be unauthorized (key not authorized in lock, timezone violation, etc.).

Deleting a Controller

This option allows you to delete all database information for a particular controller. This option should only be used if the controller which was programmed with the information has been removed from your INTELLIKEY system.

Activate the Delete Controller option from the Main Menu by selecting **Controllers | Delete**. Select the controller(s) to be deleted. Quantum will display the building and door for each controller, and then it will verify that you want to delete it. Select ***Yes*** to remove the controller from your database.

Quantum will then prompt for the next controller(s) to be deleted. To return to the Controller menu without deleting another controller, select ***Cancel***.

Canceling a Controller

The Quantum system will not allow you to program two controllers with information from the same database record. This is done to guarantee that the database contains a unique and accurate record of information for each controller in your system. It may, however, be necessary from time to time to reprogram a controller from the database. If, for example, the controller electronics for a door is upgraded to a newer model, the new controller should be programmed identically to the old controller. To do this, the status of the controller information in the database must be changed to 'not programmed into a controller' before it can be used to program the new controller hardware. This is the purpose of the Cancel Controller option.

Activate the Cancel Controller option from the Main Menu by selecting **Controllers | Cancel**. Select the controller(s) to be cancelled. For each controller you select, Quantum will display the building and door, and it will then verify that you want to cancel it. Select ***Yes*** to mark the database information as available for programming. You may now use the Program Controller function to transfer the information to a new controller.

Quantum will then prompt for the next controller to be canceled. To cancel another controller, enter the description or select a controller from the controller list box, then select ***Ok***. To return to the Controller menu without canceling another controller, select ***Cancel***.

Returning a Controller

Returning a controller is similar to cancelling a controller. When you return a controller, you not only mark its database information as being available, you also remove the programming from the existing controller. You would use this function, for example, on a temporary controller, installed for a short time. When you are finished with the controller, you "return" it to your stock, so that it may be programmed again for another function. You can also use the Return function to un-program a networked controller programmed with the wrong infomation.

To return a controller, select **Controllers | Return**. Quantum prompts you to insert the CPU into each controller to be returned.

Managing Users and Keys

User Names

Quantum defines a user as someone who has a permanent Quantum database record, and to whom an INTELLIKEY key has been (or will be) issued. The User menu allows you to enter or modify data for users, delete users from the system, or to modify the default settings for user groups.

Each user is identified by a first name ("John") and a last name, or surname ("Smith"). You must supply at least one of the name fields; either First Name or Last Name may be left blank, but not both. You may have two or more users with the same name, but each should have a different ID field (see below) to distinguish them.

If a user has only one name (Janitor or Security1, for example), you should enter the name in the slot which makes the most sense for your system. If you leave the last name blank, the user will appear at the beginning of an alphabetized list. This allows you to have all "special" user names together in your list. If you leave the first name blank, the name will appear in it's proper alphabetical location (Janitor would appear with the J's, for example).

The User ID is an optional field which may consist of any combination of letters, numbers, and symbols (!@#$%). You may use whatever system you like to assign ID codes. The ID field is long enough to hold Social Security numbers, or you may use employee numbers or student numbers.

One thing to keep in mind is that Quantum always treats the information in the user's name fields as characters, even if it contains numbers. This can cause some unexpected results when you look at a listing of your users sorted by name. For example, if you decide to assign users sequential numeric names, and enter the first ten users with names of "Janitor 1", "Janitor 2", "Janitor 3", "Janitor 4", "Janitor 5", "Janitor 6", "Janitor 7", "Janitor 8", "Janitor 9", and "Janitor 10", Quantum will display them alphabetically as

Janitor 1
Janitor 10
Janitor 2
Janitor 3
Janitor 4
Janitor 5
Janitor 6
Janitor 7
Janitor 8
Janitor 9

This happens because Quantum (like most computer programs) alphabetizes the user information based on the first character it sees in a description. Thus, the "1" in "10" causes the "10" to appear before "2" or "3", instead of after the "9", as you would expect. If you had users with names "Janitor 11" through "Janitor 19", they would appear alphabetically between "Janitor 10" and "Janitor 2". Similarly, users 21 - 29 would appear between "2" and "3".

It's very simple to keep your listings in the correct order. All you have to do is put enough characters in front of the digits to make all of your similar names the same length. For example, if you know that your largest number will be 100, you should make sure that all numbers in user names contain 3 characters. You could enter the user number 1 as either " 1" (two blanks, followed by a 1) or "001". If you enter all numeric user names in this manner, they will always appear in the correct order in any Quantum reports.

User Defaults

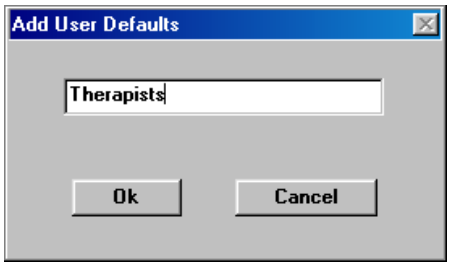
In a large installation with many users, it's common for groups of users to have similar access needs. For example, everyone who works for the maintenance department of a university will need access to the same doors, or all of the second shift employees might have the same Time Zone settings.

To simplify the user setup process, Quantum supports user default configurations, or groups. You can define different access information for each of these groups. When you add a user to your system, you simply select to which group the user belongs, and Quantum fills in the user's information with the settings for the group. All you have to do then is to change the few items which are unique to the user, such as access to a particular office.

You may give each group a meaningful name. For example, you might assign the first group to all employees who work first shift, and call the group "First Shift". You may set the time zone information for this group to correspond to the work times assigned to the shift. Similarly, a second group might be the second shift employees, with a different set of time zones.

Adding User Defaults

To add a user default configuration, select **Users | Defaults | Add**. Quantum will first prompt you for a name for the configuration.



You should give the configuration a meaningful name, such as "Maintenance Dept.", or "Third Shift". You may not have two user configurations with the same name.

Quantum next presents the User Main Screen to allow you to specify the settings for the group. Enter feature and access information which applies to all or most users

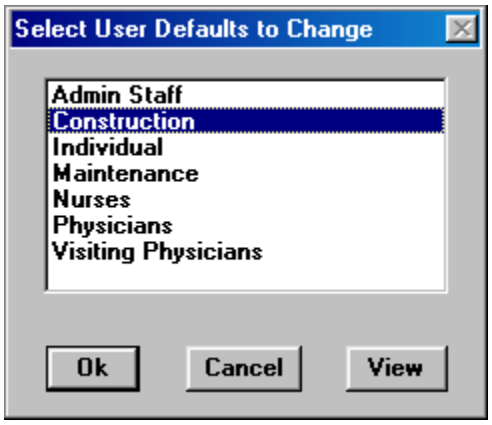
who will be added with this configuration. For example, if you want all users in the Maintenance Department to have the audit trail function enabled in their keys, check the appropriate boxes on the User Feature Screen. You may change the name of the group using the ***Group Name*** button, but the name must still be unique - it cannot be the same as another group.

If the configuration you are creating is similar to an existing group, you may copy the existing group and change only the appropriate information for the new group. See "Copying Controller Defaults" below.

If you are using the Vertical keying system, refer to "Setting Default Copy Numbers" below for information regarding setting copy numbers in user default configurations.

Selecting a User Default Configuration

When changing, copying, or deleting, Quantum displays a selection screen listing all of your user configurations.



You may select the appropriate default configuration by double-clicking on its name, or by highlighting it in the list, then selecting ***Ok***. To see what the settings are in a default configuration without selecting it, single-click on its name, then select ***View***. Quantum will display the User Main Screen to allow you to view the settings. You will not be able to change any settings.

When Quantum is first installed, it creates one user default configuration, named "Individual". Until you add more configurations, Quantum will automatically select this configuration, rather than prompt you to select one.

Changing User Defaults

You may change the settings for a user default configuration by selecting **Users | Defaults | Change**. Quantum prompts you to select the group to change, then presents you with the User Main Screen to allow you to set the default values for the group. You may change any of the settings here, including the name of the configuration.

Note that if you are using the Holidays feature, and change the system level holiday settings each year you do not have to change the default settings. Each time you update a user's key, Quantum updates the user's holiday information from the system level settings.

Copying User Defaults

If you want to create a user configuration which is similar to an existing group, you may copy the existing group and change only the appropriate information for the new group. Select **Users | Defaults | Copy**, select the existing group, then enter a name for the new group. Quantum then presents the User Main Screen to allow you to make the changes necessary for the new group.

Deleting User Defaults

To delete a user configuration, select **Users | Defaults | Delete**, and select the group to be deleted. Once the group has been selected, click the ***OK*** button. Quantum will then verify that the selected user defaults are to be deleted. Click ***Yes*** for the deletion to occur or click ***No*** to cancel the deletion process. Quantum will then prompt for the next controller(s) to be deleted. To return to the Controller menu without deleting another controller, select ***Cancel***

Setting Default Copy Numbers

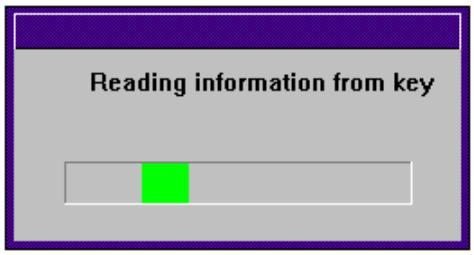
There is one special characteristic of the user default values, and that relates to the copy numbers used in the Vertical keying system. The User Keying Screen under user defaults does not have the button for automatic copy number assignment. Rather, it has a numeric field for the copy number, which you may fill in yourself. If you leave this field set to 0 when you enter the default controller identification data (Building and Door), Quantum will automatically assign a copy number to each user when it reads the default values. However, if you set the copy number to anything other than 0, Quantum will use this copy number for all users assigned to the default group. This allows you to have a group of users -- the maintenance department, for example -- share the same copy number

Using The Key Processing Unit (KPU)

Most of the Key operations involve inserting a key into the Key Processing Unit (KPU). Quantum prompts you to do so with a message box:

Quantum will monitor the KPU until a key is inserted, then will continue with the operation. If you wish to skip the operation, select ***Cancel***.

While Quantum is communicating with the KPU, it displays a message box indicating the operation being performed, along with a moving status marker to indicate that the system is busy.



Quantum will prompt you to remove the key when it has finished reading or programming the key. In general, you should not remove the key until Quantum prompts you to do so. There is an exception to this, however. Occasionally, the KPU will report to Quantum that a key has already been removed after a programming operation. When this happens, Quantum will not prompt you to remove the key, but will instead prompt you to either insert the next key, or for the information necessary to restart the operation you are doing. If this occurs, it is safe to remove the key.

When you insert your key into the KPU, and as long as the KPU recognizes that the key is present, the green light on the front of the KPU should be lit. If the light ever changes to red, or goes out completely, the KPU is having trouble communicating with the key.

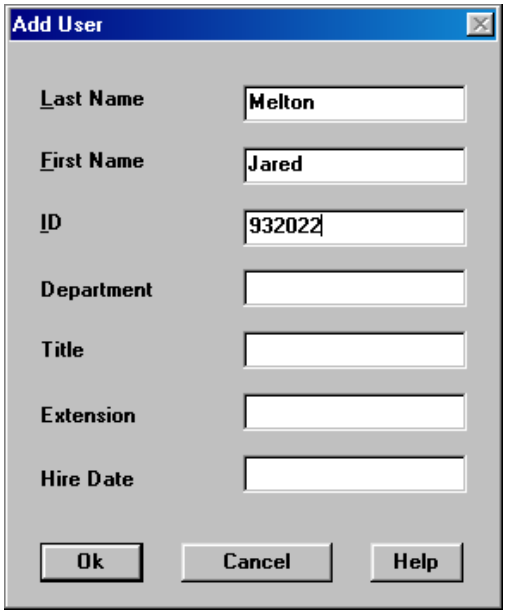
If Quantum should ever appear to "freeze up" for more than a few seconds, you should try to clear the communications link between the PC and the KPU by pressing CTRL-C (press the Ctrl and C keys at the same time). Quantum should display a message such as *Unable to communicate with KPU. Retry?*. Select ***Yes*** to have Quantum attempt to reestablish communications with the KPU. If the "unable to communicate" message appears several times in a row, press the reset button on the back of the KPU, then wait until the KPU indicator light flashes green twice before selecting ***Yes***.

User Operations

Adding a User

The Add User function adds a new user to your database. This creates a user who may be given access to any existing doors. If you want to create a Master Key, which will be able to access any door in your system, including those which haven't been defined yet, refer to the section **Creating Special Function Keys.**

Start the Add User operation from the Main Menu by selecting **Users | Add**. Quantum presents the user description screen for you to enter the user's personal information.



You must fill in at least one of the name fields; either *First Name* or *Last Name* may be left blank, but not both. Quantum will search the user database to see if there is already a user with the same name. If so, Quantum will tell you so, and ask you if you still want to add this user. It is possible that you have already entered the user's information, or that there is another user in your system with the same name. If you want to add this user, select ***Yes***; otherwise select ***No***, and Quantum will let you modify the user's description again.

When you have finished filling in the user's description, select ***Ok***. If you have more than one default configuration specified, Quantum next presents you with the list of user default groups to specify the user's access information. Select the configuration which most closely matches the user's access information. Quantum next displays the User/Key main menu to allow you to customize the user's access information. For example, you will need to change the user's access rights if it doesn't exactly match the defaults. When you have finished modifying the user data, select ***Ok*** from the User/Key menu.

If you have entered access information for user, and your Quantum operator rights allow it, Quantum will next ask you if you wish to issue a key to the user. If you are ready to program a key for the user, select ***Yes***, otherwise select ***No***. If you select ***No***, you may program the user's key later using the Issue Key option.

If you select ***Yes***, Quantum prompts you to insert key into the KPU Unit. Quantum verifies that the key is not already programmed, then programs the key with the settings entered for the user. Remove the key when Quantum prompts you to do so.

Quantum next presents the personal information box for you to add another user. To add another user, enter the data, then select ***Ok***. To return to the User menu without adding another user, select ***Cancel***.

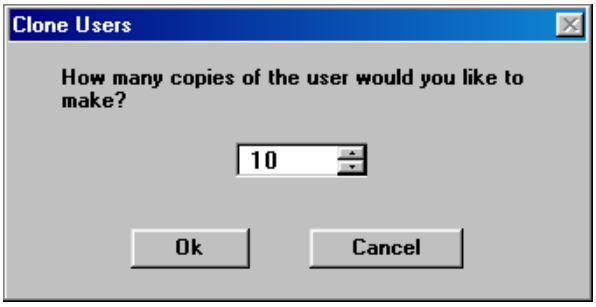
Adding Several Identical Users

There are some instances when it is convenient to create several identical keys, even when they aren't issued immediately. For example, you may be programming all of

the controllers for a new building, and want to create a group of keys which will have access to all doors in the building, even though you don't have anyone specific to issue the keys to yet. You would first define the controllers, then, before programming the controllers, create a group of users who have access to the controllers. This would add the users' names to the controllers' list of authorized users, so that when the controllers are programmed, the keys are already authorized. You could issue the keys at any time, knowing that they will be enabled in the controllers, without the need to use the Auto-Enable feature to enable them.

The *Clone Users* feature allows you to make several copies of a user. Select **Users | Clone Users**. Quantum follows the same steps as in "Adding a User" to let you enter the user's access and feature information. For the user description, you should provide a **Last Name** which describes the group of keys -- Maintenance, Dorm 3, etc. Quantum will create the names for the copied keys by appending a number to the last name: Maintenance 001, Maintenance 002, etc. Typically you would leave the **First Name** and **ID** fields blanks, since you will fill these in when you actually issue a key to someone.

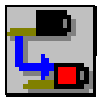
When you finish entering the information, instead of asking if you want to issue a key, Quantum next asks how many copies of the user/key you want to make:



Select the number of copies, then Ok. Quantum creates the specified number of copies, sequentially numbering the **Last Name** field.

When the time comes to issue one of these keys, you simply select the **Users | Change** function, and select one of the cloned keys. Change the clone name to the name of the person to whom the key is being issued, enter the proper ID, and any other description fields as necessary. You may also add or delete access information to the key. After you make the changes, Quantum will allow you to issue the key.

Changing a User's Information



This option allows you to modify the database information for an existing user. You will typically use this option when a user's access requirements change. For example, if a user needs access to controllers for which he was not initially authorized, this change must be entered in the user database, then transferred to the user's key.

Activate the Change User operation from the Main Menu by selecting **Users | Change**. Quantum prompts you to select the user or users whose information is to be changed (see "Selecting Users"). For each user you select, Quantum will display the User/Key Main Screen to allow you to make the necessary changes to the user's feature or access information. When you are finished, select ***Ok***. If you made any changes, Quantum will ask you if you want to update the user's key now. If the key is available, select ***Yes***, otherwise select ***No***. If you select ***No***, you may update the key later using the **Users | Update Key** command.

If you select ***Yes***, Quantum prompts you to insert the user's key into the KPU. Quantum verifies that the key is the one originally issued to the user, then programs the key with the new settings. Remove the key when Quantum prompts you to do so.

Quantum will prompt you to enter the name of the next user(s) to be changed. To change more users, select the appropriate ones from the list box and select ***Ok*** . To return to the main menu without changing another user, select ***Cancel***.

Deleting User(s)

The Delete User operation removes all information pertaining to a user or users from the database. This option would typically be used when an employee leaves a company, or at the end of the school term when students leave for the summer.

Before deleting a user, Quantum verifies that there are no keys currently issued to the user. Since each issued key is connected, through the database, to a user, Quantum will not allow you to delete a user until all keys issued to the user have been accounted for. Keys must be returned to the database, or logged as lost or not returned. These operations are described below, under "Key Operations".

Activate the Delete User operation from the Main Menu by selecting **Users | Delete**. Quantum will prompt you to select the user or users to be deleted. Quantum will locate and read each selected user's information from the database.

After Quantum verifies that the user may be deleted (has no keys issued), it prompts you with the user's name and ID code, and asks you to verify that this is the user to be deleted. To delete the user, select ***Yes***; to leave the user in the database, select ***No***.

Quantum next prompts you to select additional users to be deleted. To return to the User menu without deleting another user, select ***Cancel***.

Key Operations

Quantum keeps track of the relationship between users and keys. When you issue a key to a user, Quantum records this fact, and will not allow you to issue a second, duplicate key to the user. This protects the integrity of your access control system. You will always know which users have keys, and which controllers they are allowed to operate.

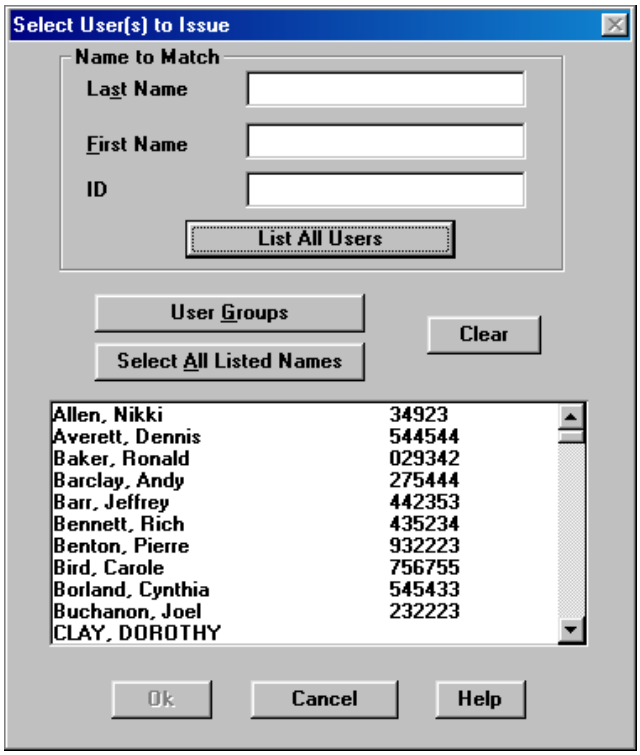
Issuing a key

Issuing a key involves transferring access control information into a key's memory, and maintaining a record indicating to whom the key was issued. Issuing a key to a user involves programming a key with information you have entered earlier in the user database.

Quantum will also print an issue receipt, indicating the key number, to whom the key was issued, the date and time, and the controllers which the key will operate. The receipt is printed on your currently selected printer, and provides lines for the user to

sign when receiving the key. You can select whether or not you want tickets printed from the Key menu. This feature is enabled by selecting **Users | Print Receipt**. To deactivate the issuing of a receipt, select **Users | Print Receipt** so that the check mark no longer appears next to it.

Activate the Issue Key operation by selecting **Users | Issue Key** from the Main Menu. Quantum prompts you to select the users to whom keys are to be issued.



For each user you select, Quantum verifies that the user's database information is valid, and that no key has been issued to the user. Quantum then prompts you to insert a key in the KPU, verifies that the key is not programmed, then transfers the user's access information to the key. If you have the Print Issue Receipt feature enabled, Quantum prints the issue receipt for the key. Quantum then asks you to remove the key.

Quantum next prompts you for the names of additional users to be issued keys. To return to the main menu without issuing another key, select ***Cancel***.

Creating Special Function Keys

Quantum can program standard INTELLIKEY keys to perform special functions. Each special function key is created from the **Users | Special Keys** menu.

Special function keys are added to the Quantum database and assigned key numbers just like any other key. Many of the special function keys store information read from controllers. To read this information, use the **User | Query Key** function.

When you are finished with a special function key, use the **Users | Return Key** function (see “Returning a key”, below) to remove it from your database.

Controller Audit Key

A Controller Audit Key is used to read audit trail information from a Model 4 controller into the key's memory. Quantum can then read this information from the key and generate a report based on the controller's audit information. Each key may audit one controller at a time, and holds the most recent 250 records from the controller.

To create a Controller Audit Key, select **Users | Special Keys | Controller Audit**. Insert a blank key in the KPU when prompted.

You may use this Audit key in any Model 4 controller. Each time you insert the key in a controller, the controller overwrites any data stored in the key with new audit information.

To use the key, simply insert it into the controller that you wish to audit. The controller beeps once, then emits a series of "chirps" while it transfers its audit information to the key. When the controller is finished, it beeps twice. You may then remove the key.

To read the audit information, select either the **Users | Query Key** or **Audit | User Key** functions. Refer to "Audit Operations - Reading a Controller Audit Key" for details on reading the information from the key.

Controller Update Key

A Controller Update Key is used to transfer new feature and access information to a Model 4 Controller. You first edit the controller's information using Quantum's Change Controller function, then load the information into the key through the KPU, then transfer the information to the controller by inserting the key into it.

To create a Controller Update Key, select **Users | Special Keys | Controller Update**. Quantum next prompts you to select the controller which this key will be used to update. Insert a blank key in the KPU when prompted.

To use the key, simply insert it into the controller that it is programmed to update. The controller beeps once, then emits a series of "chirps" while it transfers the programming information to its memory. When the controller is finished, it beeps twice. You may then remove the key. If you insert the key into a controller other than the one for which it is intended, the controller will beep twice, and will not read the information from the key.

Whenever you create a Controller Update Key, Quantum marks the controller's information in the database as "Update Key created". This notation, which shows up in a controller report, indicates that the controller may not be in synch with the database. After you have updated the controller with the key, and returned the key, Quantum marks the database information as "Programmed" to indicate that the controller now matches the information in the database.

.

Emergency Key

An Emergency Key overrides the shutout function and any time-related access control functions, such as time zones or holidays. If you are using the Vertical keying system, an Emergency Key also overrides the copy number checking function.

To create an Emergency Key, select **Users | Special Keys | Emergency Key.** Quantum next prompts you for a list of controllers for which the key will be authorized. Insert a blank key into the KPU when prompted to do so.

An emergency key is utilized just like any other key. Due to its extreme power, especially its inability to be disabled from a door, an Emergency Key is automatically assigned only a 24-hour lifetime by the Quantum software.

Guard Tour Key

A Guard Tour key records the lock ID number and date and time of each controller into which it is inserted. You may optionally select a list of controllers that the key will be able to open. These would include doors to areas where a guard needs to check that everything is turned off or locked up.

To create a Guard Tour Key, select **Users | Special Keys | Guard Tour** . Quantum will next prompt you to select controllers that the key will be authorized to open. Note that the Guard Tour function will work in any controller, but the key will only be able to open those that you specify.

To use the key, simply insert it into the designated controllers along the Guard Tour route. The controller will sound one long beep followed by one short beep to indicate that it has recorded the appropriate date and time information in both the key and controller. If the key is authorized to open the door, the Guard may unlock the door and enter the room for inspection.

To read the tour information from the key, select either the **Users | Query Key** or **Audit | Guard Tour Key** function. Refer to "Audit Operations - Guard Tour Functions" for details on reading the information from the key.

Disabler Key

A Disabler Key will disable keys in controllers. You would use this function typically when someone loses a high level key that is authorized for many controllers. You can create several copies of a Disabler Key to be used in deleting the lost key from all affected controllers.

To create a Disabler Key, select **Users | Special Keys | Disabler**. Quantum prompts you to select the user whose key is to be disabled. Insert a blank key into the KPU when Quantum prompts you to do so. Note: Each disabler key will only disable one user. You must create a separate Disabler key for each key you wish to disable.

To use a Disabler Key, insert it into any controller for which the lost key might have been authorized. The controller will sound a short beep to indicate it has recognized the key. If the key was authorized, the controller will remove the key from its list of authorized keys. When the controller is finished, it will sound three short beeps to indicate that you may remove the key.

Refer to "Audit Operations - Disabler Key Functions" for details on reading the information from the key.

Shutout Key

A Shutout Key temporarily blocks access to a controller by an key except an Emergency key.

To create a Shutout Key, select **Users | Special Keys | Shutout**. Quantum next prompts you to select the controllers for which the shutout key will work. Insert a blank key into the KPU when prompted to do so.

To use a Shutout Key, insert it into the controller that is to be locked with the shutout function. The controller will sound two short beeps to indicate that the shutout function has been activated. At this point, no standard key will operate the controller. Controller Audit Keys and Controller Update keys will work in the controller.

To take the controller out of shutout mode, insert the Shutout Key again. The controller will sound a short beep to indicate that it is back to normal operating mode. An Emergency Key will also take a controller out of shutout mode.

Grandmaster Key

A Grandmaster Key is automatically authorized to operate all controllers. You must enable the Grandmaster Key function and specify how many keys to configure as Grandmaster keys when you first install Quantum.

To create a Grandmaster Key, select **Users | Special Keys | Grandmaster Key**. Insert a blank key when prompted to do so.

A Grandmaster Key is used like any standard key. The only limitation on it is that its lifetime is limited, to reduce security problems if the key is lost. The lifetime of Grandmaster Keys can be set by selecting Utility | Site Setup | Functions. If a Grandmaster Key expires, you can reauthorize it by updating the key (see "Updating a key").

Updating a key

The Update Key operation transfers new database information to a user's key. You would typically use this option after you have updated a user's database information. For example, if you add masterkeying information for a user, you must update the user's database information first, then update the user's key.

Activate the Update Key operation by selecting **Users | Update Key** from the Main Menu. Quantum prompts you to insert the key to be updated into the KPU. Quantum reads the key ID number from the key, matches the number to the user to whom the key was issued, and reads the user's access information from the database.

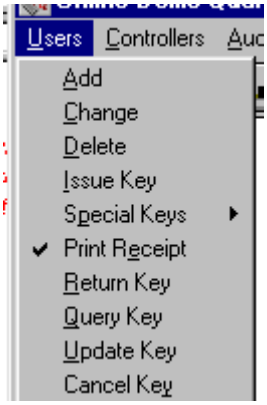
If the database information does not match the information already programmed into the key, Quantum reprograms the key with the new database information. If you have the **Print Receipt** feature enabled, Quantum prints an update receipt for the key. Quantum then asks you to remove the key.

Quantum then prompts for another key to be inserted for update. To update another key, insert it in the KPU. To return to the main menu, select ***Cancel***.

Turning Receipt Printing On and Off

The **Users Print Receipt** option allows you to control the printing of issue tickets. The menu item will have a check mark next to it if receipt printing is enabled. Each time a key is issued or updated, Quantum will print a recept for the key, with a space for the keyholder to sign. You can also print receipts from the **Report** menu.

*The check mark alternates between checked and not checked each time you select the **Print Receipt** menu item.*



Returning a key

When you return a key, Quantum updates its database to reflect the fact that the key is no longer issued to anyone, and disables the key so that it may not be used until it is reprogrammed and reissued.

When you select the Return Key operation, Quantum first asks you if you want to delete the user after returning the key. If you are returning a user's key and know that you no longer need the user's database information, select ***Yes***, otherwise, select ***No***. If you select ***No***, Quantum will retain all of the user's information, but will note that the user has not been issued a key.

Using the "delete user after returning key?" feature simplifies some of your database operations, but does take longer than simply returning the key. If you are in a situation where you are returning a large number of keys at once, (students checking out at the end of the term, for example) you might want to simply return the keys now, and use the Delete User functions (see "Deleting User(s)", above) to delete the user information later.

Activate the Return Key option by selecting **Users | Return Key** from the Main Menu. Quantum will then prompt if you want to "delete user after returning key?". If you select ***Yes***, Quantum prompts you to insert the key to be returned into the KPU. Quantum reads the key ID number from the key, and displays a message at the bottom of the screen indicating to whom the key was issued. Quantum then updates the database information to reflect the fact that the key is no longer issued. Do not remove the key from the KPU until Quantum prompts you to do so.

Quantum then prompts for another key to be inserted for return. To return another key, insert it in the KPU. To return to the Key menu, select ***Cancel***.

Querying a key

The Query Key operation allows you to read and display the current settings of a key, but not to modify them. You can use this function to verify the programming of a key or to identify a key.

Activate the Query Key option by selecting **Users | Query Key** from the Main Menu. Quantum prompts you to insert the key to be read into the KPU. Quantum reads the programming information from the key, and displays the User/Key Main Screen to allow the individual settings to be viewed. Note that all of the data entry items on each screen are grayed out -- you may not change any of the displayed information. When you have finished viewing the key data, select ***Ok*** from the User/Key Main Screen.

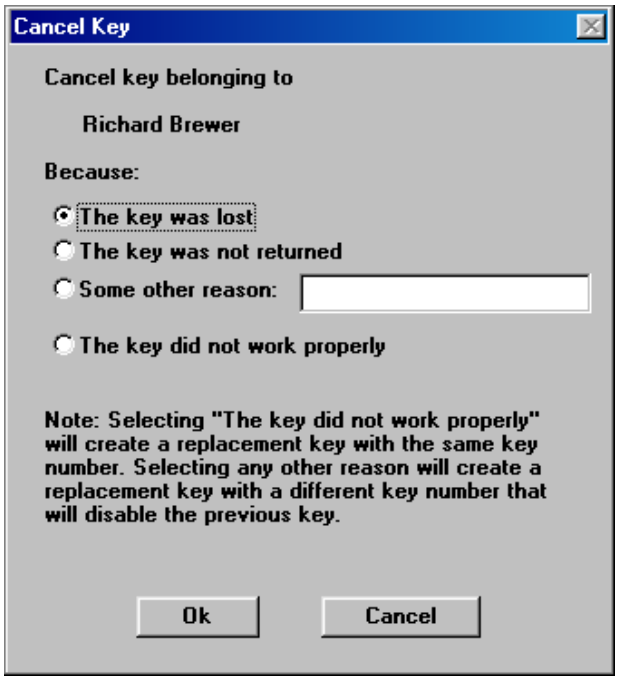
Quantum then prompts for another key to be inserted for reading. To read another key, insert it in the KPU. To return to the Main menu, select ***Cancel***.

Canceling a key

The Cancel Key operation provides a method of removing keys from the Quantum database without having the key physically present. You would typically use this option when a key is lost, or otherwise not returned by a user. Quantum removes the key from its active database and marks the key as not being issued to anyone. Quantum creates a record in a separate database, however, of the key ID number, the user at the time it was deleted, and the reason it was deleted. Thus, if someone finds and attempts to use a lost key, its history can still be tracked.

Canceling a key also releases the user's access information to be reprogrammed into another key. Thus, if a user loses a key, you may cancel the key, then issue another key to the user using the **Users | Issue Key** function.

Activate the Cancel Key operation from the Main Menu by selecting **Users | Cancel Key**. Quantum prompts you to select the user whose keys are to be canceled. For each key to be canceled, Quantum prompts you to supply a reason.



Select the appropriate reason, then select ***Ok***. Note that if you select ***Some other reason*** you may fill in the explanation box to give more detail. This information will be included in a key or user report. To return to the main menu without canceling the key, select ***Cancel***.

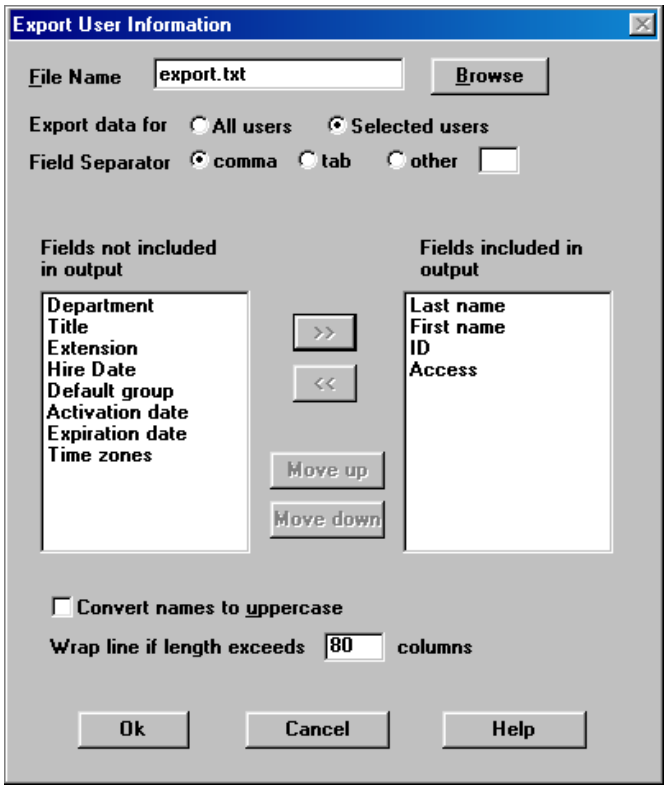
Exporting and Importing User Data

Quantum's data files are stored in Borland's Paradox® format. Some of the information in the files is in binary format, not easily readable by other applications which might need access to it. To make the information more accessible, Quantum provides functions for importing and exporting its database settings.

Exporting User Data

The Export Users function writes user information to an ASCII file which may be read by other applications, such as spreadsheets or word processors. You may select which data fields to export, which users to export, and the format of the exported data.

To export user information, select **Utility | Data Files | Export Users**. Quantum prompts you to specify the export settings:



Field	Function

File Name	The name of the file to contain the exported data. This may include a path name. Select ***Browse*** to open the standard Windows Open File dialog box for selecting a file.
Export data for	Select which users are to have their data exported. Select *All Users* to export data for all users in your database. Select *Selected Users* to choose specific users to export.
Field Separator	The character used to separate fields in the output file. For standard "comma separated value" (csv) files, this will be a comma.
Fields not included in output	This list box contains a list of user data fields which are not in the output file. To specify that one of these fields should be included in the export file, select the field so that it is highlighted, then select the right arrow button.
Fields included in output	This list box contains a list of user data fields to be exported, in the order in which they will be exported. To remove a field, select it so that it is highlighted, then select the left arrow button. To change the order of fields, select a field, then move it up or down in the list by selecting the Up Arrow or Down Arrow buttons. Note that the **Access** field will always remain the last item in the list.
<< >>	These buttons move items between the "Fields Included" and "Fields not included" lists. Select the field in the list box, then select the appropriate arrow button to move the field to the other list.
Move up Move down	These buttons rearrange the order of items in the "Fields Included" list box. Select the field in the listbox, then select the appropriate arrow button to move the field up or down in the list. Note that the **Access** field will always remain the last item in the list.
Convert to upper case	If this box is checked, Quantum will convert all exported data to upper case.
Wrap line if length exceeds ...	This function lets you specify the maximum length of a line in the output file. Quantum inserts a carriage return and starts the next output field on a new line when the current line reaches this length.

If you selected *Export Data for Selected Users*, Quantum asks you to select which users. You may select individuals, or access groups.

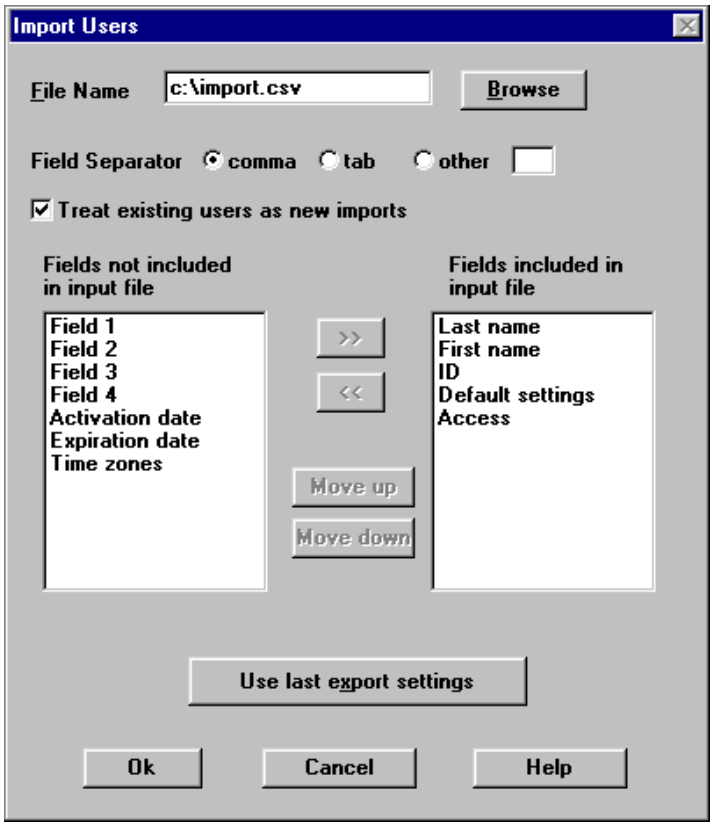
Quantum writes the selected fields, for the selected users, to the specified output file. See “Import/Export Data Format” for a description of the format for the exported data.

Importing User Data

At some sites, the information for new users is already available from another application, such as a university registration system or badging system. To simplify adding users, Quantum allows you to import data provided by these other applications. You may import just user names, and manually add the rest of the user information, or import everything there is to know about the user. It all depends on how much information is available from the other application.

Another use for the User Import function is to simplify mass changes to user information. You may export settings for some or all of your users, use a word processor or spreadsheet to make changes to one or more fields (such as expiration date) for the users, then import the changed file. When you import data for a user who is already in your database, Quantum updates the user's data rather than creating a new user. “Import/Export Data Format” describes the format Quantum expects for each of the user data fields.

To import user data, select **Utility | Data Files | Import Users** . Quantum prompts you to specify the import data:



Field	Function
File Name	The name of file containing the import data. This may include a path name. Select ***Browse*** to open the standard Windows Open File dialog box for selecting a file.
Field Separator	The character used to separate fields in the input file. For standard "comma separated value" (csv) files, this will be a comma.
Treat existing users as new imports	If this box is checked, and a user specified in the input file is already in the database, the import function will replace the user’s information with the information from the import file. This primarily affects the user’s access information. If the input file includes access information, and this box is not checked, all of the user’s access information is deleted, and only the access information from the input file is added to the user’s database. If the box is checked, the access

	information from the input file is added to the user's access information. See "Considerations When Importing Users" for more information.
Fields not included in input file	This list box contains a list of user data fields which are not in the input file. To specify that one of these fields is used in the import file, select the field so that it is highlighted, then select the right arrow button.
Fields included in input file	This list box contains a list of user data fields contained in the input file, in the order in which they are present. To remove a field, select it so that it is highlighted, then select the left arrow button. To change the order of fields, select a field, then move it up or down in the list by selecting the Up Arrow or Down Arrow buttons. Note that the **Access** field will always remain the last item in the list.
<< >>	These buttons move items between the "Fields Included" and "Fields not included" lists. Select the field in the list box, then select the appropriate arrow button to move the field to the other list.
Move up **Move Down**	These buttons rearrange the order of items in the "Fields Included" list box. Select the field in the listbox, then select the appropriate arrow button to move the field up or down in the list. Note that the **Access** field will always remain the last item in the list.
Use last export settings	If you are importing data from a file you have previously exported, you may select this button to automatically select the settings you used to create the export file, including the name of the file.

Note: *It is very important that the data in the "Fields included in input file" list is correct. Quantum attempts to interpret the data it reads from the import file based on what it expects to see for a particular field. Although Quantum performs validity checks on the imported data before adding it to the database, it is possible that some data may be misinterpreted, resulting in invalid user settings*.

When you select ***Ok***, Quantum reads each record from the input file and updates the user database accordingly. If the record specifies a user who is already in the database, the user's data is updated to reflect the imported settings. If the record contains a new user, the user is added to the database, and assigned a key number. If the import file contains the user's access information, all you need to do is issue a key to the user; otherwise you may have to manually edit the user's information first.

Considerations When Importing Users

When importing user data, Quantum verifies all names – default settings, building and door names, time zones, etc. – contained in the input file before adding a new user or updating an existing one. Names are not case sensitive (for example, "Individual" and "individual" are the same thing) but spelling is important ("Research Building" and "Research Bldg" are not the same thing). A misspelled name in any field of the import line is enough to prevent Quantum from processing the information for a user. At the end of the import process, Quantum displays a report listing any problems it found in the import file – unknown door names, for example. It's usually enough to correct the error(s) in the input file, then re-do the

import. Any users who were added correctly the first time the import was done will simply have their database records updated with the same information.

When adding a new user through the import function, Quantum follows these steps:

- If the import information includes a default configuration name, those settings are loaded as a starting point for the user's information. If no specific default configuration is given, Quantum loads the default configuration named "Individual".
- The default settings are replaced by specific information from the import file: ID, activation and expiration dates, etc.
- If there is any access information specified in the default settings, it is assigned to the user. If there is access information included in the import file, it is added to the information from the default settings.
- The user is assigned a keystamp number and added to the database.

When updating a user's information through the import function, Quantum follows these steps:

- The user's existing database information is loaded.
- If the import file specifies a default configuration, the information from the defaults replaces the user's information read from the database.
- The user's information (activation and expiration dates, etc) is replaced by specific information from the import file.
- The user's access information is handled differently, depending on whether or not the ***Treat existing users as new imports*** box is checked:
    - If the box is checked, the user's existing access information is retained (as if it had been read from a default configuration), and any access information in the import file is added to the user's information. This is the most common usage, and allows user information to be correctly imported more than once (to correct errors in the import file, for example).
    - If the box is not checked, the user's existing access information is deleted, and then only the access information contained in the import file is assigned to the user. This setting could be used, for example, to add or delete doors for several users. The user access information would first be exported to a file, the file edited to remove the door(s) and/or add new doors, then the information re-imported. The access information from the import file would completely replace the access information for all of the users in the file.

Import/Export Data Format

This section describes the format for each field in the import or export data file. These files are standard ASCII text files, and may be created or read by most spreadsheet, word processor, or database applications.

An import/export data file is a collection of records, each representing one user. A record may span several lines, depending on how much data it contains. Each line starts at the left column. If a record requires more than one line, each line except the

last must have the character string "+++" at the end of the line, following the last data field on the line. (See examples below). Each line ends with an ASCII "carriage return, line feed" sequence.

Individual fields within the record are delineated by a separator character, specified in the **Field Separator** field of the Import Settings or Export Settings dialogs. The most common separator is a comma (CSV or "comma separated value" file), although other characters may be used, depending on the application reading or writing the data file.

Quantum expects the data for each field to be in a specific format, and exports data in this format. It is the responsibility of any application creating a file to be imported into Quantum to ensure that the data is formatted properly.

Every record in an import file must contain all of the fields specified in the "Fields included in input file" listing. Empty fields are allowed, however. An empty field contains no data -- Quantum will use whatever the current default is for the field. Empty fields are indicated in the import file by two adjacent separator characters. For example, if the input format for a comma separated file includes "**Last Name, First Name, ID, Defaults, Activation Date**", the following input record is valid:

Smith,John,,,10/03/96

The record contains values for **Last Name** and **First Name**, no data for **ID** or **Defaults**, and a value for **Activation Date**.

When Quantum first reads a record from an import file, it sets up default values for the user, either based on the Default group specified in the input record, or from Quantum's *Individual* default group. The only information you need to include in the import record is data which is different from, or in addition to the default data. For example, if the default settings specify an activation and expiration date for the user, you do not need to repeat the settings in the input record for each user, unless the user's settings differ from the default. Note that you do have to include an empty field (described above) in each record that does match the defaults.

The following sections describe the format for each field.

Last Name, First Name, ID, Site-specific Fields

These are all standard ASCII strings. They may contain any character, including blanks, except for the separator character.

Default Group

This field names the default group for the user. The name must match the name in Quantum's database exactly. If an import file does not contain a Default group field, Quantum assigns default values to the user from the *Individual* group.

Activation and Expiration Dates

These fields specify the dates on which the user's key becomes valid or expires. Either or both fields may be included in the import/export record. They are ASCII strings in the form MM/DD/YY or DD/MM/YY or YY/MM/DD, depending on the date format you have selected for your site.

Time Zones

This field lists all time zones specified for the user. In the Horizontal keying system, the user may have 2 time zones, in the Vertical system up to 8. Time zones are listed by name, with a ~ character following each name, including the last. An example time zone specification would be: **1st Shift~2nd Shift~**

Access

The user's access is always the last information contained in the import/export record, since its length may vary greatly from user to user. The access fields should only specify controllers not included in the user's default group settings, or which have different time zone settings than the defaults.

Each controller to which the user has access is listed as a separate field, followed by the separator character. The format of the information is *building~door@timezone*. The @timezone field is a number indicating which timezone in the list should be applied to the door. If the user's time zone field is **1st Shift~2nd Shift~,** any controllers restricted to 1st Shift would have **@1** appended to the *building~door* name; any controllers restricted to 2nd Shift would have **@2**. The *@timezone* field is optional; if it is not included, the user will have access to the door at any time.

Example:

The user's time zone fields are specified as **1st Shift~Office Hours~** . The user is authorized to enter "Research Front" at any time, "Research Lab 1" only during office hours (the second time zone listed), and "Shipping Front" only during First shift (the first time zone listed). The user's access fields would look like:

Research~Front,Research~Lab 1@2,Shipping~Front@1

Examples

This section shows some sample import/export records. For all examples, the list of fields included is:

Last Name
First Name
ID
Site Specific field 1 (Department)
Site Specific field 2 (Title)
Site Specific field 3 (Phone)
Default group
Activation Date
Expiration Date
Time zones
Access

The default group *Individual* grants access to "Admin Front", "Research Front", and "Shipping Front".

The default group *Shipping* grants access to "Shipping Front".

Example 1:

John Smith, ID #129323 has access to all doors in the Individual group, plus "Research Lab 1". His key is valid from January 1, 1996 until December 31, 1996. The import/export record for John would be:

Smith,John,129323,Research,Manager,x333,Individual,1/1/96,12/31/96,, +++
Research~Lab1

Note that since the record spans more than 1 line, the first line ends with +++. If the record were more than 2 lines long, then lines 2 through the next-to-last line of the record would end in +++. Also, since John's default settings come from the Individual group, that field could have been left empty. The following would also be valid for John:

Smith,John,129323,Research,Manager,x333,,1/1/96,12/31/96,, Research~Lab1

If the Individual group specifies a key's lifetime as being January 1, 1996 to November 31, 1996, John's record could be:

Smith,John,129323,Research,Manager,x333,,,12/31/96,, Research~Lab1

Note that you don't have to include John's activation date, since it matches the default setting, but you must include his expiration date since it is different.

Example 2:

Brenda Jones, no ID #, has access to "Shipping Front" only during first shift. Since the default group Shipping specifies access to "Shipping Front" without any time restrictions, you must supply time zone information:

Jones,Brenda,,Shipping Team,Packer,,Shipping,,,1st Shift~,Shipping~Front@1

This line indicates that Brenda has no ID value, works in the "Shipping Team" department (field 1), has the job title of "Packer" (field 2), has no phone (field 3), gets all default settings from *Shipping*, has activation and expiration dates which match the defaults, has one assigned time zone (1st Shift), and has access to one door, restricted to that time zone.

Remote Key Programming

Some sites are spread out geographically. The headquarters may be located in one building, with other buildings some distance away, perhaps even in other cities. It is usually more efficient to maintain one Quantum setup, with one site code, to allow users to have one key which can access doors at any of these sites.

Unfortunately, in this type of setup, it usually isn't convenient to have a single location for key programming and querying. When users have to come from miles away to get new keys or to have their keys updated, the advantages of the INTELLIKEY system quickly evaporate.

To solve this problem, Quantum supports key programming by means of a modem. This allows a site to have Key Processing Units (KPUs) located at remote locations. These KPU's are connected to a modem rather than to a PC, and the modem in turn connected to a phone line. The computer running the Quantum software also has a modem by which it can communicate with the Remote KPU's.

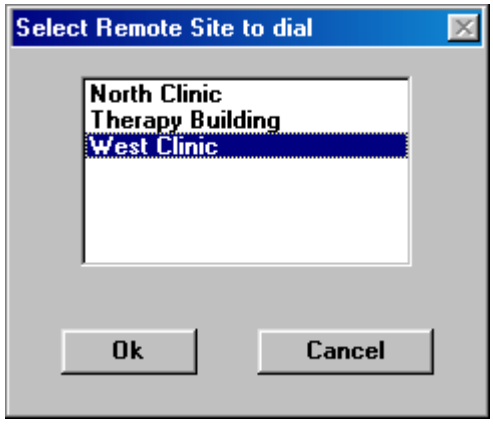
When someone at a remote location needs a new key, or to have a key updated, or to have a key queried (a Controller Audit Key, for example), all they have to do is insert the key into the Remote KPU. The Quantum operator uses Quantum's Remote Key Programming functions to connect to the Remote KPU. Once connected, the operator can perform all of the standard key programming and query functions described under "Key Operations", just as if the key were inserted in a KPU connected to the Quantum PC.

Note that this setup typically requires two phone lines between the central (Quantum) location and the remote location. The first line is for voice communication, so the Quantum operator can prompt the remote user when to insert or remove a key. The second line is for the modem connection between the Quantum PC and the Remote KPU.

The functions to set up and modify the information needed for connecting to remote key programming sites are available from the **Utility** menu.

Connecting to a Remote Site

Before performing any remote key programming functions, you must first connect to the site. You must have entered the settings for one or more remote sites. See "Adding a Remote Site" below for how to add remote sites. Select **Utility | Remote Key Functions | Connect to Site** to call a remote site. Quantum prompts you to select the remote site.



Double-click on the desired site, or scroll to the appropriate name and select ***Ok***. Quantum then calls the remote site and establishes connection with the KPU at the site. Once the connection is established, Quantum displays a message box to this effect.

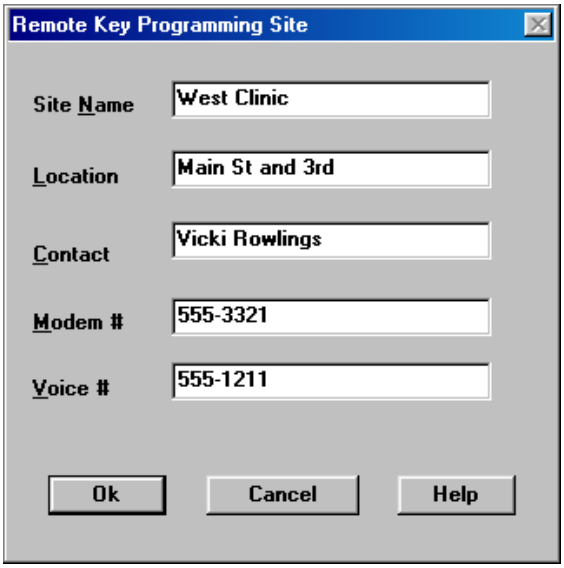
You can now perform any key programming or interrogation operation through the modem connection.

Disconnecting from a Remote Site

When you are finished with all remote key operations for a site, you must instruction Quantum to disconnect from the site by selecting **Utility | Remote Key Functions | Disconnect**. If you attempt to exit from Quantum while connected to a remote site, Quantum automatically disconnects before closing.

Adding a Remote Site

Select **Utility | Remote Key Functions | Add Site** to create a new remote site. Quantum displays the Remote Site screen to allow you to enter the information for the site.



The only mandatory fields are *Site Name* and *Modem #*. The *Site Name* field specifies the name by which you will select the site for dialing or modifying, and must be unique. The *Modem #* field contains the phone number to connect to the modem at the site. Note that field contains only the phone number, and not any other modem codes, such as outside line or long distance codes. Modem control values are specified under the operator setup screen. (**Utility | Operators | Change**).

Editing a Remote Site

Select **Utility | Remote Key Functions | Edit Site** to change the information for a remote site. Quantum first prompts you to select the site. Double-click on the desired site, or scroll to the appropriate name and select ***Ok***. Quantum then displays the Remote Site screen to allow you to change the information.

Deleting a Remote Site

Select **Utility | Remote Key Functions | Delete Site** to delete the information for a remote site. Quantum first prompts you to select the site. Double-click on the desired site, or scroll to the appropriate name and select ***Ok***. Quantum prompts you to verify that you want to delete the site; if you confirm the deletion, Quantum removes the remote site from its list.

Audit Operations

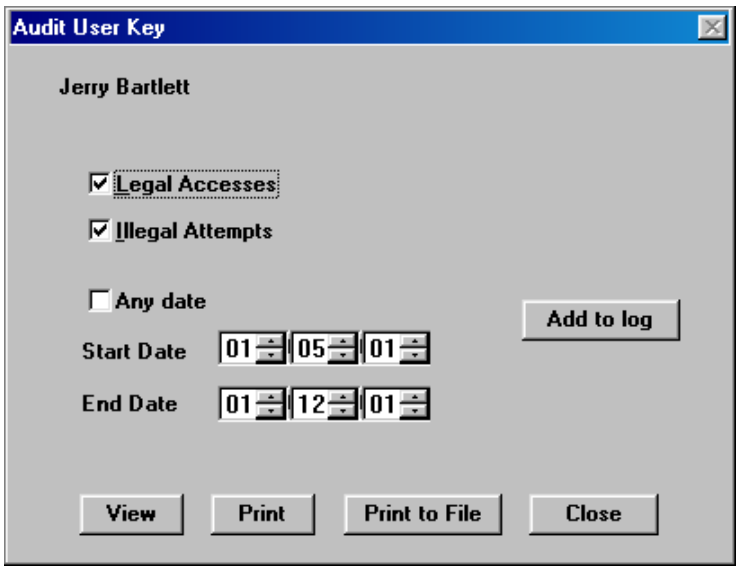
Keeping Track of Everybody

In addition to determining who is allowed to go where, an access control system must also provide **accountability**. In this context, accountability means the ability to determine, after the fact, where a person has been, and when. Quantum's audit functions provide this capability. These functions allow you to do such things as read the audit trail from a user's key or from a controller's memory, and to determine if a user's lost key has been denied access to all controllers.

The reports created by the Audit functions may be viewed in two ways: either on the screen or printed. Refer to "Displaying and Printing Information" in the "Reports" chapter for details. You may stop the generation of a report by pressing the **ESC** key.

Auditing a User's Key

The Audit User's Key function allows you to read the audit trail information from a user's key, showing which doors the user has been through recently. The Audit function must be enabled for the user (see the User/Key Features Screen). When you select **Audit | User's Key**, Quantum prompts you to insert the key into the KPU. When you do so, Quantum reads the audit information from the key, and allows you to specify which information you want printed.



Select the types of accesses (***legal*** and/or ***illegal***) which you wish to see, then select ***View*** to see the report on your screen, or ***Print*** to have the report printed on the currently selected Windows printer. Select ***Print to File*** to have the report saved as an ASCII file. Select ***Add To Log*** to add the information from the user's key to the User Activity Log.

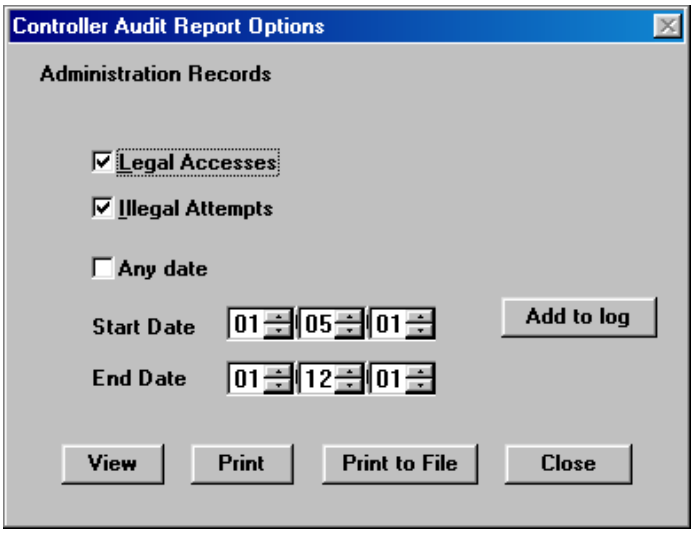
After viewing or printing the information, select ***Cancel.*** Quantum will ask you if you want to clear the audit information from the key. Select ***Yes*** to clear it, or ***No*** to leave it intact. Since the key always maintains the most recent audit information for the user, there is usually no reason to clear it. Remove the key from the KPU when prompted to do so.

Quantum then prompts you to insert the next user's key. To read another key, insert it into the KPU and select ***Ok***. If you have no more keys to read, select ***Cancel***.

Reading a Controller Audit Key

A Controller Audit Key reads audit trail information from a Model 4 controller's memory. The key stores the records for the most recent 250 users who have accessed the controller. The Audit Controller Audit Key function allows you to read this information and view or print it as a report. See "Creating Special Keys" for a description of how to make and use a controller audit key.

When you select **Audit | Controller Audit Key**, Quantum prompts you to insert the key into the KPU. When you do so, Quantum reads the audit information from the key, and allows you to specify which information you want printed.



Select the types of accesses (***legal*** and/or ***illegal***) which you wish to see, then select ***View*** to see the report on your screen, or ***Print*** to have the report printed on the currently selected Windows printer. Select ***Save*** to add the information from the Controller Audit Key to the User Activity Log.

After viewing or printing the information, select ***Cancel***. Remove the key from the KPU when prompted to do so. You may now use the key to audit another controller.

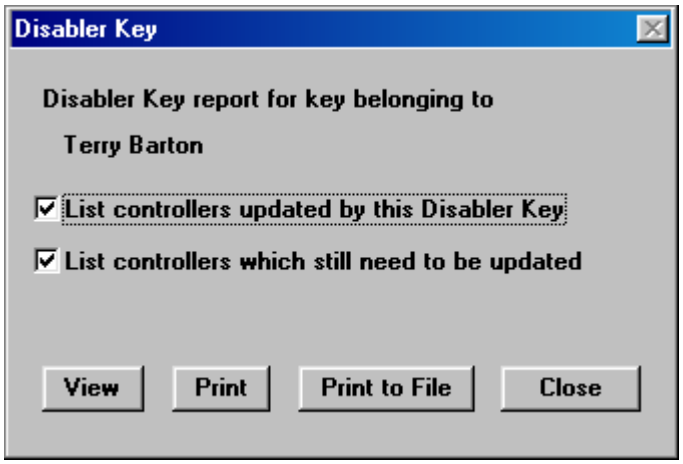
Quantum then prompts you to insert the next Controller Audit key. To read another key, insert it into the KPU and select ***Ok***. If you have no more keys to read, select ***Cancel***.

Disabler Key Operations

A Disabler key allows you to disable lost or stolen keys using a standard INTELLIKEY key. See "Creating Special Keys" for a description of how to make and use a Disabler key. Disabler keys programmed from KU16K devices record an audit trail of the controllers into which they have been inserted.

Reading a Disabler Key

When you select **Audit | Disabler Key | Read Disabler Key**, Quantum prompts you to insert a Disabler key into the KPU. Quantum reads the controller information from the key and allows you to specify how you want the information reported.



Select *List controllers updated by this disabler key* to see a list of controllers in which this Disabler key was used. Select *List controllers which still need to be updated* to see a list of controllers for which the user is still authorized. Select ***View*** to see the information on your screen, ***Print*** to have it printed on the currently selected Windows printer, or ***Print to File*** to have the report saved as an ASCII file. The information consists of the controller name and description for each controller updated by the Disabler key. When you have finished viewing the information, or if you do not wish to view it at all, select ***Cancel***, and remove the key when prompted to do so.

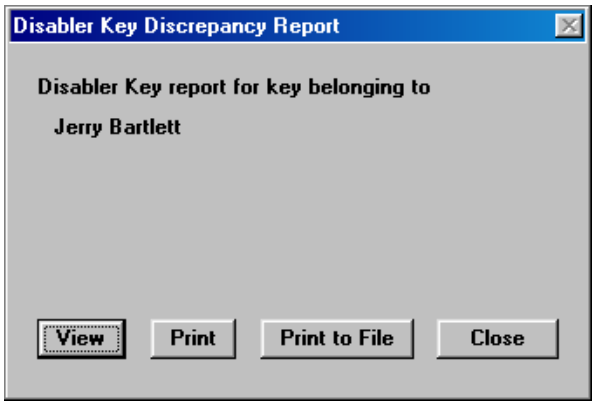
Quantum then prompts you to insert the next Disabler key. To read another key, insert it into the KPU and select ***Ok***. If you have no more keys to read, select ***Cancel***.

Quantum also saves the controller information in a log file. This allows you to collect the information from several Disabler keys and print a report of doors which have been updated, and those for which the user is not yet disabled (see "Listing Controllers", below).

Listing Controllers

Quantum can generate a consolidated report of the controller information from several Disabler keys. Quantum can also cross-reference the controller listings read from Disabler keys with a user's access information to determine for which controllers the user is still potentially authorized. It does so by creating a list of controllers which the user was authorized for prior to using the Disabler key(s), then subtracting the controllers updated by the Disabler key(s).

To use this function, select **Audit | Disabler Key | Discrepancy Report**. Quantum asks you to select a user (see "Selecting a User"). For each user you select, Quantum prompts you for what information to report.



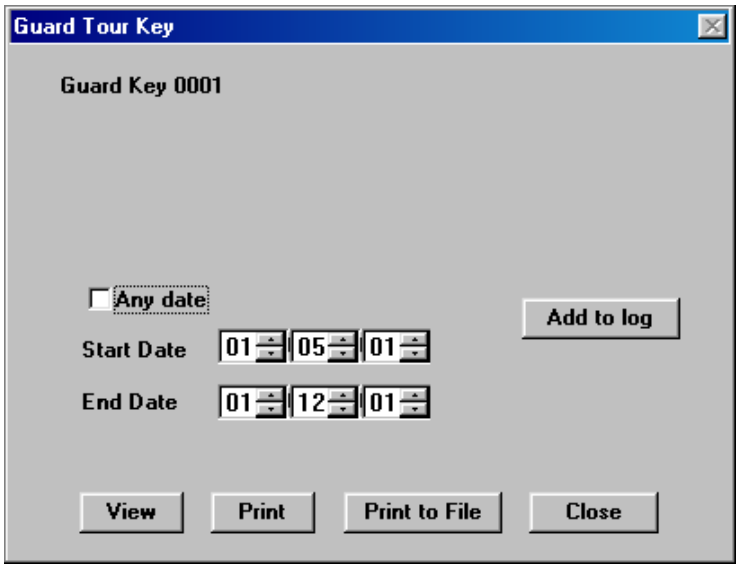
Clearing The Disabler Log

Selecting **Audit | Disabler Key | Clear Disabler Data** allows you to clear all information from the log file created by reading Disabler keys.

Guard Tour Functions

Guard Tour keys record an audit trail of the controllers into which they have been inserted, including the lock number, date, and time. The Guard function will display or print the information contained in a Guard Tour key, and allow you to clear the contents of the key for the next guard tour. See "Creating Special Keys" for a description of how to make and use a Guard Tour key.

Reading a Guard Tour key is almost identical to reading the audit information from a user's key. When you select **Audit | Guard Tour Key**, Quantum prompts you to insert the key into the KPU. When you do so, Quantum reads the tour information from the key, and allows you to specify how you want the information reported.



Select ***View*** to see the report on your screen, or ***Print*** to have the report printed on the currently selected Windows printer.

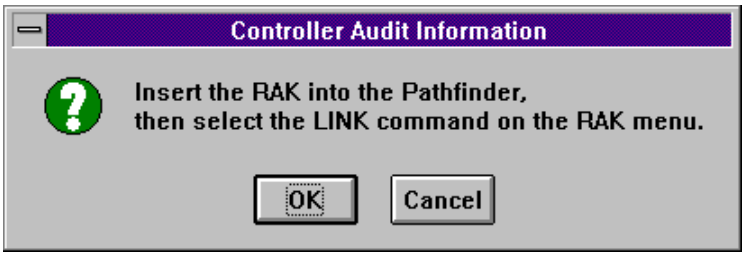
After viewing or printing the information, select ***Cancel***. Quantum will ask you if you want to clear the tour information from the key. Select ***Yes*** to clear it, or ***No*** to leave it intact. Remove the key from the KPU when prompted to do so. If you do not clear the information, the key will append new Guard Tour information to the end of the existing information. This allows a guard to keep a running summary of activities for an entire shift, for example. After the last tour of the night, you can clear the information so that the key is clean for the next night's tours.

Quantum prompts you to insert the next Guard Tour key. To read another key, insert it into the KPU and select ***Ok***. If you have no more keys to read, select ***Cancel***.

Showing History from a RAK

The Restricted Authorization Key has a function which allows it to read and store audit information from several controllers. The **Audit | RAK** function allows you to read this information from the RAK and print or display it. For this function, you must have your KPU connected to the serial channel specified in your hardware setup. The KPU will be used to communicate with the Restricted Authorization Key.

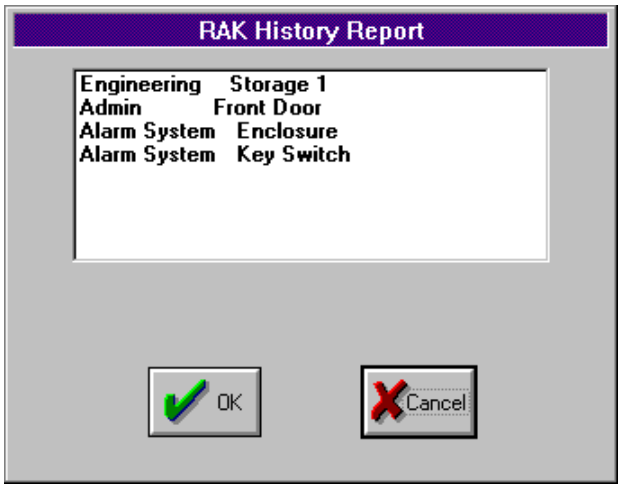
When you activate the RAK function, Quantum prompts you to insert the RAK into the KPU:



Insert the key blade of the RAK into the KPU and turn the RAK on. Select the Link command from the RAK's menu, then immediately select ***Ok*** from the Quantum screen. Quantum will next read the controller audit data from the RAK. While the data is being transferred, Quantum will display an activity box, and the RAK display will indicate the number of history records remaining to be transferred.

When the information transfer is complete, you may remove the RAK from the KPU and optionally delete the RAK's history file. It's usually a good idea to not delete the RAK file until you're sure you have all of the necessary information from it. You can always delete the file the next time you start reading audit trail information from controllers with the RAK.

Quantum will display a listbox showing the names of each controller the RAK had data from.



Select the controller whose history you want to see by double-clicking on the name, or by highlighting the name and selecting ***Ok***. Quantum allows you to specify the type of accesses (legal and/or illegal) and the date range to report on:

The default date range is for the past week; you can adjust the starting or ending dates to change the range. Select ***View*** to see the report on the screen, ***Print*** to print the report on the Windows printer, or ***Print To File*** to save the report as an ASCII file. Select ***Add to Log*** to add the information to the User Activity Log. Select ***Cancel*** when you have generated all the reports you wish for this controller.

Quantum returns to the list of available controller histories. Select another controller to view its audit information, or select ***Cancel*** if you don't want to see any more information.

Reports

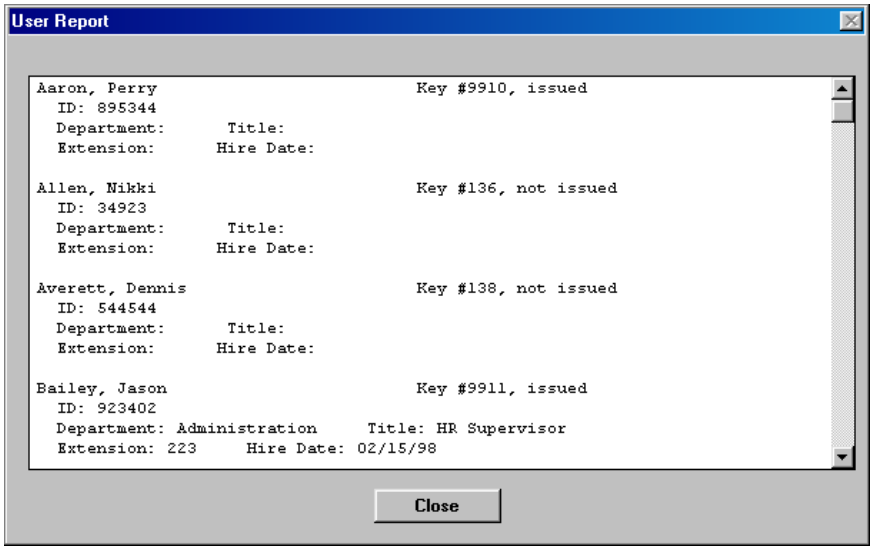
Displaying and Printing Information

The Report menu allows you to generate reports showing information about your users, keys, controllers, and system setup. You may either view the reports on your screen, print them on your printer, or save them as an ASCII file.

Quantum reports do not use any special characters or printer functions, and so should print on just about any PC compatible printer. The reports are formatted to fit on an 8½ x 11" page, with a wide left margin for binding or insertion in a notebook.

While Quantum is generating a report, it displays a progress box to indicate how far along it is in the process. You may cancel the report at any time by selecting the ***Cancel*** button on the progress box, or pressing the **ESC** key.

Reports may be viewed in two ways. The first way is to display the information on your screen. This option is typically activated by selecting the ***View*** button on the screen which defines your report options. Quantum presents a scrollable viewing screen containing the report as follows:



Use the scroll bar at the right hand side of the screen to move forward or backward through the report. Select the ***Ok*** button at the bottom of the screen when you are finished viewing the report.

Reports may also be printed. You can have reports printed by selecting the ***Print*** button on the report options screen. Normally, reports are printed on the currently selected Windows default printer. Refer to your Windows manual for information on selecting the default printer. If you want to print the report to another printer, press the left Shift key while selecting the ***Print*** button. Quantum will present a screen allowing you to select a specific printer. Whichever printer you select, either the default or a specific printer, is referred to in the report descriptions as the "Windows Printer".

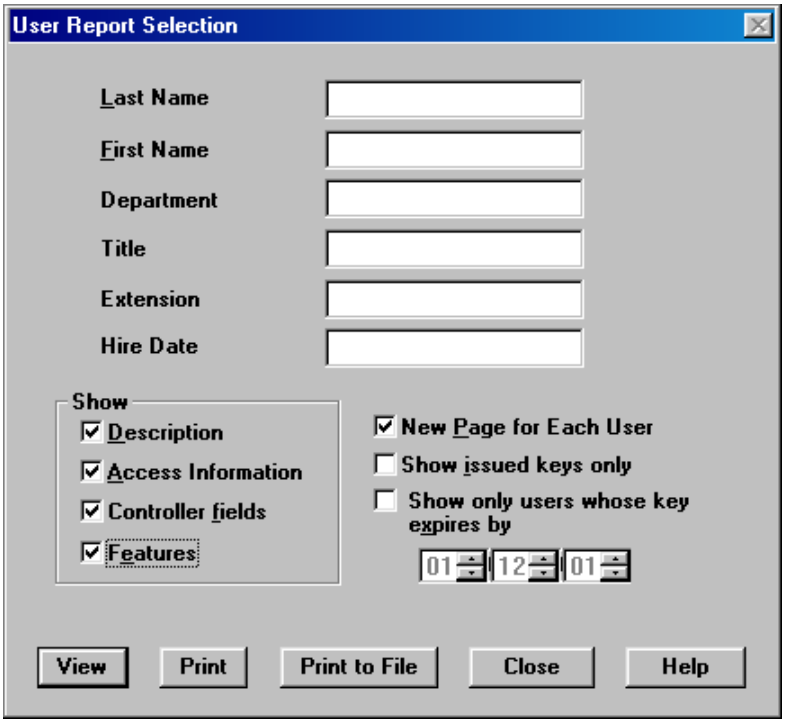
Reports may also be placed into an ASCII file. You can have a report placed into a file by selecting the ***File*** button. Next, assign a file name for the report, or if you are updating the contents of a report, you may reuse the filename that was previously given . If you are uncertain as to where to place the contents of a file, use the ***Browse*** button to select a directory and then apply a filename. Once you are done, select the ***OK*** button. If you are do not want to create another report, select the ***Cancel*** button.

For additional reporting options, see "Audit Operations".

User Reports

The User Reports function allows you to generate reports about your system users, or keyholders.

Selecting User Reports



The User Reports Screen lets you specify which users should be contained in the report, and how much information should be reported for each of them. You can activate this function by selecting **Reports | Users**, and the above illustrated

screen will appear. The first six text fields let you specify which user or users to report on. These correspond to the name and optional data fields entered when adding a user to your system. Quantum will generate a report for users whose database record matches what you enter in these fields. To generate a report on a specific user, enter his first and last names in the appropriate fields.

If you leave a field blank, Quantum matches any record for that field. So, to report on every user in your database, leave all of the fields blank. To report only on users whose last name is Smith, enter "Smith" in the *Last Name* field, and leave the other fields blank. To report on all users whose last name is Smith, and who work in the Maintenance Department (assuming the first optional field contains the user's department) enter "Smith" for the *Last Name*, and "Maintenance" for the first data field.

Quantum will also match partial entries. For example, if you enter "Smith" for the *Last Name*, and "T" for the *First Name,* Quantum will report on all users with the last name Smith and the first initial "T" (Tom Smith, Ted Smith, etc.) If you enter "Sm" for the Last Name, Quantum will report on all users whose last name starts with "Sm" (Smith, Smythe, Smathers, etc.).

The check boxes in the area marked *Show* let you specify how much information to report about each user. If you select *Description*, the user's ID and optional data fields are reported. *Access Information* reports for which controllers the user is authorized, and *Features* reports on how the users' features (holidays, anti-passback, etc.) are configured. Generating a report with none of the boxes checked yields a report containing only the users' names and key numbers.

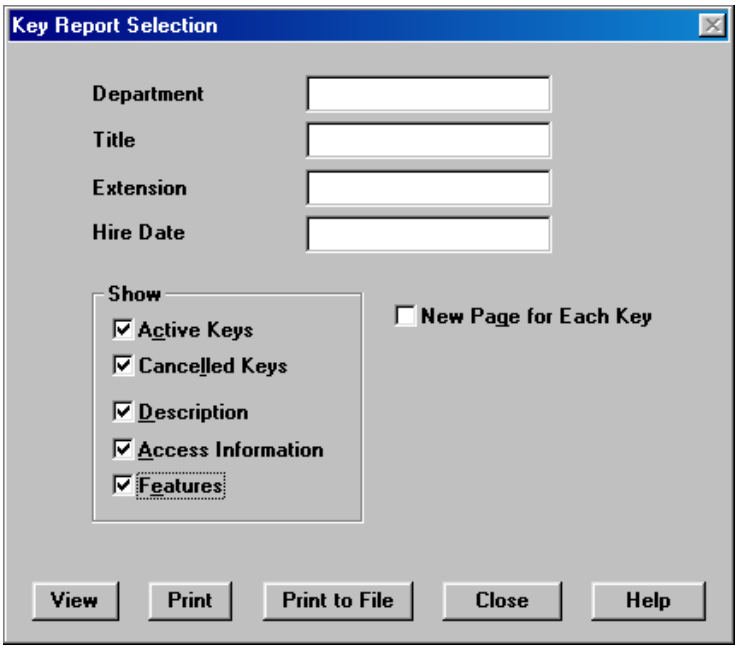
If the *New Page for Each User* check box is checked, Quantum starts the report for each new user on a separate page. This feature comes in handy if you frequently add or change user information, and need to keep an up-to-date printout of each user's information.

Note: Quantum determines whether or not a key will operate a controller based solely on the key's masterkeying information. If the key's copy number is not enabled in the controller, the key will not be able to operate the controller, even though the access report says it should.

Key Reports

The Key Reports function presents the same information as the User Reports, but arranged by key number rather than by user name.

Selecting Key Reports



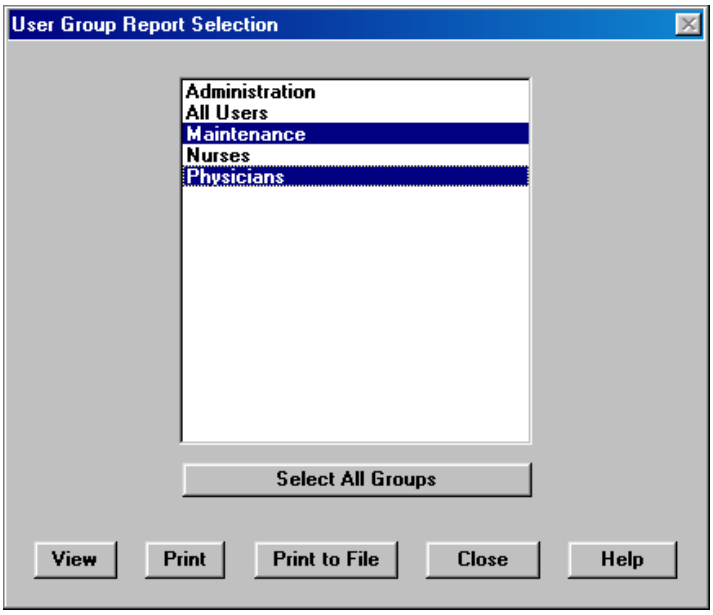
The Key Reports Screen lets you specify which keys should appear on the report. To use this function, select **Reports | Key**, and the above illustrated screen will appear. The four text fields are the same as for the User report - enter the data describing the users whose keys are to be included in the report.

The *Description*, *Access Information*, *Features* and *New Page for Each Key* check boxes also serve the same functions as for the User's Report. The *Active Keys* and *Cancelled Keys* check boxes let you select which types of keys to show in the report. Active keys are those currently in use, or which have not yet been issued. Cancelled keys are those which have been removed from the Quantum system using the Cancel Key function.

User Group Reports

The User Group Report list the members of one or more user groups.

Selecting User Group Reports

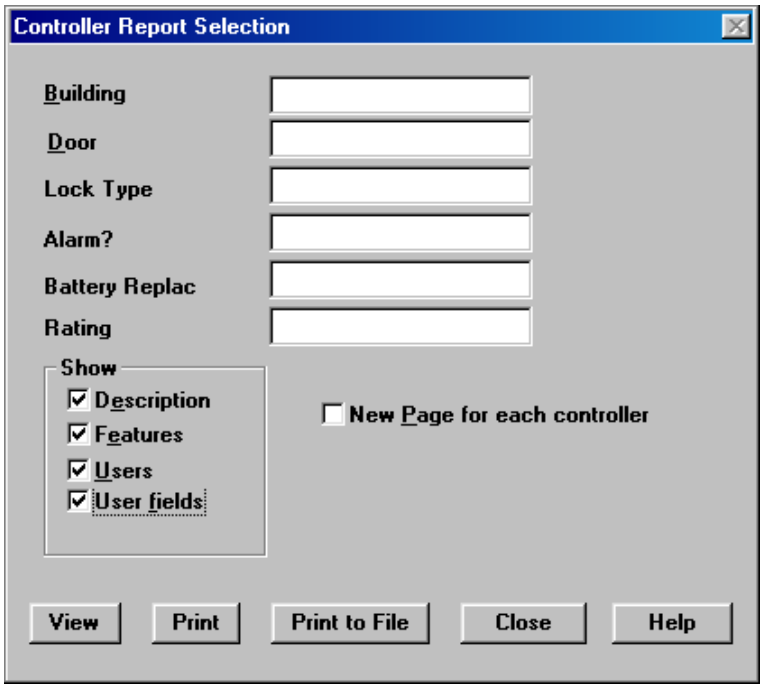


To create User Group Reports, select **Reports | User Groups**, and the above illustrated screen will appear. Select the User Group(s) to report on, then select the appropriate **View**, **Print**, or **Print to File** button.

Controller Reports

Controller reports contain information about your system doors and locks. You can report on feature settings, and list users authorized for each controller.

Selecting Controller Reports



The Controller Reports Screen lets you specify which controllers should be contained in the report, and how much information should be reported for each of them. To use this function, select **Reports | Controllers**, and the above illustrated screen will appear.

The first six text fields let you specify which controller or controllers to report on. These correspond to the Building, Door, and optional data fields entered when adding a controller to your system. Quantum will generate a report for controllers whose database record matches what you enter in these fields. To generate a report on a specific controller, enter the Building and Door names in the appropriate fields.

If you leave a field blank, Quantum matches any record for that field. So, to report on every controller in your database, leave all of the fields blank. To report only on the controllers in the Research Building, enter "Research" in the *Building* field, and leave the other fields blank. To report on all controllers in the Gymnasium which are offices (assuming the second optional field contains the door type) enter "Gym" for the *Building* and "office" for the second data field.

Quantum will also match partial entries. For example, if you enter "Housing" for the *Building*, Quantum will report on all controllers with the first word "Housing" in their name (Housing 1, Housing 2, etc.).

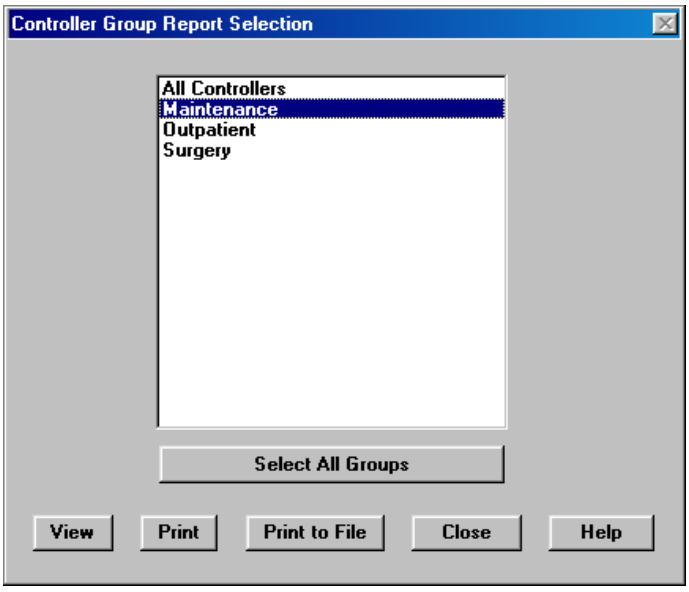
The check boxes in the area marked *Show* let you specify how much information to report about each controller. If you select *Description*, the controller's description and optional data fields are reported. *Features* reports on how the controller's features (operating mode, security settings, etc.) are configured. *Users* reports a list of users authorized for the controllers. Be careful with this setting, as it can generate lengthy reports at large sites. *Keying* reports the controllers masterkeying and copy number information, for the Vertical system. Generating a report with none of the boxes checked yields a report containing only the controller' names and lock numbers.

If the *New Page for Each controller* check box is checked, Quantum starts the report for each new controller on a separate page. This feature comes in handy if you frequently add or change controller information, and need to keep an up-to-date printout of each controller's information.

Controller Group Reports

The Controller Group Report list the members of one or more controller groups.

Selecting Controller Group Reports

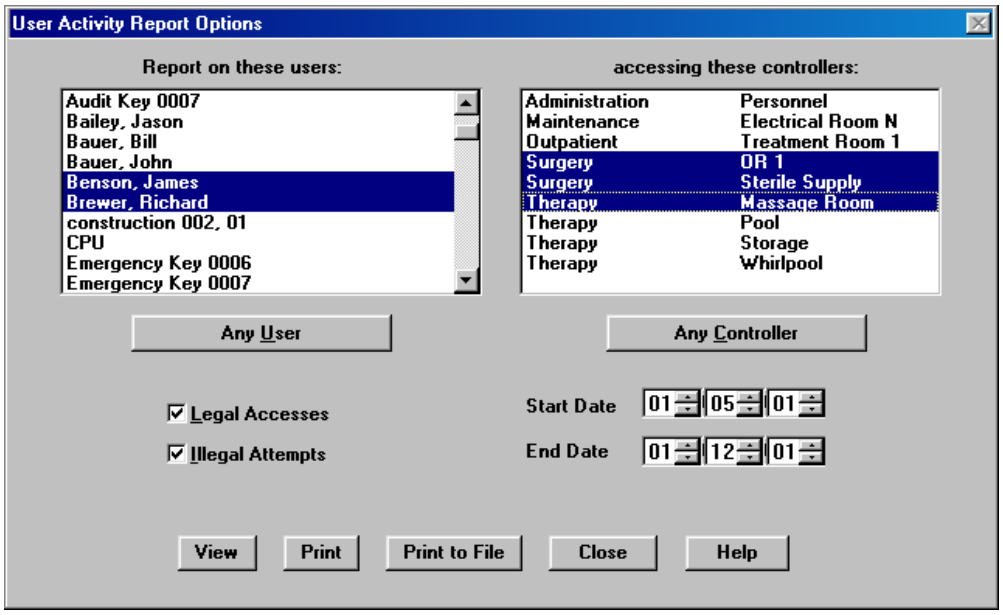


To create Controller Group Reports, select **Reports | Controller Groups**, and the above illustrated screen will appear. Select the Controller Group(s) to report on, then select the appropriate **View**, **Print**, or **Print to File** button.

User Activity Reports

User activity reports summarize the information stored in the Quantum user activity log. This log is updated whenever you select the ***Save*** option on any controller audit or user audit report screen. Quantum stores the audit trial information, including the key, controller, date, and time. The User Activity Report lets you generate a listing of this information by specifying a particular controller and date range.

Selecting User Activity Reports



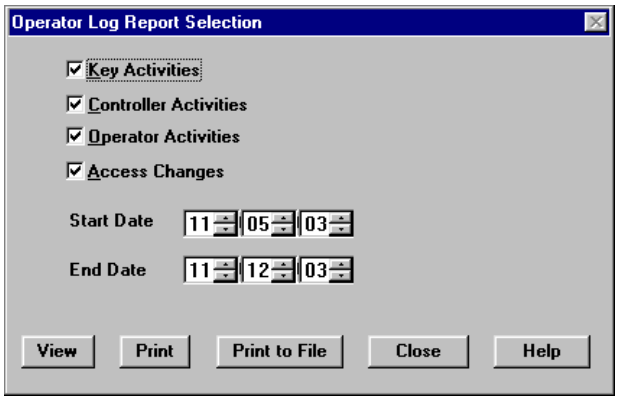
The User Activity Report Screen lets you select the activity information on which to report. To use this function, select **Reports | User Activity Report**, and the above illustrated screen will appear. The two list boxes contain the names of the user and controllers for which audit trail information is available. Select the appropriate entries, specify which records to show (***legal*** and/or ***illegal***) and the date range of interest. Select ***View*** to see the report on your screen, or ***Print*** to send the report to the Windows printer.

Note: You must have something selected in both the *Report on these users* and *accessing these controllers* listboxes to enable the ***View*** and ***Print*** buttons.

Operator Activity Reports

Operator activity reports describe the day-to-day operations performed with the Quantum software. The reports list all activities related to issuing and returning keys, and programming controllers.

Selecting Operator Activity Reports

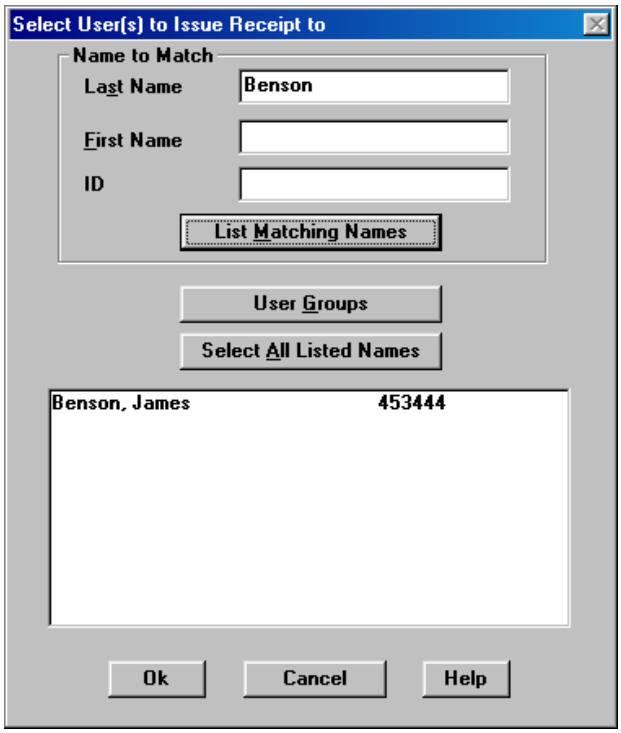


The Operator Activity Reports Screen lets you specify what operator information should be reported. To use this function, select **Reports | Operator Activity**, and the above illustrated screen will appear. Next, select the appropriate category(s) and the date range of interest. Select ***View*** to see the report on your screen, or ***Print*** to send the report to the currently selected Windows printer.

Issue Receipt

The Issue Receipt function will allow you to print an issue receipt for a key that has already been issued. This function is useful if a receipt was not printed when a key was issued to a user.

Selecting Issue Receipt



Utilities

Maintaining the Quantum System

The Utility menu functions allows you to perform various maintenance or "housekeeping" operations associated with your Quantum system:

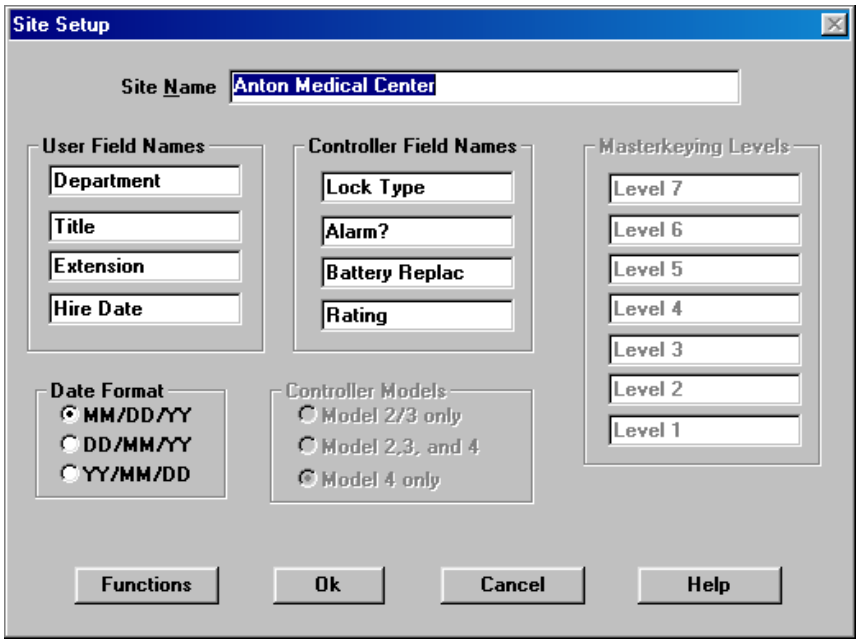
Choice	Function
Site Setup	Specify how your site is configured. See "Site Setup".
Operators	Add, Delete, or Change the configuration of Quantum operators. See "Operators"
Time Zones	Add, Change, Copy, or Delete a time zone definition
Devices	Transfer Site Code information into KPUs and Controller Programming Units
Data Files	Backup, Restore, or Rebuild your Quantum data files
Dates	Update your system level holidays and Daylight Savings Time values
Remote Key Functions	Call a site and connect to a Remote Key Processing Unit. Add, Change, or Delete remote key programming sites.

Site Setup

The **Utility | Site Setup** function allows you to change some of the basic settings about your system.

Site Setup Screen

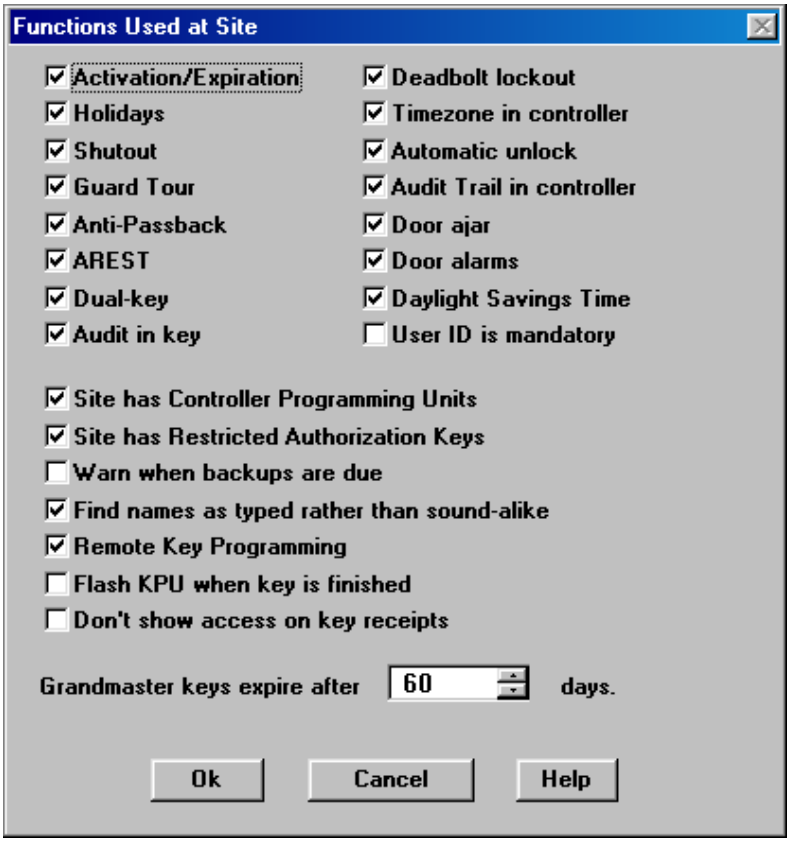
The System Setup screen allows you to change some of the descriptive information about your site.



Field	Function
Site Name	Change the name which appears at the top of the Quantum main window, and on Quantum reports
User Field Names	The names to be used for the 4 site specific user data fields
Controller Field Names	The names to be used for the 4 site specific controller data fields
Masterkeying Levels	The names to be used for the 7 levels of the Vertical keying system. Note that the bottom item is the lowest level, and the top item the highest level. If you are using the Horizontal keying system, this field will be disabled.
Date Format	The format in which dates will be entered and printed on reports
Controller Types	For sites which use a mix of controller types. If you specify that your site uses *Model 2,3, and 4* Quantum will prompt you for the controller type each time you add a new controller. If you are using the Horizontal keying system, this field will be disabled, since the Horizontal system only works with Model 4 controllers.
Functions	Activate the Site Functions Screen to allow you to specify which Quantum functions will be used at this site.

Site Functions Screen

This screen allows you to specify which INTELLIKEY features you use at your site. Only the features actually used will appear on the Key and Controller data entry screens, simplifying setting up your keys and controllers.

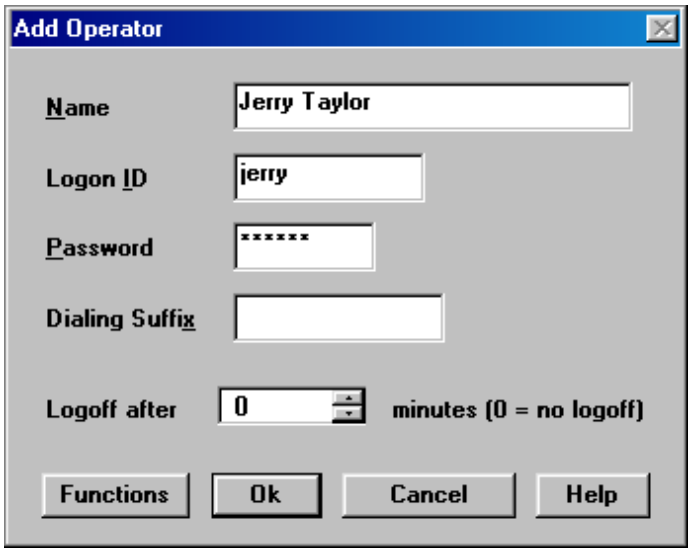


Operators

The Operators option provides the means for adding and deleting Quantum operators, and changing operator passwords. Only operators with the appropriate rights are allowed to add or delete operators, but any operator may change his own password.

Operator Settings Screen

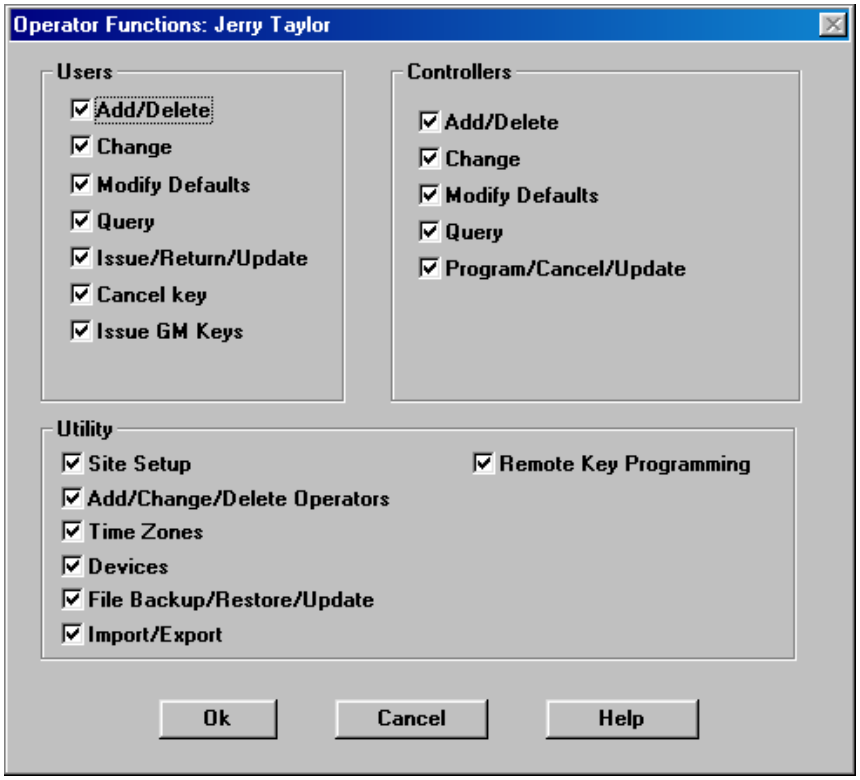
The Operator Settings Screen specifies information about a Quantum operator.



Field	Function
Name	The operator's full name
Logon ID	The code the operator will enter into the Quantum Logon screen. This is 1-9 characters long, and may consist of letters, numbers, and symbols (!@#$%^)
Password	The operator's password. This is 1-6 characters long, and may consist of letters, numbers, and symbols (!@#$%^).
Dialing Suffix	When connecting to a remote key programming site, Quantum will send the text contained in this field to the modem after dialing the remote site. This field could contain a long distance authorization code, for example. This field will be disabled if you have not enabled *Remote Key Programming* on the *Site Functions* screen.
Logoff after … minutes	For extra security, Quantum will automatically log an operator off if there has been no activity for the specified number of minutes. If this value is set to 0, the automatic logoff function is disabled for this operator.
Functions	Selecting this button activates the Operator Functions Screen, which allows you to change the Quantum functions the operator may perform.

Operator Functions Screen

The Operator Functions screen allows you to select which Quantum operations an operator is authorized for. Selecting ***Functions*** from the Operator Settings Screen brings up the Operator Functions screen:



If the checkbox beside the function name is checked, the operator will be allowed to perform it.

To create an operator who does not have access to this screen (i.e. who cannot change his own or any other operator's access rights) uncheck the box marked *Add/Change/Delete Operators.* Note: Make sure that at least one operator has the right to add other operators.

Adding an Operator

The **Utility | Operators | Add** function allows you to add new Quantum operators. Quantum presents the Operator Settings Screen to prompt you for information on the new operator. You must enter the operator's full name, a logon ID code (typically the operator's initials), and the operator's password. The logon ID and password are what the operator will use when logging on. The operator's password will be visible as you are typing it, so make sure no one is watching what you type. This is to allow you to verify that you are entering the data correctly. Later, when the operator enters the password as part of the logon process, the password will not be visible on the screen.

You should also select the communication channels (COM1 - COM4) which the operator will use to communicate with the Key and Controller Programming Units, and with the remote Key Programming modem, if the site uses this feature . If this is the only PC used to run Quantum, these channels will be the same as those used by the System Manager. If Quantum is being run on several PC's (on a LAN, for example), each PC might have a different communications setup.

Next, you should select the ***Functions*** button to choose the Quantum functions for which this operator will be authorized. This activates the Operator Functions Screen

to let you select which functions the new operator will be allowed to perform. If you uncheck the box marked *Add/Change/Delete Operators* on the Operator Function screen, the new operator will be able to change his password and communications settings, but will not be able to change his access rights.

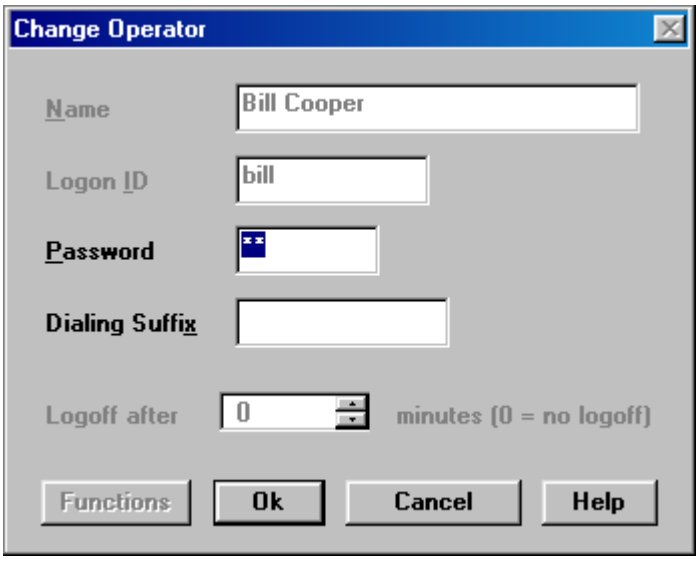
Changing an Operator's Settings

The **Utility | Operators | Change** function allows you to change the information associated with an operator. An operator must be authorized to add and delete operators (*Add/Delete/Change Operators* on the Operator function screen). Quantum first presents a list of system operators for you to select from:

Select the operator whose information you wish to change, then select ***OK***. Quantum presents the Operator Settings Screen to allow you to change the operators settings and functions.

Changing an Operator's Password and Port Settings

If you are the current Quantum operator, and do not have full Operator Add or Change authorization, you may still change your password and communications port settings. To do so, select **Utility | Operators | Change**. Quantum displays the Operator Settings screen, with most of the fields disabled:



You will be able to change your password and the settings associated with your programming equipment, but nothing else.

Deleting a Operator

If you are authorized to add and delete operators (Add, Delete and Change Operators on the Operator function screen), the **Utility | Operators | Delete** function allows you to delete operators from the system. Quantum first presents you with the list of system operators to select from.

To delete a operator, select the operator from the list, then select ***OK***. Quantum will display the operator's name and ask you to verify that you really want to delete the operator. Select ***Yes*** to delete the operator, ***No*** to leave the operator on the system.

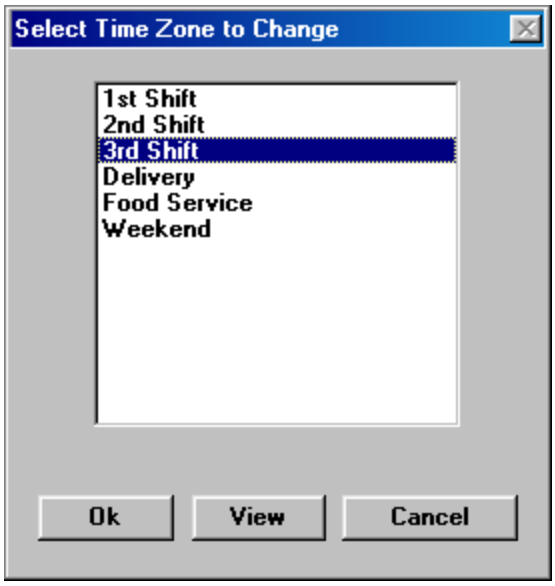
There must always be at least one operator defined for the Quantum system. Thus, Quantum will not allow you to delete the last operator.

Time Zones

This function lets you set up and modify the time zone information for your Quantum system. Time Zones are used for several functions - controlling access by users, controlling access to doors, and for automatically unlocking doors.

Selecting a Time Zone

For all operations which require you to select a time zone, Quantum displays a selection screen:



You may select the appropriate time zone by double-clicking on its name, or by highlighting it in the list, then selecting ***Ok***. To see what the settings are in a time zone, select it by single-clicking on its name, then select ***View***. Quantum will display the Time Zone Screen to allow you to view the settings. You will not be able to change any settings.

When Quantum is first installed, it creates one Time Zone configuration, named "Time Zone 1".

Adding Time Zones

To add a Time Zone , select **Utility | Time Zones | Add**. Quantum will present an empty Time Zone Screen for which you must supply a name and the time zone information. You should give the time zone a meaningful name, such as "Office Hours", or "Third Shift". You may not have two time zones with the same name.

If the time zone you are creating is similar to an existing one, you may copy the existing time zone and change only the appropriate information for the new time zone. See "Copying Controller Defaults" below.

Changing Time Zones

You may change the settings for a Time Zone by selecting **Utility | Time Zones | Change**. Quantum prompts you to select the time zone to change, then presents you with the Time Zone Screen to allow you to set the values for the new time zone. You may change any of the settings here, including the name of the time zone.

If you change the time zone information, Quantum will ask you if you want to update the keys and controllers which use that time zone. Select ***Yes*** to have the new information transferred into the database records for the keys and controllers.

Copying Time Zones

If you want to create a time zone which is similar to an existing one, you may copy the existing time zone and change only the appropriate information for the new time zone. Select **Utility | Time Zones | Copy**, select the existing time zone, then enter

a name for the new time zone. Quantum then presents the Time Zone Screen to allow you to make the changes necessary for the new time zone.

Deleting Time Zones

To delete a user configuration, select **Utility | Time Zones | Delete**, and select the time zone to be deleted followed by the ***OK*** button. If you don't want to delete a time zone, select the ***Cancel*** button.

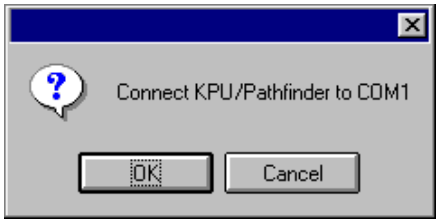
Reprogramming Devices

The **Utility Devices** option allows you to initialize KPUs, Controller Programming Units, and Restricted Authorization Keys for use at your site. Initializing a device loads it with the appropriate site code and authorizes it to create new keys or controllers.

To initialize devices, select **Utility | Devices | Program KPU, CPU, RAK**. Quantum will ask you if you want to program each type of device. The steps for programming each device are described below.

Programming the KPU

Quantum first prompts you to connect the KPU to be programmed to the proper serial channel.

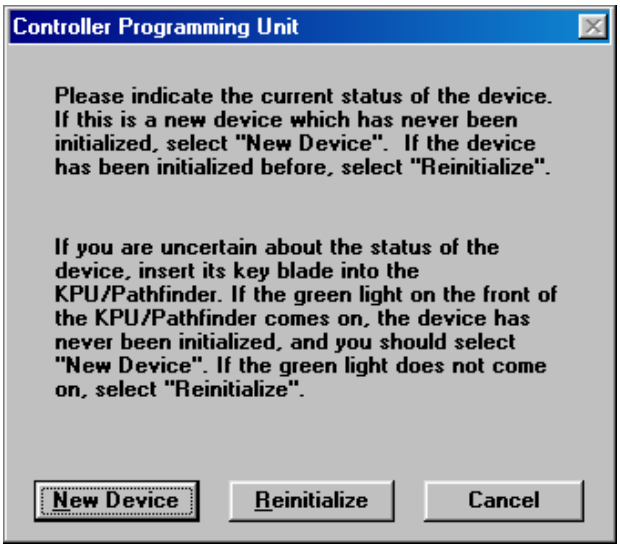


Make sure the KPU is connected, then select ***Ok***. Quantum verifies that the KPU is connected properly, then reprograms it.

Programming the Controller Programming Unit

Controller Programming Units are programmed through the KPU. The programming sequence for Controller Programming Units depends on the state of the CPU - programmed one or more times, or never programmed. CPU's received from the factory have never been programmed.

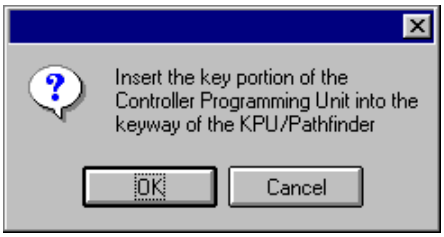
Quantum first asks you about the status of the Controller Programming Unit, in order to determine the proper programming sequence.



You can determine the status of the Controller Programming Unit by inserting its keyblade into the keyway of the KPU (the power to the KPU must be plugged in). If the green light on the front of the KPU comes on, the CPU has never been programmed, so you should select ***New Device***. If the KPU light does not come on, the CPU has been programmed at least once, so you should select ***Reinitialize***.

Programming a New CPU

If you select ***New Device***, Quantum next prompts you to insert the CPU into the KPU.



Insert the keyblade of the CPU into the keyway of the KPU, make sure that the KPU is connected to the serial port specified in your operator setup, then select ***Ok***. Quantum then programs the Controller Programming Unit.

Reprogramming a CPU

If you select ***Reinitialize***, Quantum asks you to insert the keyblade of the CPU into the keyway of the KPU, then connect the CPU to the serial port specified in your operator setup. When you have done so, select ***Ok***. The green light on the front of the KPU should be lit. Next, Quantum asks you to connect the KPU to its assigned serial channel.

If you have configured your Quantum system to have both the KPU and CPU use the same serial channel, disconnect the CPU from the serial channel, but do not remove it from the KPU keyway. Connect the KPU to the channel, verify that the green light is still on, then select ***Ok***. Quantum will then program the CPU.

Programming the RAK

Restricted Authorization Keys are programmed through the KPU. The programming sequence for RAKs depend on the state of the RAK - programmed one or more times, or never programmed. RAKs received from the factory have never been programmed.

Quantum first asks you about the status of the RAK, in order to determine the proper programming sequence.

You can determine the status of the RAK by inserting its keyblade into the keyway of the KPU (the power to the KPU must be plugged in). If the green light on the front of the KPU comes on, the RAK has never been programmed, so you should select ***New Device***. If the KPU light does not come on, the RAK has been programmed at least once, so you should select ***Reinitialize***.

Programming a New RAK

If you select New Device, Quantum next prompts you to insert the RAK into the KPU.

Insert the keyblade of the RAK into the keyway of the KPU, make sure that the KPU is connected to the serial port specified in your operator setup, then select Ok. Quantum then programs the RAK.

Reprogramming a RAK

If you select Reinitialize, Quantum asks you to insert the keyblade of the RAK into the keyway of the KPU.

Turn on the RAK, and select the LINK command from the RAK's main menu. The green light on the front of the KPU should come on. Select Ok to reprogram the RAK. You must select Ok within 10 seconds of selecting the RAK LINK command, otherwise the RAK will assume that it was unable to communicate with the KPU, and will break the link between them. The green light on the KPU will go out if this happens, and you must remove the RAK from the KPU and restart the reprogramming sequence.

Disabling CPU's and RAK's

For security reasons, it is often desirable to disable Controller Programming Units and Restricted Authorization Keys when they are not in use. Disabling these devices removes their site code, and prevents their use. The devices can be reenabled by initializing them as described in "Reprogramming Devices".

Once a device is disabled, you don't need to disable it again. To determine if a CPU or RAK is disabled, insert its key blade into a KPU which has power connected. If the green light on the front of the KPU comes on, the CPU or RAK is already disabled.

To disable CPU's select **Utility | Devices | Disable CPU**. To disable RAK's select **Utility | Devices | Disable RAK**. Quantum will prompt you for each step in the process.

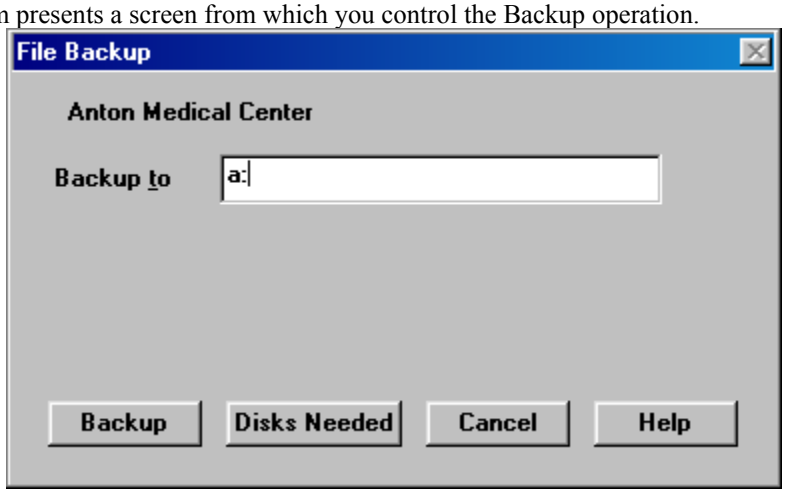
Data Files

Backing Up Your Data

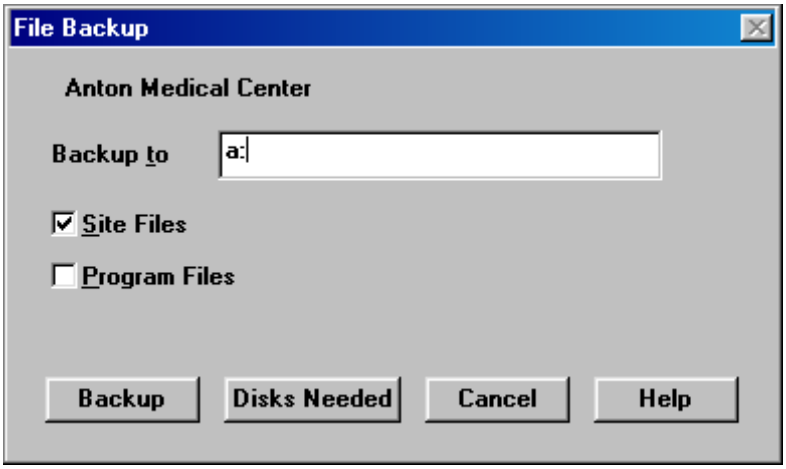
The Backup feature allows you to save a copy of all of your Quantum files on floppy disks. This copy can be used to restore your database files in the event of hardware problems with your PC, or accidental deletion of critical information. The backup copy should be kept in a secure place, preferably at a different location from the PC running Quantum. Ideally, the backup copy should be kept with a copy of the Quantum program disks, to facilitate the file restore operation. The process for restoring backed up files is described in the next section.

You should backup your files as often as necessary to prevent losing important information. If you do frequent data entry or key issuing, you should backup files at least once a week. Quantum "remembers" the date of your most recent backup, and reminds you if 3 weeks have elapsed since your last backup. You may disable the reminder feature by unchecking the box labeled *Warn when backups are due* on the Site Functions Screen.

To make a backup copy of your files, select **Utility | Data Files | Backup**. Quantum presents a screen from which you control the Backup operation.



End-User Quantum



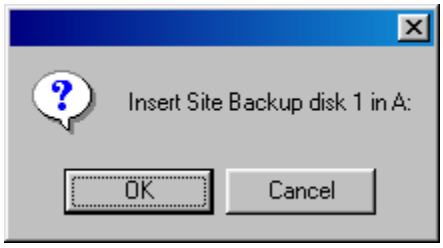
Dealer Quantum

Field	Function
Backup to	Specify the path to which to write the backup files. This can be a floppy drive (a: or b:), a directory on your hard drive, or a directory on a network drive.
Site Files	If this box is checked, the backup operation will make a backup copy of the data files for the currently selected site. (The end-user version of Quantum automatically backs up site files)
Program Files	If this box is checked, the backup operation will make a copy of your Quantum program files. (The end-user version of Quantum automatically backs up program files).
Backup	Start the file backup operation
Disks Needed	Display the number of floppy disks which will be needed for the backup operation
Cancel	Exit without performing a backup

If you are backing up your files to floppy disk, you should first select ***Disks Needed*** to determine how many floppy disks you will need for the backup operation. Note that you must have formatted floppy disks available. If you do not

have the required number of formatted disks, Cancel the backup operation by selecting ***Done***, then activate *My Computer* to format the necessary disks. Refer to your Windows manual for instructions on how to format a disk.

When you select the ***Backup*** button, Quantum begins the backup process. If you are backing up to a floppy disk, Quantum prompts for a disk to be inserted in the selected drive.



Insert a formatted floppy in the drive, then select ***Ok*** to proceed with the Backup operation. Quantum will prompt for each successive disk as required. If the backup operation requires more than one floppy, label the disks by number, as indicated in Quantum's prompts.

If you are using the Dealer version, Quantum will perform separate backup operations for your data and program files, depending on which options you selected.

You may reuse backup disks without reformatting. Quantum first checks for an old copy of the backup information on the floppy before copying new information. If Quantum finds an old backup file, it deletes the old information before writing the new information. It is good practice to alternate between two sets of backup disks.

The backup files are stored in a proprietary format which can be retrieved only by using the File Restore operation described in the next section.

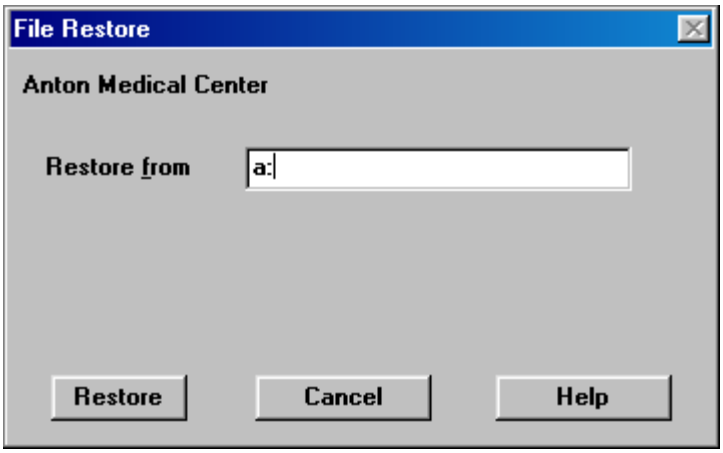
Restoring Files from a Backup

The Restore operation copies files saved with the Backup operation from the floppies to your hard drive. This allows you to rebuild your Quantum System in the event of a hard disk failure, or if you accidentally delete important information from your files.

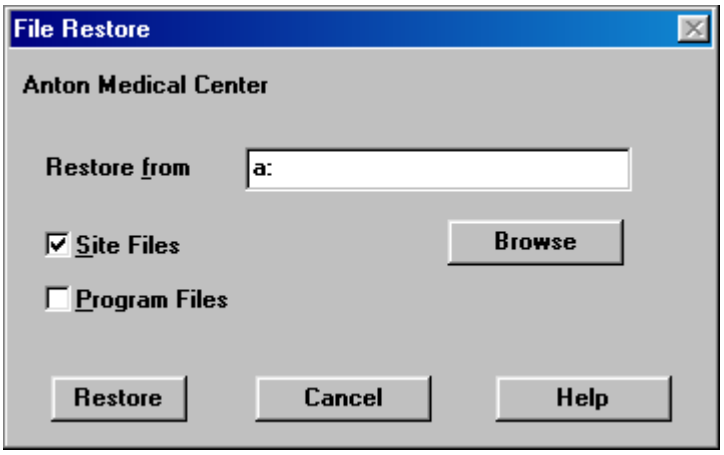
Note: The File Restore operation overwrites any existing data files, so it should be used with caution.

Restoring Data Files

To restore files from a backup copy, select **Utility | Data Files | Restore**. Quantum presents a screen from which you may control the Restore operation.



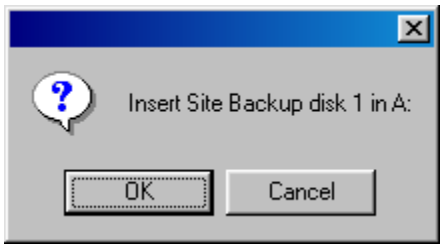
End-User Quantum



Dealer Quantum

Field	Function
Restore from	Specify the path to the backup files. This can be a floppy drive (a: or b:), a directory on your hard drive, or a directory on a network.
Site Files	If this box is checked, Quantum will restore the data files for the currently selected site. (The end-user version of Quantum automatically restores site files)
Program Files	If this box is checked, Quantum will restore your Quantum program files -- operator settings, dealer default settings, etc. (The end-user version of Quantum automatically restores program files)
Restore	Initiate the File Restore operation
Cancel	Exit without restoring files

When you select the ***Restore*** button, Quantum starts the restore process. If you are restoring from floppy disks, Quantum prompts you to insert the first disk in the backup set:



Insert the disk, and select ***Ok***. Quantum verifies that the proper disk has been inserted, then copies the saved files to your Quantum directory, overwriting any versions of the files already there. If more than one floppy was required for the backup, Quantum will prompt for each in turn.

If you are using the Dealer version, Quantum will perform separate restore operations for your data and program files, depending on which options you selected.

Rebuilding Data Files

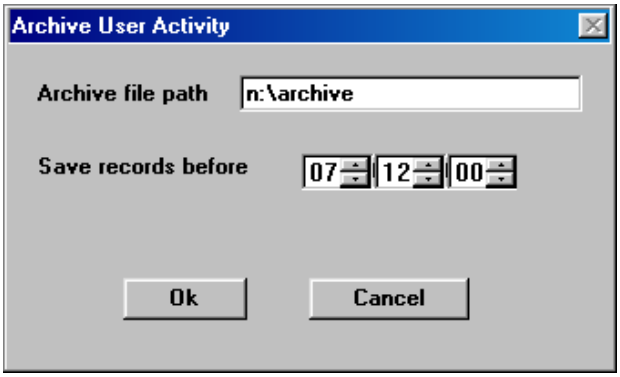
Unexpected events such as power failures or hard disk crashes can cause the data in Quantum's files to become scrambled or confused. The **Utility | Data Files | Rebuild** function reconstructs Quantum's data files.

Archiving Data

Quantum maintains two log files which chronicle events occurring in your system - the Operator Activity Log and the User Activity Log. The Operator Activity Log tracks events such as adding users, issuing keys, programming controllers, etc. Quantum automatically adds entries to this log as the events occur. The User Activity Log tracks user access in doors - legal and illegal. Any function which reads audit information from a key or controller can add the information to the User Activity Log.

Both of these logs accumulate data, and can become very large. This not only takes up disk space, but can result in long delays in generating reports based on the logs. Quantum provides functions for copying the information in the logs to a backup medium, such as a floppy disk, then deleting the information from the log. This ensures that the log files contain only the most recent information. Quantum also provides functions for reloading the information from the backup files back into the log, in the event that you need to review the older information.

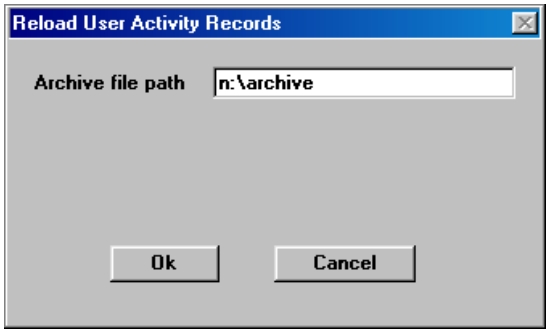
To archive one of the log files, select **Utility | Data Files | User Activity Log | Archive/purge data** or **Utility | Data Files | Operator Log| Archive/purge data** . Quantum prompts you for where to place the archive (backup) file, and how much information to delete.



Enter the location for the backup file in the *Archive file path* field. This may be either a floppy drive (a: or b:), or a hard drive. If there is already an archive file at the specified location, Quantum will append the new data to it; otherwise, Quantum creates a new archive file. To save data before a specific date, set the *Save records before* field to the appropriate date. By default, Quantum supplies the date of the most recent archive.

When you select Ok, Quantum copies all records prior to the specified date, then deletes the records from the log. If you specified a floppy disk to hold the archive data, Quantum prompts you whenever it needs a new disk inserted. If the archive data won't fit on a single disk, Quantum automatically continues it on other disks. As each disk is complete, Quantum displays the date range for the records contained on the disk. You should copy this information onto the disk label in case you need to reload a specific period back into the log at a later date.

To reload data from an archive back into the log, select either **Utility | Data Files | User Activity Log | Restore data** or **Utility | Data Files | Operator Log | Restore data.** Quantum prompts you for the location of the archive file.



By default, Quantum supplies the location you selected for the most recent archive. When you select Ok, Quantum reads the data from the archive file and reloads it into the log file (if it isn't already there).

If the archive covers several floppy disks, you must reload each one separately.

System Dates

The Utility Dates functions allow you to set your system-level holidays and Daylight Savings Time adjustment values. These are the values which are automatically used

for new and updated keys and controllers. This feature allows you to set these values one time, once a year, and have them take effect for everyone.

Holidays

When you select **Utility | Dates | Holidays**, Quantum presents the Holiday Screen to allow you to set up the holiday dates for use by the system. These are the default dates that will be applied to both keys and users. Holidays in keys restrict access during the holiday periods. Holidays in controllers override the automatic unlock function.

Daylight Savings Time

When you select **Utility | Dates | Daylight Savings Time**, Quantum presents the Daylight Savings Time Screen to allow you to set up the system level DST adjustment dates. These are the default values which will be applied to all controllers.

The Dealer Version

Dealer Requirements

As mentioned earlier, the Quantum software is available in two versions, the *End-User* version for sites which will handle all of their key and lock control, and the *Dealer* version. The Dealer version provides INTELLIKEY dealers with the functions needed to support multiple INTELLIKEY sites. Often these sites will initially have only a few INTELLIKEY controllers and keys. In many cases, it is difficult for the customer to justify the additional overhead of programming devices and software to maintain their system.

In these situations, the dealer needs a way to provide key and controller programming services for several sites. Dealer Quantum sets up data files for a number of customer sites, and allows you to specify a particular customer whose controller and key programming information you wish to work with. This customer is your "current customer", or "current site". When you change controller or user information, you are changing information for the current customer only; none of your other customers' data files are affected.

The Dealer Quantum also allows you to reconfigure your KPU, CPU, and RAK to match the current customer's keys and controllers. This means you only need one set of programming equipment to service any number of customers.

Differences Between the Versions

The End-User and dealer Quantum software packages function identically. The main difference is that the dealer version contains an extra menu item listing the extra functions needed for selecting between customers.

The extra menu functions are described in separate sections, below. Quantum features which differ with the Dealer version are:

Directory Structure

Quantum uses two types of files, *program* files and *data* files. *Program* files are the files which determine how Quantum operates - these include such things as the operator information (passwords and authorizations). *Data* files contain the information about the site -- key and controller information, site name, field names, etc.

The End-User Quantum software creates a single directory on your hard drive to contain all of the Quantum program and data files. The Dealer version creates one directory to hold the Quantum program files, then creates separate directories for the data files for each site. Quantum keeps track of which sites are contained in which directories, freeing you from this chore.

Reports

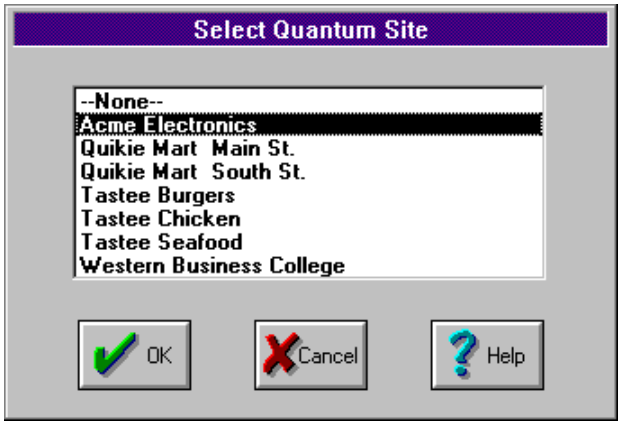
Reports contain information from the data files of the currently selected site. The Quantum Report function is described under "Reports".

File Backup

With the Dealer version, you can back up and restore the data files for the current site, and you may backup your Quantum program files separately. The Backup and Restore functions are described under "Utilities".

Selecting a Site to Work With

The Select Site function allows you to specify the site whose data you wish to use. When you select **Dealer | Select Site**, Quantum displays a listbox showing all of your sites.



Select the desired site by either double-clicking on its name, or pressing the **Tab** key until the name is selected, then selecting ***Ok***. The selected site becomes your current site, and its name will be displayed at the top of the Quantum window. You will be working with this customer's database files for adding or changing controller and key information.

Note: Be sure you have the correct site selected. The Quantum software treats all sites equally. Since keystamp and lockstamp numbers are assigned independently from site to site, it is very likely that you will have more than one site with the same keystamp and lockstamp numbers, and possibly the same keyholder names and identification codes. If you issue a key to a keyholder from Site A, but have the database files for Site B selected, the key will contain the site code and keying information for Site B, and will not work at Site A. Similarly, if you return a Site B key with Site A selected, Quantum will locate the key, by its keystamp number, in the Site A database, and log the key as returned by the wrong keyholder.

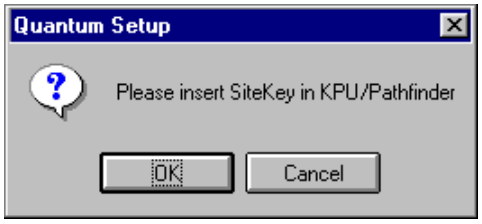
Adding a Site

Quantum provides two methods of adding sites to your Dealer system.

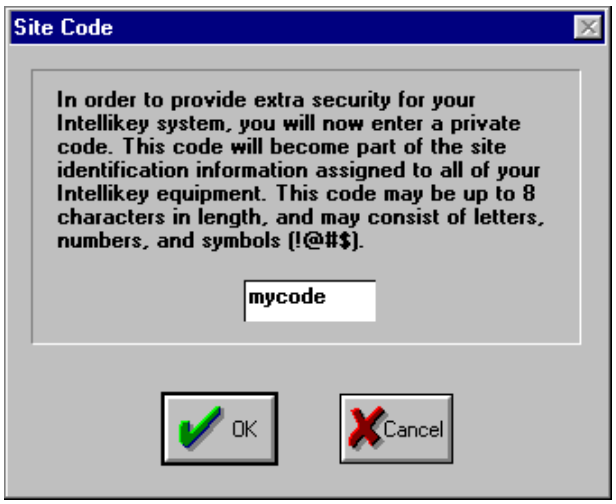
Creating a New Site

The New Site function lets you create a site completely from scratch. The site will contain no user or controller information. The basic site information, such as names for the extra key and controller fields, will come from your Dealer Site Defaults (see below).

Select **Dealer | Create Site | New Site** to create a new site. Quantum first asks you to insert a SiteCode Key into the KPU.

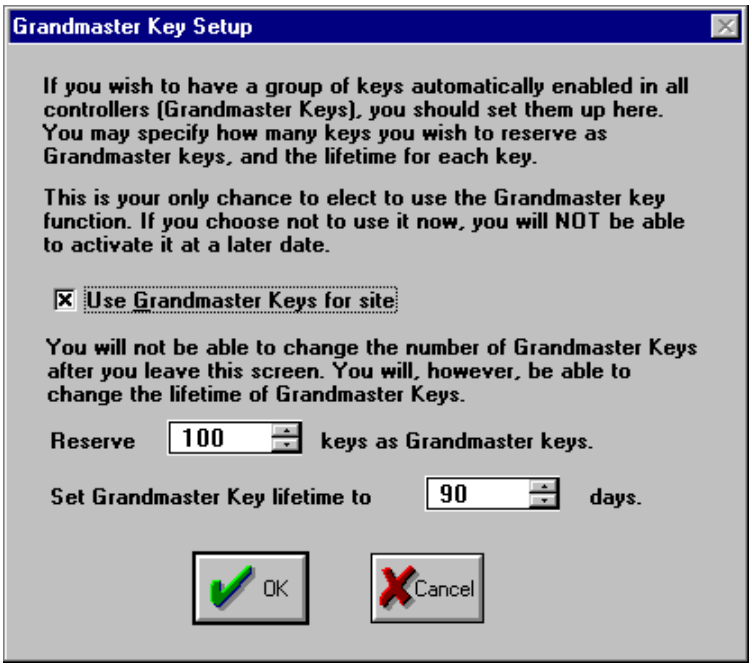


From this SiteCode Key, Quantum will read the site code for the new site. Insert the key, then select ***Ok***. Quantum reads the Site Code information from the key, then asks you to provide the last level of information for the Site Code:



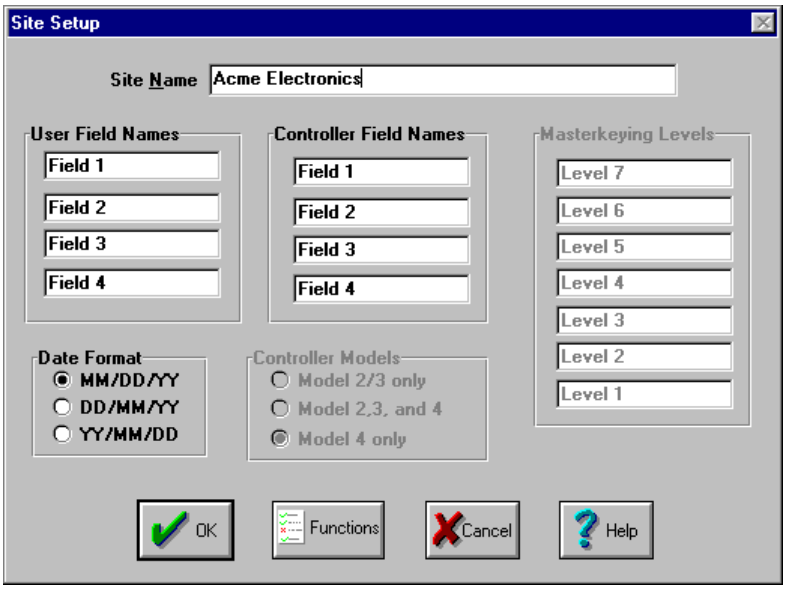
This allows you to create a Site Code whose full contents are known only to you. This prevents anyone else from creating keys which are able to access this site. Enter a code, up to 8 characters long, then select ***Ok***.

Quantum next asks if you want to use the "Grandmaster Key" feature. Grandmaster Keys are automatically enabled in all controllers, and would typically be issued to security or maintenance personnel. You must elect to use the Grandmaster Key function, and select how many keys to reserve as Grandmaster Keys now - **you won't be able to change these settings later**.



This screen allows to reserve a fixed number of keys to be Grandmaster Keys. The default is 100, but you can adjust the number based on your site requirements. Grandmaster Keys also have a limited lifetime, in case they are lost. You can set the initial lifetime here, and change it later using the Site Functions screen.

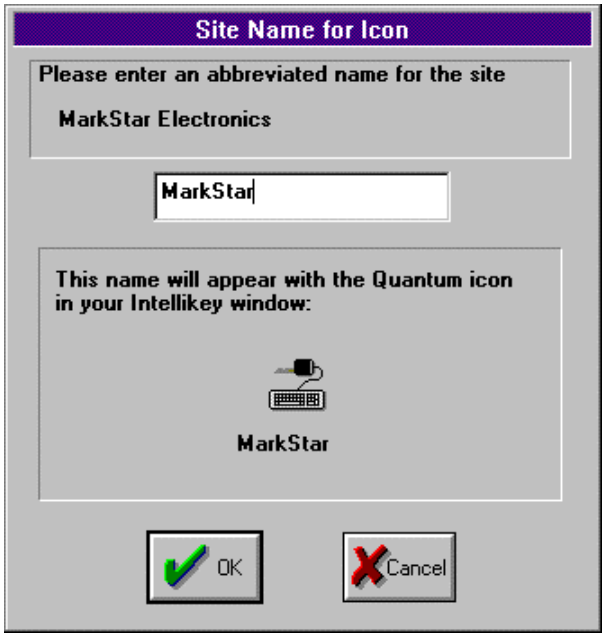
Quantum next presents the Site Setup Screen to allow you to customize settings for the site.



Make any changes as needed to the default information. You must, as a minimum, enter a site name. You should also select the ***Functions*** button and make sure the functions used at the site are enabled. Select ***Ok*** when you are finished.

Quantum next creates the empty data files for the site.

Quantum next asks you for a label to assign to the Windows icon for the site. Creating a site icon allows you to start Quantum with the site already selected. This saves the step of having to select the site after starting Quantum. The label should typically be an abbreviated form of the site name.



Quantum will create an icon in your **INTELLIKEY** program group, consisting of the Quantum logo, and the name you supplied. Clicking on this icon will start

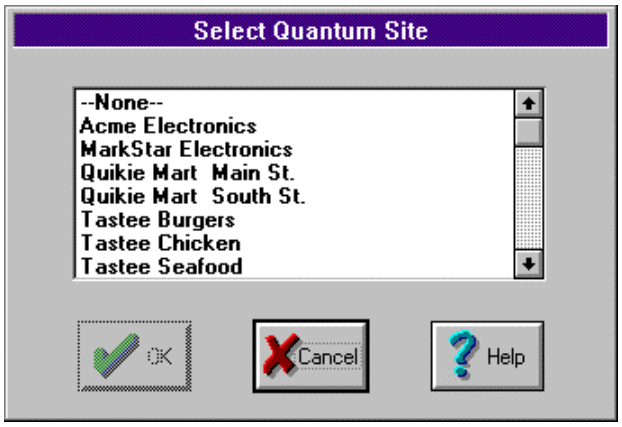
Quantum with the site already selected. Note, however, that there may be only one copy of Quantum running on a PC at a time; if you select another site icon while Quantum is already running, Windows will display the currently running copy of Quantum, with the current site, not the newly selected site.

After creating the new site, Quantum makes it the current site, and offers to initialize any programming equipment (KPU, CPU, and RAK) with the new Site Code, so you may begin operations on the site immediately.

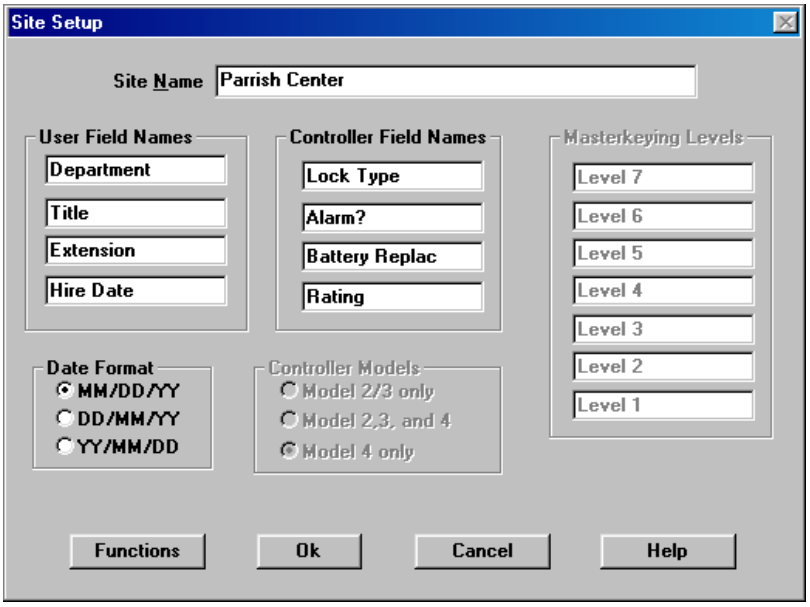
Copying an Existing Site

Sometimes it is useful to create a new site by copying an existing one. You would use this function, for example, to create a site to use as a *template,* or pattern for creating other sites. You might create a site consisting of 5 doors and 20 users, with all users authorized in all doors. If you need to create a new site with a similar number of keys and doors, you could copy the template site to a new site, then just make the changes to the new site.

Select **Dealer | Create Site | Copy Site** to copy an existing site. Quantum asks you which site to copy.

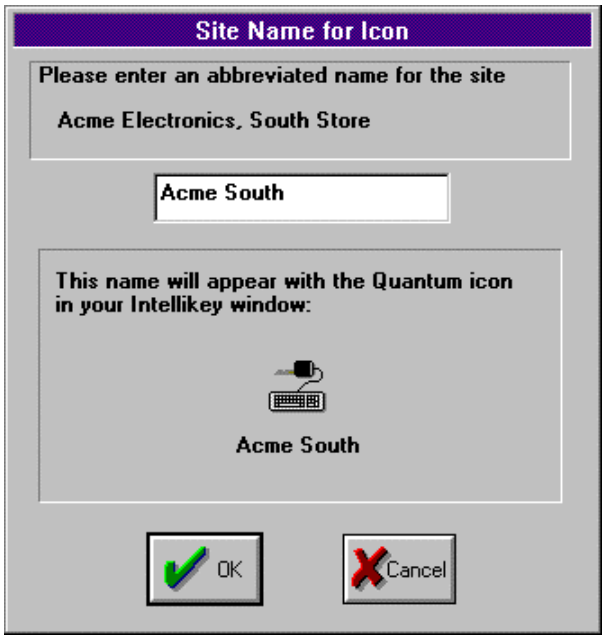


Select the original site by either doubling-clicking on its name, or by using the **Tab** key to highlight the name, and selecting ***Ok***. Quantum next asks you to insert a SiteCode Key, to provide the site code for the new site. Insert the key, then select ***Ok***. Quantum next presents the Site Setup Screen to allow you to change the settings for the new site.



As a minimum, you must supply a unique name for the new site. When you select ***Ok***, Quantum copies the site files from the original site to the new site.

Quantum next asks you for a label to assign to the Windows icon for the site. Creating a site icon allows you to start Quantum with the site already selected. This saves the step of having to select the site after starting Quantum. The label should typically be an abbreviated form of the site name.

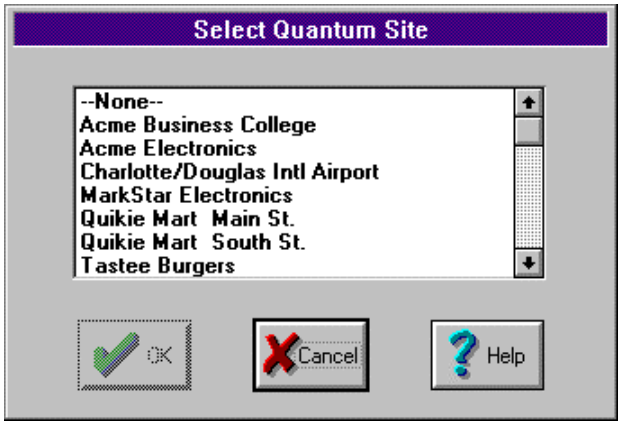


Quantum will create an icon in your **INTELLIKEY** program group, consisting of the Quantum logo, and the name you supplied. Clicking on this icon will start Quantum with the site already selected. Note, however, that there may be only one copy of Quantum running on a PC at a time; if you select another site icon while Quantum is already running, Windows will display the currently running copy of Quantum, with the current site, not the newly selected site.

After creating the new site, Quantum makes it the current site, and offers to initialize any programming equipment (KPU, CPU, and RAK) with the new Site Code, so you may begin operations on the site immediately.

Deleting a Site

If you no longer support a site, you may delete it from your system. To do so, select **Dealer | Delete Site**. Quantum asks you which site to delete.

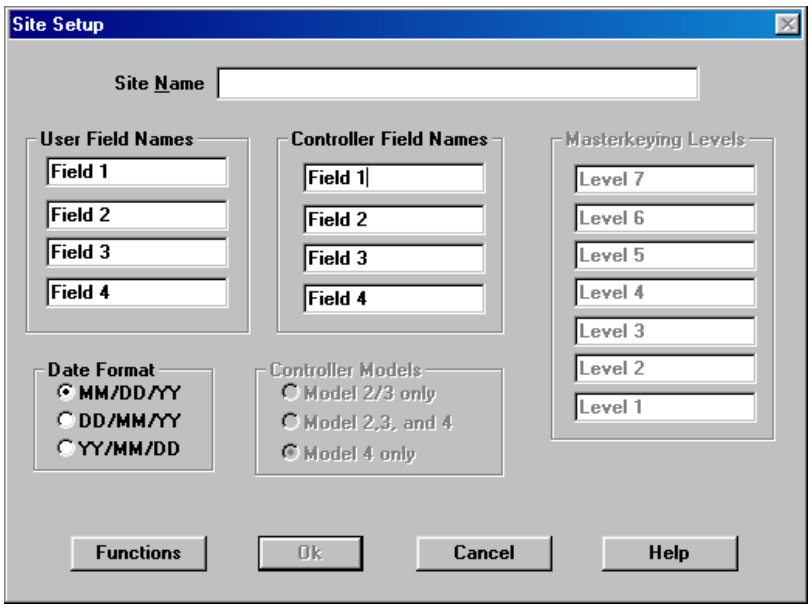


Select the appropriate site (which cannot be the current site). Quantum asks you to confirm that you really want to delete the site. If you indicate that you do want to delete it, Quantum erases all of the data files associated with the site, along with the icon for the site (if any).

Note: There is no way to recover the information for the site once it is deleted, so if there is any chance you may need the information later, you should backup the site files before deleting them. See "Utilities" for information on backing up files.

Setting Up Site Defaults

The Dealer Site Defaults specify the initial setup for a new site. The setup includes such things as names for the extra key and controller data fields, controller types, and date format. When you select **Dealer | Site Defaults**, Quantum presents the Site Setup Screen, showing your site defaults.



Change any settings you want to have common to your new sites, then select ***Ok***.

Reprogramming Devices

You may reprogram KPUs, CPU's, and RAK's for use at any of the sites your Quantum software supports. This allows you to have a limited number of programming devices, but still be able to service a large number of customer sites. Each time you need to program or update a customer's controllers or keys, you can use this option to program a KPU, CPU and RAK to match the customer's site code. You may also disable CPU's and RAK's when not in use to prevent their unauthorized use.

Refer to the **Utilities** chapter for information on reprogramming your devices.

Note that it is typically not necessary to reprogram a KPU for a new site. When you select a new site (see "Selecting a Site to Work With"), Quantum automatically reprograms the KPU, if present, for the new site code.

Feedback

We want to hear from you

No software is ever complete or perfect. There will always be new features and improvements to make the product even better. Although the software is tested thoroughly, there will always be, unfortunately, a few bugs. (or, as one software developer calls them, "UFO's - Unintentional Features and Options").

We at INTELLIKEY want to provide you with the best products possible. The Software Feedback Form on the next page provides you with a method to let us know how we're doing. If you find a problem with the Quantum software, or would like to see a feature added or enhanced to make your job easier, let us know.

Simply copy and fill out the Software Feedback Form, then send it to us:

Mail
INTELLIKEY Corporation
4325 Woodland Park Dr. Suite 102
W. Melbourne FL, 32904
Attn: Software Feedback

Fax
(321) 724-5695

If you have Internet access, you can fill out an electronic version of the form at INTELLIKEY's web site **www.intellikey.com .** Look in the Technical Support section.

Make as many copies of the form as you need. We know you have lots of good ideas. The only thing we ask is that you limit yourself to one suggestion or problem report per form -- this makes our tracking process a lot easier.

Thank you again for selecting INTELLIKEY for your access control. Now let us know how we can serve you even better!

Software Feedback Form

One problem or request per sheet, please. And please type or print neatly.

Your Name	_____	Phone	_____
Site Name	_____	Fax	_____
Address	_____	Email	_____
	_____		

☐ Problem Report

Product _____ Version _____

Description of Problem (Please be as thorough as possible. Describe what you were trying to do, or expected to see, and what actually happened. Include any error messages that appeared).

☐ Feature Request

Product _____

What would you like to see added or changed?

For INTELLIKEY use

Log # _____ Date received _____

Disposition:

Appendix A - Controller Signals

Controller Signals

During normal operation, the INTELLIKEY controller uses its built-in "beeper" to signal the result of various operations. These signals usually occur when a key is inserted.

Normal Operation

Signal	Meaning
1 long	Access is granted
2 long	Access is denied or the unlock period for a rotating cylinder has expired
1 long, 1 short	Guard Tour key. May be followed by 1 long if key is granted access to the lock.
1 short, (delay), 3 long	Disabler key
1 short, 1 long, 1 short	First key of dual-key pair inserted
4 short (after access)	Battery is low
1 short	Lock is unlocked during automatic unlock period and configured to remain unlocked.

Controller Audit Key

Signal	Meaning
1 short, series of "chirps", 2 short	Controller is loading audit information into key. The two short beeps indicate the operation is finished and the key may be removed.

Controller Update Key

Signal	Meaning
series of "chirps", series of "chirps" - different tone, 2 short	Controller is loading programming information into its memory. The two short beeps indicate the operation is finished and the key may be removed.

Shutout Key

Signal	Meaning
2 short	Lock is in shutout mode. Shutout key must be inserted again to return lock to normal mode.
1 short	Lock is in normal mode.

Appendix B - Installing Quantum

Installation Requirements

Your Quantum software is delivered on CD-ROM or floppy disks, and must be installed before it may be used. It's not enough to simply copy the files from the floppy to your hard drive. Some of the files are in a compressed format, to save disk space, and must be expanded before use.

Quantum uses the industry-standard InstallShield® technology in its setup program. If you have installed other Windows programs, you are probably familiar with InstallShield and its installation process. If not, the InstallShield setup program (referred to as *Setup* in the descriptions) walks you through the installation, prompting for each piece of information it needs, and allows you to move forward to the next step, or backward to change any previous entries.

There are several scenarios for installing Quantum, depending on whether you are a new INTELLIKEY user, or have an established INTELLIKEY system, and whether you are an End-User or Dealer. If you have your own programming equipment -- KPU, Controller Programming Unit, and RAK -- and will be maintaining your INTELLIKEY access control system, you are an End-User. A Dealer typically supports several smaller INTELLIKEY sites, which have only keys and controllers, but no programming equipment.

Running Quantum on a Local Area Network

Quantum allows operation in a networked multi-user environment, in which several operators may be performing different functions -- adding users, editing doors, issuing keys -- at the same time. Quantum keeps track of who is doing what, and prevents two operators from trying to change the same piece of information (such as the list of doors for which a key is authorized) at the same time. In this configuration, Quantum is usually installed on a shared hard drive, which is accessible by all PC's running the software.

In order for Quantum to operate properly in this configuration, there are a few restrictions on how it must be installed. The primary rule is: **all PC's must use the**

same letter to refer to the drive on which Quantum is installed. This means that if one PC identifies the Quantum drive as J:, all other PC's running Quantum must also identify the drive as J:. The choice of drive letter is arbitrary, and depends on your network setup; it simply must be a drive letter available to all PC's which will be running Quantum. This is generally a very minor restriction, and is easy to accomplish.

If you are running a server-based network such as Novell®, each PC will typically have a login script which associates drive letters with directories located on the server (for example, the Novell **map** command creates a shared drive, with a specific letter). In this setting, make sure that the same letter is used for the Quantum drive on all PC's which will be running Quantum.

If you are running a *peer-to-peer* network such as Lantastic® or the Windows network, you should share the hard drive on the PC on which Quantum is installed, then connect the other PC's to this drive, always using the same drive letter. However, the PC on which Quantum is installed must refer to its hard drive by the same letter, at least when referring to Quantum. How this is done depends on which version of Windows you are running:

Installing Quantum

Whether you are installing Quantum for the first time, or are updating to the latest version, the first part of the installation process is the same. This involves running the InstallShield setup program to copy the new Quantum files to your hard drive. Then, the first time you run Quantum, it will complete any steps necessary for installation.

Note: If you are updating an existing copy of Quantum, you are STRONGLY advised to backup your data files with the existing version before installing the new Quantum. The installation program and subsequent file update functions have been thoroughly tested, but there is always the chance of something unexpected happening. It is much easier to restore files from a backup than to recreate lost data. (One corollary to Murphy's Law states that the probability of losing data is directly proportional to the difficulty of reproducing it).

To start the Quantum installation process, insert Quantum Disk 1 into your floppy drive.

- From Windows 3.1 or 3.11, select **File | Run** from the Program Manager menu, then enter **A:SETUP** or **B:SETUP** depending on which drive contains the floppy.

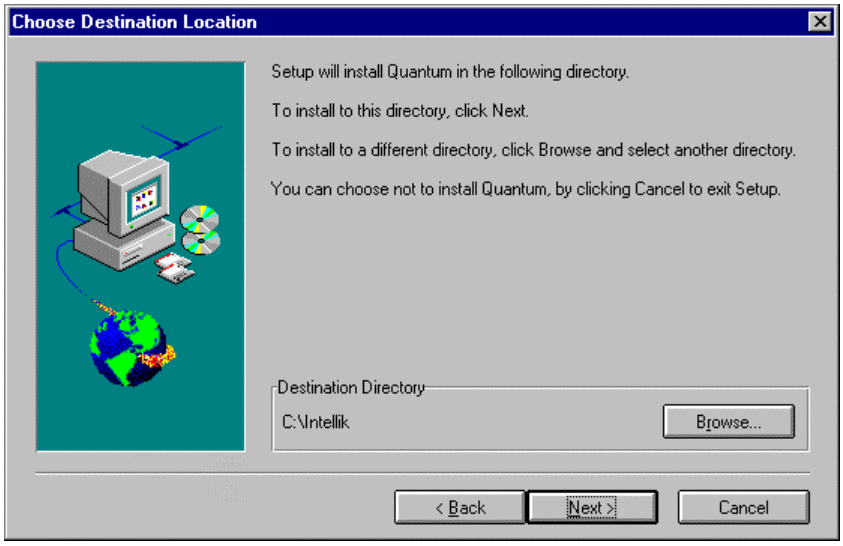
You may also start the installation from the Windows 3.1 File Manager . Select the drive containing the Quantum floppy, then from the list of files displayed, double-click on **SETUP.EXE**.

- From Windows 95, press the ***Start*** button, select *Run*, then enter **A:SETUP** or **B:SETUP** depending on which drive contains the floppy.

You may also start the installation from the Windows 95 Explorer or *My Computer*. Select the drive containing the Quantum floppy, then from the list of files displayed, double-click on **SETUP.EXE**.

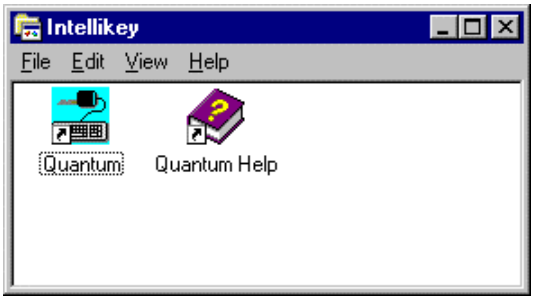
The InstallShield setup program will prompt you for various pieces of information. Follow the instructions presented on each screen, and enter the appropriate values. In general, you should use the default settings provided by InstallShield.

The only value you might typically change is the drive on which to install Quantum:



Setup will default to installing Quantum on your hard drive. If you plan to have several users sharing Quantum over a Local Area Network, you should change the drive letter to match the shared network drive from which everyone will be able to access the program. Select ***Browse*** and change drive letter (J:, for example). Refer to the section on *Running Quantum on a Local Area Network* for information on installing Quantum on a shared drive.

You can run Quantum by selecting its icon in your **INTELLIKEY** group:



The first time Quantum runs, it finishes up the installation process. The steps involved in finishing the installation depend on whether you are an end-user, or a dealer, and whether or not you have an earlier version of Quantum installed. Read the following descriptions to determine which installation procedure applies to you:

- **New End-User**: If you are an end-user, and have no existing INTELLIKEY software installed, proceed to *Running Quantum 1.7 for the First Time:New End-User*.

- **Existing End-User**: If you are an end-user, already have Quantum installed, and have received an updated version of Quantum, proceed to *Running Quantum 1.7 for the First Time:*
- *Existing* End-User.
- **New Dealer**: If you are a dealer, and have no existing INTELLIKEY software installed, proceed to *Running Quantum 1.7 for the First Time:*.
- **Existing Dealer**: If you are a dealer, already have Dealer Quantum installed, and have received an updated version of Quantum, proceed to *Running Quantum 1.7 for the First Time: Existing Dealer.*

Running Quantum 1.7 for the First Time

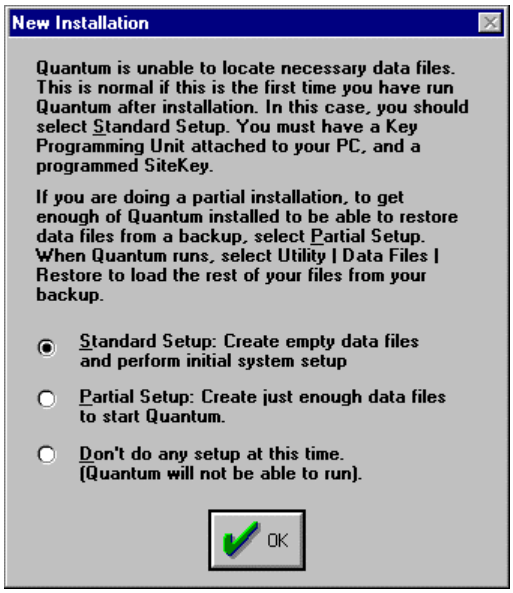
New End-User

Before running Quantum for the first time, you will need the following:

- A KPU unit, connected to a communications port (COM1 - COM4) on your computer, and plugged into its power supply. You may verify that the KPU is operating properly by pressing the Reset button on the back. The light on the front of the KPU should glow orange for about 2 seconds, flash green twice, then go out.
- A SiteCode Key, programmed with site code information.

You must also know which INTELLIKEY keying system (Horizontal or Vertical) you will use for your site. Refer to the chapter "Access Control" for descriptions of the two systems.

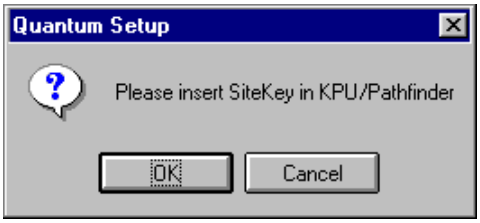
When Quantum starts, it will tell you that it can't find its data files, and asks how to proceed:



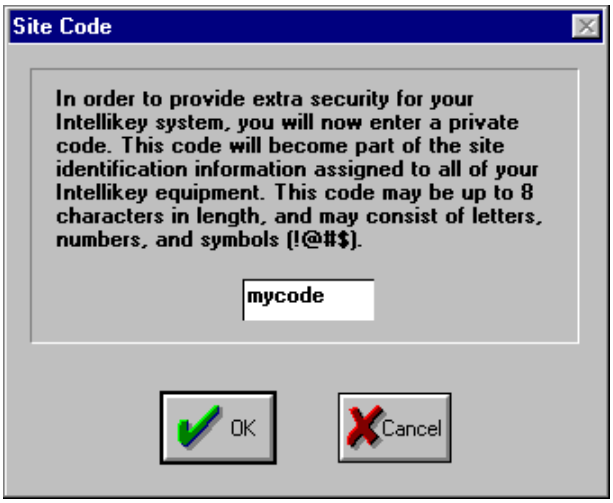
This is normal, since the data files haven't been created yet. Select *Standard Setup* (the default), then ***Ok***.

Quantum next asks to which communications port your KPU is connected:

Select the appropriate port number, then select ***Ok***. Quantum will verify that the KPU is connected properly, will ask you to insert your SiteCode Key:



Insert the SiteCode Key provided with your Quantum Installation kit, then select ***Ok***. Quantum reads the Site Code information from the key, then asks you to provide the last level of information for your Site Code:

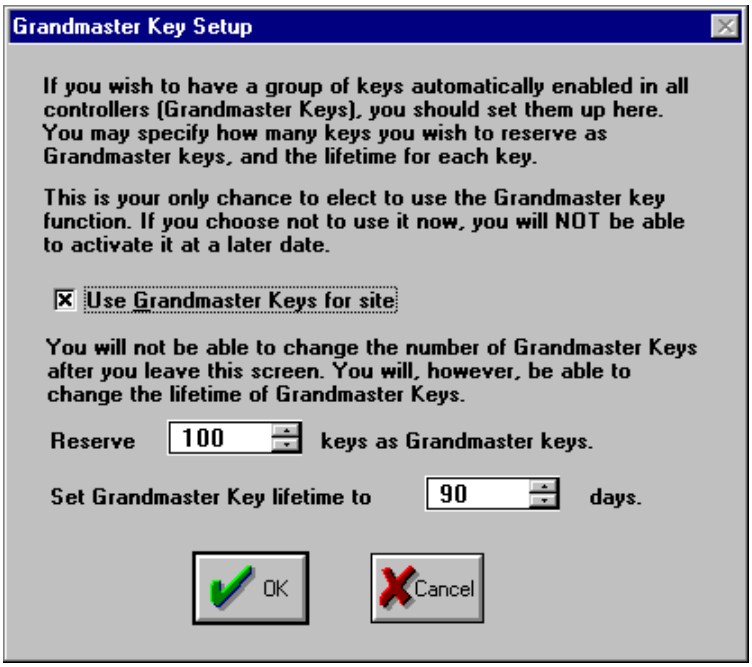


This allows you to create a Site Code whose entire contents are known only to you. This prevents anyone else from creating keys which will be able to access your site. Enter a code, up to eight characters long, then select ***Ok***.

Quantum next asks if you want to use the "Grandmaster Key" feature. Grandmaster Keys are automatically enabled in all controllers, and would typically be issued to

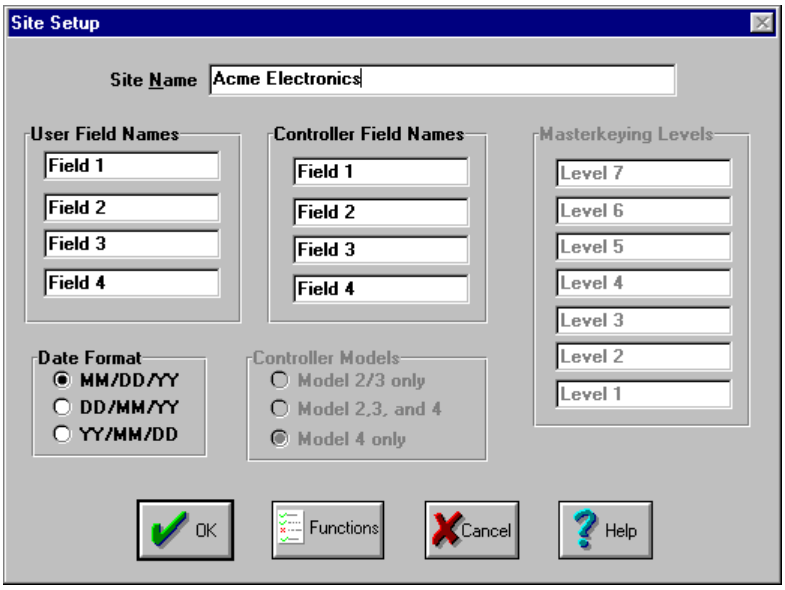
security or maintenance personnel. You must elect to use the Grandmaster Key function, and select how many keys to reserve as Grandmaster Keys now.

Note: You cannot enable the Grandmaster Key feature after you leave this screen, so if you don't enable it now, you will not be able to use this feature in the future. Also, the number of keys you reserve as Grandmaster Keys will be set permanently; you won't be able to change it later, either.



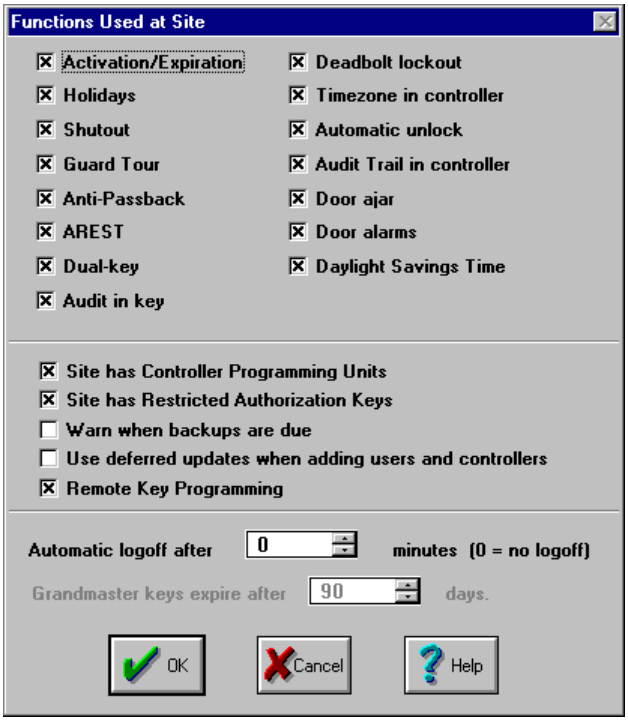
This screen allows you to reserve a fixed number of keys to be Grandmaster Keys. The default is 100, but you can adjust the number based on your site requirements. Grandmaster Keys also have a limited lifetime, in case they are lost. You can set the initial lifetime here, and change it later using the Site Functions screen.

Quantum next asks you to enter some configuration information for your site:



This includes such things as the site name, names for the extra user and controller fields, types of controllers used at the site, and names for the keying levels (if you elected to use the Vertical keying system). Note that if you elected to use the Horizontal key system, the *Controller Models* and *Masterkeying Levels* sections will be disabled, as they apply only to the Vertical system.

Select ***Functions*** to enable or disable various Quantum functions to be used at your site:



Any features you deactivate (by removing the check next to them) will not be available to anyone entering data for keys and controllers. (You can enable and disable features at any time while running Quantum).

Select ***Ok*** to return to the Site Setup screen, then select ***Ok*** again when you have finished making changes. You can change your site setup at any time using the **Utility | Site Setup** function. Refer to the chapter "Utilities" for details.

After you have entered the Site Code information, Quantum next creates the initial site data files.

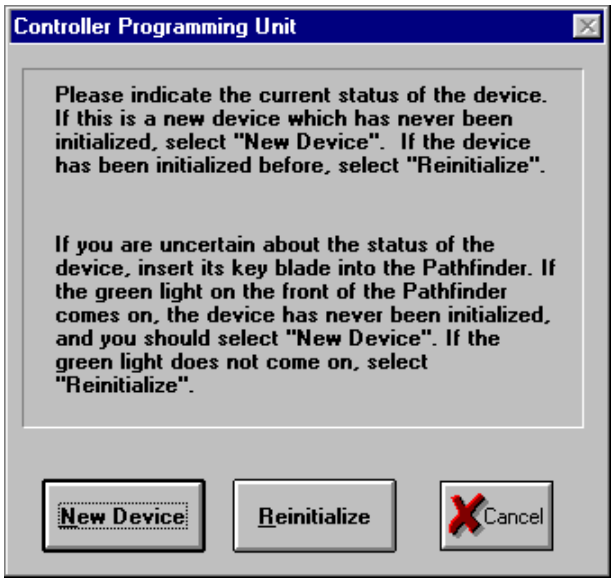
Quantum next asks if you want to program any KPUs, Controller Programming Units, or Restricted Authorization Keys for use at your site. The programming operation loads your site code into the various devices so that they may be used with your keys and controllers. You may program these devices now or later from the **Utility** menu.

Quantum first asks if you want to program any KPUs. If you indicate that you do, Quantum first prompts you to connect the KPU to be programmed to the proper serial channel.

Make sure the KPU is connected, then select ***Ok***. Quantum verifies that the KPU is connected properly, then programs it.

Quantum next asks if you want to program any Controller Programming Units. Controller Programming Units are programmed through the KPU. The programming sequence for Controller Programming Units depends on the state of the CPU - programmed one or more times, or never programmed. CPU's received from the factory have never been programmed.

Quantum first asks you about the status of the Controller Programming Unit, in order to determine the proper programming sequence.



You can determine the status of the Controller Programming Unit by inserting its keyblade into the keyway of the KPU (the power to the KPU must be plugged in). If the green light on the front of the KPU comes on, the CPU has never been programmed, so you should select ***New Device***. If the KPU light does not come on, the CPU has been programmed at least once, so you should select ***Reinitialize***.

If you select ***New Device***, Quantum next prompts you to insert the CPU into the KPU.

Insert the keyblade of the CPU into the keyway of the KPU, make sure that the KPU is connected to the serial port you specified earlier, then select ***Ok***. Quantum then programs the Controller Programming Unit.

If you select ***Reinitialize***, Quantum asks you to insert the keyblade of the CPU into the keyway of the KPU, then connect the CPU to the serial port you specified earlier. When you have done so, select ***Ok***. The green light on the front of the KPU should be lit. Next, Quantum asks you to connect the KPU to its assigned serial port.

Disconnect the CPU from the serial channel, but do not remove it from the KPU keyway. Connect the KPU to the channel, verify that the green light is still on, then select ***Ok***. Quantum will then program the CPU.

Finally, Quantum asks if you want to program any Restricted Authorization Keys (RAKs). RAKs are also programmed through the KPU. The programming sequence for RAKs depends on the state of the RAK - programmed one or more times, or never programmed. RAKs received from the factory have never been programmed.

Quantum first asks you about the status of the RAK, in order to determine the proper programming sequence.

You can determine the status of the RAK by inserting its keyblade into the keyway of the KPU (the power to the KPU must be plugged in). If the green light on the front of the KPU comes on, the RAK has never been programmed, so you should select ***New Device***. If the KPU light does not come on, the RAK has been programmed at least once, so you should select ***Reinitialize***.

If you select ***New Device***, Quantum next prompts you to insert the RAK into the KPU.

Insert the keyblade of the RAK into the keyway of the KPU, make sure that the KPU is connected to the serial port specified in your operator setup, then select Ok. Quantum then programs the RAK.

If you select ***Reinitialize***, Quantum asks you to insert the keyblade of the RAK into the keyway of the KPU.

Turn on the RAK, and select the **LINK** command from the RAK's main menu. The green light on the front of the KPU should come on. Select ***Ok*** to reprogram the

RAK. You must select ***Ok*** within 10 seconds of selecting the RAK **LINK** command, otherwise the RAK will assume that it was unable to communicate with the KPU, and will break the link between them. The green light on the KPU will go out if this happens, and you must remove the RAK from the KPU and restart the reprogramming sequence.

Your Quantum installation is now finished. In the future, you may start the Quantum software as described in "Running Quantum". Quantum creates an operator named "System Manager" with an Operator ID of 1234 and a password of 1234. You may use these values to log on the first time you use Quantum.

Depending on the Quantum features you will be using, there may be a few more setup items you should do before entering any access control data:

- Change the operator ID and password for the System Manager, and create any other operators, with appropriate access to Quantum functions.
- Enter the holiday (**Utility | Dates | Holidays**) and Daylight Savings Time (**Utility | Dates | Daylight Savings Time**) settings for your site. These values are automatically transferred to all new users and locks.
- Either modify the preconfigured user and controller default settings (the settings for both are named "Individual") (**User | Defaults | Change** or **Controllers | Defaults | Change**) or create new settings (**Users | Defaults | Add**, **Controllers | Defaults | Add**) appropriate for your site.
- Create any user and controller groups appropriate for your site. (**Users | Access Groups | Add, Controller | Access Groups | Add**).

The instructions for each of these operations are in other chapters in this manual.

This ends the installation process for a new end-user

Existing End-User

If you already have an earlier version of Quantum installed, the first time you run version 1.7 Quantum first moves the data files from the earlier version into the new Quantum 1.7 directory, then deletes the old directory. Quantum then performs an update on the data files, to add new information and fields for version 1.7. This process can take anywhere from a few minutes to a couple of hours, depending on the speed of your computer, and the size of your data files. When this process is complete, Quantum is ready to use.

This ends the installation process for an existing end-user

New Dealer

Before running Quantum for the first time, you should have a Key Processing Unit, connected to a communications port (COM1 - COM4) on your computer, and plugged into its power supply. You may verify that the KPU is operating properly by pressing the Reset button on the back. The light on the front of the KPU should glow orange for about 2 seconds, flash green twice, then go out.

The first time you run Quantum, it will ask which communications port your KPU is attached to:

If you have a KPU attached, select the appropriate port, then select ***Ok***; otherwise, select ***Cancel***. If you select ***Ok***, Quantum will verify that the KPU is attached and working properly.

After you specify the KPU setup (Quantum needs this information for reading SiteCode Keys when creating new sites), Quantum starts normally. At this point, you have no sites available, so most of Quantum's menu items are disabled. You can create your first site by selecting **Dealer | Create Site | New Site**. Refer to the chapter on the "Dealer Version" for more information on creating and maintaining sites.

This ends the installation process for a new dealer

Existing Dealer

If you have an earlier version of Dealer Quantum installed, the new Quantum will make a couple of small changes, but will otherwise leave your original installation intact. The first time you select each of the sites created under the earlier Quantum, the new Quantum will update the data files to match the version 1.7 format.

This ends the installation process for an existing dealer

Running Quantum on Networked PC's

The Quantum setup program creates a program group and icon to start Quantum on the PC from which the setup program was run. After installing the Quantum software once on the shared drive, you should set up other PCs to access the software by using the Workstation Setup utility from the Quantum directory. From each PC, select the ***Start*** button, then *Run…,* then enter **J:\INTELLIK\Quantum\WSSETUP** and press ***Ok***. Replace the **J** with the drive letter of the shared drive. This program will add the proper settings to the PC, and create the icons necessary for running Quantum from the shared drive.

You can use the newly created icon to run Quantum from the networked PC. For each PC, you should create a different operator, with the appropriate KPU and CPU communications settings for the PC. For example, the KPU might be attached to COM1 on one PC, and to COM2 on another. By creating separate operators for each PC, the communications settings will be set up correctly when the operator logs on.

Glossary of Terms

Anti-Passback

Prevents a key from being used twice in succession in the same controller. The key must be used in another controller first.

audit trail

A list of access information, including location, date, and time, stored in the memories of INTELLIKEY keys and controlles.

automatic enable period

The time period during which a key will be authorized into a controller the first time it is used in the controller. This feature eliminates the need to update individual controllers when new users and keys are added to a site.

Backup

To make a copy of your data files, which can be used to restore your information in case something happens to the original copy.

Controller Audit Key

A key configured to read audit information from a controller.

Controller Update List

A list of controllers whose user access information is out of date as a result of changes to users.

Copy number

Part of the INTELLIKEY masterkeying system which distinguishes individual copies of a key from each other. The controller maintains a table of which copies are authorized.

Dealer Function Key

A special INTELLIKEY key which authorizes Quantum to perform special functions required by dealers.

Defaults

The values initially configured for a user or controller.

Dual-key mode

A controller operational mode in which two specific keys must be inserted within 15 seconds of each other to operate the lock.

Emergency key

A key which overrides certain security functions.

Fixed cylinder

An electronic cylinder which functions as a key reader only. The key is inserted into the cylinder, but not turned.

IACS

INTELLIKEY Access Control System. IACS was a DOS-based ancestor of Quantum.

Issue receipt

A form indicating to whom a key was issued, and the controllers for which the key is authorized. The receipt will be printed when a key is issued or updated. The Key Print Ticket Menu item turns this function on and off.

LAN

Local Area Network.

Online

Connected to the IntelliNet network

Relock mode

In Relock Mode, the controller automatically secures the locking mechanism after a selectable period of time.

Rotating cylinder

An electronic cylinder which activates a mechanical locking mechanism.

Site Code

A digital code which identifies the keys, controllers, Pathfinders, Controller Programming Units, and RAK's at a site. This information is loaded into the memory of each device and must match before the devices are able to communicate with each other.

Toggle mode

In Toggle mode, the controller alternates the locking mechanism between locked and unlocked as keys are inserted.

User Activity Log

A file containing audit trail information recorded from user keys, controller audit keys, and querying controllers. The file contains a list of dates and times various users accessed controllers.

Index

S

T

U

W