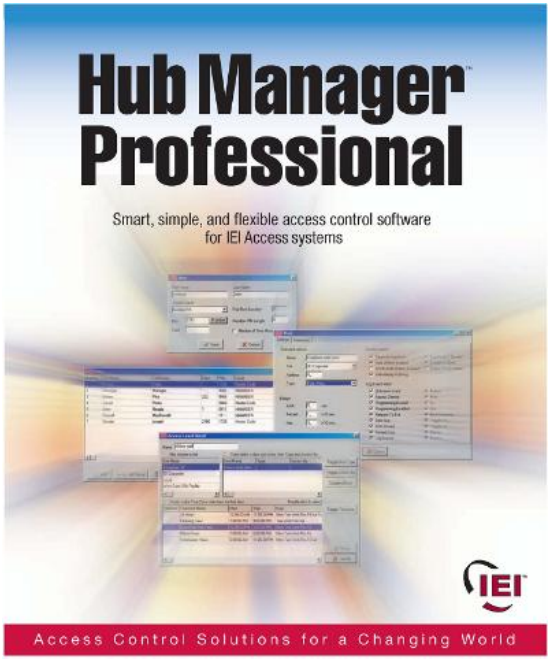
International Electronics, Inc.
Hub Manager™ Professional v8
Access Control Software
User Manual



This equipment is designed to be installed and serviced by security and lock industry professionals.

For Support Please Contact:

Company Name: _____

Phone: _____

Hub Manager™ Professional v8
Software User Manual \ Help File
6045011, Rev 8.0, D8

Table of Contents

Chapter 1: Using Online Help

1 Using Help 1

Chapter 2: Foreword

Chapter 3: Installation

1 Installation 6

Chapter 4: Overview

1 General Overview 15
2 Initial Set Up 23
3 Menu System 28
4 Running the software 30
5 System Setup Tasklist 32
6 PDA Software 35
7 Uninstall 47

Chapter 5: System

1 System Menu 50
2 System Manager 50
3 Login 70
4 Logout 71
5 Change Login Password 71
6 Exit 72

Chapter 6: Database

1 Database Menu 73
2 Operators 73
3 Operator Wizard 76
4 Sites 77
- Site Wizard 82
- Serial Connection 83
- PDA Connection 83
- Data Transfer Device (DTD) Connection 85
- SEG LAN/WAN Connection 106
  - Dynamic IP Address 113
  - Dynamic IP Address, non-expiring lease 117
  - Static IP Address 117
- Modem Connection 127
- Managing Stand-Alone Controllers 129

5 Time Zones 131
6 Doors 134
HC500, Hub+\Max, Max 2 v1 and Max 2 v2 149
prox.pad plus IR 150
prox.pad plus, Max 3 v1 and Max 3 v2 152
LS2\P 160
Door Wizard 161
7 Access Levels 162
8 Access Level Wizard 169
9 Users 172
User Import Wizard 195
Add User Group 198
10 Holidays 200

Chapter 7: Communications

1 Communications Menu 204
2 Security Chip 204
3 Import Door Settings 204
4 Import\Export Doors 205
5 Network Query 209
6 System Dashboard 211

Chapter 8: Tools

1 Tools Menu 216
2 Log Archiving 216
3 Audit Archiving 217
4 Database Backup/Restore 218
5 Database Conversion Utility 220
6 Run COM Port Test 223
7 Scheduled Log Import 224
8 Scheduled Log Import Reminder 225
9 Table Initialization 226
10 Application Initialization 227
11 Indexing 228
12 Options 230

Chapter 9: Reports

1 Reports Menu 235
2 Printer Options 235
3 Log Filter 236
4 Time Management 240
5 Misc. Log Reports 244

6 Assignment Reports 245
7 Database 252
8 Audit 254
9 Archive Viewer 254
10 Generate Data for External Report Writer 256
11 Scheduled Log Import Errors 256

Chapter 10: Help

1 Help 257
2 Online Support 257
3 Check for Updates 257
4 Check for Custom Updates 259
5 Upgrading Hub Manager™ Professional 260
6 About 261
7 Glossary 263

Chapter 11: Obtaining Technical Support

1 Obtaining Technical Support 265

Chapter 12: Copyright Information

1 Copyright Information 266

Index 267

Chapter 1: Using Online Help

1.1 Using Help

Hardcopy Version

Some references in this manual are designed for use with the electronic version. The electronic PDF version can be found in the following folder:
C:\Program Files\IEI\HMP8\Manual.exe

If you did not install Hub Manager™ Professional to the default location, then browse to the custom installation folder you specified during install:

<Installation Path>\IEI\HMP8\Manual.exe

Electronic Version

The electronic help system provided with Hub Manager™ Professional quickly displays instructions about the software when you select the **Help** item from the menu bar or by pressing ***F1.*** You can obtain this online help without interrupting the work you are doing and without looking through a paper manual.

In addition, this help system is context sensitive, meaning that if you press ***F1*** while any screen is open the section pertaining to that feature is displayed. For example if you are in the User edit screen, then press ***F1***, the help file opens to the users section.

NOTE: Some utilities may not have ***F1*** functionality.

After the Hub Manager™ Professional Online Help window opens, you'll see a choice of tabs: Contents, Index, Search and Favorites

- Select the ***Contents*** tab to browse through topics by category, much like the Table of Contents to a book.
- Select the ***Index*** tab to see a list of index entries: either type the word you're looking for or scroll through the list.
- Select the ***Find*** tab to search for words or phrases that may be contained in a Help topic.
- Select the ***Favorites*** tab to save a bookmark to certain Help topics for quick reference at a later time.

Chapter 2: Foreword

About This Manual

This manual is designed for users of IEI Hub Manager™ Professional v8 software in conjunction with HC500, Hub+\Max, Max 2 v1, Max 2 v2, LS2\P, Max 3 v1, Max 3 v2, prox.pad plus IR and prox.pad plus controllers. All installation, setup, operational information and procedures, accompanying screen captures and other relevant material is contained in this manual.

Safety Warnings and Cautions

When handling a printed circuit board, to guard against possible static discharges, touch a grounded object BEFORE touching the board. Static shock can render the product unusable.

Disclaimer

Due to design changes and product improvements, information in this manual is subject to change without notice. IEI assumes no responsibility for any errors that may appear in this manual.

Reproduction

Neither this manual nor any part of it may be reproduced, photocopied, or electronically transmitted in any way without the written permission of IEI.

Technical Support

Should you experience any difficulty installing or operating the Hub Manager™ Professional software, please contact your installation/service company or IEI at 800-343-9502.

Using this Manual

This manual, your reference to the Hub Manager™ Professional software, accompanies the Hub Manager™ Professional software installed with your access control system. This manual contains the following topic sections, along with others.

Installation

This section discusses the procedure for installation Hub Manager™ Professional software, the PDA software and the DTD Printer Utility software.

Overview

This section provides a description of this software's functionality.

System

This section explains the menu choices available on the System menu.

Database
This section describes the various program databases.

Communications
This section details how to use the 'Export to Doors' and 'Import Transaction Log' functions.

Tools
This section details the Tools menu options.

Reports
This section supplies procedure for selecting the various types of available reports and shows examples of each.

Obtaining Technical Support
This section describes how to obtain technical support for this software, and how to prepare to make a technical support request.

Glossary
This section contains commonly used terms and definitions.

Manual Conventions: Keys, Selections, and Commands

The type style, terminology, and references to important information used in this manual are intended to make the manual easy to use. The following sections describe these conventions.

The following terms are used to indicate commands, which you must execute, or selections you must make, using the mouse or keyboard.

Bold Face Italicized Type
Text that is both written in ***bold face*** and ***italicized*** type corresponds directly to text that appears in the software.

<F7>
Keyboard keys you must press are contained within carets.

<Alt> <F>
Represents a Windows accelerator key or combination key you must press. Hold down the <Alt> key, and then press the indicated key.

Click

The Click command means you must click the LEFT mouse button once, unless the right mouse button is indicated (as in Right-Click). [For command buttons, you can also use the Windows accelerator key (<Alt> plus the underlined character) associated with the item to activate the item. For example, the accelerator key for the Start menu's Run... command is <Alt>+R.]

Double-Click

Indicates two rapid clicks of the left mouse button. [You can also select the specified item by highlighting it (using the arrow keys or <Tab> key), pressing the space bar to select it, then pressing the <Enter> key.]

Select or Highlight

Select or highlight an item by clicking on it or by using the TAB key to bring focus to a component and then acting upon that component by pressing the <ENTER> key or the SPACEBAR.

Press

Press the specified key or keys on the keyboard.

Drag

The Drag command follows standard Windows usage: select the desired item, click and hold down the left mouse button, move the mouse pointer to the desired location, then release the mouse button.

Menu Selections

When a series of two or more menu choices is presented, the menu commands are separated by a right facing caret like this: System > Login. A menu choice is always specified by its complete choice path. That is, the Main menu selection is given first, along with any subsequent menu selections needed to get to the final menu choice. For example, Database > Doors means first choose Database from the Main menu, then choose Doors.

Save, Cancel, and Done Commands

Most screens and\or dialog boxes contain two command buttons that are used to close the dialog box: Save and Cancel.

When you select the Save button, the program saves the current data or settings and returns to the previous screen.

When you select the Cancel button, the program discards any and all edits and then returns you to the previous screen.

A Done button will be displayed when no data is being edited, such as when you are viewing one of the directories: Sites, Time Zones, Doors, Access Levels, Users, Holidays or Operators. When you select the Done button, the program will simply close the current screen (window) and return you to the main screen of Hub Manager™ Professional.

Window Types

This software uses Microsoft Windows conventions and terminology regarding how information is presented on screen. In general, information is displayed in bordered windows called dialog boxes, or windows, or screens, or forms. For further information, refer to the Microsoft Windows documentation.

Window or Dialog Type Description

Application dialog used for operator data entry, or to present information for operator selection; usually referenced by the title of the application dialog, such as Password dialog.

Confirmation dialog

Presents the OK or Cancel command button choices to accept or reject an action.

Main window

Displays initially whenever the software starts up; contains a menu and command buttons that provide access to program functions.

Message box

Presents information that the operator must acknowledge.

Dialog Tabs

Some dialog windows or boxes use a tabbed display to categorize information. Selecting a tab displays the information or data entry items associated with that tab. The location of such information is referred to by the name of the tab, such as the Door Settings tab or the Time Zones tab.

Chapter 3: Installation

3.1 Installation

This section provides a general description of the IEI Hub Manager™ Professional v8 software. It also supplies procedures for installing or using various Hub Manager™ Professional v8 software components. Hub Manager™ Professional is an access control management program for Microsoft Windows operating systems used in conjunction with IEI's access control equipment.

If you are upgrading from a previous version of Hub Manager™ Professional please go to the Upgrading Hub Manager™ Professional section of this manual.

Operating Systems

Hub Manager™ Professional is qualified to work on Windows XP Home, XP Professional, Vista Home Premium, Vista Business, Server 2003 Standard, Server 2003 Enterprise, Server 2008 Standard and Server 2008 Enterprise only. **If you are not running one of these supported operating systems, the software installation will be denied.**

NOTE: All software must be installed using a Windows Administrator user account. The program can be used by a standard Windows logon but requires an Administrator to grant that user account full read/write access to the following folders and files:

- <Installation Path>\IEI\HMP8\ (default is C:\Program Files\IEI\HMP8)
- C:\Program Files\Common Files\Borland Shared\
- C:\PDOXUSRS.NET

Installing the Hub Manager™ Professional software onto the PC

Follow the steps below to install Hub Manager™ Professional onto your PC.

1. Insert the installation CD.

   NOTE: On most computers, the Autorun program launches automatically. If it doesn't, select ***Start > Run***, browse to the CD-ROM drive, select the ***Autorun.exe*** file, then select ***Open*** and ***OK***.

2. Select Install ***Hub Manager™ Professional v8***, which is the top choice on the screen. You are then prompted with a confirmation screen stating the files for Hub Manager™ Professional will be installed. Click ***Yes*** to continue.
3. When the setup ***Welcome*** screen appears, click ***Next*** to continue to display the ***License Agreement***. Use the scroll bar to read through the ***License Agreement***, then select ***I accept the agreement*** to indicate your acceptance and click the ***Next*** button.
4. Next you are prompted to a ***Select Destination Location*** to install the program. The default location is C:\Program Files, but you are allowed to install Hub Manager™ Professional to any folder you choose, on your local PC.

   NOTE: Do not attempt to install the software on removable media, a network drive or directly to the root of a local drive (ie. do not install directly to D:\, but D:\Programs).

5. After choosing your installation location, click ***OK*** to proceed with the installation. The next screen you are presented with shows a progress bar and various files being copied to your PC.
6. Once the progress bar is complete, the ***Information*** screen appears, containing the software ***Release Notes***, which is the ***ReadMe*** file included in the installation folder. Please read the ***ReadMe*** file because it contains the most up to date information about new features and important changes to the

software.

7. Click ***Next*** to continue, then click ***Finish*** on the final screen to complete the Hub Manager™ Professional v8 software installation.

LS Link Installation

LS Link is qualified to work on Windows XP Home and XP Professional only. **If you are not running one of these supported operating systems, the PDA software installation will be denied. PDA's are not supported by Hub Manager™ Professional when installed on Windows Vista, Windows Server 2003 or Windows Server 2008.**

NOTE: Refer to the PDA Software section for additional details about using LS Link.

System Requirements

The following is a list of required equipment in order to use LS Link:

- IEI's Hub Manager™ Professional v8 software
- Windows XP Home or Windows XP Professional Operating System
- PDA with Palm OS 3.5, 4.x, or 5.x
- Palm Desktop and HotSync Manager software (provided by PDA vendor)
- 250KB of available memory on the PDA for each controller you are managing

IMPORTANT NOTE FOR CURRENT PDA APPLICATION USERS: If you are currently using a version of the PDA application that was distributed with a version of PC software that was released prior to Hub Manager™ Professional v8, then you must install the latest version of the PDA application that ships with Hub Manager™ Professional v8. Use of the previous version of PDA software will result in incorrect operation. The version of PDA software you must have to operate with Hub Manager™ Professional v8 must be version 4 or greater. To check your version of PDA software, go to the main screen of the PDA software, and tap the title bar at the top of the screen to open the ***Help*** menu. Select About to display the software version number. If this number is less than 4, then you must install LS Link from the Hub Manager™ Professional v8 installation CD as detailed below.

Installation Procedure:

NOTE: On most computers, the Autorun program launches automatically. If it does not, select ***Start > Run***, browse to the CD-ROM drive, select the ***Autorun.exe*** file, then select ***Open*** and ***OK***.

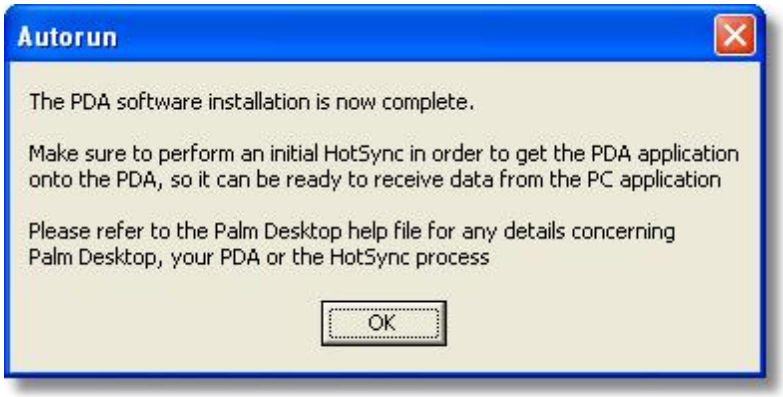
1. Select ***Install LS Link***.
2. The install program displays a confirmation screen to remind you that Palm Desktop and HotSync Manager software must be installed prior to installing LS

Link software. In addition, if either of these applications are running, the installation asks if you want it to turn them off for you, because the install won't continue until both applications are closed.

3. Select ***OK***.
4. Select the individual PDA's you want to install the PDA application onto or check the ***Install onto all PDA's*** checkbox to install the application onto all of the PDA's in the system. Click ***Install*** to continue.

5. If Palm Desktop is not found in the standard Palm installation folder, the following message appears. Click ***OK*** to close the message, then browse the to the Palm Desktop program folder, where ***Palm.exe*** is located.

6. When PC portion of the installation is complete, the following screen appears.



7. Finally, HotSync with each PDA that you selected above. When the HotSync process is complete, the PDA application's logo appears on the main screen of those PDA's, as shown below.

DTD Printer Utility Software Installation

This DTD Printer Utility is designed for use with the Data Transfer Device operating in Printer Mode, which is available in firmware version 00.40 or later. When the DTD is in Printer Mode it's used to capture infrared printer data from products supporting the infrared dump feature. The DTD Printer Utility retrieves this data from the DTD and stores it in a text file on your PC. This software is installed and used separately from the Hub Manager™ Professional software and separate from the LS Link software. It is not required for using the DTD within the Hub Manager™ Professional software.

The DTD Printer Utility is qualified to work on Windows XP Home, XP Professional, Vista Home Premium, Vista Business, Server 2003 Standard, Server 2003 Enterprise, Server 2008 Standard and Server 2008 Enterprise only. **If you are not running one of these supported operating systems, the software installation will be denied.**

NOTE: Refer to the Data Transfer Device (DTD) Connection section for additional details about using the DTD hardware.

Installation Procedure

1. Insert the installation CD

   NOTE: On most computers, the Autorun program launches automatically. If it doesn't, select ***Start > Run***, browse to the CD-ROM drive, select the ***Autorun.exe*** file, then select ***Open*** and ***OK***.

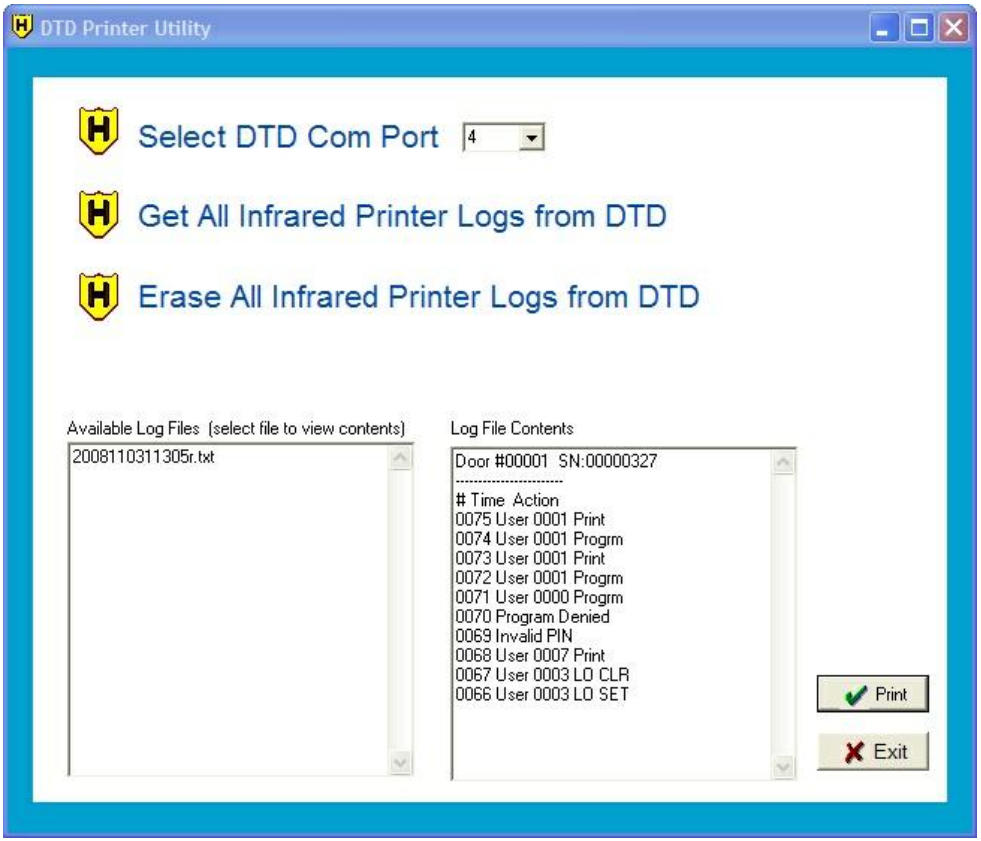
2. Select the ***Install DTD Printer Utility*** option.
3. When the setup ***Welcome*** screen appears, click ***Next*** to continue to display the ***License Agreement***. Use the scroll bar to read through the ***License Agreement***, then select ***I accept the agreement*** to indicate your acceptance and click the ***Next*** button.
4. Next you are prompted to ***Select Destination Location*** to install the program. The default location is C:\Program Files, but you are allowed to install the DTD Printer Utility to any folder you choose, on your local PC.

   NOTE: Do not attempt to install the software on removable media, a network drive or directly to the root of a local drive (ie. do not install directly to D:\, but D:\Programs).

5. After choosing your installation location, click ***OK*** to proceed with the installation. The next screen you are presented with shows a progress bar and various files being copied to your PC.
6. Once the progress bar is complete, a screen indicating the installation is complete appears. Click ***Finish*** on the final screen to complete the DTD Printer Utility software installation.

Using the DTD Printer Utility

Once you've installed the DTD Printer Utility you can start it by going to the Windows Start Menu and browse to the ***DTD Printer Utility v1.0*** folder in your program list, then click ***DTD Printer Utility***. You can also double-click on the desktop icon. Once launched, the screen below appears.



Before using the DTD Printer Utility, you must select the ***Com Port*** that you plugged the DTD into. Since this is a USB device, Windows automatically assigns it a Com port. You now have to find out the Com port number. See the Data Transfer Device (DTD) Connection section for more information on determining the Com port number that was assigned. Once selected, this Com port is automatically selected the next time you run the software.

To retrieve the infrared printer logs from the DTD click on ***Get All Infrared Printer Logs from DTD***. The software then imports the files to your PC. You can see the files it imported on left side under ***Available Log Files***. The right hand side under ***Log File Contents*** shows the content of each file, when you select it.

To print a log file, select the file on the left, then click the ***Print*** button. When you click the button, the file is immediately printed using your PC's default printer. You can also print files using any other text editing program, such at Notepad or Wordpad. Open the text editor, then browse to the ***DTD Printer Utility\LogFiles*** folder (located in the installation location you chose when you installed the software and print the file.

To remove the printer log files from the DTD click on ***Erase All Infrared Printer logs from DTD***. Please note this only removes printer files and does not delete any files created in DTD mode using Hub Manager™ Professional software, including export files and transaction log files.

To change modes on the DTD:

1. Power on the DTD.
2. Go to the main menu by pressing the 5 key on the DTD.
3. Select STATUS.
4. Select SET MODE.
5. Move the cursor to the desired mode setting and then press the ENTER (5 key) to set the current mode.
6. Press the back arrow or the * key to return to the main welcome screen.

For quick reference, the current mode is displayed at the top on the main menu on the DTD.

Chapter 4: Overview

4.1 General Overview

Additional information not contained in this manual may be found in the ReadMe.txt file located at:

Start > Programs > Hub Manager Pro v8 > ReadMe

Operating Systems

Hub Manager™ Professional is qualified to work on Windows XP Home, XP Professional, Vista Home Premium, Vista Business, Server 2003 Standard, Server 2003 Enterprise, Server 2008 Standard and Server 2008 Enterprise systems only.

NOTE: All software must be installed using a Windows Administrator user account. The program can be used by a standard Windows logon but requires an Administrator to grant that user account full read/write access to the following folders and files:

- <Installation Path>\IEI\HMP8\ (default is C:\Program Files\IEI\HMP8)
- C:\Program Files\Common Files\Borland Shared\
- C:\PDOXUSRS.NET

Major Features in Hub Manager™ Professional v8

Operator Logon and Password Security

Hub Manager™ Professional requires you to login to the software using an operator name and password. You can create up to a maximum of 99 operators in the software with each assigned a unique set of privileges. You can assign operators with full access, read only access or no access to specific areas of the software. The default login in name is HUBMAN and the default password is HUBMAN. **IEI recommends that you change the default login information immediately after installing the software.** You should also change your password periodically. Remember, that the name and password are case sensitive.

Main Menu Screen

From the main screen you can access each area of the software used to setup and configure your access control system. You can use either the toolbar buttons or the main menu options at the top to access each area of the software.

Sites

A Site is a group of similar controllers with a common connection type. Hub Manager™ Professional can hold up to 1,000 sites containing a limited number of doors based on the controller type you select. If you have more doors than a site allows, then you must create another site and add the additional doors to the second site. The chart below contains the maximum number of doors allowed per Site, depending on the controller type.

Controller Type	Maximum Doors Allowed Per Site
HC500	64
Hub+\Max	64
Max 2 v1	64
Max 2 v2	64
LS2\P	300
prox.pad plus	64
Max 3 v1	64
Max 3 v2	64
prox.pad plus IR	300

Access Levels

Access Levels are used to link the users in the database to each door controller. This is also where you define which doors each user has access to, the user type (such as standard, passage, etc), access condition (code OR card; code AND card) and the Time Zones during which the user is allowed access. You use Access Levels to group users together that have similar access privileges. Access Levels allow you to modify a group of users, rather than requiring you to edit each user individually. You can create up to a maximum of 1000 unique Access Levels.

Users

Hub Manager™ Professional can store a maximum of 20,000 users in the database. Each door controller can store a limited number of those users, based on the user capacity of the controller type. When you add a user you specify the user's name, their code or card information, but you don't directly select the doors the user has access to. Rather than directly assigning users to door controllers, you assign then to an Access Level, which determines the doors the user has access to, as described above.

Default Users

By default, the user database has two pre-defined users: Master User with a code of 1234 and a Supervisor User with no code defined. These users cannot be deleted.

In addition to adding users one at a time, Hub Manager™ Professional offers two features allowing you to add groups of users:

- Add Group
- User List Import Wizard

Add Group

You can add a group of users with common settings such as access level, sequential card numbers, and random generation of code using the Add Group feature.

User List Import Wizard

With the User List Import Wizard you can import a CSV file containing a list of user names. A CSV file is a simple text file that separates the fields with commas. This is convenient if you already have a list of users in a separate CSV file.

Time Zones

Time Zones are used to specify when user's are allowed access. In addition, you can designate a Time Zone as an Auto-Unlock Time Zone, so the door unlocks on a schedule. You can create up to a maximum of 1000 unique Time Zones in Hub Manager™ Professional. Each door controller can store up to eight Time Zones from that list. The Hub Manager™ Professional database ships with seven pre-defined common Time Zones. If these pre-defined Time Zones do not meet your requirements you can either leave them unused, delete them or edit them to suit your needs.

Auto-Unlock Time Zones

As mentioned above, you can designate a Time Zone as an Auto-Unlock Time Zone. An Auto-Unlock Time Zone means the door will unlock and relock on a schedule. You can also enable the First-In Auto-Unlock option, which means the door won't automatically unlock until a valid user gains access. Of the eight Time Zones that you can assign to most controller types, each one can be designated as Auto-Unlock. Refer to the Auto-Unlock section for further details.

Holidays

Holidays are used to determine when a user is allowed access. When you set up a Time Zone, you must specify whether or not the Time Zone applies to holidays. You can specify up to 16 single date holidays per system and 16 block holidays per system (block holidays are not supported by all controller types).

Communications

Hub Manager™ Professional contains a number of communications options, which are discussed below.

Exporting to Doors

This is the process used to send data to your door controllers. You have two options when exporting data. You can choose to either perform a full export, which sends all the data or to send changes only, which only sends the changes you made since the last export. The software automatically keeps track of all the changes you make, so when you choose to export, it knows which doors have new data.

When you export to controllers for the first time, IEI recommends that you perform a full export, rather than changes only. This recommendation applies to existing devices as well as new devices. This option ensures that all the data in the controller is completely synchronized with the database and there is no data that shouldn't be there.

Export Time/Date

This option allows you to set the time and date in the controllers. You cannot export the time or date directly to a Handheld connected controller from the PC software. However, the Handheld device is able to send the time to the controller using the time and date of the Handheld itself.

For directly connected controllers (if available) the PC's clock is used to set the time and date. Before you perform this operation, verify that the time and date on the PC are correct.

Importing Transaction Logs

Each door controller stores it's own transaction event log which the Hub Manager™ Professional software can import into the database. All new transaction log data is appended to the existing transaction log data currently stored in the database. You can use this information to print reports to see activity from your door controllers.

Scheduled Import of Transaction Logs

Hub Manager™ Professional contains a feature called Scheduled Log Import, which allows the system to automatically import the transaction log from your controller's on a schedule that you define. First, you choose a time you want the import to occur, then select how often to import. You can specify how many days between each import, with a minimum of once a day. When the schedule time is reached, the import process will occur automatically. All new transaction log data is appended to the existing data. This feature is not available with controllers that are managed using a handheld device.

> **NOTE:** You must log out, but not exit, for Scheduled Log Import to work properly. If an operator is logged in to Hub Manager™ Professional the log retrieve will not start automatically.

Importing of Door Settings

This features allows you to import all the door settings, including user information, contained in a door controller. You can use this information to verify the controller has the correct information or to print the imported data so you can enter it into the software, in case you have lost your database. This feature is not available with controllers that are managed via handheld device. Please keep in mind that Access Level information is not stored in the controllers. If you have lost your database for some reason, you will have to rebuild your Access Levels prior to entering the data you retrieved from the controllers using this feature. The best way to ensure that you maintain your information is to use the built-in backup feature in Hub Manager™ Professional.

Network Query

The Network Query feature is used to determine the online status of a connected controller (either through serial (or USB) com port, modem or SEG connection). In addition, the Network Query returns the door type and firmware information (if supported by the controller). Before this feature will function, you must connect to the Site through the ***Sites*** directory using the Connect button. Once the connected status is indicated, you can use this feature. You must perform this operation for each Site, if you want to query multiple Sites.

> **NOTE:** This feature is not available when using a Handheld connected controller.

Transaction Log Reports

Below is a brief explanation of some of the transaction log report features.

Transaction Log Report Filter

This options allows you to customize the transaction log report to show only those items that meet your filter criteria, such as a date range, a specific user, a specific access level, any combination of doors or any combination of events.

Archiving Transaction Logs

Hub Manager™ Professional contains a Log Archiving feature, which is used to archive your current transaction log. To use this feature go to ***Tools > Log Archiving***. The archive file is stored in CSV format in a folder of your choice. You can open a CSV file with Microsoft Excel or other CSV viewing program. Once you perform this operation, the log events are removed from the Hub Manager™ Professional database, stored in the archive file and are no longer available in the Log Filter report. To view the data within Hub Manager™ Professional use the Archive Viewer feature.

Misc. Log Reports

Three types of pre-defined reports are available. The first report type lets you see the very first and very last events on a particular day for each door controller. The second report type allows you to see a list of the different days that a particular user had used the access control system. The last report type shows all the users that used the access control system on a particular day.

Time Management Report

The Time Management report is used to calculate how long a user was inside the protected area during a given time period. This report includes both total time (gross time) over a given period, as well as, the total time minus any time outside the building during the same time period (clear time). This report requires controllers that can produce both ***User IN*** and ***User OUT*** events. If the controllers in the system do not have both events, this report can not calculate the amount of time a user was in the building. See Time Management for more details.

Database Tools

Hub Manager™ Professional contains the following database tools, which can assist you in managing your data.

Database Table Initialization

> **WARNING:** Performing this operation will result in data loss. Please perform a backup before performing this operation.

The Table Initialization feature is used to place the database back to an out-of-box initialized state. You have three database options to choose from: ***Database*** , ***Transaction Log*** and ***Audit Trail***. The ***Database*** option, initializes all your access control data, including users, doors, access levels, etc. The ***Transaction Log*** option initializes your transaction event log data. The ***Audit Trail*** option initializes the audit trail database table. When you perform this operation, all data relating the option you choose is removed. This data cannot be retrieved again. It is recommended that you perform a database backup, as discussed below, prior to initializing any database.

Database Backup

Use this feature to create a backup of your existing databases to avoid losing your data. You can then copy these backup files to removable media or other location off the local PC. If the computer's hard drive crashes, you could then reinstall Hub Manager™ Professional and then copy the backup files back to your local PC then restore the database.

Database Restore

This feature allows you to restore your Hub Manager™ Professional database from your backup files, discussed above. With this feature, you can easily recover from a hard drive crash or simply go back to a previous version of your database.

Database Conversion

The Database Conversion Utility is used to convert/migrate your data from any previous version of Hub Manager™ Professional to the latest version of Hub Manager™ Professional. You would use this feature after upgrading to the latest version. This utility program is run from ***Tools > Database Conversion Utility***.

Database Reports

The following two database reports are available in Hub Manager™ Professional.

Assignment Reports

Assignment Reports are a collection of reports that show which items are assigned to other items, such as which access levels contain certain doors or which users are assigned to certain doors.

Database Reports

These reports shows all programmed items within a certain database table. You select, for example, to print a report of all the users in the database.

Operator Audit Trail

The software maintains a time/date-stamped audit trail of most activities performed by the operators within Hub Manager™ Professional. This includes which operator logged in, a brief description of the screens that operator accessed and a brief description of what the operator did in each screen. The report does not give details about exactly what the operator did, but it does show what areas the operator made a change in. You can't produce a customized report within the Hub Manager™ Professional software itself, but you can send it to a file and open the data in another program such as Microsoft Excel or Crystal Reports.

Operator Audit Trail Archiving

This feature provides the ability to archive the audit trail database table. This removes the data from the database and stores it in CSV format in a location of your choice, for later viewing.

Help File

The help, which you are reading now, is available in both electronic PDF and CHM format, as well as, in hard copy form. To access the help file, simply press the ***F1*** key or go to the ***Help*** menu.

4.2 Initial Set Up

Organizing for Hub Manager™ Professional Access Control

Getting ready for programming your access control system is a simple matter, as the software employs the concept of "facility work groups-schedules" for access control. This section describes the concepts involved and provides relevant procedures.

Facility Work Groups

To create and control electronic access for each door in your facility, the Hub Manager™ Professional software uses facility work groups; examples include office workers, supervisors, or work shifts combined with their corresponding normal work times, days, and the doors they can access normally. This latter idea is known as "Access Levels." It minimizes required software programming to a simple action of transferring a mirror image of the existing facility's employee work groups and schedules into the corresponding Hub Manager™ Professional software screens. Access is granted by issuing each person access credentials such as a card, RF Fob, Personal Identification Number (PIN), or other form of credential, and then assigning that person to an identified facility work group called Access Level (an Access Level is a combination of each person's work group, doors, times, and days), and then downloading this access level data to the controllers.

Creating Access Levels

1. Create Access Levels by first identifying and grouping employees according to the following parameters:
   - Logical work groups such as office, factory, supervisors, and marketing for the employees assigned to each work group
   - The normal group work schedule for each work group
   - The doors that each work group can access
   - The times that each work group can access the specified doors
2. Once you finish identifying and grouping employees, transfer this access level information into the corresponding software screens ("forms") used to program facility access control parameters into the Hub Manager™ Professional software.
3. When you finish transferring access level information into the software screens, download each completed software screen ("form") into the system's controllers, to control specified door access with Readers and Keypads.

Database Programming Screens ("forms")

The major Hub Manager™ Professional database programming screens (a.k.a. forms) include:

Sites
If more than one location is involved, input and identify the additional sites in this form.

Time Zones
Input logical facility work group schedules by days and times.

Holidays
Dates when access can be denied to some and granted to others, based upon the setup of the Time Zones.

Doors
Identify each controlled door by name and specify a few basic monitoring parameters here.

Access Levels
Combines the doors and times into an assignable access control structure that can be assigned to each user.

Users
Assign each employee or visitor an access credential combined with an Access Level that can control employee or visitor access by door, time, day of week and even holiday automatically.

Preparing for Access Control Programming

Use normal employee work times to create logical automated access control by group and doors as follows:

1. For each site in your facility, identify and list all doors to be controlled by name and location.
   Example: Lobby, Computer Room, Accounting, Manufacturing, etc...
2. List the groups of people who work at or regularly visit the facility, their normal work schedules, and the doors they can access.

Examples:

General Office Workers
8 AM through 6 PM. M-F
Lobby, Employee Entrance, and Computer Room
Names: (List them here)
(First and Last names)

General Supervisors
24 hours a day, 7 days and holidays

All doors
Names: (List them here)
(First and Last names)

Marketing
7 AM through 7 PM M-F
All but Accounting
Names: (List them here)
(First and Last names)

Tech Support
7 AM through 7 PM, M-F

Lobby
Names: (List them here)
(First and Last names)

3. Transfer the information into the Hub Manager™ Professional software as described in the Transferring Work Schedule section.
4. Download the access control information to the controllers as described in the export to doors section.

Preparing Work Schedule

To transfer your current facility's work schedule into the Hub Manager™ Professional software, follow subsections below.

Preparing Sites

If your system controls more than one site, use the Sites screen in the Hub Manager™ Professional software to identify each site, identify its controllers, and establish the necessary information for communications. Programming, reporting, and communication routes with each site are then linked automatically into the Hub Manager™ Professional software.

Preparing Time Zones

In the Hub Manager™ Professional Time Zone programming screen, transfer the times that reflect the various schedules identified in the previous section.

Example: For Time Zone, fill in each line to reflect each separate possibility of times, days, and holidays applicable to your employee work schedules.

General Office Workers: 8 AM through 6 PM. M-F
General Supervisors: 24 hours a day, 7 days and holidays
Marketing: 7 AM through 7 PM M-F
Tech Support: 7 AM through 7 PM, M-F

Preparing Doors

In the Hub Manager™ Professional Door programming screen, transfer each door's identification into the system by entering the door name and Time zones that are active for the door. In this screen, enter the activities to be monitored and reported, such as extended lock timer, auto unlock-relock, forced door, and door ajar (propped door) events.

Preparing Access Levels

As noted earlier, the Access Level concept allows a single-phase entry method for assigning employees and visitors to the appropriate door and time access control.

1. Using the Hub Manager™ Professional Access Levels programming screen, transfer the identified work groups from your list.
2. Assign logical titles for each group's access level by their type of employee work group.
3. Select appropriate time zones and doors.
   Example:
   Marketing: 7 AM through 7 PM M-F
   All doors but Accounting
4. Create an Access Level titled "Marketing," and then select the appropriate time zone number(s) and doors that reflect the Marketing" group.

Preparing Users

Using the Hub Manager™ Professional User screen, fill in the names, access credentials and select the Access Level (for example, marketing, supervisor). This single step directs the software to create each employee's access privileges automatically.

Managing and Programming System Alarms

Door Contacts can be monitored, and door ajar (propped door), forced door events annunciated for response.

1. Define how long each door can remain open before the door open event is annunciated.
2. Transfer the identified times for each door's information to the Doors screen in the Hub Manager™ Professional software.
3. To annunciate a held open or a forced door event, first define the action to be taken. Examples include "report the event" or "close a relay"; then add this desired action to the door information.

Providing for a Secure System

This procedure involves defining operators and the respective privileges for each.

1. Define which operators are allowed to program the Hub Manager™ Professional system and exactly which programming actions each are permitted.
2. Using the Operator screen, specify all tasks/parameters that each operator is allowed to control, change, report on, or save. Each operator has his/her own password for logon and then can access only their assigned tasks.

4.3 Menu System

Below is complete list of all the available menu options:

SYSTEM
- System Manager
- Login
- Logout
- Change Password
- Exit

DATABASE
- Operators
- Sites
- Time Zones
- Doors
- Access Levels
- Users
- Holidays

COMMUNICATIONS
- Import Door Settings
- Import\Export Doors
- Network Query
- System Dashboard

TOOLS
- Log Archiving
- Audit Archiving
- Database Backup/Restore
- Database Conversion Utility
- Run Com Port Test
- Scheduled Log Import
- Table Initialization
- Indexing
- Application Initialization
- Options

REPORTS
- Log Filter
- Time Management
- Misc Log Reports
- Assignment Reports
- Database

Audit
Archive Viewer
Generate Data for External Report Writer
Scheduled Log Import Errors

HELP

Help
Online Support
Check for Updates
Check for Custom Updates
About

System Main Menu Commands

Below is brief description of each main menu option.

System

Provides a means of:

- launching the System Manager feature which allows you to create, delete, and switch between other Hub Manager™ Professional databases you have created
- logging into the program
- logging out of the program
- modifying current login password for the currently logged in operator
- exiting the program

Database

Contains options necessary for setting required system parameters to operate the door controllers, according to rules established for secure access to protected areas.

Communications

Allows you to export data to the door controllers or import the transaction log from the door controllers, which documents user activity from individual door controllers, to the personal computer database.

Tools

Permits you to maintain the program's databases, back up the databases, ensure proper communications with door controllers, as well as gain access to other utilities.

Reports

Supplies tools for processing and extracting of data from the program's databases, such as summary forms, user lists, user activity lists, forms, etc...

Help

Supplies access to online help information.

4.4 Running the software

Starting the Software

Once the Hub Manager™ Professional program is installed successfully, you can start it in one of two ways:

1. Double-Click the Hub Manager™ Professional v8 shortcut icon that the install program placed on your computer's desktop
2. Browse to the shortcut in the Windows Start Menu Hub Manager™ Professional v8 shortcut.

In either case, you are presented with the ***Login*** screen, unless you have the auto-login feature enabled.

> **NOTE:** The first time you start the program, you are prompted to enter support contact information in a small dialog box. Enter the contact information and select ***Save*** to save it. This information can be changed later by going to ***Help > About*** while an operator is logged in.

Entering Your Login

The default login ***Name*** is "HUBMAN" and the default ***Password*** is "HUBMAN". Please note, the ***Name*** and ***Password*** fields are case sensitive. When you login for the first time you are logged in under the default operator named HUBMAN. For details about creating additional operators see the Operators section. For details about changing your password see the Change Login Password section.

> **NOTE:** If you want the software to auto-login (ie. the software automatically enters your name and password) go to ***Tools > Options > General Options***. Refer to the Options section for details.

Navigating through the Program

The following steps describe the path of a typical operator through the software. Your situation may differ somewhat and depends on the door controller and communication type you are using.

1. Change the default Login (***Name*** and ***Password***), as soon as possible, after installing the Hub Manager™ Professional software.
2. Review the entire General Overview section to learn the basic concepts about setting up Sites, Time Zones, Holidays, Doors, Access Levels, and Users.
3. Run the Hub Manager™ Professional program.
4. Create all of your Sites using ***Database > Sites***.
5. Create the Time Zones required for your system.
6. Create Holidays as applicable.
7. Create Doors and assign the Time-Zones needed in each door controller and modify any of the default controller configurations as needed.
8. Analyze your system by identifying the common groups of users that have identical access privileges (Access Levels). Identify the different possible groups such as managers having 24 hour access to all doors in all sites, a cleaning crew that only has access on the front doors at certain times of the day and week, 1st, 2nd, and 3rd shift workers that only have access during their respective shift periods, normal Monday through Friday 9-5 AM employees, etc…
9. Go to Access Levels and create the Access Group privileges for that Access Level based on your analysis.
10. Go to Users and create the names and define the users access credential fields.
11. Choose ***Communications > Import\Export Doors*** to export data to each door controller in the system.
12. If you are using a DTD to manage your controllers, you must connect the DTD to the PC prior to running the Import/Export operation. If you are using a PDA to manage your controllers, you must cradle your PDA and run HotSync after performing the Import/Export operation. You must then visit each door controller with the Handheld device. Refer to the PDA Software or Data Transfer Device (DTD) Connection sections for the details on sending/receiving data. You must also return to the PC with the Handheld device and perform an import with Hub Manager™ Professional to complete the process. This final step is required to let the PC know that you successfully communicated to the controller.

4.5 System Setup Tasklist

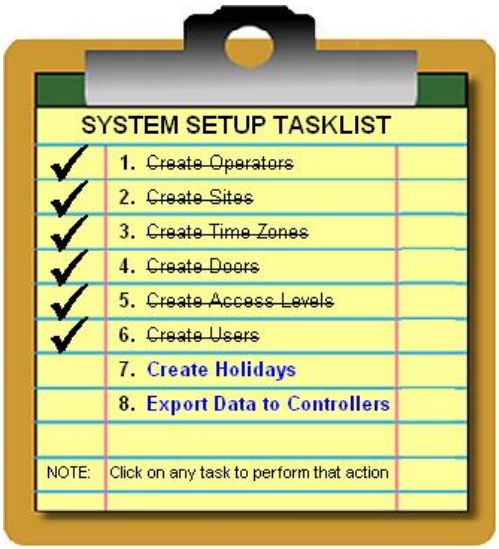
Overview

The System Setup Tasklist is displayed to help guide you through the steps needed to set up a new system.

If you are managing multiple Systems using System Manager, then each new System you create will have a fresh Tasklist, since all of these Tasks are related to each individual System.

Clicking on any of the blue links will bring you to the specific screen that performs that action. For example: if you click on the Create Sites link, then the Sites directory will be opened, where you can then select the Add button to create a new Site.

Once a task is completed, that task will be crossed off the list, the link to that task will no longer be active, and a checkmark will appear next to it showing you that the Task is completed.



Inactive links will become active again, if the action that removed that link is no longer true. For example: if you delete a Site and there are no longer any Sites left in the System then the Create Sites link will once again become active.

There are some Tasks that do not require that you actually Add an item, but it is required that you at least visit that screen in order to have that Task seen as completed. The Tasks that you are required to at least visit are: Create Time Zones, Create Holidays, and Create Operators. The other Task that is not actually monitored for success is Export Data to Controllers. Just the act of opening the Export screen is enough to complete this particular Task.

It is recommended that the Tasks be performed starting with the first Task and ending with the last Task. Several Tasks require that other Tasks be completed first. In these cases, you will be brought to the Task that is required. For example: if the very first Task you select is Create Doors, you will receive a message saying that you must create a Site before you can add a door, and you will then be brought to the Sites directory where you should then add a Site.

Once all of the items in the System Setup Tasklist are complete, the list will be removed from sight. Once the Tasklist is removed, certain actions you perform may make the Tasklist visible again. These actions include:

- performing a Database Restore from a dataset that does not have all of the required Tasks completed (***Tools > Database Restore***)
- performing a ***Tools > Database*** Initialization
- enabling the option that says to display the Tasklist even if all tasks are completed. This option is located at ***Tools > Options > General***.

4.6 PDA Software

LS Link is designed for communications between Hub Manager™ Professional and IEI's LS2\P and prox.pad plus IR controllers. These are standalone electronic access control door controllers that communicate via infrared to a Palm OS PDA. These controllers have two-way infrared communications capability. By using a PDA and the PDA application, you can manage your door controllers with Hub Manager™ Professional.

NOTE: Refer to the Installation section for details about installing the PDA application.

The PDA acts as the connection between Hub Manager™ Professional and your door controllers. Using Hub Manager™ Professional in conjunction with Palm HotSync Manager, you can transfer the data from your PC to your PDA device, then to your door controller. This process is discussed below.

LS Link System Requirements

The following are a list of required equipment in order to use LS Link:

- IEI's Hub Manager™ Professional v8 software
- Windows XP Home or Windows XP Professional Operating System
- PDA with Palm OS 3.5, 4.x, or 5.x
- Palm Desktop and HotSync Manager software (provided by PDA vendor)
- 250KB of available memory on the PDA for each controller you are managing

NOTE: PDA's are not supported by Hub Manager™ Professional when installed on Windows Vista, Windows Server 2003 or Windows Server 2008.

Exporting From Hub Manager™ Professional to the PDA

When you export to a PDA connected site, Hub Manager™ Professional creates data files containing all your controller data and stores this on your PC. You must then run HotSync Manager, which takes those data files and transfers them to your PDA. The following steps guide you through this process. For additional information, refer to the Export to Doors section.

1. Choose ***Communications > Import/Export Doors***, enable the ***Export Changes Only*** option, then select the doors you want to export to, if not already selected. Then press the ***Start*** button to create the export data files. Wait until the entire process is complete before continuing.

   NOTE: If you are exporting to a controller for the first time, it is recommended that you choose ***Export ALL the data*** to completely synchronize the controller hardware with the Hub Manager™ Professional database. A warning message is displayed until you choose the Export ALL option. This is done as a security measure to ensure you are aware that the controller may not necessarily match your database completely.

2. Next perform the HotSync operation with the PDA.
3. Now take the PDA to each controller and export the data using the ***Imp/Exp*** button in LS Link, and follow the on-screen prompts.
4. When finished with all controllers, go back to the PC and HotSync with the PDA. Any transaction log data that was imported is now on your PC awaiting import into Hub Manager™ Professional.
5. Choose ***Communications > Import\Export Doors***, enable the ***Import Transaction Log*** option, then select the ***Start*** button and wait for the import process to finish.
6. When complete, all data between Hub Manager™ Professional and the controller is synchronized.

LS Link automatically handles all existing door data during the HotSync Manager process. All door export data from the Hub Manager™ Professional stored on the PDA prior to the start of the HotSync Manager session is deleted from the PDA memory. All log event data from the doors stored on the PDA prior to the start of the HotSync Manager session is transferred to the PC for import by Hub Manager™ Professional. Once the HotSync Manager has completed, run LS Link from the PDA main Screen. LS Link's main screen has three buttons and a Site drop down list.

The title bar information symbol (in the upper right) is functional in all LS Link screens. Select the information symbol to display the definitions, descriptions of the features/ functions and data presented in the current screen.

***Imp/Exp* Button**

This button is short for Import/Export and it's used to initiate communications with the controller. This includes door identification, importing event data from the controller and exporting new configuration data to the controller.

***Files* Button**

Pressing this button displays the door management screen, which shows you a list of doors in the current site. This area also provides access to more advanced features. Any door controller with a check mark in the ***C*** column denotes that configuration data is stored on the PDA that hasn't been sent to the controller. This is useful to know what doors you still need to visit. Any door controller with a check mark in the ***L*** column denotes that transaction log data is on the PDA that hasn't been transferred to the PC via a HotSync operation.

***Settings* Button**

This area contains the settings for LS Link.

***Site* Drop Down List**

This drop down list contains an alphabetical list of the Sites with door data currently in the PDA's memory. The Site shown in the Main Screen is the currently active site. All operations within LS Link are performed on this active site. When LS Link is launched, the Site drop down list contains a single entry for each site for which doors were exported. By default, the first Site in the list is displayed when you first launch the software.

LS Link Configuration Screen

You can now select a site from the Site drop down list on the Main Screen. If you only have a single site, it's automatically selected when LS Link is launched. After you select a Site, select the ***Settings*** button to open the ***Configuration*** screen. LS Link offers a number of program preferences that you can select in this screen. These items are global, which means they influence the way LS Link functions, regardless of what site is selected.

The ***Configuration*** screen has several settings: ***Auto Export Time/Date***, ***Auto Import Log***, ***Comm Method*** and ***Comm Speed***. These are discussed below.

Auto Export Time/Date

When selected, LS Link automatically updates the controller's time and date whenever communication is established. This option is turned on by default, but can be turned off if you do not want to send the time and date to the controller, for example if you are crossing a Time Zone boundary and know the time is off.

Auto Import Log

When selected, LS Link automatically retrieves the event log from the device without prompting you. When this option is not selected, LS Link displays a message box telling you how many events the device contains and then prompts you to retrieve the log if you want. This option is turned off by default.

Comm Method

This drop down list allows you to select the specific ***IR Channel*** (Infrared) LS Link requires to function using your PDA. This is required because the various Palm PDA devices handle IR communication differently and this channel is tailored for each specific model.

Here is a list of known compatible PDA's and the ***IR Channel*** (infrared) setting that you must select in LS Link.

Make	Model	'IR Channel' Setting (infrared)
Aceeca	Meazura	2
Handspring	Visor	2
Kyocera	7135 Smart Phone	2
Palm	IIIc	1
Palm	IIIx	1
Palm	IIIxe	1
Palm	m105	2
Palm	m125	2
Palm	m130	2
Palm	m500	2
Palm	m505	2
Palm	m515	2
Palm	V	1
Palm	Vx	1
Palm	VIIx	1
Palm	Tungsten E	3
Palm	Tungsten E2	5
Palm	Tungsten T	3
Palm	TX	5
Palm	Tungsten T2	3
Palm	Tungsten W	2
Palm	Tungsten C	4
Palm	Zire	2
Palm	Zire 21	3
Palm	Zire 71	3
Palm	Zire 72	5
Palm	Zire 31	5
Sony	Clie SJ20	2

Models with known problems:

- Palm Tungsten T3
- Palm Zire 22

An updated list of known compatible PDA's is also available at www.ieib.com or in the ReadMe file located at: ***Start > Programs > Hub Manager™ Professional v8 > ReadMe***.

If your PDA is not in the known compatible PDA list then there is still a chance that it may work, but there is no guarantee. You may also use the following PDA descriptions to help you choose the best IR Channel (infrared) setting:

- IR Channel 1 (infrared) - Older PDA's, such as the Palm IIIxe require this setting
- IR Channel 2 (infrared) - This setting is used for PDA's running Palm OS 4.x or 5.x and the PDA does not have an OMAP logo on the back of the PDA
- IR Channel 3 (infrared) - Select this setting for PDA's that display an 'OMAP' logo on the back of the PDA, see the OMAP logo below.
- IR Channel 4 (infrared) - See the list above for PDA models that use this setting
- IR Channel 5 (infrared) - See the list above for PDA models that use this setting
- Emulator - This setting should never be selected

Comm Speed

Drop-down list allowing selection of the baud rate to communicate to the device. The default setting is 19200 and should not be changed.

LS Link Files Screen

To see the list of door files currently on your PDA for the selected site, select the ***Files*** button from the main screen. This area of the LS Link is referred to as the door management screen. This screen is made up of 3 columns: ***Door Name***, ***C L***, and ***Action.*** Below is description of each of these columns.

Door Name

This entry matches the name you gave the controller in the PC software.

C / L

Indicates what operations are pending for the door. A check mark is placed in column C when LS Link has new configuration data available to upload to the device. A check mark is placed in column L when LS Link has received new event log data from the controller that hasn't been returned to the PC via HotSync.

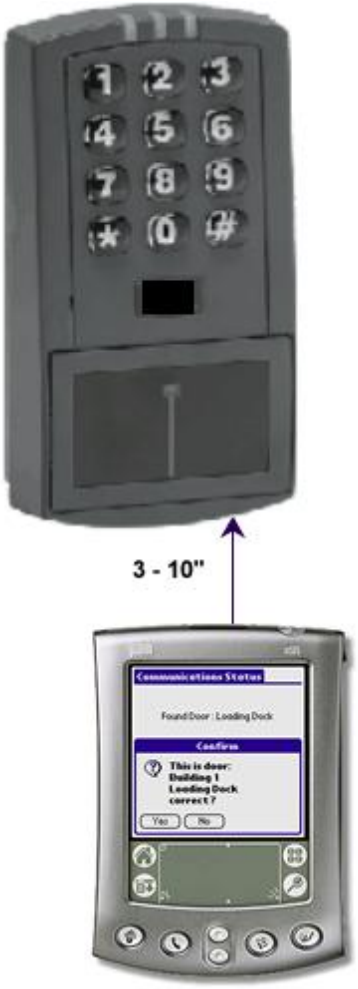
NOTE: Some doors on the PDA may not have new configuration data.

Action

The Action list is a drop-down list of advanced functions that can be performed at the door. These actions include checking the current Time/Date on the controller or looking at the current configuration details. Some actions such as the ***Remove*** option should not be performed unless you are asked to do so by a Technical Support representative.

Communicating with a Controller

1. Select the ***Imp/Exp*** button of the LS Link main screen and point the infrared port of the PDA at the infrared port on the controller, as shown in the following diagrams. See the installation manual for further details on the infrared ports of the controllers.



NOTE: The optimal distance between the PDA and the controller is approximately 3" to 10". Some PDA's perform better at the shorter range and some perform better at the longer range due to the variations in the infrared lens of the PDA hardware. Longer export and import times may result from putting the PDA either too close or too far away from the infrared receiver of the controller. This extra time is due to retries that may result from communication errors.

2. The PDA application first prompts you to "***Please enter your communications code at the door***". The process of unlocking communications is required in order to communicate with the controller.

3. Enter a valid Communications Unlock user credential at the controller. See The Access Levels section for more details on using Com Unlock codes. You can also use the Master Code to unlock communications (the factory default Master Code is 1234*).
4. If this is your first visit to this door, LS Link prompts you to select the door from the list. When you visit this door again, LS Link will automatically recognize that you have communicated with this door before and only prompts you to confirm the door name as noted in the next step.

5. If you have communicated with this controller hardware before, or you just selected the door from the list in the step above, then LS Link asks you to verify the door controller you are communicating with.

6. LS Link then queries the controller to find out how many events it has stored and prompts you with a choice to retrieve them or not. For demonstration, select ***Yes***. LS Link now displays a status bar, retrieves the events from the door and displays how many events it retrieved from the controller.

7. LS Link then determines whether the configuration data stored on the PDA is newer than the data in the controller. If the data is newer, you will be prompted with a choice to send the data to the device or not.
8. If you select Yes, LS Link displays a status bar and transmits all new data to the device.

   NOTE: An export of 2000 users may take about 90 seconds. For security reasons, a full export will occur if you have entered programming mode on the controller or if you have changed the door or site name in Hub Manager™ Professional. Normally, only changes are sent, which takes only a few seconds if you only made a few changes.

9. When finished, LS Link displays a ***Complete*** message.

4.7 Uninstall

Uninstalling Hub Manager™ Professional

WARNING: Uninstalling Hub Manager™ Professional may result in a loss of all database data that you have created.

NOTE: Any files that you created while using Hub Manager™ Professional, such as reports, backups, or other files that were created by the program itself, will not be removed from the hard drive. You will need to remove those files manually. Only files that were placed onto the hard drive by the installation program will be removed, including the entire database.

Windows Server 2003 and XP:

1. From the ***Start*** menu open ***Control Panel***, then select ***Add or Remove Programs.***
2. When the list of programs loads, find the application named Hub Manager™ Professional v8 and select it.
3. Click the ***Remove*** button on right side.

Windows Server 2008 and Vista:

1. From the ***Start*** menu open ***Control Panel***, then select ***Programs and Features.***
2. When the list of programs loads, find the application named Hub Manager™ Professional v8 and select it.
3. Click the ***Uninstall*** button at the top.

NOTE: For further information about uninstalling programs from your PC, please refer to your Windows documentation.

Uninstalling LS Link

LS Link is uninstalled using the installation CD that came with the product.

1. Insert the installation CD.

   NOTE: On most computers, the Autorun program launches automatically. If it doesn't, select ***Start > Run***, browse to the CD-ROM drive, select the ***Autorun.exe*** file, then select ***Open*** and ***OK.***

2. Click on ***Uninstall LS Link***, which is located in the lower right underneath ***Other Options.***
3. You are then prompted with a message stating all the files relating to LS Link will be removed. Click ***Yes*** to continue.
4. When the uninstall is complete, a message indicating it was successful is displayed. Click ***OK*** to close the message.
5. Finally, click the ***Exit*** button on the Autorun screen to close it, and remove the CD.

NOTE: You will have to remove LS Link from the PDA itself. Please refer to the PDA's documentation for instructions on removing applications from the PDA.

Uninstalling the DTD Printer Utility

WARNING: Uninstalling the DTD Printer Utility will result in a loss of all log files currently stored in the ***DTD Printer Utility\LogFiles*** folder. If you want to save these files, you must copy them out of this folder and place them in a different folder on your PC, prior to uninstalling the software.

Windows Server 2003 and XP:

1. From the ***Start*** menu open ***Control Panel***, then select ***Add or Remove Programs***.
2. When the list of programs loads, find ***DTD Printer Utility*** and select it.
3. Click the ***Remove*** button on right side.

Windows Server 2008 and Vista:

1. From the ***Start*** menu open ***Control Panel***, then select ***Programs and Features***.
2. When the list of programs loads, find ***DTD Printer Utility*** and select it.
3. Click the ***Uninstall*** button at the top.

NOTE: For further information about uninstalling programs from your PC, please refer to your Windows documentation.

Chapter 5: System

5.1 System Menu

Selecting the System Menu Item

The System option contains menu choices that allow you to log into the system, log out of the system, change your password, and exit from the program. Select ***System*** from the main menu to display the ***System*** drop-down menu.

You can access the following standard program functions via the System menu:

System Manager
Login
Logout
Change Login Password
Exit

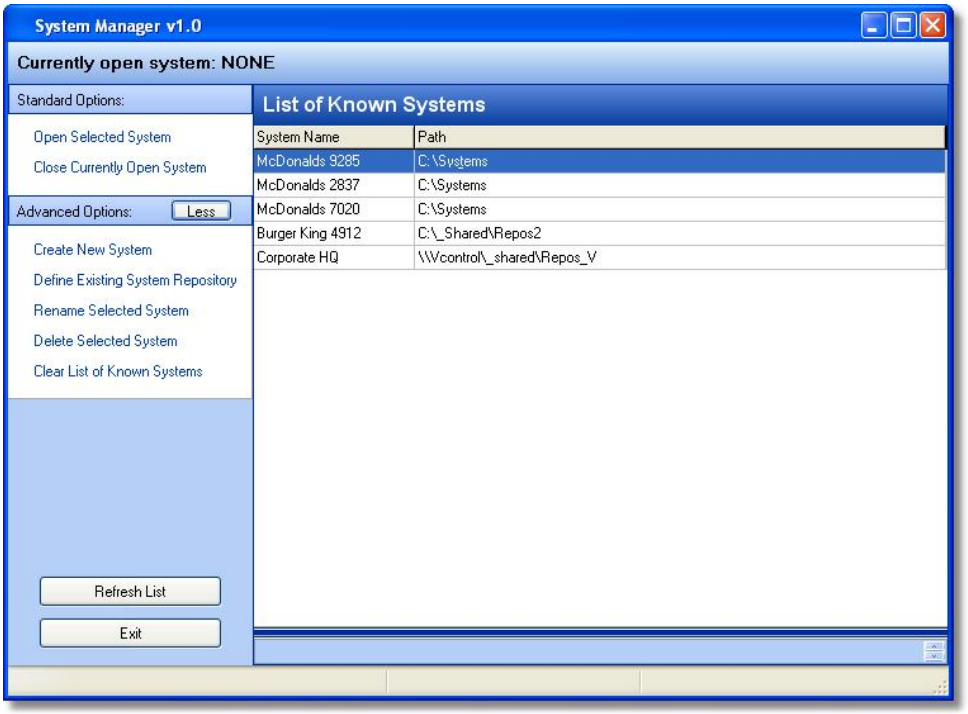
5.2 System Manager

System Manager allows Hub Manager™ Professional to manage any number of individual discrete system databases.

System Manager can also allow access to those Systems by additional PC's on your network. The operators of those PC's must have sufficient network access rights to the folders that store the System data.

A "system" consists of a database and files directly associated with that particular database. Each System is data independent of the other "Systems" you have created.

When a system is created it is stored in a folder that you specify. That folder is called a "System Repository". System Repository folders can be created in any network location that the creating PC has read and write access to. Any number of System Repositories can be created, and a System Repository can store any number of Systems.


System Manager v1.0
Currently open system: NONE
Standard Options:
Open Selected System
Close Currently Open System
Advanced Options:
Less
Create New System
Define Existing System Repository
Rename Selected System
Delete Selected System
Clear List of Known Systems
Refresh List
Exit
List of Known Systems
System Name
Path
McDonalds 9285
C:\Systems
McDonalds 2837
C:\Systems
McDonalds 7020
C:\Systems
Burger King 4912
C:_Shared\Repos2
Corporate HQ
\\Vcontrol_shared\Repos_V

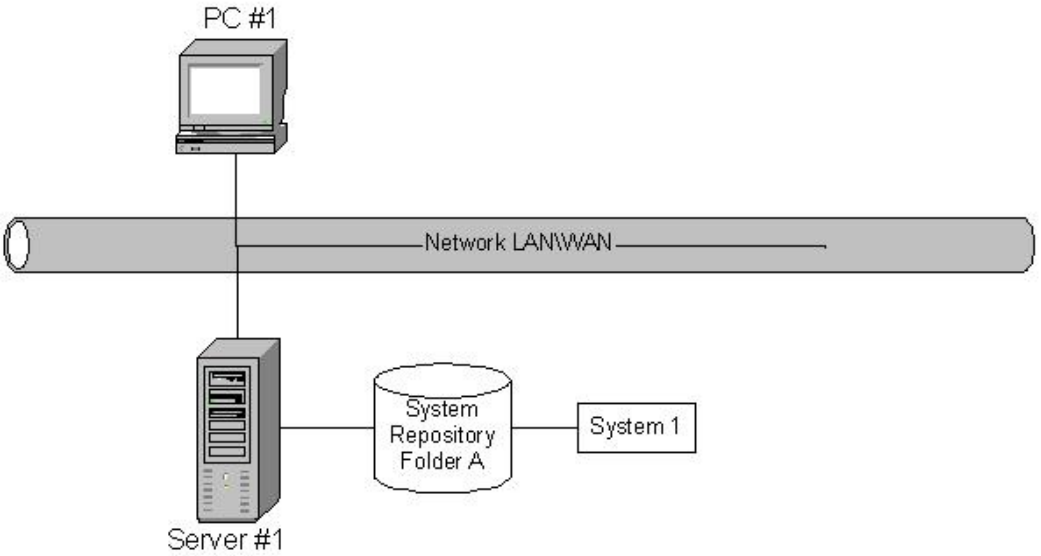
Applications

One operator manages one system

System Manager allows a single operator to manage a single System database. This is nothing new and was always the case in prior versions of Hub Manager™ Professional. But when using System Manager, you have the added advantage that the system dataset can be stored remotely on a server in a folder that is included in automatic backups. That folder is the "System Repository" folder.

NOTE: The act of backing up in this scenario is not performed by System Manager or Hub Manager™ Professional, but would be performed by the backup program running on your server.

Application Example: A single person within a company is responsible for managing the access control system in that company. Hub Manager™ Professional and System Manager are installed on that persons PC. The System may be stored on that PC or somewhere else on the network.

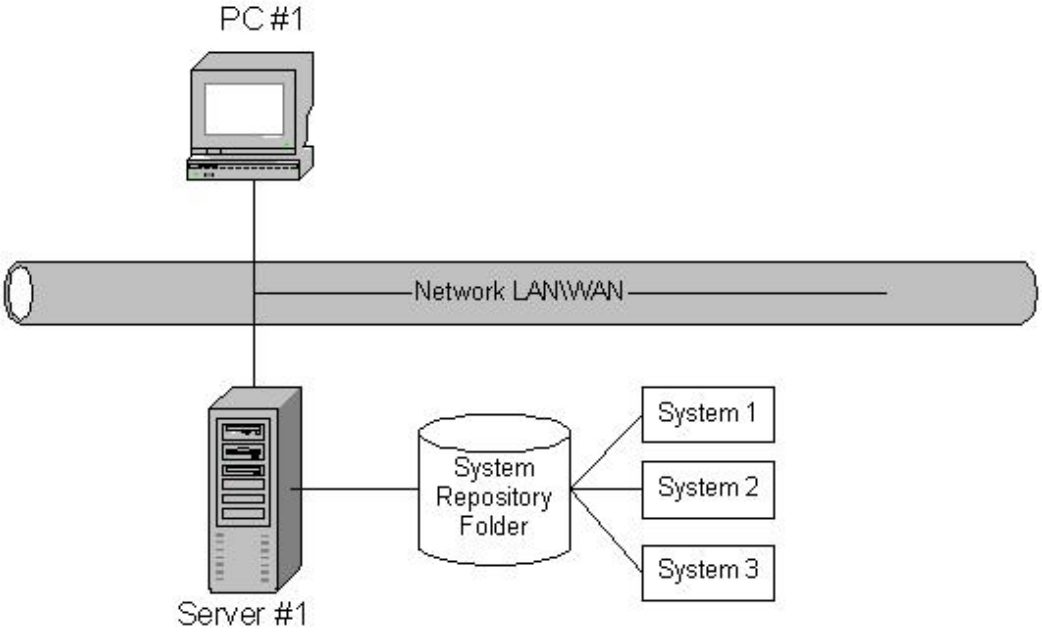


One Operator Manages One System

One operator manages many systems

System Manager allows a single operator to manage multiple discrete system databases, such as those of multiple independent customers. In this scenario, it is likely that all data is stored on the operators PC, or in a folder on a server that only that operator has access to, and this operator can communicate to the access control hardware via the communication type relative to the door controller hardware.

Application Example: A dealer acts as a central station and manages the databases for several customers. He can either connect to the hardware via modems, PDA's, DTD's, or network connection, dependent upon which communication types the access control hardware supports.



One Operator Manages Many Systems

Many operators manage one system

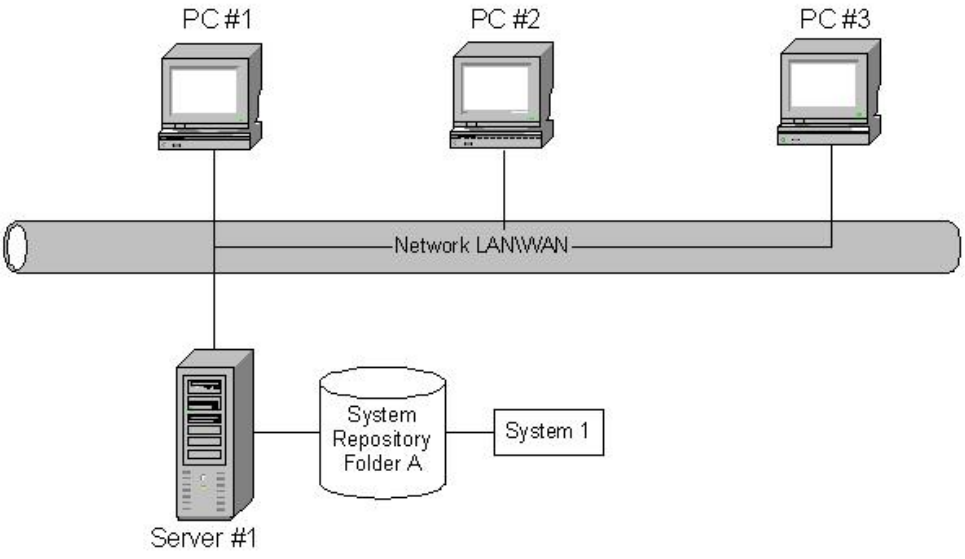
System Manager can be used to allow multiple operators on different computers to manage a single database that is stored on the network and is accessible by all of the operators that wish to manage the data. This is helpful if a company has several people responsible for adding, deleting, and editing users within their own department.

Application Example: A company with several departments manages its own system. Each department head is responsible for managing the users in their own department. Hub Manager™ Professional and System Manager is installed on each department heads PC. The Network Administrator creates a new folder on a server somewhere on the network and grants each department head access to that new System Repository folder.

System Manager is then run on any of the PC's. The operator then selects "Create New System", at which point the operator will select to create the new system in the new System Repository folder that the network administrator had created.

Each department head can then run System Manager and attempt to open that System dataset stored in the System Repository. After all changes are made and exported to the controllers, the department head will then close the System, at which point the system dataset is sent back to the System Repository folder on the network and is ready for access by another department head.

NOTE: If a department head in attempting to open a system that is already in use by another department head, access will be denied. A "Close System Request" can be issued at that point. Please see the section in this topic labeled "Open Selected System (while that system is already opened on another PC)" for more details.



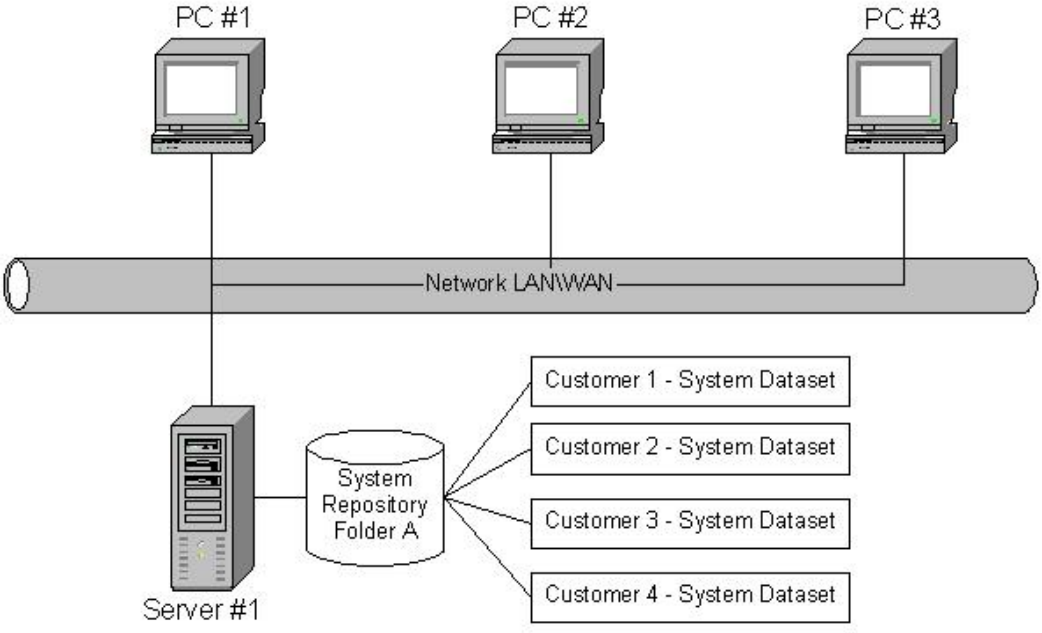
Many Operators Manage One System

Many operators manage many systems

System Manager was designed to be used to maintain multiple individual databases across a network, by multiple operators.

Application Example #1 - Central Station: You're a dealer who manages the access control systems for several of your "end user" customers, and you have multiple employees at your central station who are allowed to modify the data of those customers.

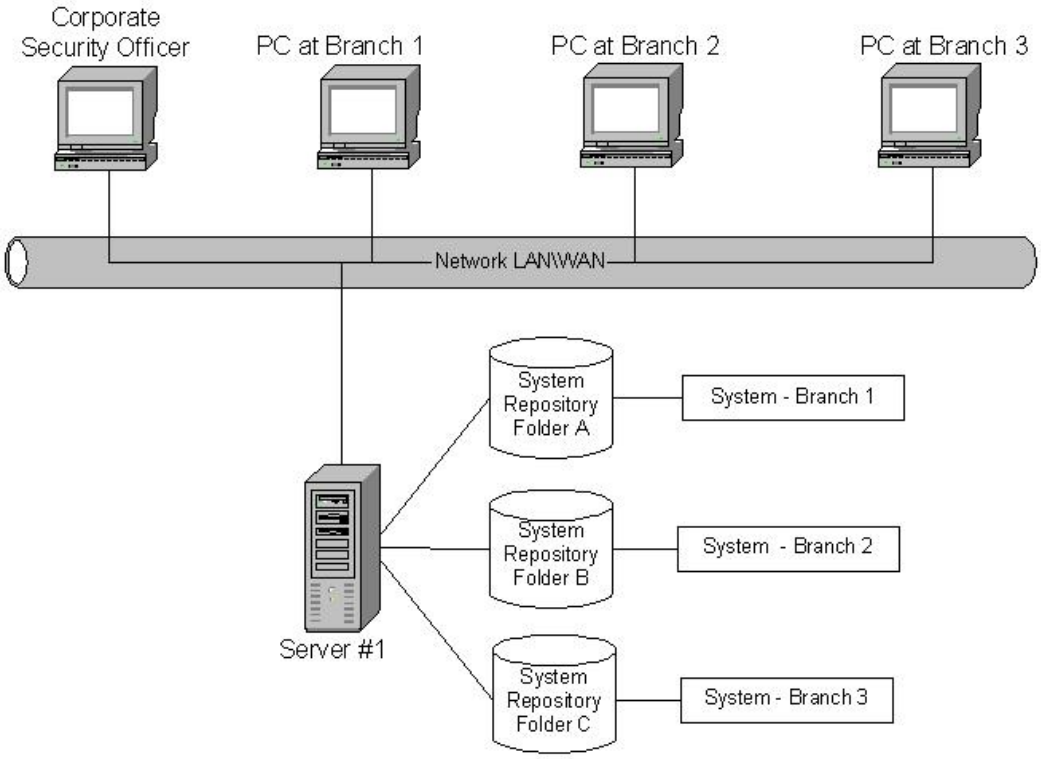
Hub Manager™ Professional and System Manager is installed on each employee's PC that may be managing a customer system. System Manager is run on any of those PC's, and is used to create a new System for each customer. Those systems can be stored in a folder anywhere on the network, as long as that folder is accessible to the other employees that may also be managing that customer's system. All systems can be stored in one System Repository folder or each system can be stored in its own System Repository folder, thereby allowing it to be completely separate. This could be helpful if you do not want to give certain employees access to a particular system. You could simply have the network administrator create a folder on the network that is inaccessible to a particular employee, and then store that customers system in that folder.



Many Operators Manage Many Systems - Central Station Example

Application Example #2 - Multiple Bank Branches: A Corporate Security Officer wants to be able to manage the access control for all branches of a bank, and also allow each Branch Manager to manage the data of their own branch. All bank branches are on the corporate network.

The Corporate Security Officer would instruct the Network Administrator to create a separate System Repository folder on a server for each of the bank branches (as shown in Server #1 in the following diagram). The Network Administrator will also set the network access privileges of each folder to only allow the Corporate Security Officer and the Branch Manager of that particular branch. System Manager is then used to create a system in each of those System Repository folders.



Many Operators Manage Many Systems - Multiple Bank Branches Example

Terms

System Manager
System Manager is a program that is responsible for accessing the System Repository and loading System datasets onto the local PC. System Manager also sends that same dataset back to the System Repository.

System Repository (aka Repository, or Repository folder)
A 'System Repository' is a folder that can store any number of System Datasets. Any number of System Repository folders can be created based upon your security needs. All systems stored in that repository can be accessed by any installation of System Manager that has network privileges to see that particular System Repository folder.

System Dataset (aka Dataset or System)
A 'System Dataset' is a compressed zip file that stores all the data that is related to that particular System, currently including (but not limited to) the complete contents of the following folders: Archive, Backup, Database, Gateway, Maps, DTD, PDAFiles, Print, and ReportDB.

Operator
A person who is using the Hub Manager™ Professional and System Manager software.

Overview of System Manager

Security
System Manager does not restrict access to any of the System Repository folders in any way. Access to the repository folders is based on the network privileges you were given by the network administrator.

A System Repository may be located either on the local PC or in any folder on the network. The security of the stored data is only as good as the security of the folder that stores the data. System Manager uses the security infrastructure of the PC as set up by the Network Administrator.

The software will use whatever means of network connectivity that is provided by the client PC. This may be a shared folder, network folder, mapped folder, VPN, etc...

Launching and Closing System Manager
System Manager can be seen running in the System Tray (typically in the lower right corner of your screen, see below)

System Manager is automatically launched when Hub Manager™ Professional is launched, but System Manager is not automatically closed when Hub Manager™ Professional is closed. This allows System Manager to be able to process messages from other installations of System Manager running on other PC's. One type of request could be that an operator on another PC needs to access to the dataset that is open on your PC, in this case the operator on the other PC will perform a 'Request to Close'.

Basics of Operation

When a System is opened, the System Manager program will actually make a local copy of the data for use during program operation and will store the data back to the System Repository folder upon selecting to close the system. This copy is also created even if the data repository folder is on the local PC.

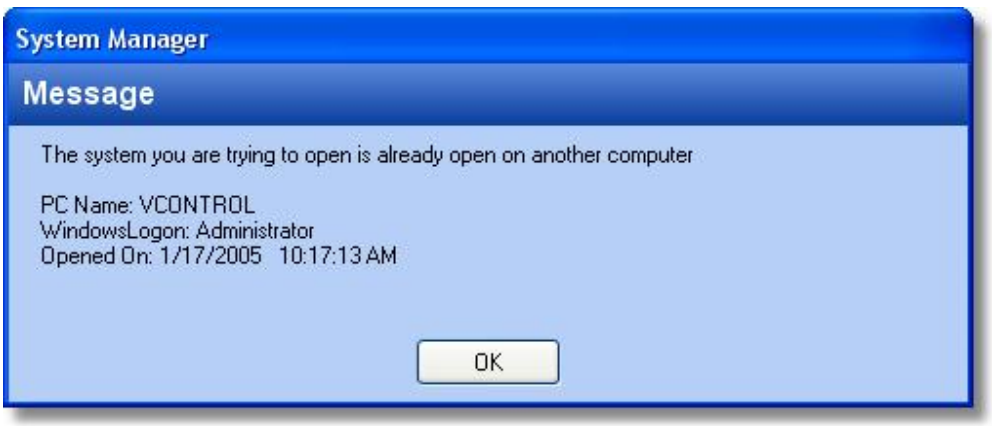
Standard Options

Open Selected System (while the system is not opened on another PC)
This option is used to open the system that is selected in the list. If this option is selected and a different system is already open, then the open system will be closed first, and then the selected system will be opened.

Open Selected System (while that system is already opened on another PC)

- If a system is already open when you select this option, then that system will be closed prior to opening the new system.

- After selecting the "Open" option, System Manager must check to see that the selected system is not currently open on another PC running System Manager. If the system you selected to open is already open on another PC, a message will be displayed showing information relative to the PC that has the system open: the name of the computer, the name of the person logged in when the system was opened, and the time\date when the system was opened by that operator.



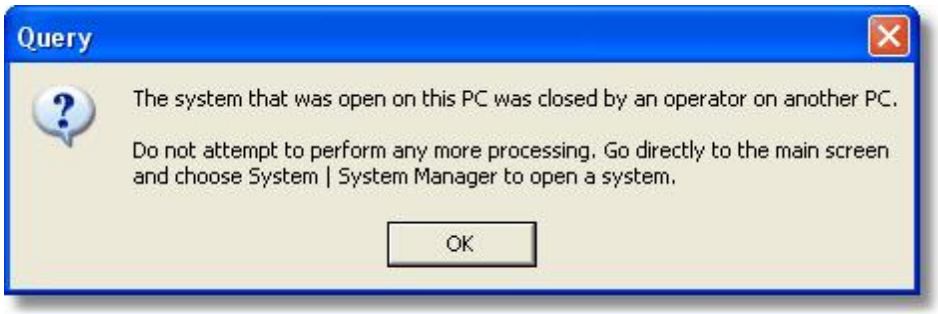
Upon selecting OK, you will then be asked if you want to send a "Close System" request to the PC that has that system open. Selecting OK, will start the "Close System" process.

At this time the PC requesting the close will send a "Close Request" and will continuously waits for a "Close Successful" response from the PC that is closing the system dataset.

NOTE: In order for the close request to be processed by the PC that has the system open, ALL of the following MUST be true:

- the other PC is powered up.
- the other PC is logged into Windows properly.
- the other PC has System Manager actively running. Hub Manager™ Professional does not need to be running, just System Manager. If System Manager is not running, then run Hub Manager™ Professional (if it is not already running) and select System > System Manager from the main menu of Hub Manager™ Professional.
- the System Manager application running on the other PC must be in the typical idle state, and not be in use by the operator, and must not have any messages displayed that require a response from an operator.

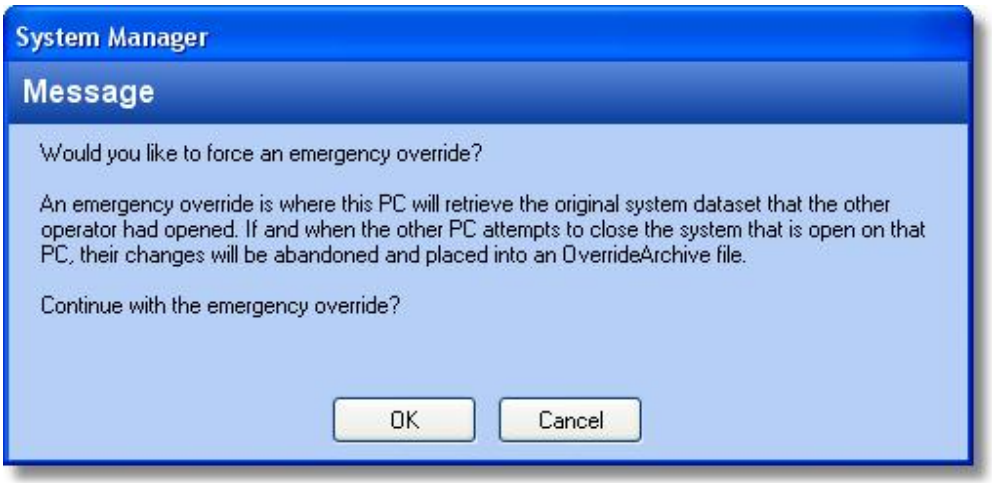
Assuming all of the requirements are met, then the other PC will typically see the close request. The "Close Request" will typically be processed by the other PC without any operator intervention required. During the automatic closing of the system on the other PC, any operator logged into Hub Manager™ Professional will be logged out and the system dataset will be closed normally. If Hub Manager™ Professional was running at the time, then a message will be displayed alerting the operator that the system was closed by another operator on another PC.



If any of the requirements are not met and the other PC does not respond with a "close successful" response within the predetermined amount of time (default is 30 seconds), then a message will be displayed alerting you that the "Close Request" was not processed.

At this point you have 2 options:

- Select OK and wait another 30 seconds for the close successful response from the other PC. You may want to do this if you knew you were having network connection problems, or you contacted the owner of the other PC and had that operator put the PC into the required state as noted above.
- Select Cancel, which will cancel any further waiting, but will then display another message asking if you want to force an "emergency override".



An "emergency override" is NOT recommended and should only be used in rare cases. The reason an emergency override is not recommended is because any changes made to the dataset while that dataset was open on the other PC will be discarded when the other PC gets around to closing the dataset.

If an "emergency override" is executed, then the PC requesting the close simply opens the copy of the system dataset that is stored in the System Repository. That copy of the dataset will not contain any of the modifications made by the other operator who had it open. After the dataset is opened on your PC, a message will be displayed to the other operator that will inform the other operator that their data was overridden and that the dataset they currently have open will be abandoned when that system is eventually closed.

NOTE: In all cases, any changes made to a System dataset while it was open on the other PC will need to be reentered if that System was overridden.

An "emergency override" is known to be helpful in the following situations:

- The other PC, that had the system dataset you need, has crashed and the data on the hard drive can't be recovered. The override will simply cause System Manager to abandon the dataset that was open by that operator, and allow you to open the last saved dataset.
- You need to make a critical change to the system such as deleting an employee and you need to get the data exported to the controllers immediately.

Close Currently Open System

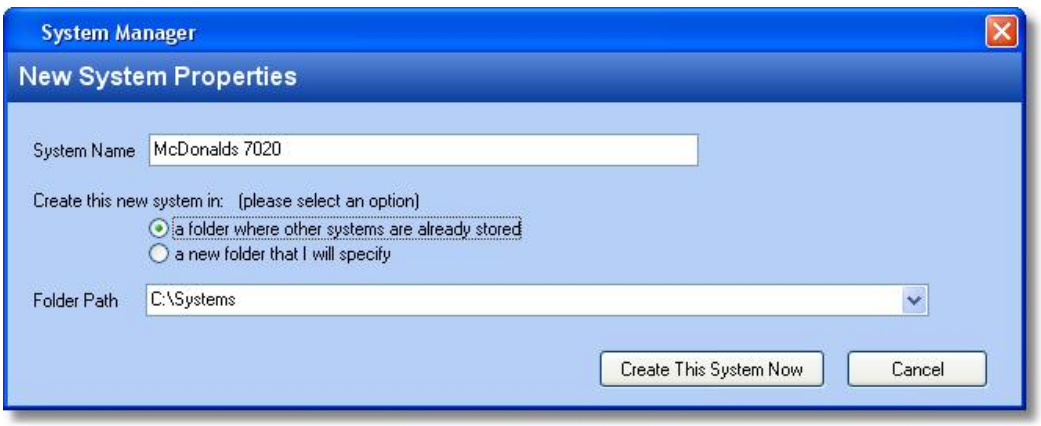
This option takes all of the data associated with the currently open system, compresses it into a single file and sends that "dataset" back to the System Repository from which that dataset was opened from.

Advanced Options

Create New System

Creating a system is the process of creating a new discrete dataset in a folder that you specify. The system name is typically the name of a company, or a subset of a company. The folder that you specify may be either an existing System Repository folder or the operator may choose to specify a new folder that will be considered an additional System Repository folder.

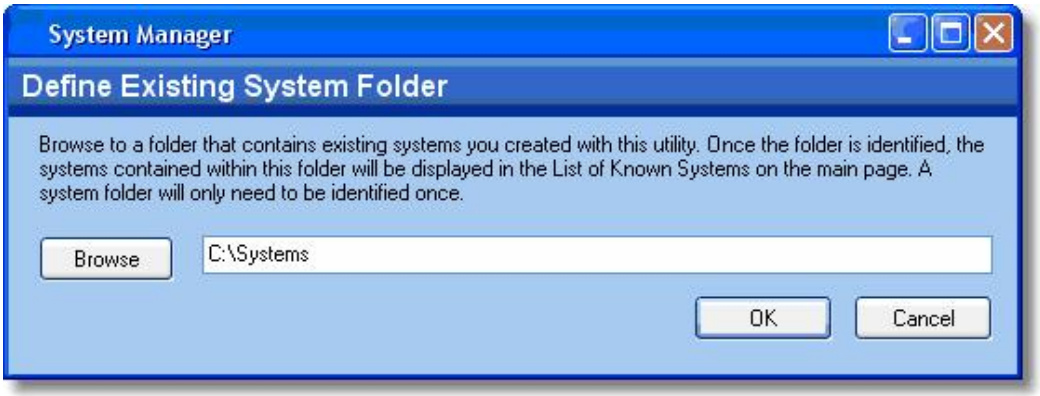
NOTE: If a new system is created, and the option named 'a folder where other systems are already stored' is selected, then that new system will become available to other installations of System Manager that already have network access to the selected System Repository folder. Choosing to use the same System Repository folder to store all systems may be helpful if every installation of System Manager on your network is to have access to all systems that are created. If all installations of System Manager are not going to have access to all the systems you create, then it is recommended that you create a separate System Repository folder for each system you create.



Locate / Import Repository

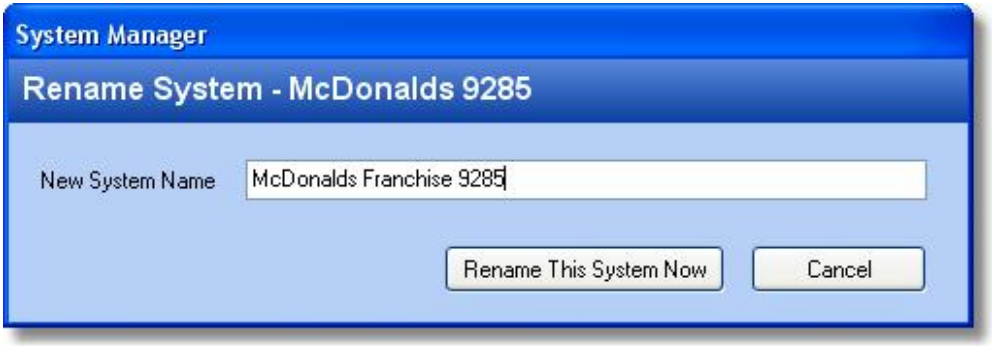
This is the process of using a particular installation of System Manager to navigate to a "System Repository" folder that is currently not "known" by this particular PC. Once you have browsed to that folder, select OK. Now all Systems stored in that System Repository folder will be displayed in your list of known systems.

NOTE: In order to properly access a System Repository folder your Network Administrator must have given you full Read and Write privileges to that folder.



Rename Selected System

This option changes the name of the selected system. Once a system is renamed, the next time an operator runs System Manager the new system name will be displayed in the list of known systems. A system should be closed before it is renamed.



Delete Selected System

WARNING: This option will result in the permanent loss of the selected system data.

This option completely removes all data associated with the selected system. A system must be closed before it is deleted.

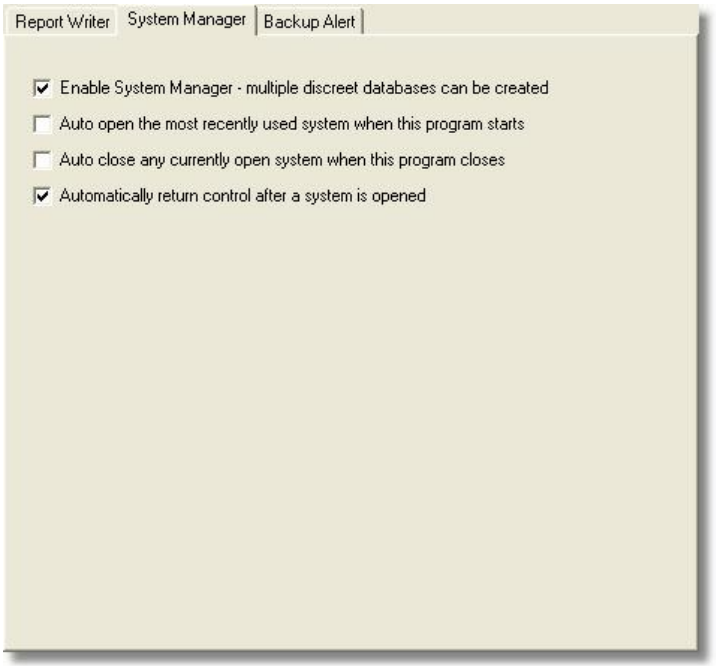
Clear List of Known Systems

This option clears the list of known System Repository folders which are stored locally on this particular PC. This will in turn remove all system names from the list of known systems. This is helpful if you have previously browsed to a System Repository that you no longer want to see the contents of, then this option will clear the entire list and start from scratch.

Refresh List
Forces an update of the "Known Systems List". This option is rarely required.

Exit
Selecting Exit will not close the System Manager program, but will simply minimize the program to the Windows System tray (typically in the lower right corner of the screen). If you want to completely close System Manager then you must right click on the System Manager program icon in the system tray (see below) and select 'Exit System Manager'.

System Manager Related Options Selectable in Hub Manager™ Professional



Enable System Manager - multiple discrete databases can be created

When enabled, this option will enable the System Manager feature. If you are not using any of the features of System Manager as described is this section, you can disable this option. Disabling this option will remove System Manager from the System menu of Hub Manager™ Professional and any opening and closing of system datasets from a system repository folder will cease.

Disabling System Manager will cause Hub Manager™ Professional to handle a database as if only one system exists and the currently open system is always open.

NOTE: Disabling System Manager is recommended only if the following are true:

- You have only one system
- The dataset to reside on the local PC
- The only operator that is going access the data is an operator of that particular PC

Auto open the most recently used system when the program starts

NOTE: This option requires that the 'Enable System Manager' option above is enabled.

Enabling this option will cause System Manager to automatically open the System that was most recently used, without the need to intentionally run System Manager. The opening of that system will automatically occur when Hub Manager™ Professional is launched. Enabling this option is helpful if you are typically using Hub Manager™ Professional to edit the same System over and over again.

Enabling this option is helpful if you have installed Hub Manager™ Professional on an operators PC and you feel that operator would have no need to know about System Manager. If this is your reason for enabling this option then you will also want to enable the 'Auto Close' option below.

Auto close any currently open system when this program closes

NOTE: This option requires that the Enable System Manager option is enabled.

Enabling this option will cause System Manager to automatically close the currently open system when the Hub Manager™ Professional program is closed. This is useful if you have multiple operators that access a particular database, because it increases the chances that when an operator is done exporting changes and closes Hub Manager™ Professional that the System Dataset will be sent back to the System Repository and made available to other operators on other PC's running System Manager.

Automatically return control after a system is open

NOTE: This option requires that the Enable System Manager option is enabled.

Enabling this option will cause System Manager to give control back to Hub Manager™ Professional directly after a system is loaded, without requiring that you exit System Manager, once the operator has selected 'OK' after the system has been successfully opened. Once you have an understanding of how System Manager works, enabling this option can help speed up the System Open process a little, but isn't required.

5.3 Login

To obtain access to the Hub Manager™ Professional program's features, you must enter a valid login, which consists of two entries, ***Name*** and ***Password*** , into the Login dialog box. The factory default ***Name*** is "HUBMAN" (all upper case letters) and the default ***Password*** is also "HUBMAN" (all upper case letters). IEI recommends that you change the default operator name and password immediately after initial installation.

1. Select ***System > Login*** from the main menu. The Login dialog box displays.

2. Enter your ***Name*** on the first line of the ***Login*** dialog box (the factory default is HUBMAN) This field is case sensitive.
3. Next enter your ***Password*** second line (the factory default is HUBMAN). This field is case sensitive.
4. Click ***OK*** to log into Hub Manager™ Professional.
5. If you enter a valid login, the Hub Manager™ Professional program activates, giving you access to program options you are allowed to use. Your operator privileges are defined in ***Database > Operators***.
   NOTE: If the login is not valid, the ***Invalid login name or password*** message appears. Check your login name and password, then re-enter it. Both fields are case sensitive so verify that Caps Lock is not turned on.

5.4 Logout

The ***Logout*** option allows an operator to log out or quit the Hub Manager™ Professional software without actually exiting the program. Whenever you choose this option, you must login to the system again to use the Hub Manager™ Professional software. To access this feature, select ***System > Logout*** from the main menu.

For example, a reason to Logout and not exit the program is if you enable ***Schedule Log Import*** under the ***Tools*** menu. To use this feature, you must log out but not exit the program completely before the automatic transaction log import can occur.

In a PDA connected system, when a HotSync is performed, transaction logs are retrieved from the PDA and placed onto the PC, but are not stored in the Hub Manager™ Professional database. By using the scheduled Log Import feature, you can have those transaction log events automatically imported into the database on a schedule. This is helpful if you want to have someone responsible for using the PDA to retrieve transaction logs from the door controllers, but not give them access to the Hub Manager™ Professional program itself. Now that person can simply visit each controller and then HotSync the PDA afterwards. The log import to the database is then be performed automatically, without user intervention.

5.5 Change Login Password

IEI strongly recommends that you edit the default operator using ***Database > Operators*** as soon as possible after installing the Hub Manager™ Professional software. Make sure you write down the name and password and store them in a safe location. Once you are logged into Hub Manager™ Professional, you can change your password using the ***Change Password*** option.

1. Select ***System > Change Password*** from the main menu to open the ***Change Password*** dialog box.

2. Enter your ***Current Password*** on the first line, then enter your ***New Password*** on the second line. You must re-enter your new password on the ***Confirm Password*** line for confirmation.

   NOTE: If you changed the initial password but do not remember your current password, contact IEI technical support.

3. Finally, press ***Save***. After you successfully change your password, a confirmation box appears indicating success.

5.6 Exit

The ***Exit*** option exits you from the Hub Manager™ Professional software. Once selected, the Hub Manager™ Professional main window closes and you must restart the program to access its features. Select ***System > Exit*** from the main menu.

Upon exiting, the software may prompt you that changes to some number of doors has occurred, but you have not exported the changes to those door controllers yet.

In addition, a prompt may display stating that Scheduled Log Import is enabled. The Scheduled Log Import feature does not function if you exit the software. For it to work properly, you must log out of Hub Manager™ Professional, but do not exit the software.

Chapter 6: Database

6.1 Database Menu

You can access the following sections via the ***Database*** menu system:

Operators
Sites
Time Zones
Doors
Access Levels
Users
Holidays

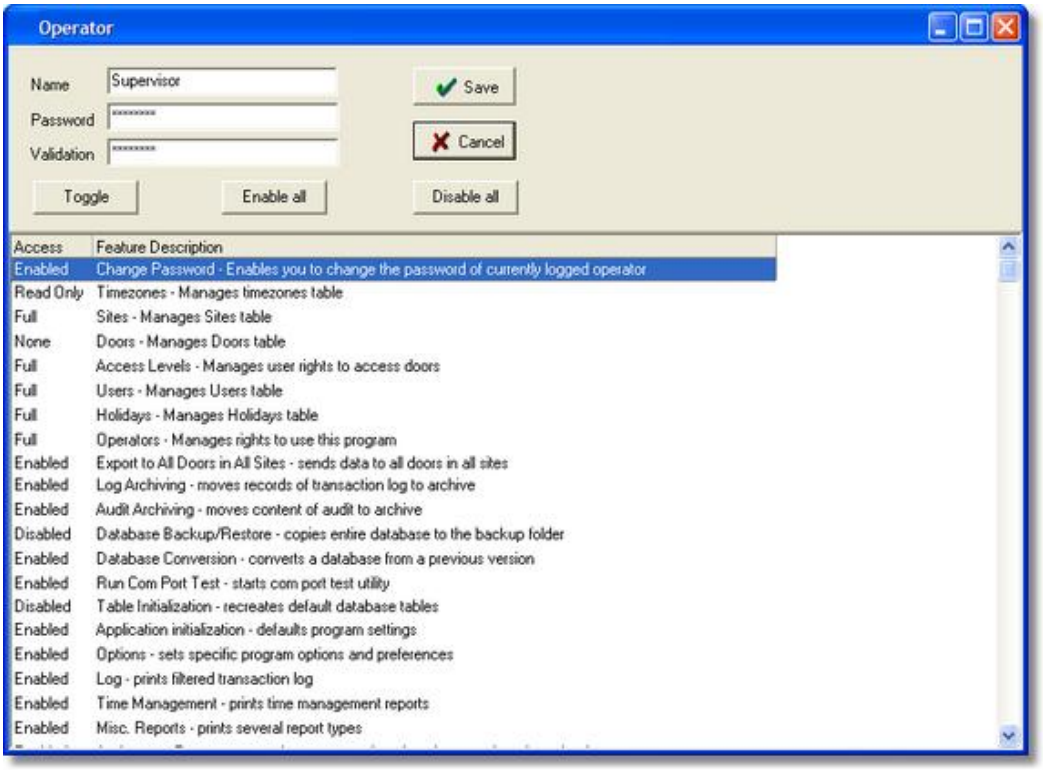
6.2 Operators

Operators Option

The Operators option lets you add operators with the ability to create, view, or manipulate data in the Hub Manager™ Professional databases. Detailed screens allow you to specify which activities a particular operator can perform. All operators having any type of access to Hub Manager™ Professional databases are listed. To select the Operators option, select ***Database > Operators***. The Operators screen displays. An operator is a combination of ***Name*** and ***Password*** that is used to login to Hub Manager™ Professional.

Adding an Operator

1. Select the ***Add*** button on the ***Operators*** screen.



2. Enter the operator ***Name***, ***Password*** and re-enter the password in the ***Validation*** field.
3. Choose which features you the operator to have access to. Select a feature and either click the Toggle button to move through the three options, or click directly on the ***Access*** field to switch between options.
4. Select ***Save*** to save the operator data to the operator database.

Field/Button Description

Name
Specifies the name of the operator.

Password
Specifies the password for this operator.

Validation
Text box used to re-enter the password for this operator.

Access
Lists the authorization required, if any, for all parts and databases of the Hub Manager™ Professional program.

Full: operators with this authorization can view records, add new records, and modify or delete existing records.

None: operator with this authorization cannot modify records, or view data or records.

Read only: operators with this authorization can view records, but cannot add new records, or modify or delete existing records.

Feature Description
This area describes the software feature you are controlling access to.

Toggle
Cycles through the available options for a particular feature. Or you can double-click the feature to cycle.

Enable All
Enables full access to all features in Hub Manager™ Professional.

Disable All
Disables access to all features in Hub Manager™ Professional.

Save
Saves the current operator data to the operator database.

Cancel
Discards all changes to this operator and returns you to the previous screen.

6.3 Operator Wizard

The Operator Wizard presents you with a step-by-step process to creating an Operator that can log into Hub Manager™ Professional. This wizard was created to allow you to create an operator with the least amount of effort (mouse clicks) required, as well as allowing you to select from a number of 'canned' operator types. It will also help you to create multiple operators with consistent access privileges you have selected.

Initial option

The initial option asks you to specify whether you want to add a single operator or multiple operators with the same privileges.

Step 1 of 1 - SINGLE OPERATOR

- Simply define the name and login password.
- When assigning privileges you can either choose from a predefined 'canned' profile, with the respective options enabled, or you can choose to copy the privileges from an existing operator.
- Regardless of which option you choose, the privileges can always be customized before the operator is created.

Step 1 of 2 - MULTIPLE OPERATORS

- Specify the number of operators you want to create.
- When assigning privileges you can either choose from a predefined 'canned' profile, with the respective options enabled, or you can choose to copy the privileges from an existing operator.
- Regardless of which option you choose, the privileges can always be customized before the operator is created.

Step 2 of 2 - MULTIPLE OPERATORS

- This is where you specify how you want to define the multiple operators login name and password.
- You can either let the wizard create the names for you, or you can tell the wizard to prompt you for each operators name and password.
- You can always edit any of the operator settings after the operator is created.

6.4 Sites

Setting up a Site is the first step in creating your access control system. A Site is defined as a group of controllers with the same connection type. You may create as may Sites with the same or different connection type as you require. Each Site must have a unique name.

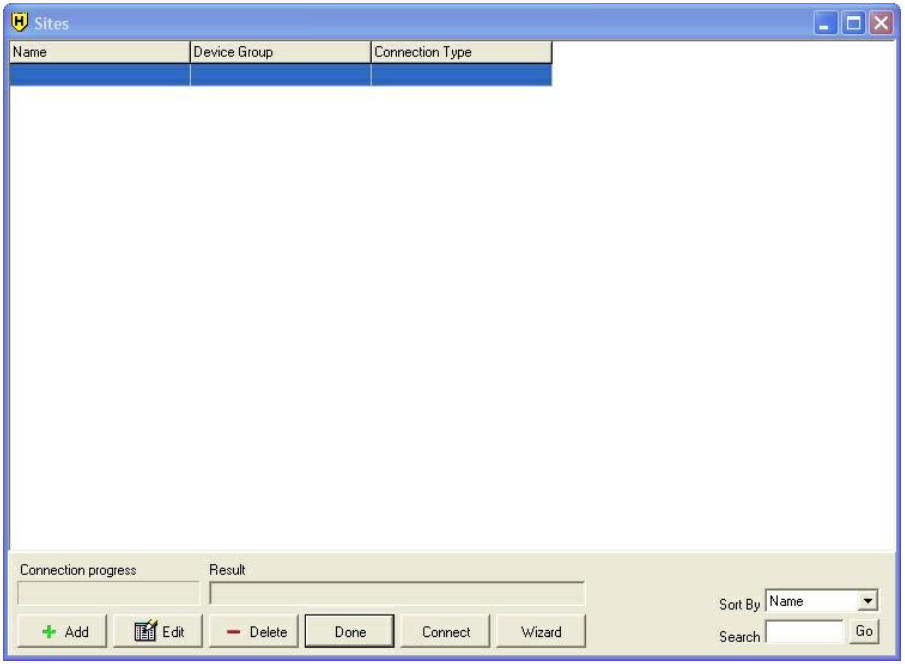
The following table shows which connection types are supported by each controller type:

Controller Type	Serial (RS-232)	Serial (RS-485)	SEG (LAN)	Modem	PDA / DTD
HC500	X		X	X	
Hub+\Max	X		X	X	
Max 2 v1	X		X	X	
Max 2 v2	X		X	X	
LS2\P					X
prox.pad plus		X	X	X	
Max 3 v1		X	X	X	
Max 3 v2		X	X	X	
prox.pad plus IR					X

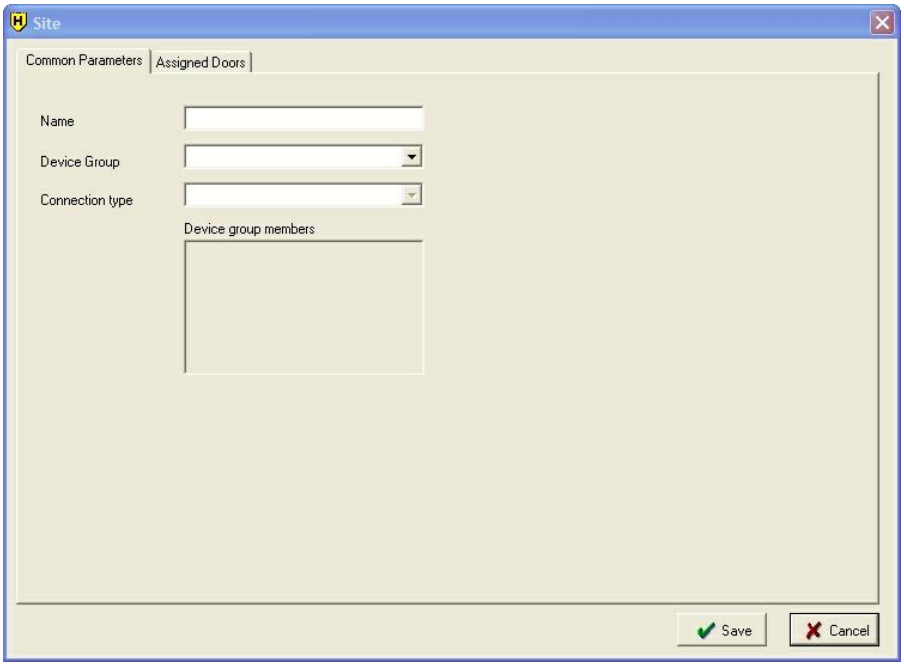
NOTE: The Palm OS PDA option is only supported when Hub Manager™ Professional is installed on Windows XP.

Adding a Site

1. Select ***Database > Sites*** to open the ***Sites*** directory.



2. Click the ***Add*** button on the ***Sites*** screen to open the ***Site*** edit screen.



3. Enter the ***Name*** of your site.
4. Select the ***Device Group*** that contains the controller type for this site. You can only choose a single Device Group.
5. Select the ***Connection type*** you want to use to connect to the controllers in this site.
6. When you select the ***Connection type***, a tab appears next to the ***Common Parameters*** tab, indicating the connection type you've selected. Next, select this new tab and make the appropriate settings changes specific to the connection type. For more information regarding each connection type see the following topics:

   PDA Connection
   Data Transfer Device (DTD) Connection
   Serial Connection (RS-232 or RS-485)
   LAN/WAN Connection (SEG)
   Modem Connection

7. Select ***Save*** to save the site information to the database.

Sites Directory Field/Button Description

Search
Use the ***Search*** edit box to search the ***Sites*** directory for a certain word, such as a Site name. To search, type in the text you want to search for, then click the ***Go*** button.

Go
The ***Go*** button is used when searching for a word entered into the ***Search*** text box.

Sort By
The ***Sort By*** drop down box allows you to sort the ***Site*** directory by any column at the top of the screen, such as the ***Name***, ***Device Group***, ***Connection Type***. To sort the list, click on the down arrow next to ***Sort By***, then choose an item in the list. The list will then automatically re-sort itself based on your selection.

Connection progress
Shows the connection progress while attempting to connect to this site. In order to successfully connect to a modem site, the Master Code in the database must match the Master Code in the controller with the Door Address of 1.

Result
During the connection process the ***Result*** box displays text describing the connection progress. When this process is complete this box contains the end result of the connection (ie. whether it succeeded or failed).

Add
Click the ***Add*** button to add a single Site.

Edit
To edit a Site, select the Site in the list and click the ***Edit*** button. You can also double-click a Site to edit it.

Delete
Use the ***Delete*** button to remove a Site from the database.

> **NOTE:** If you currently have doors assigned to the site, you must remove the door from the site you are trying to delete.

Connect/Disconnect
Use this button to connect to a specific Site. First, highlight the site, then click the ***Connect*** button. The button name changes to ***Disconnect*** after a successful connection.

You must be connected to each individual Site before performing a ***Network Query*** of a Site. It is not required, however, when using the ***Import\Export Doors*** feature since the software automatically connects to each site during this process.

Done
To close the ***Sites*** directory, click the ***Done*** button.

Site Add/Edit Field/Button Description

Name
Enter the ***Name*** of your site here. (30 character max)

Device Group
Select the ***Device Group*** containing the controller type you are are using from the drop down list.

Connection Type
Select the communication method you plan to use for this site from the drop down list.

Save
Click the ***Save*** button to save your changes to the Site you are adding or editing.

Cancel
If you want to discards all edits you made, click the ***Cancel*** button. After clicking the button, you are returned to the ***Sites*** directory.

Assigned Doors Tab

The ***Assigned Doors*** tab contains a list of all the doors that are currently assigned to this site.

6.4.1 Site Wizard

The Sites Wizard presents you with a step-by-step process to creating Sites. This wizard was created to allow you to create Sites with the least amount of effort. The option to create a single Site is to using Hub Manager™ Professional to create a single site. The real benefit of the wizard comes when creating multiple sites at once, because once the settings are specified, they are copied to each of the multiple sites created.

Adding a Single Site

First, choose the option ***Add a single site***, then follow the on-screen instructions.

Step 1

Simply specify the ***Name***, ***Device Group***, and the ***Connection Type*** you are using.

Step 2

Here is where you specify the ***Connection Type*** parameters. These settings are different depending on what connection type you selected in step 1.

Adding Multiple Sites

First, choose the option ***Add multiple sites with common parameters***, then follow the on-screen instructions.

Step 1

Simply specify the (***number) # of sites*** you want to add, the ***Device Group***, and the ***Connection Type*** you are using.

Step 2

Here is where you specify the ***Connection Type*** parameters. These settings are different depending on what connection type you selected in step 1.

Step 3

This step asks you how you want to name your sites. You have two options to choose from. You can either add all the sites at once and name them later or you can set up the sites individually using the wizard. If you choose the second option, you must enter the name for each site as you are prompted.

6.4.2 Serial Connection

A serial connected site is connected using the PC's COM Port, which is RS-232, or a USB port. The HC500, Hub+\Max, Max 2 v1, and Max 2 v2 communicate using RS-232 and can connect directly to the PC COM port using the appropriate connections. If you're PC does not have a COM port, you can connect the system to the USB port, using a USB to RS-232 converter.

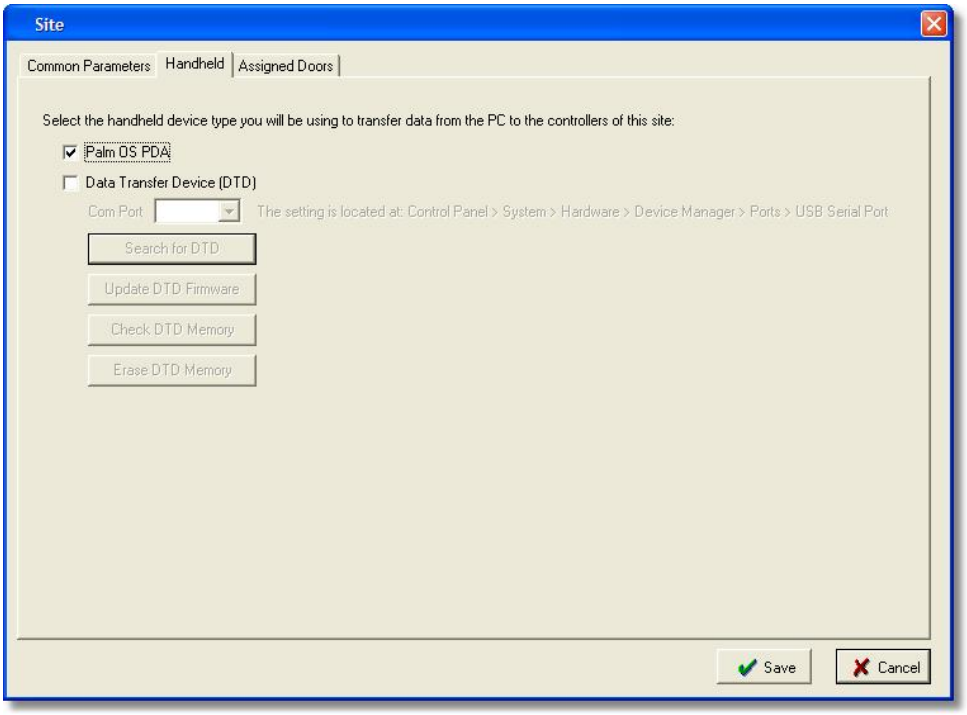
The prox.pad plus, Max 3 v1 and Max 3 v2 controllers communicate via RS-485. To make a serial connection to these products you must install either an RS-232 to RS-485 converter or a USB to RS-485 converter between the PC COM port or USB port and the first controller in the network.

6.4.3 PDA Connection

A PDA connected site is defined if you are using your PDA as a transfer device between Hub Manager™ Professional and your prox.pad plus IR and LS2\P controllers. There are no additional settings to define for this connection type.

> **NOTE:** The Palm OS PDA option is not supported when Hub Manager™ Professional is installed on Windows Vista, Windows Server 2003 or Windows Server 2008. If you are using these operating systems, you must use the Data Transfer Device (DTD) as your communication device.

To use a PDA as your communication device select ***Palm OS PDA*** in the ***Handheld*** tab on the ***Site*** edit screen.



See PDA Software for more details on using the PDA software.

6.4.4 Data Transfer Device (DTD) Connection

Data Transfer Device vs. PDA Operation

The Data Transfer Device (DTD) is a handheld battery powered device used to send and receive data with prox.pad plus IR and LS2\P controllers.

The main difference between the Data Transfer Device and a PDA is the way data is transferred from the PC to the DTD. Unlike the PDA, which requires Palm Desktop software, HotSync Manager and LS Link, the DTD does not require any additional software and interfaces directly with Hub Manager™ Professional via the PC's USB port.

The Data Transfer Device (DTD) is compatible with a USB port (v1.1 or v2.0) and requires Hub Manager™ Professional v7.3 (or higher) to operate.

Before using the DTD you must install the USB drivers. The DTD is plug and play, so when you plug it in, your PC should recognize the and attempt to install the drivers. You can either tell Windows to search automatically or browse to the drivers yourself, which are located on the Software Installation CD and are also installed onto the PC when you run the software installation.

Installing the USB Drivers

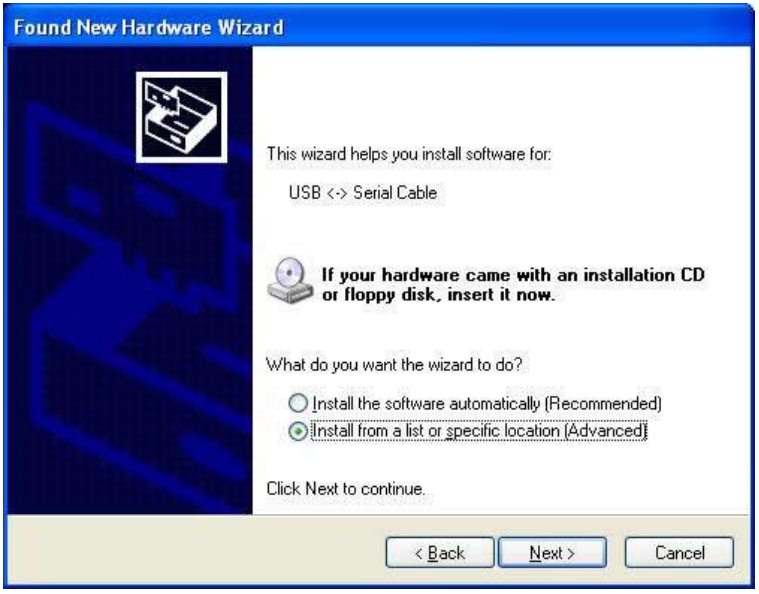
The following steps are part of the Microsoft Windows ***Add Hardware Wizard*** and varies in the different Windows versions, but the overall concept is the same. These USB drivers are for use with the following operating systems: Windows Server 2003, Windows Server 2008, Windows XP and Windows Vista.

To use the DTD you must install the USB drivers on the PC. The DTD is plug and play, so when you plug it in, your PC should recognize the new hardware and launch the ***Found New Hardware Wizard*** as shown below.

> **NOTE: Please note that this hardware wizard runs twice. Follow the same steps both times.**
>
> **NOTE:** These instructions are for a typical Windows XP system. If you are using a different version of Windows, or these steps do not match your PC, please refer to the instructions for your system.

1. On the first screen of the wizard select ***No, not this time***. then click the ***Next*** button.

2. After clicking the ***Next*** button, choose the option that says ***Install from a list or specific location (Advanced)*** and click the ***Next*** button.

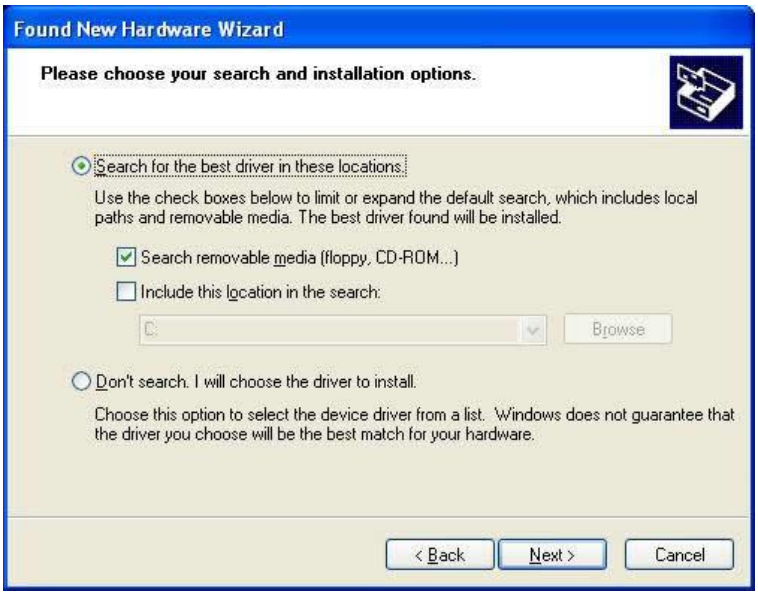


3. On the next screen select ***Search for the best driver in these locations*** at the top. If you've already installed Hub Manager Professional onto the PC, select ***Include this location in the search*** and browse to the following path:

   NOTE: The folder path below is the default installation path. If you did not install the software to C:\Program Files, you must browse to your custom installation path.

   C:\Program Files\IEI\HMP8\Utilities\USB_Driver\FTDI

NOTE: If you haven't installed Hub Manager™ Professional, the USB drivers are also located on the CD. Choose the option ***Search removable media (floppy, CD-ROM…)***. For reference, the USB drivers are located in the following folder on the CD: E:\Driver_USB\FTDI (Note: This folder path is an example; Your CD drive letter may not be E.). Click ***Next*** to continue.



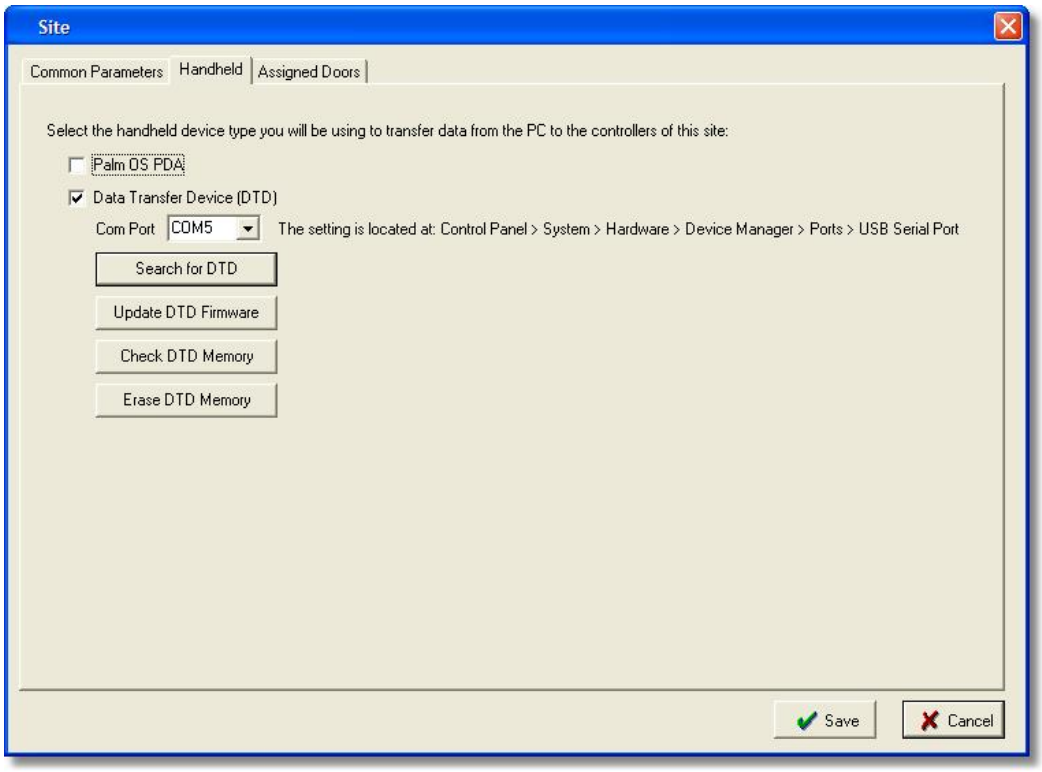
4. Next a screen appears indicating the files are being copied, then you're presented with the following screen to indicate the process is finished. Click on the ***Finish*** button to close the ***Found New Hardware Wizard***.

   Please note that this hardware wizard runs twice due to requirement of the USB hardware manufacturer. Visit the knowledge base on www.ftdichip.com for details. Follow the same steps both times the wizard runs.

Site Settings - Handheld Device Type Selection

To use the DTD as your connection type in the ***Site*** settings screen, go to the ***Handheld*** tab. Here you are given a choice of Handheld devices. Select ***Data Transfer Device (DTD)***. After choosing the DTD, several other items related to the DTD selection appear. These are described below.

NOTE: When using Hub Manager™ Professional on a Windows Vista, Windows Server 2003 or Window 2008, the DTD is the only option.



Field/Button Description

***Com Port* Drop Down List**

This is where you to specify the COM port number that Microsoft Windows assigns to your DTD when you connect it to your USB port. See the section below named Determining the USB COM Port Number to learn how to find the COM port number. Hub Manager™ Professional only allows you to use COM ports 1 through 9 with the DTD. If Windows assigned a Com Port higher than 9 to your DTD, then you can change it through the advanced settings of your USB drivers. Contact Technical Support if you need assistance.

> **NOTE:** If you are using System Manager to maintain multiple DTD systems or you have multiple DTD sites within a single system, but you only have one DTD, make sure that all your DTD sites are set to use the same COM Port. This is important because once Windows assigns the DTD a COM port number, it always uses the same number each time you connect the DTD .

***Search for DTD* Button**

Use this button to search for the DTD on the COM Port set in the drop down list of this screen. If the DTD is not found on the specified com port, then you will be asked if you want to search the other COM Ports 1 through 9.

***Update DTD Firmware* Button**

This option updates the DTD firmware if a new version exists. This process takes approximately 2 minutes or less, depending upon the speed of your PC.

> **IMPORTANT NOTE:** Once you start this process, do not disconnect the DTD from your PC. You must wait until the process is completely finished before disconnecting the DTD.

***Check DTD Memory* Button**

This option displays a summary of the door file information that is currently stored on the DTD including firmware revision and part number, total door capacity, existing export files, existing log import files and mode of operation.

***Erase DTD Memory* Button**

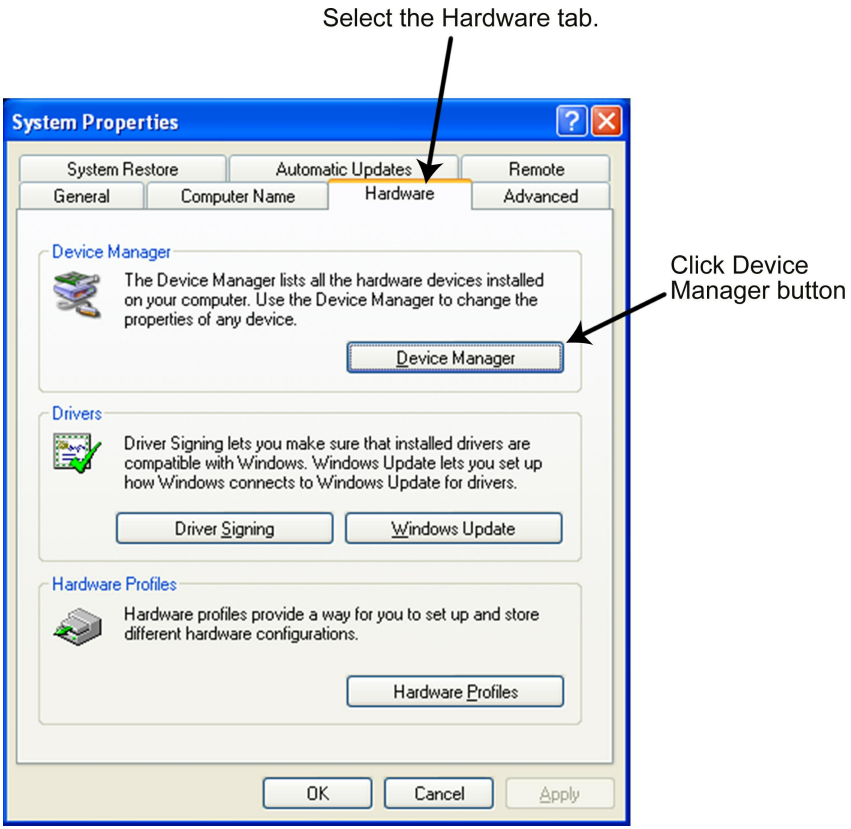
This option erases the entire memory of the DTD bringing it back to an out-of-box state. It takes a maximum of 10 seconds to complete. Any data on the DTD, such as imported event logs, is erased and cannot be recovered.

Determining the USB COM Port Number

When you connect the Data Transfer Device to your computer's USB port, the PC automatically assigns it a COM port number. You must then select this COM port in the software to communicate to your DTD. You can either use the automatic search feature in Hub Manager™ Professional or follow the instructions below to determine the COM port number. Note: These instructions are for Windows XP. If you are using a different Microsoft Windows operating system please refer to the instructions for that operating system.

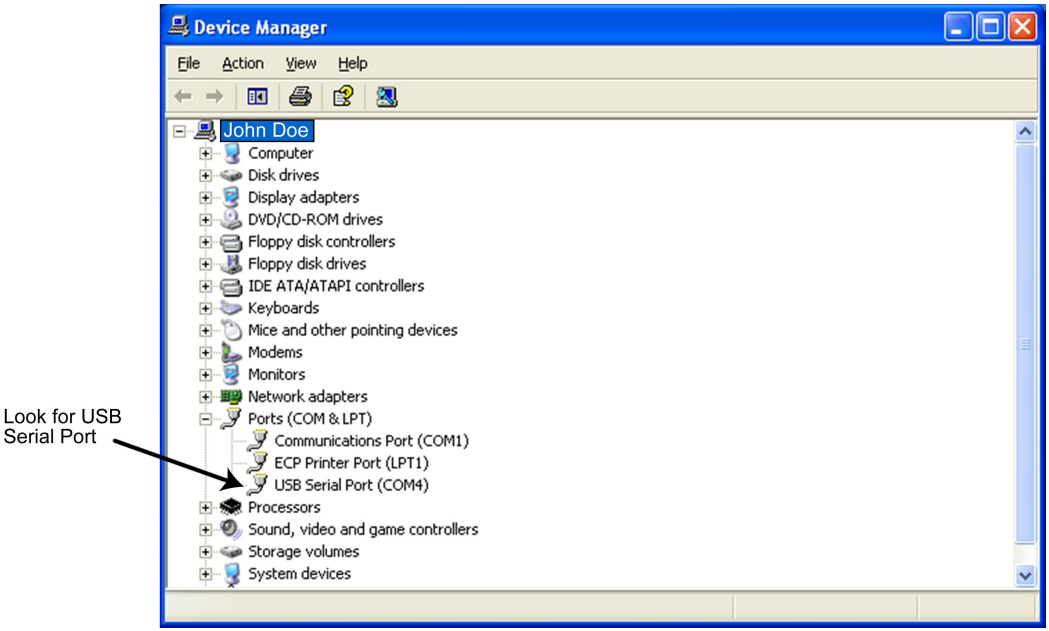
1. Right click on the My Computer icon on your desktop and select properties from the drop down list.

2. When the System Properties screen opens select the Hardware tab, then click on the Device Manager button.



3. When the device manager list opens, expand Ports (COM & LPT) by clicking the + symbol. Under this is a list of the COM ports on your PC. Look for USB Serial Port (COMx) in the list. The COM port is shown to the right. The example below shows the DTD is assigned to COM4.

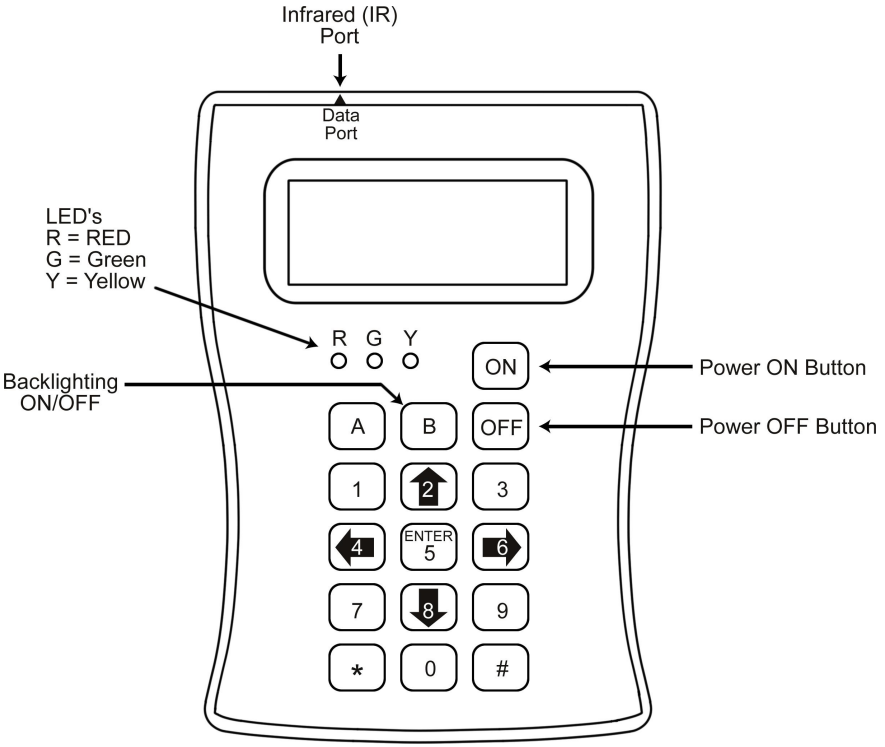
NOTE: If you are unsure of which device it is, unplug the USB cable and the screen will refresh. Take note of which devices are in the list. Then plug the cable back in and notice which device re-appears in the list.



NOTE: If you unplug the DTD from the USB port and plug it into a different physical port on the PC or on a USB Hub, the COM port number will remain the same.

DTD Diagram

Below is a diagram of the DTD. It shows the location of the Power On/Off buttons, the backlighting button and the LEDs. These are explained in detail in later sections. The IR (infrared) port is located at the top of the unit above the display where it says “Data Port.” When transferring data to the door controller aim the IR (infrared) port on the DTD at the IR (infrared) port on the door controller.



Aiming the DTD

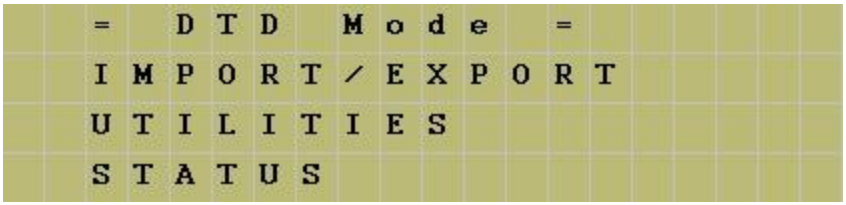
The following diagrams show how to aim the DTD at your product.

DTD Menu System

From the factory, the DTD is set in DTD Mode. This mode is used to send data and retrieve transaction event logs from controllers that support two way communications

When the DTD is first powered-up the the Start-up Screen is displayed. To access the DTD menu system press the ENTER key, which is the number 5 key in the center.

Next you are presented with the DTD Mode Main Menu: IMPORT/EXPORT, UTILITIES and STATUS. The IMPORT/EXPORT menu is used to export data to the controller or import transaction logs. The UTILITIES menu contains options to retrieve information from the door controller, time and date options and communications options. The STATUS menu contains door information, DTD information, as well as an option to change the operating mode. These menu options are described in more detail in later sections.

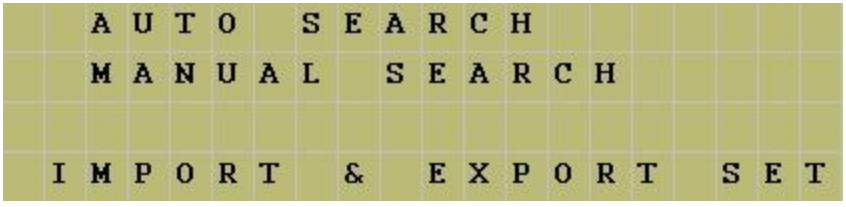


To navigate through the menu system, press the down arrow, which is the number 8 key in the lower center or the up arrow, which is the number 2 key in the upper center. The blinking cursor on the left of the DTD display moves up and down next to the various options. To select and option press the ENTER key. To move back to a previous menu press the left arrow, which is the number 4 key on the left center.

NOTE: If at any time you want to return to the Start-up Screen press the * key in the lower left corner. Also pressing the left arrow brings you back to the previous menu.

IMPORT/EXPORT Menu

The IMPORT/EXPORT menu is used to export data to the door controller and import transactions from it. There are two options: AUTO SEARCH and MANUAL SEARCH. These options are described below.

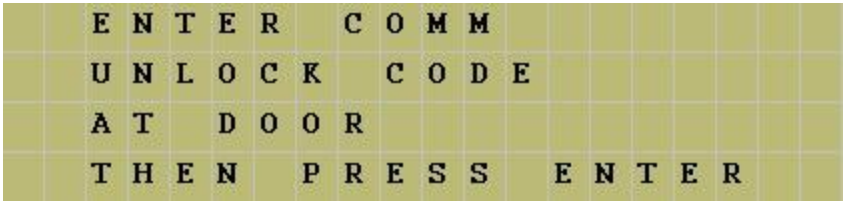


NOTE: The bottom line of this screen indicates which import/export option is set.

Exporting using the AUTO SEARCH Menu

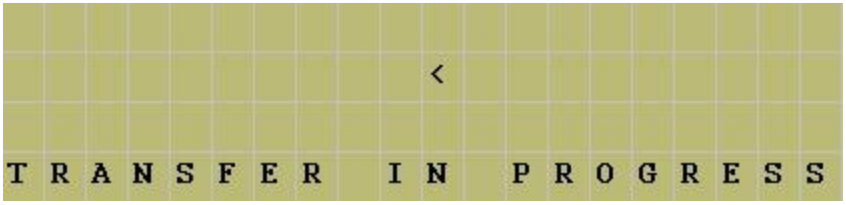
The AUTO SEARCH option is used to communicate to a door automatically. When communications begin the DTD reads the serial number out of the door controller and compares that to the serial numbers in the door files stored on the DTD. When it finds the matching door file, the import/export begins. Note: If a matching file is not found, the DTD prompts you with a warning message. When you press ENTER, you are sent to manual search mode (see section 3.1.2), where you select the door from a list.

First, enter your Com Unlock code on your door controller, then press the ENTER button on the DTD to select AUTO SEARCH. If communications are not established, you are prompted with the message below, which indicates you either entered the wrong code or the DTD is not aligned properly. Press ENTER to continue.

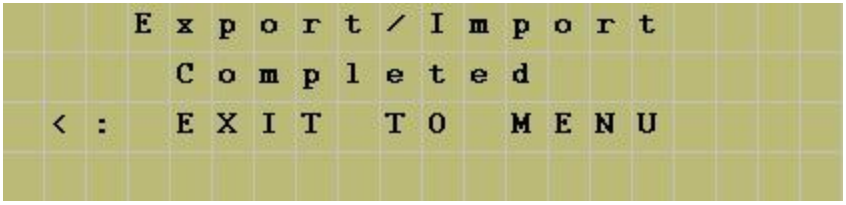


If a matching door file is found, the following screen appears indicating the name of the matching door it found. Press ENTER continue the import/export process.

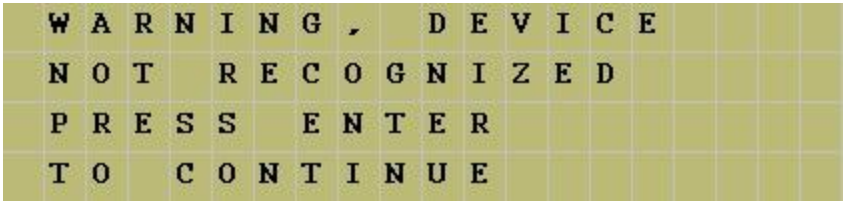
When the transfer begins the following screen appears and the green LED turns on. If at any point you lose communications with the door controller, the red LED turns on. You have 10 seconds to move the DTD back into range.



When the data transfer is complete the following message appears. Press the left arrow to exit to the menu.



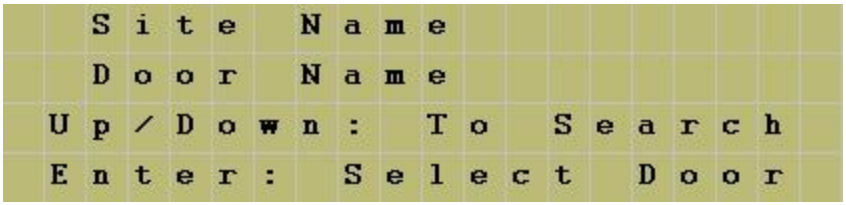
If a matching door file is not found, the following message appears. When you press ENTER you are brought to the manual search screen, which allows to choose a door from the list. Please refer to the following section discussing the MANUAL SEARCH menu.



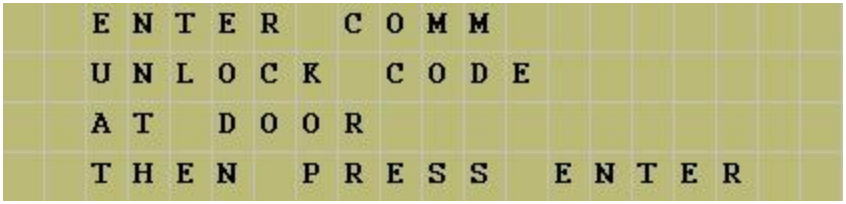
Exporting using the MANUAL SEARCH Menu

The MANUAL SEARCH option is used when you are communicating to a door controller for the first time or if a door is not found. When you select this option, the search screen is displayed. To navigate through the list of doors use the up and down arrows.

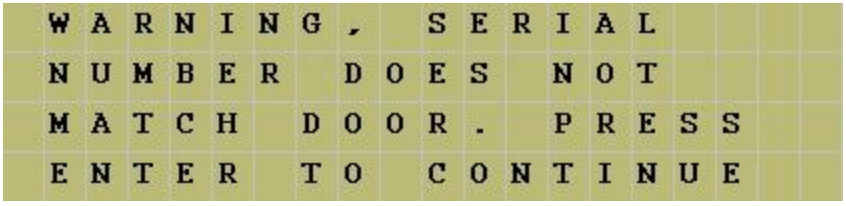
The doors are displayed as shown below. The site name is on the first line and the door name is on the second line.



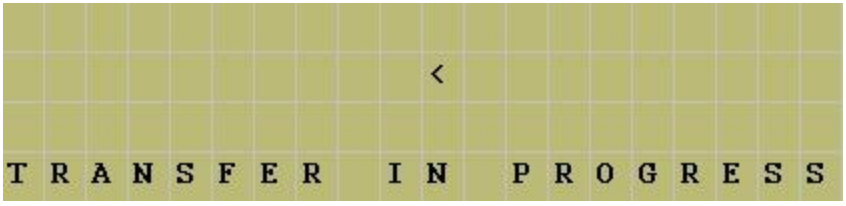
When you reach the door you are looking for, stop. Now enter your Com Unlock code on your door controller and aim your DTD at the Infrared (IR) port on the door controller and press the ENTER key. If communications are not established you are prompted with the following message (either you entered the wrong code or are not aligned properly). Try again, then press ENTER to continue.



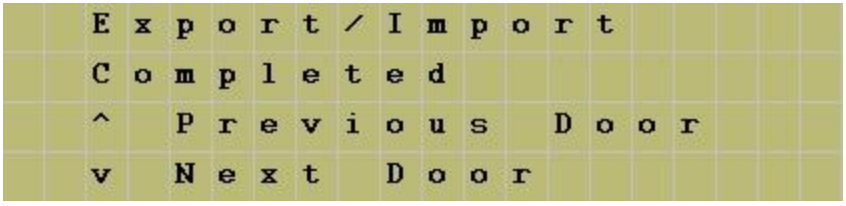
If the serial number in the export file you are trying to send does not match the serial number in the controller, you are prompted with a warning message. This message means one of two things: either the serial number in the door file you chose does not match the serial number of the door controller or this is the first time you've attempted to communicate with the door.



If you wish to proceed, press the ENTER key to continue. When the transfer begins, the following screen appears and the green LED turns on. If at any point you lose communications with the door controller, the red LED turns on. You have 10 seconds to move the DTD back into range.

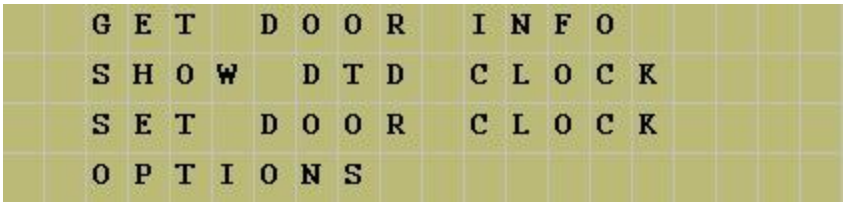


When data transfer is complete, the message below appears. Press the up or down arrows to move through the door list.



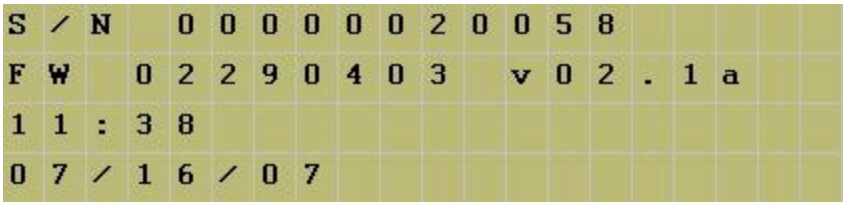
UTILITIES Menu

To access the UTILITIES Menu press the ENTER button from the Start-up Screen. Next you a presented with three choices. Press the down arrow to move the cursor to the UTILITIES option and press the ENTER key. You have four choices in this menu, as shown below.



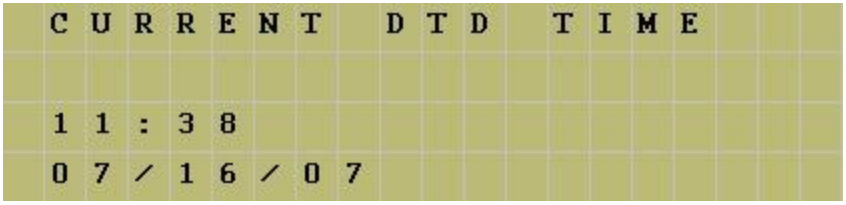
GET DOOR INFO

The GET DOOR INFO menu item is used to retrieve information from the door controller. First, enter your Com Unlock code on the door controller. Next aim your DTD at the Infrared (IR) port on the controller and press the ENTER key. If successful, the door information is immediately displayed on the DTD screen. This information includes the door controller serial number, firmware part number and version, time and date.



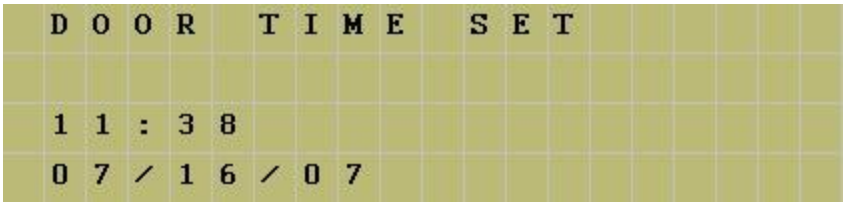
SHOW DTD CLOCK

The DTD maintains the current time and date that it receives from the PC. To view the current DTD time and date, select this menu option. You can only update this time and date using the PC software.



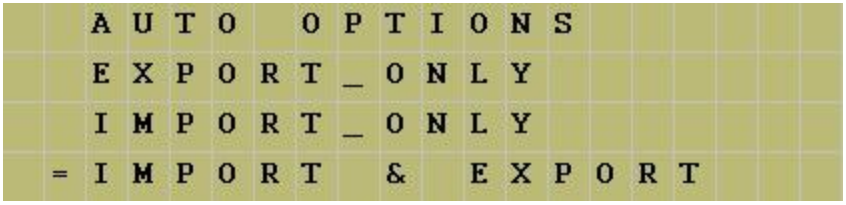
SET DOOR CLOCK

Hub Manager Professional has an option to automatically set the time and date in the controller when you export. You also have the option to set the time and date in the door controller using this menu option. First, enter your Com Unlock code on the door controller. Next aim your DTD at the Infrared (IR) port on the controller and press the ENTER key. If successful, the message below is displayed on the DTD screen.



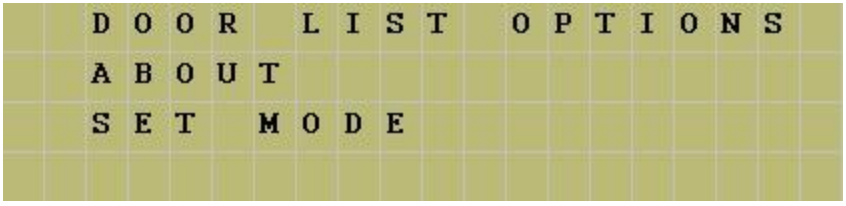
OPTIONS

The OPTIONS menu allows you to set the DTD to the following three options: EXPORT ONLY, IMPORT ONLY or IMPORT & EXPORT. If you only wish to export data to the controller, choose EXPORT ONLY by pressing the ENTER key with the cursor next to that option. When set, the DTD displays a confirmation message. Press the left arrow to exit the message and return to the menu. The "=" symbol indicates which options is currently set. Select the IMPORT ONLY option when you only want to import transaction log data from the door controller without exporting any data to it. The IMPORT & EXPORT options performs both operations.



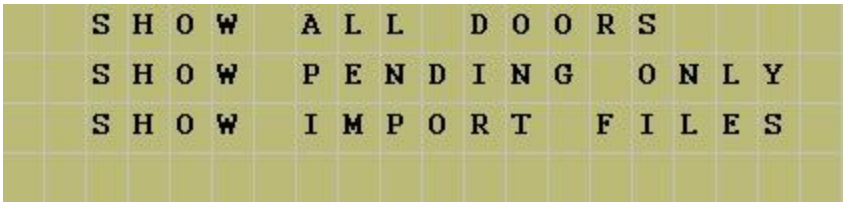
STATUS Menu

The STATUS menu has three options. The first displays information about the doors stored on the DTD, the second has information regarding the DTD unit and third option allows you to select the DTD operating mode.



DOOR LIST OPTIONS

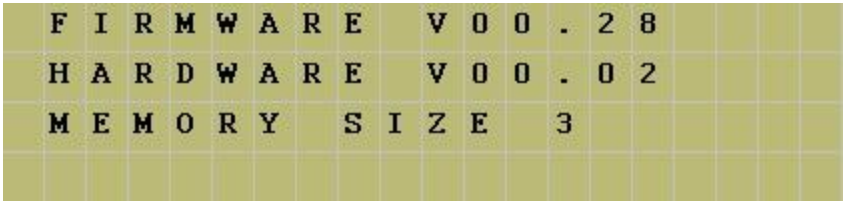
The DOOR LIST OPTIONS menu is used to view the status of the doors currently on the DTD. The first option, SHOW ALL DOORS, displays a complete list of export files on the DTD. This list shows which doors are still pending (ie. Doors you haven't exported to yet) and which are complete. The second option, SHOW PENDING ONLY, only displays the doors that are still pending. The third option, SHOW IMPORT FILES, contains a list of all import files currently on the DTD.



To select a menu option move the cursor to the option you want to view and press the ENTER key on the DTD. You are now presented with the following screen. Pressing the up or down arrow on the DTD moves you through the list of doors. When you reach the door you want to view, press the ENTER key.

ABOUT

The ABOUT screen displays the DTD firmware and hardware versions, as well as, the memory capacity. A“3” indicates there are three memory chips installed, which supports 95 doors.



SET MODE

This options allows you to change the operating mode of the DTD. From the factory the unit is configured for DTD Mode, which is indicated by the = symbol. To change to Printer Mode use the down arrow (8 key) to move the cursor next to SET PRINTER MODE, then press ENTER (5 key). Refer to section 4, which discusses Printer Mode.

Security Risk Warning (W01)

When the DTD attempts to communicate to the door controller during the import/ export process, it first asks the controller if program mode was entered. If program mode was entered on the controller via the keypad or the program button on the controller, the following warning is displayed. This warning means that someone may have programmed data into the controller that doesn't match the PC software database. When this message is displayed you can either ignore it for the time being and continue with your import/export or you can press the back arrow (4 key) to cancel the operation. To correct the situation return to the PC and choose the full export options. Please refer to the PC software documentation for complete details about performing this action.

6.4.5 SEG LAN/WAN Connection

SEG Connected Site via LAN/WAN (either SEG-1 or SEG-M)

The SEG (Secured Ethernet Gateway) is a LAN/WAN (TCP/IP to serial) interface that enables existing or new IEI access systems to use the end user's network infrastructure and to be programmed and managed at any network PC running Hub Manager™ Professional software. The TCP/IP connection type is only available when using the following controller types: HC500, Hub+\Max, Max 2 v1, Max 2 v2, Max 3 v1, Max 3 v2 and prox.pad plus.

IEI offers two versions of SEG products called the SEG-1 and SEG-M. The SEG-1 is a self-contained unit that requires an external power supply and separate communication wiring to the controller. The SEG-M, however, is a printed circuit board level product that is plugged directly onto the Max or MiniMax backplane. All the connections between the SEG-M and backplane are made through the connector, with the exception of the RS-485 wire harness when using a Max 3 product, which means it does not require an external power supply or any wiring and thus reducing installation time.

These instructions explain how to configure your SEG-1 and SEG-M TCP/IP product (referred to as "SEG" from this point forward).

There are 3 methods that can be used to configure the IP Address of the SEG:

- Dynamic IP Addressing via DHCP server with an IP that can change (this is the recommended method but it requires SEG firmware v1.3 or greater)
- Dynamic IP Addressing via DHCP server with non-expiring lease (can be performed on any version of SEG)
- Static IP Address (can be performed on any version of SEG)

NOTE: If your SEG has a firmware version of 1.3 or higher and there is a DHCP server on the network, please refer to the Dynamic IP Address section.

Setup Method Definitions

Dynamic IP Address via DHCP server, IP Address in SEG can change

This method means the SEG is assigned an IP Address by the DHCP server on your network. Once the DHCP servers knows the MAC Address of the SEG, the IP Address can change and Hub Manager™ Professional will automatically retrieve the IP Address from the SEG each time it attempts to communicate to it. This is the recommended method but it requires SEG v1.3 or greater firmware. Refer to the Dynamic IP Address section for further details.

Dynamic IP Addressing via DHCP server with non-expiring lease, IP Address in SEG does not change

Using this method, you simply give the IT department the MAC Address of the SEG and ask them to assign it an IP Address with a non-expiring lease. Refer to the Dynamic IP Address non-expiring lease section for further details.

Static IP Address, IP Address in SEG does not change

You would use this method if you want to assign the SEG a fixed or static IP Address that does not change. The static IP address is set through the serial port of the SEG using the PC's serial communications port (or through the USB port using a USB to RS232 adapter). This method allows you to configure the IP address of the SEG without any network devices such as a router or a network switch interfering. Refer to the Static IP Address section for further details.

SEG Site Parameters

IP Address

The IP address of the SEG.

IP Port

The IP Port is a channel that the SEG is configured to listen on for communications from Hub Manager™ Professional. This is set to 9997 by default, but can be changed both in Hub Manager™ Professional and in the SEG, if necessary.

NOTE: Do not change the IP Port value unless instructed to do so by your IT Administrator.

SEG Serial Net Number

This number refers to the serial port located on the SEG device itself. The SEG is capable of connecting to both RS232 and RS485 products, which are Serial Net Numbers 1 and 2 respectively. This parameter is displayed for reference only and cannot be changed.

Security Key

The security key is a 128-bit AES encryption key used to encrypt the data sent between the PC and the SEG. The security key is stored in Hub Manager™ Professional in each SEG site and it must match the security key stored in the SEG. You can change this key at any time, but you must make sure the SEG and Hub Manager™ Professional have the same number.

> **WARNING:** It is highly recommended that you change the encryption security key during the initial SEG setup. All new SEG devices are shipped with the same initial security key and Hub Manager™ Professional is also shipped with this same security key. If you don't change the security key, anyone running Hub Manager™ Professional on their PC somewhere else on your LAN would be able to communicate with your door controllers. Once you change the security key to a new 128-bit number, then all the data that is passed out the ethernet port of your PC is encrypted with that key and decrypted by the SEG using the same key.

Generate Random Security Key

This button generates a random 128-bit security key and displays the hexadecimal representation in the ***Current Security Key*** field, as shown in the example below.

To send the new security key to the SEG, refer to the ***Set the above Security Key into the SEG*** section below.

Set the above Security Key into the SEG

Use this option to set the security key stored in the ***Current Security Key*** field into the SEG. Hub Manager™ Professional then attempts to communicate with the SEG and change the security key stored in the SEG. Once this new key is successfully set into the SEG a confirmation message is displayed.

> **NOTE:** In order to change the security key in a SEG, Hub Manager™ Professional must know the existing security key stored in the SEG. If you think there has been a mix up, and you think Hub Manager™ Professional may not know the SEG's security key, then you should perform the steps to Reset the Security Key to all 0's as noted in the sections below. When the process is complete, you can then change the security key.

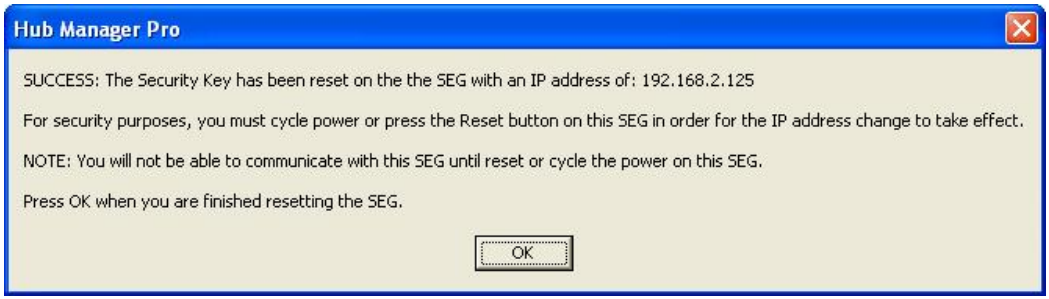
Reset the Security Key in the SEG to all 0's for SEG v1.3 Firmware or Greater

The following instructions apply if your SEG firmware version is v1.3 or greater. Refer to the section named Reset the Security Key in the SEG to all 0's for SEG Firmware Prior to v1.3 if you have a older version of SEG firmware.

This feature allows you to reset the security key in the SEG back to all 0's, which is the default out-of-box state. Resetting the security key in the SEG is required if you are replacing a SEG with a previously used SEG that already has a security key set into it and you don't know what the security key is, or if you are setting up a new site and want to communicate with an existing SEG that is already installed and already has a security key set. This process may also be necessary if you have used the Restore Database function of Hub Manager™ Professional and the security key stored in the restored database does not match the security key currently stored in the SEG.

1. First go to the SEG and either cycle power to it or press the little black reset button on the SEG.
2. Within 10 minutes, go back to the PC and select the button called ***Reset the Security Key in the SEG to all 0's***.
3. The warning message shown below is then displayed, which describes the requirements for using this feature. Once you have met all the requirements press the ***OK*** button.

4. If the Key was reset properly then the confirmation message shown below is displayed.



5. As a security measure, you must now go back to the SEG and either cycle power or press the reset button on the SEG. This sets the new security key into non-volatile memory. If you do not reset the SEG after the security key is reset you will not be able to communicate with the SEG.
6. The process is complete and the security key is reset to all 0's in both the SEG and PC. You should now be able to communicate to your SEG.

Reset the Security Key in the SEG to all 0's for SEG Firmware Prior to v1.3

The following instructions explain how to reset the Security Key of the SEG back to an out-of-box setting of all 0's, and when used in conjunction 'Reset Security Key in PC to all 0's' will allow you to synchronize the Security Key of the SEG with the Security Key in the Site Settings screen in the Hub Manager™ Professional software.

This procedure ***must*** be followed if the firmware version of the SEG is prior to v1.3.

NOTE: Steps 10, 11, and 12 are directly related to resetting the Security Key, these steps should be followed exactly. The other steps specify the out-of-box default values for the other security settings in that menu system. You can enter the default values specified here, or other settings can be changed by a Network Administrator as required. Please refer to the section named Static IP Address > SEG Menu System for more details on the individual Security menu items.

1. Follow the procedure located in the Static IP Address section to enter the SEG menu.
2. Once the SEG menu is open select option **6 *Security***, by pressing ***6*** followed by the ***Enter*** key.
3. You will now be presented with each security setting (not all settings are displayed on all revisions of SEG).
4. Disable SNMP ? Press **N**
5. SNMP Community Name (public): Enter nothing, just press **Enter**
6. Disable telnet Setup ? Press **N**
7. Disable TFTP Firmware Update ? Press **N**
8. Disable Port 77FEh ? Press **N**
9. Disable Web Server ? Press **N**
10. Disable Web Setup ? Press **N**
11. Enable Encryption ? Press **Y**
12. .....Change Key? Press **Y**
13. Enter pass key of 32 hex digits (16 bytes) . Press **0 32 times** This resets the security key
14. Disable Echo ports ? Press **Y**
15. Enable Enhanced Password ? Press **N**
16. When complete and the 'Change Setup' menu appears, select option ***9 save and exit*** by pressing ***9*** followed by the ***Enter*** key.

The security settings of the SEG is now set back to IEI out-of-box defaults. Refer to the section relevant to your application to reconfigure your SEG.

NOTE: Once the Security Key is rest to all 0's, you need to follow the to Reset the Security Key in the PC to all 0's, then specify a new security key and use the ***Set the***

Above Security Key into the SEG option.

Reset the Security Key in the PC to all 0's

Use this feature to reset the security key in the PC back to all 0's. Typically you would use this option if you replaced an existing SEG with a new SEG or you reset your SEG security key to all 0's.

NOTE: If you use this feature and the SEG does not have a security key of all 0's then you must also set the security key in the SEG back to all 0's.

6.4.5.1 Dynamic IP Address

Dynamic IP Address via DHCP server, IP Address in SEG can change

IEI recommends using this configuration when setting up your SEG, but it requires SEG v1.3 or greater firmware. The firmware label is located on top of the SEG.

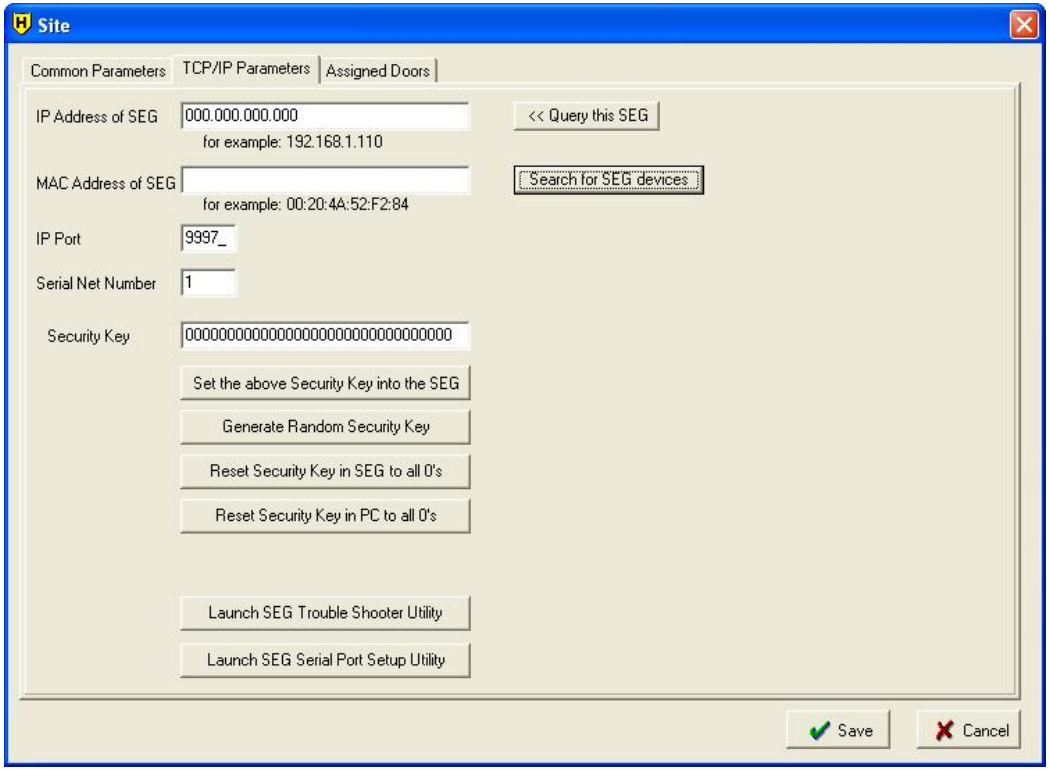
NOTE: The SEG units that shipped prior to v1.3 did not have a version label on them. If the SEG you are setting up does not have a version label, then the firmware is prior to v1.3 and you cannot use this method and you MUST use one of the other 2 methods to assign an IP Address to that particular SEG.

Using this method, no manual setup of the SEG IP Address via the SEG serial port is required.

If you are installing more than one SEG on your LAN you just need to write down the 12 digit MAC Address located on the label of the SEG and write down which controller group that SEG is connected to for reference. For example:

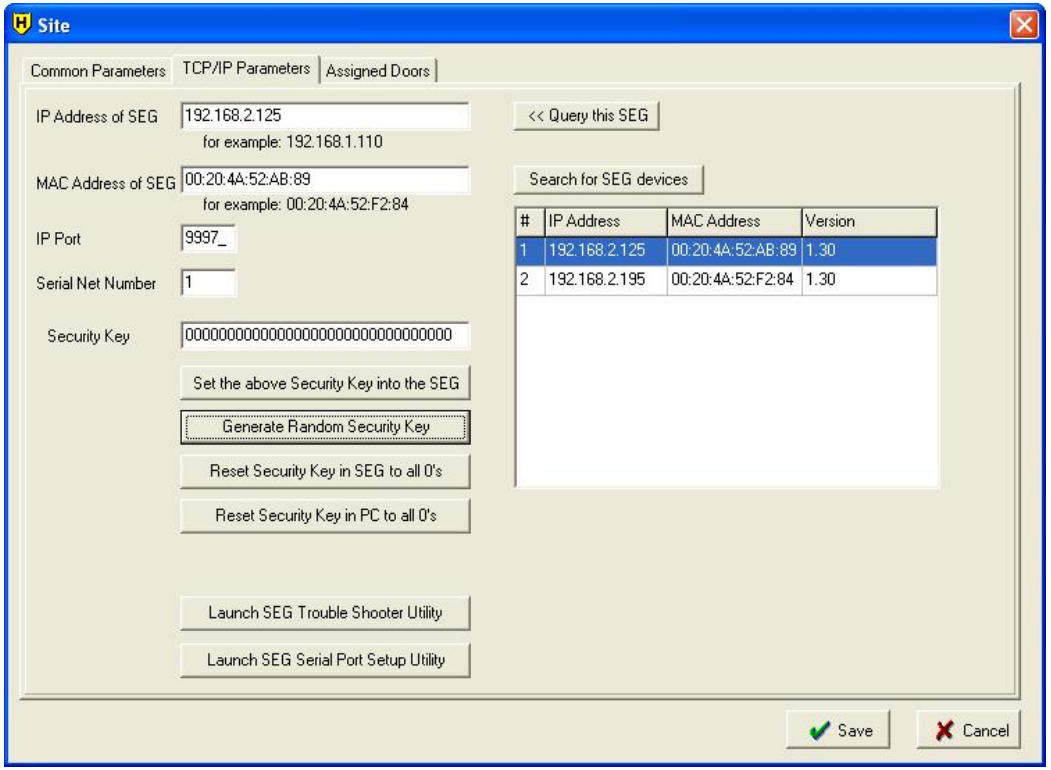
MAC Address	Description
00-20-4A-52-F2-84	Building 1, Floor 2, HubMaxII
00-20-4A-52-8B-89	Building 1, Floor 7, HubMaxII
00-20-4A-52-F4-12	Building 2, Floor 1, prox.pad plus

1. Press the button on the ***TCP/IP Parameters*** screen named ***Search for SEG Devices*** to start this process.



2. A warning message is displayed reminding you that you must have firmware version 1.3 or higher for this process to work. Select ***Yes*** to continue the search.

3. In approximately 5-10 seconds all SEG devices Hub Manager™ Professional found are displayed in a grid on the right side, as shown below.



4. The message below is displayed asking you to select a SEG in the grid. Click the ***OK*** button.

5. Now click on the SEG in the grid that has the same MAC Address as the SEG you are using for this site.
6. A message is displayed asking you to generate a new Security Key. Click on the ***OK*** button.

7. If you don't want to set the security key at this time then setup is complete, select ***Save*** to save and close the setup screen.
8. If you do want to change the security key, click the button labeled ***Generate Random Security Key***.
9. A message will then tell you to select the button labeled ***Set the Above Security Key*** into the SEG. Click the ***OK*** button.

10. Now click the ***Set the Above Security Key*** button to send the new Security Key to the selected SEG.
11. Setup is now complete.

Now that the MAC address is known by Hub Manager™ Professional, if the DHCP server were to assign a new IP Address to this particular SEG, then the next time you attempt to communicate with any of the controllers connected to this SEG, Hub Manager™ Professional will retrieve the new IP Address from the SEG and automatically save the new IP address into the Site Settings. This saves you the time needed to reconfigure the IP Address in the Site settings screen.

6.4.5.2 Dynamic IP Address, non-expiring lease

No setup of the SEG via the serial port is required. Just supply the SEG's MAC address (the 12 digit number located on the label on the SEG; for example 00-20-4A-52-F2-84) to the IT department and ask them to assign it an IP Address with a non-expiring lease, which is an IP address that will not change. Once you have the IP address that the IT department assigned to the SEG, enter that IP address into the Site Settings screen and save the site.

NOTE: Each SEG is shipped from the factory with an IP Address of 0.0.0.0. When the SEG is initially powered up (or rebooted) and it has an IP address of all 0's, it will look for a DHCP server on the network and if one is found the SEG is assigned an IP Address.

6.4.5.3 Static IP Address

Setting a Static IP Address of a SEG through a serial connection (via PC com port)

Use this method to configuring the SEG with a static IP address.

The following procedure requires a Terminal Emulation program. The instructions below describe how to configure the SEG using ***PuTTY***. To download ***PuTTY*** (***putty.exe***) go to www.putty.org.

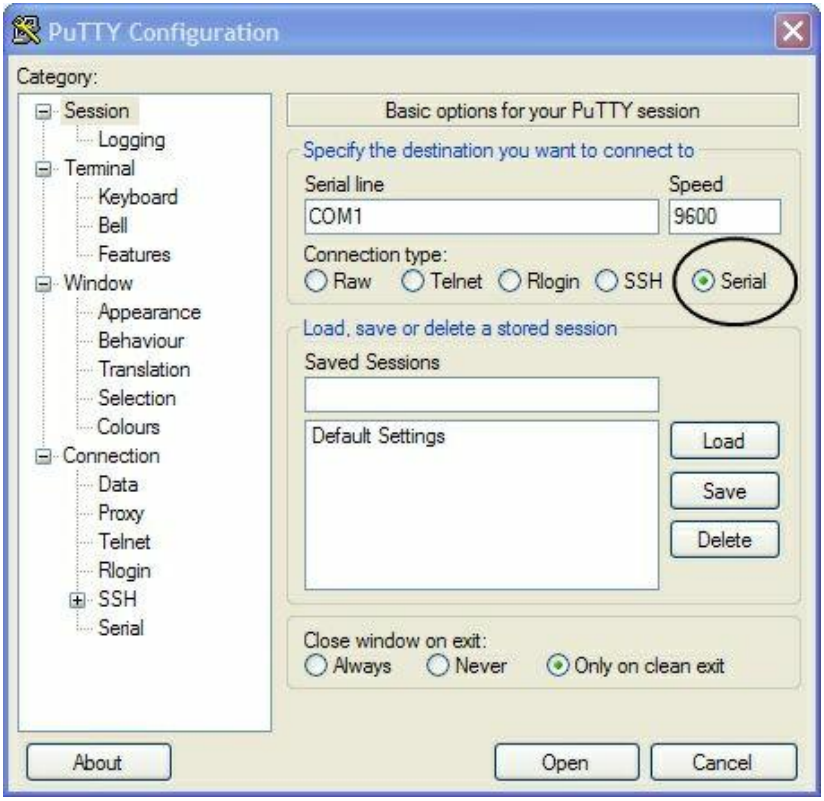
NOTE: HyperTerminal is no longer supported by Hub Manager™ Professional.

To enter the configuration menu of the SEG, you must perform the following in order:

1. Connect the DB9-RJ11 adapter labeled ***Gateway Config*** (supplied with the SEG) to your PC COM port.
2. Plug the 6' phone cord (supplied with the SEG) into the adapter labeled Gateway Config.
3. When using a SEG-1, disconnect the SEG-1 from the LAN and controller and

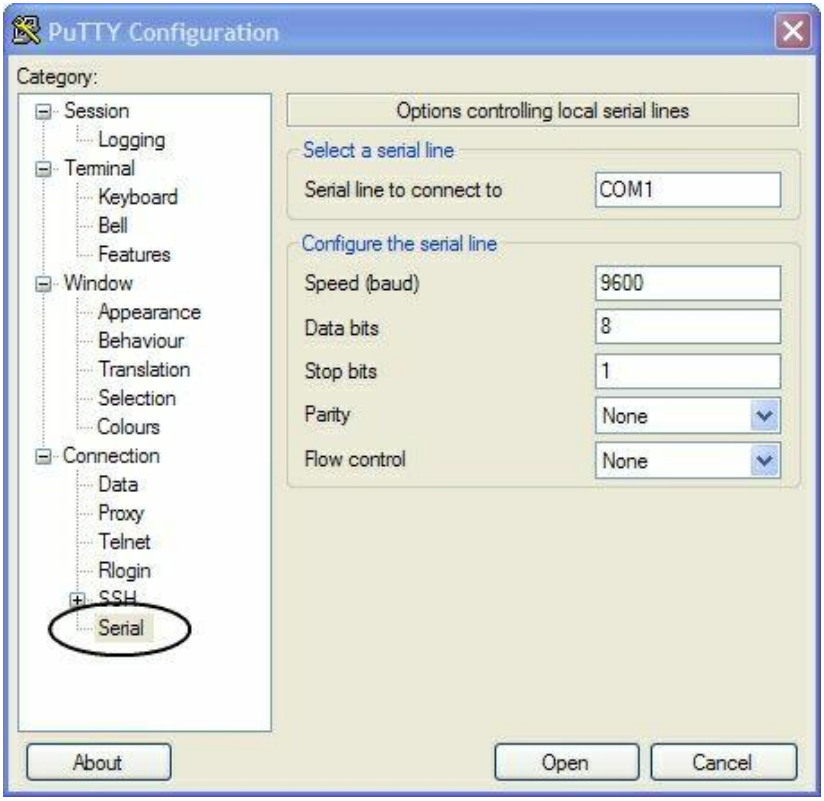
bring it back to the PC, along with its power supply. Plug the other end of the 6' phone cord into the port on the SEG-1 labeled RS232.

4. When using the SEG-M you must leave it installed on the backplane. In this case the PC (a laptop is recommended) must be close to the backplane so you can plug the 6' phone cord into the RJ-11 jack labeled RJ11C on the Max backplane.
5. Run ***putty.exe*** (double-click on the exe file) to open ***PuTTY***.
6. When ***PuTTY*** opens, the ***Session*** options are opened by default. Select the ***Serial*** option on the right, as shown below.



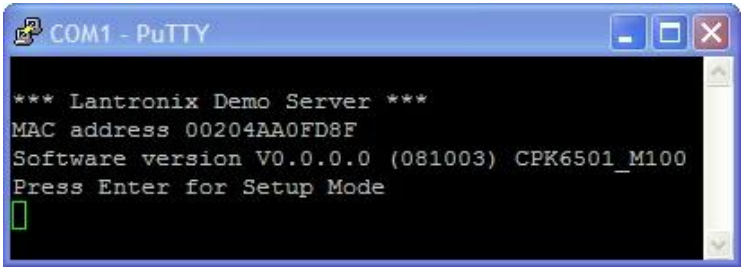
7. Next, select the ***Serial*** option at the bottom of the ***Category*** list, as shown below. In the ***Select a serial line*** section select the COM port you are using. In the ***Configure the serial line*** section use the following settings:

Speed (baud) = 9600
Data bits = 8
Stop Bits = 1
Parity = None
Flow Control = None



8. Now click ***Open*** at the bottom of the screen. A black screen should appear.
9. Disconnect power to the SEG (if it was powered up).
10. Press and hold down the ***x*** key (lowercase) on the PC keyboard while ***PuTTY*** program is running.
11. Power up the SEG.
12. In a few seconds you should get a response from the SEG asking you to press enter to go into Setup Mode, as shown below. You must press ***Enter*** within in 5 seconds.

    NOTE: If you do not press Enter within 5 seconds, you will not be allowed to enter setup mode, and you will see ***?!?*** displayed on the screen beneath ***Press Enter for Setup Mode***. If this happens you must close PuTTY and repeat the procedure starting at step 5.



13. Release the ***x*** key.

14. After pressing ***Enter*** setup mode opens, which contains the settings and menu system shown below.

15. To change the IP Address select option ***0 Server configuration*** by pressing ***0*** followed by the ***Enter*** key. A three-digit number, which is the first octet of the current IP address, is displayed in brackets (this value is 000 by default). Enter the first three digits of the IP Address then press ***Enter***. You must enter the value of all four octets of the IP Address. If any of the numbers are already set correct, you can just press ***Enter*** to leave the value unchanged.
16. Once you've finished entering the IP Address, press ***Enter*** through the remaining options until the menu scrolls by automatically.
17. From the main menu, select ***9 save and exit*** by pressing ***9*** followed by the ***Enter*** key.
18. When you receive the ***Parameters stored ...*** message you can exit this utility by clicking the red X in the upper right corner. Click ***Yes*** if you are prompted to close the program.

NOTE: Do not change the default values in any other menu option. To leave the default value, simply press the ***Enter*** key when that setting is displayed.

SEG Menu System

Below is a table showing the configurable options of the SEG's Setup Menu.

Out-of-box Value: This column lists the out-of-box default values of each option.
Can be modified by a Network Administrator: This column specifies which values can be modified by a Network Administrator, as required by the network or to restrict the configuration methods of the SEG thereby improving security.

The SEG device is factory set to leave all the the configuration methods enabled in the Security menu. After the SEG is initially setup and is communicating with Hub Manager™ Professional properly, it is recommended that your Network Administrator disables the configuration methods in the security menu which they do not want to leave open.

Out-of-box Values in ***bold italics*** should always be set to the specified values for this SEG to properly work with Hub Manager™ Professional. All other out-of-box values can be changed as required by the Network Administrator.

Menu Option	Option Name	Out-of-box Values	Can be modified by a Network Administrator	SEG v1.32 (or earlier)	SEG v1.40
0 - Server Configuration					
	IP address	0.0.0.0	0.0.0.0 for DHCP or X.X.X.X for static	*	
	Set Gateway Address	N	Y (as required)		
	Netmask	0	X.X.X.X (as required)		
	Change Telnet config password	N	Y (for greater security)		
	Change DHCP Device Name	N	Y (as required)		*
1 - Channel 1 Configuration					
	Baud Rate	***1200***		*	*
	I/F Mode	***4C***		*	*
	Flow	***00***		*	*
	Use UDP/TCP	***TCP***		*	

Menu Option	Option Name	Out-of-box Values	Can be modified by a Network Administrator	SEG v1.32 (or earlier)	SEG v1.40
	Source Port	9997	XXXX (as required)	*	*
	Destination Port	0000	XXXX (as required)	*	*
	Destination IP	0.0.0.0	XXXX (as required)	*	*
2 - Channel 2 Configuration					
	Baud Rate	***19200***		*	*
	I/F Mode	***4C***		*	*
	Flow	***00***		*	*
6 - Security					
	Disable SMNP	N	Y (for greater security)		*
	SNMP Community Name	public	Y (as required)		*
	Disable Telnet Setup	N	Y (for greater security)	*	*
	Disable TFTP Firmware Update	N	Y (for greater security)	*	*
	Disable Port 77FEh	N	Y (for greater security)	*	*
	Disable Web Server	N	Y (for greater security)		*
	Disable Web Setup	N	Y (for greater security)	*	*
	Enable Encryption	***Y***		*	*
	Change Key	N	Y (set to all 0's to reset)	*	*
	Disable ECHO Ports	N	Y (as required)		*
	Enable Enhanced Password	N	Y (for greater security)		*

- **0 Server Configuration**

- IP Address : Allows you to set the IP address of the SEG directly. You can set it to 0.0.0.0 to instruct the SEG to be served a dynamic IP address from a DHCP server, or you can set it to a static address of X.X.X.X that the Network Administrator has assigned to this specific network device. The IP address should only be set to 0.0.0.0 if the DHCP server is assigning the same IP address to this specific SEG device every time. There are several ways to enforce that the same IP address is assigned to a specific network device, and it is based upon the capabilities of the DHCP server on your network.
- Set Gateway IP Address: This can be changed by the Network administrator as required. The term 'Gateway' here refers to a network router on the LAN that separates LAN segments, not the Secure Ethernet Gateway (SEG) device you are configuring here. Do not enter the static address assigned to this SEG in this field.
- Netmask: This can be changed by the Network administrator as required.
- Change telnet config password: This can be changed by the Network administrator as required to restrict access to the Telnet setup menu of this SEG.

- **1 Channel 1 Configuration** (RS232 Port Settings)
  - Baud Rate: Communications speed between the SEG and access control equipment. **This should always be set to 1200.**
  - I/F mode: Communications protocol setting between the SEG and access control equipment. **This should always be set to 4C.**
  - Flow: Communications protocol setting between the SEG and access control equipment. **This should always be set to 0.**
  - Use TCP: Communications protocol setting between the PC and SEG. **This should always be set to TCP.**
  - Source Port: This can be changed by the Network administrator as required. If there is a need to change this, then make sure to change the Port number on the sending side to match.
  - Destination Port: This can be changed by the Network administrator as required.
  - Destination IP: This can be changed by the Network administrator as required.

- **2 Channel 2 Configuration** (RS485 Port Settings)
  - Baud Rate: Communications speed between the SEG and access control equipment. **This should always be set to 19200.**
  - I/F mode: Communications speed between the SEG and access control equipment. **This should always be set to 4C.**
  - Flow: Communications speed between the SEG and access control equipment. **This should always be set to 0.**

- **6 Security** : Here you can change the Encryption key to match the encryption key Hub Manager™ Professional is using. This is normally not necessary because Hub Manager™ Professional normally performs this function. After going through this menu item completely, the encryption settings are automatically saved and the session is closed.
  - Disable Telnet setup : This setting defaults to the N (No) option. The Y (Yes) option disables access to this Configuration Menu by Telnet (port 9999). It only allows access via the Web pages and the serial port of the unit.
  - Disable TFTP firmware upgrade: This can be changed by the Network administrator as required for greater security.
  - Disable port 77FE?: This can be changed by the Network administrator as required for greater security.
  - Disable Web Server?: This can be changed by the Network administrator as required for greater security.The Y (Yes) option disables the use of the Web page configuration tool that is built into this unit.
  - Disable web setup?: This can be changed by the Network administrator as required for greater security.
  - Enable encryption?: Encryption must always be enabled, because all data sent to the SEG is encrypted. Do not disable this option or communications between Hub Manager™ Professional, the SEG, and the access control hardware will fail.
  - XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Change key? (N) This 128 bit security key is changed via the Hub Manager™ Professional software. If this security key does not match the key stored in the site settings in Hub Manager™ Professional, then any communication attempts to your controller hardware will fail.
  - Disable ECHO Ports: This can be changed by the Network administrator as required.
  - Enable Enhanced Password: This setting defaults to the N (option), which allows you to set a 4-character password that protects the Configuration Menu via Telnet and Web pages. The Y (Yes) option allows you to set a 16 character password for protecting Telnet access.

- **7 Factory Defaults**: WARNING: This option should be used with caution. This option will reset all Server Configuration, Channel 1, Channel 2, and Security options back to Lantronix factory defaults (and not IEI factory defaults). After performing this function, you will not be able to communicate with the SEG from Hub Manager™ Professional until you have visited each of the menus: Server Configuration, Channel 1, Channel 2, and Security and set the values for each option as specified in the SEG Menu Option table. The Factory Defaults option also resets the Security Key in the SEG to all 0's, so be sure you change the security key into the SEG, via the Site Settings screen in Hub Manager™ Professional before you attempt to send any data to the door controllers. This

option will ***NOT*** change the IP address of the SEG.

- **8 Exit Without Save** : Cancels any changes you have made in setup.
- **9 Save and Exit** : Saves any changes you have made in setup and exits

6.4.6 Modem Connection

This section discusses how to configure a site for a remote modem application and configure the PC side modem. When using Max 3 products, the M3M (Max 3 Modem Module) is required at the remote location for each Max 3 site in the system. For Max 2 products, the SS-Modem is required at the remote location for each Max 2 site in the system. For information regarding the M3M or SS-Modem setup, please refer to the manual for those products.

> **NOTE:** If you are connecting via modem to a Max 2 controller, then you must perform two programming commands at the controller. First you must program the controller for remote access and second you must program the controller to use the SS-Modem modem strings. For details, please refer to the controller documentation.

Modem Parameters Field Descriptions

Below is a description of the fields and options on the ***Modem Parameters*** tab in the ***Site*** setup screen.

Port
Select the PC modem COM port from the drop down list.

Phone Number
This box is where you enter the phone number of the remote site you are dialing. Special characters, such as commas, are allow in this field. Entering a comma inserts a 2 second pause in the dialing sequence.

To access and outside line dial
If your phone system requires you to dial an additional digit prior to dialing the phone number, such as 9, to access an outside line, enter it into this field.

Number of Retries
If the modem fails to connect to your remote site for any reason, the software automatically attempts to connect to the site again. The ***Number of Retries*** field contains the number of additional attempts the software makes if the connection fails the first time. By default, this value is set to 3, which means if the connection fails the first time, the software will attempt to connect an additional three times. If you do not want the software to automatically attempt a retry, set this value to 0. The maximum

number of retries is 99.

Show Advanced Modem Settings

This option is only visible if you are setting up a ***Max 3,prox.pad plus*** site. When you enable this checkbox, several additional options are displayed. These options allow you to change the modem setup strings on the PC side. Changes to these strings are typically not required. These options are discussed in detail below.

Predefined Modem

This option allows you to select a predefined modem, which automatically loads the modem ***Init String*** and ***Dial String*** for each specific modem. If you are setting up a ***Max 3,prox.pad plus*** site, then the drop down only contains a ***custom*** option, because a specific modem is not required on the PC side for this ***Device Type***. Changing the predefined ***Init String*** and ***Dial String*** is not recommended. For Max 3 controllers IEI recommends using a USB modem on the PC side, such as the Zoom v.92 external USB modem, which is known to work, although most modems typically work with the Max 3 controllers.

If you are connecting to Max 2 controllers, however, then this drop down list contains the ***custom*** option and four additional predefined modems. The Max 2 product requires one of these four PC side modems, shown below, to operate. As mentioned above, selecting one these four modems, automatically loads the modem ***Init String*** and ***Dial String*** for each specific modem. Please note, that it's not required to install modem drivers for these modems.

Below is list of qualified modems that you must use on the PC side, when connecting to Max 2 controllers:

- Boca Modem 14.4K
- Boca Modem 33.6K
- U.S. Robotics Modem 33.6K
- U.S. Robotics Modem 56K

Init String

This box contains the specific communication initialization string for the modem on the PC side.

Dial String

This box contains the specific communication dial string for the modem on the PC side.

6.4.7 Managing Stand-Alone Controllers

A ***Stand Alone*** site is a grouping of controllers which have no physical communications connection, because those controllers either have no communications capability, or it is not possible to physically connect to that controller. Hub Manager™ Professional can only manage the user lists of these device types. There are no settings for this Site type.

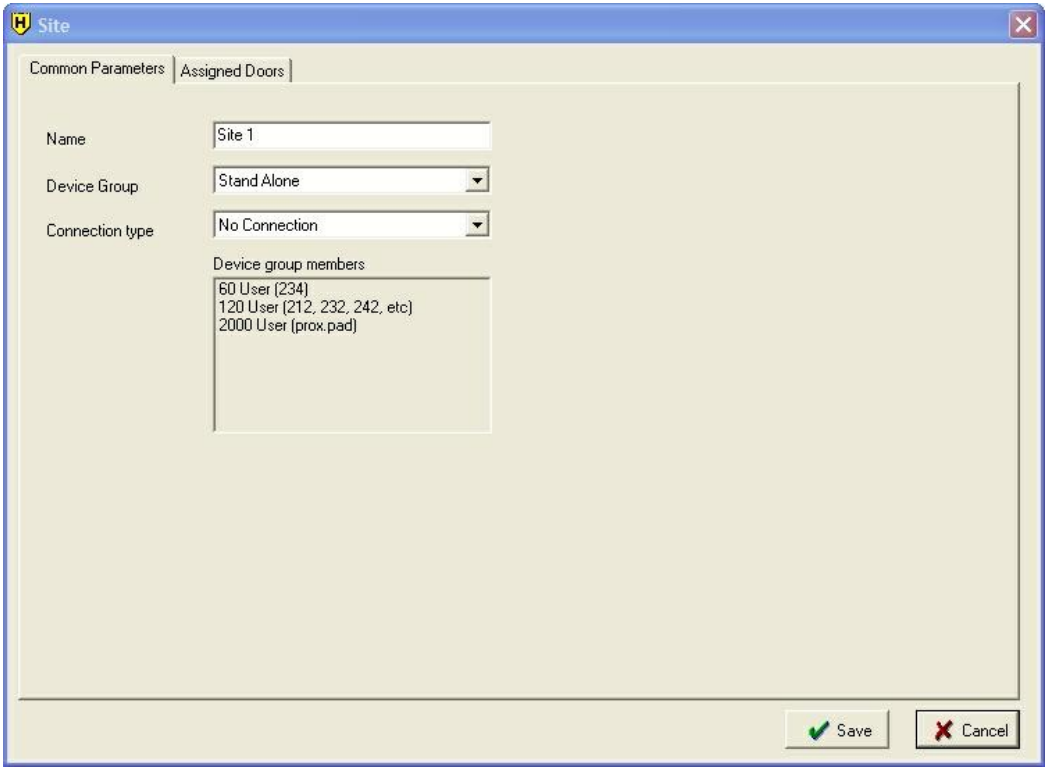
Hub Manager™ Professional allows you to manage the user codes for your 60, 120, or 2000 user Stand Alone (non-networked) keypads such as the following:

60 User: 234
120 User: 212, 232, 233, 242, LS1
2000 User: prox.pad

To manage these types of devices, follow these steps:

1. Go to ***Database > Sites*** to open the ***Sites*** directory.
2. Click the ***Add*** button to open the ***Site*** edit screen.
3. Enter the ***Name*** of your Site.

4. Select ***Stand Alone*** from the ***Device Group*** drop down list.



5. The Connection Type is automatically set to ***No Connection*** because there isn't actually a physical connection to your devices.
6. Select ***Save***.

Now you must add doors using this Site through **Database > Doors**. When adding your doors choose the Site you just created and select the Controller Type that matches your device. For example, if you are going to manage a 212i, select the 120 User option as the Controller Type. Hub Manager™ Professional does not allow you to manage any System Options or System Parameters for Stand Alone devices.

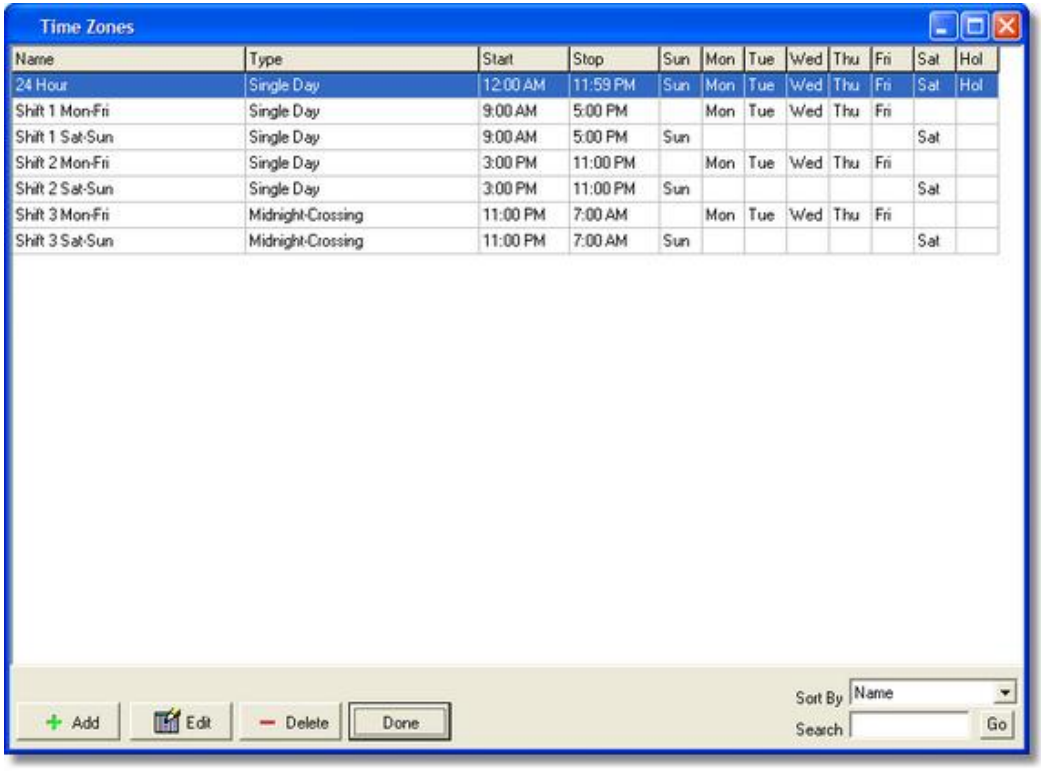
6.5 Time Zones

Time Zones are used for two purposes:

- A Time Zone can specify the days and times when a user's access credential is valid
- A Time Zone can specify an Auto-Unlock schedule for your door controllers The Auto-Unlock settings are established in the door settings for each door controller.

A Time Zone is defined by its beginning and end times and days of the week when this Time Zone is valid. You can also specify whether or not you want to include holidays defined in the Holiday database in the Time Zone. When you select ***Holiday*** under ***Days of the Week***, users are granted access on any defined holidays. To open the ***Time Zones*** directory, select ***Database > Time Zones***.

Below is a screen shot of the ***Time Zones*** directory containing the seven pre-defined Time Zones. When you first enter the screen, the Time Zones are sorted by ***Name***. Use the ***Sort*** drop down list in the lower right to sort the list by Name, Type, Start or Stop.



Defining Time Zones

Hub Manager™ Professional comes with seven pre-defined Time Zones. If these pre-defined Time Zones do not meet your requirements you can either leave them unused, delete them or edit them to suit your needs.

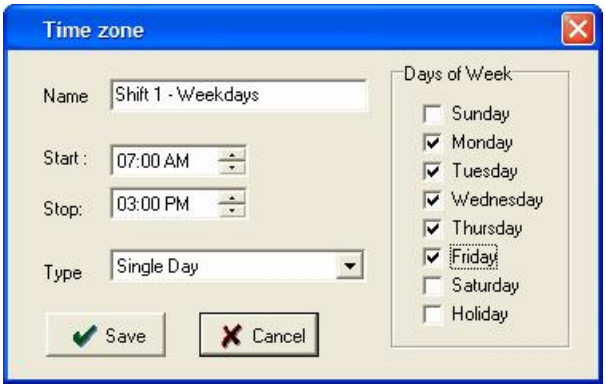
You can define up to a maximum of 1000 Time Zones in your system. Each door can store up to a maximum of eight Time Zones from that defined list. A Time Zone consists of a start time, a stop time, the Time Zone Type, and the days of the week during which the Time Zone is in effect. Here is an example Time Zone definition:

Start Time	Stop Time	Type	Days of the Week
07:00 AM	06:00 PM	Single Day	Mon, Tue, Wed, Thu, Fri

NOTE: Time Zones are defined using the AM/PM time format. The example Time Zone above starts at 7:00 AM and ends at 6:00 PM. It is in effect Monday through Friday and does not include holidays.

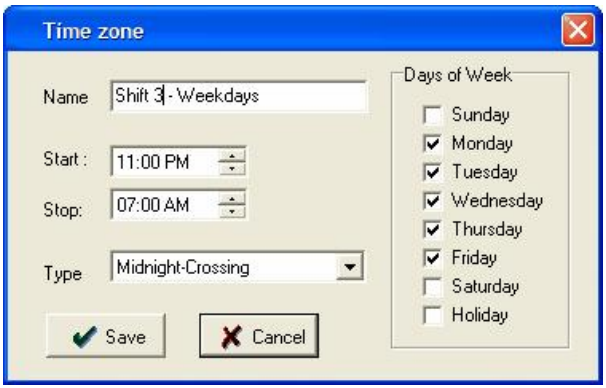
Single Day Time Zones can not cross midnight (12:00 AM).The ***Start*** and ***Stop*** times occur within a single calendar day.For example, if you want to give access from 7:00 PM - 8:00 AM, but your controller only supports ***Single Day*** Time Zones, then you need to create two Time Zones:

- (TZ1) 07:00 PM - 11:59 PM
- (TZ2) 12:00 AM - 08:00 AM



Single-Day Time Zone

Midnight-Crossing Time Zones can cross the midnight boundary (12:00 AM). You can define the ***Start*** and ***Stop*** times within a 24-hour period. For example: 7:00 PM - 8:00 AM (crossing midnight).



Midnight-Crossing Time Zone

Defining Holiday Time Zones

When you define a Time Zone, you can specify whether or not it applies to holidays by checking the ***Holiday*** checkbox. When ***Holiday*** is checked, users assigned to an Access Level containing this Time Zone are granted access on defined holidays. If ***Holiday*** is not checked, then if a holiday happens to fall on one of the Days of Week that are checked, users assigned to an Access Level containing this Time Zone are not granted access. Refer to the Holiday section for details about defining holidays.

Adding a Time Zone

1. Go to ***Database > Time Zones*** to open the ***Time Zones*** directory.
2. Click the ***Add*** button to display the ***Time Zone*** edit screen.
3. Enter the name of the time zone in the ***Name*** field.
4. Enter the beginning and ending times in the ***Start*** and ***Stop*** fields (use AM/PM time format).
5. Select the Time Zone ***Type***. If your Time Zone occurs during a single calendar day, select the ***Single Day*** option. If your Time Zone crosses midnight select ***Midnight-Crossing***.
6. Now check the days of the week to which this time zone should apply.
7. Finally, select ***Save*** to save the information to the database.

Editing a Time Zone

1. Go to ***Database > Time Zones*** to open the ***Time Zones*** directory.
2. Either double-click on the Time Zone you want to edit or highlight it and click the ***Edit*** button.
3. Modify the information as required.
4. Select ***Save*** to save the information to the database.

Deleting a Time Zone

NOTE: You can't delete a Time Zone that is assigned to an Access Level. You must first remove the Time Zone from the Access Level in order to delete it.

1. Go to ***Database > Time Zones*** to open the ***Time Zones*** directory.
2. Highlight the Time Zone you want to delete and click the ***Delete*** button.
3. When the software displays a delete confirmation prompt, click the ***Yes*** button.

Searching for a Time Zone

You can search the database for a particular Time Zone record. Enter the Time Zone's name in the ***Search*** text box in the bottom right of the Time Zone directory and click the ***Search*** button or press the ***Enter*** key.

6.6 Doors

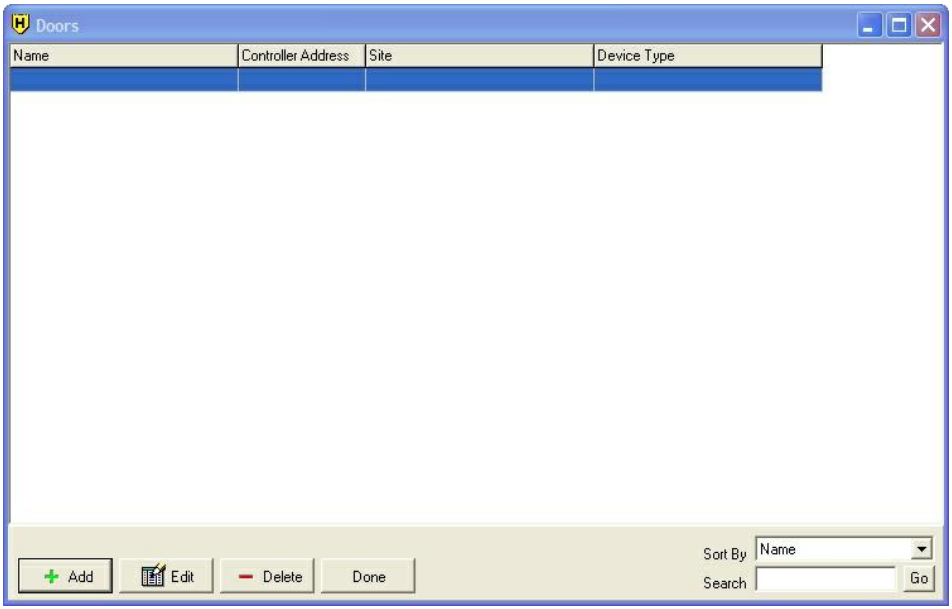
A door is defined as any entry point (doors with electrical or magnetic lock, turnstile, rising barrier, or motorized gate) controlled by a supported Controller. The Doors database stores detailed information about door controller setup parameters. The Hub Manager™ Professional program can export/import to all controllers in a site. To select the Doors option, select **Database > Doors**. The **Doors** directory screen displays. This directory shows all doors in all sites. You can double-click any door to edit the options for that particular door.

Adding a Door
Common Door Settings
Door System Options
Door System Parameters
Door Feature and Parameter Descriptions
Door Capacity
Time Zones

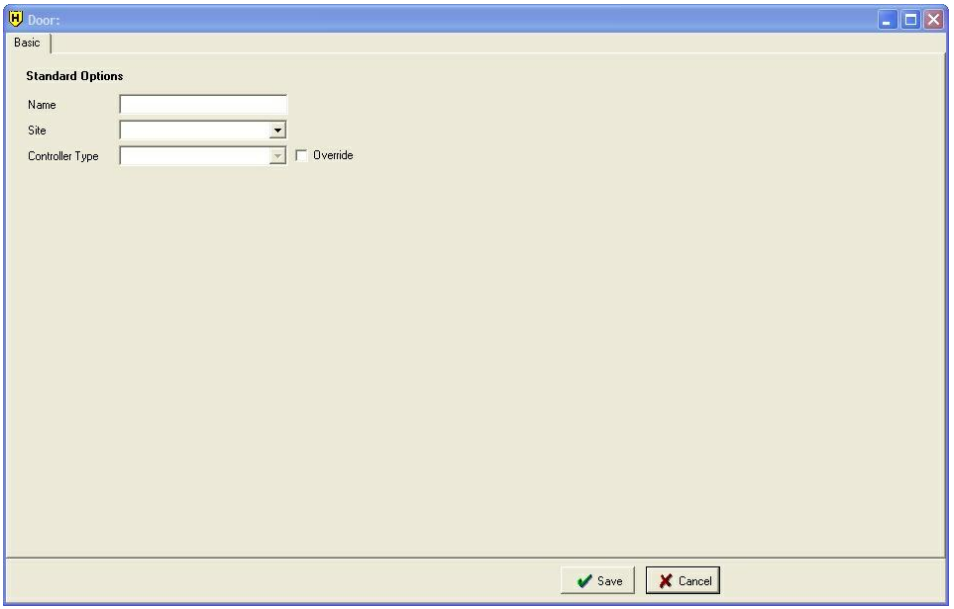
Adding a Door

The following steps guide you through adding a door for the first time:

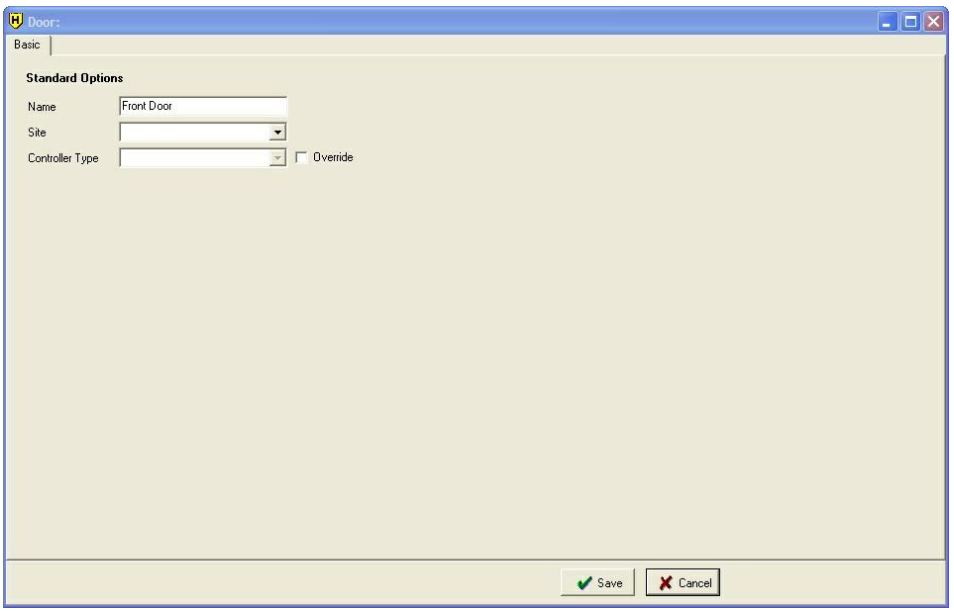
1. First, open the the Doors directory by selecting **Database > Doors** from the main menu to display the screen shown below.



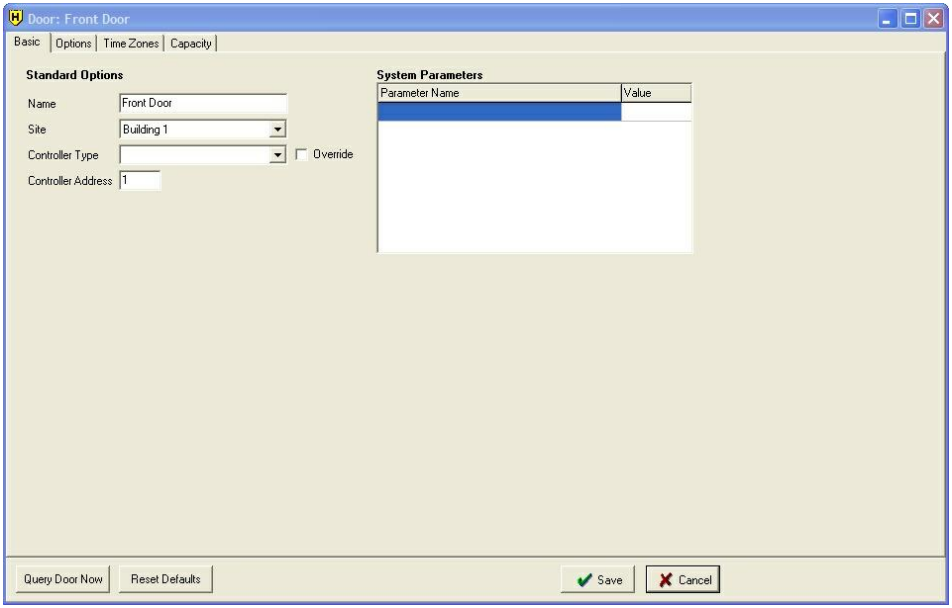
2. Click the Add button to display the Door screen shown below.



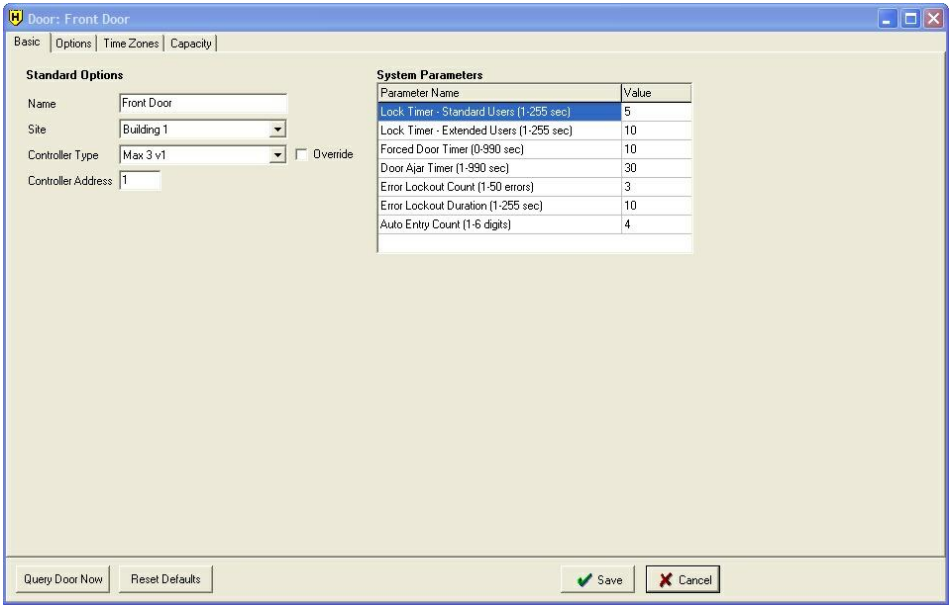
3. Enter the Name for the Door you are adding.



4. Assign the Door to a Site, by choosing a site from the drop down box.

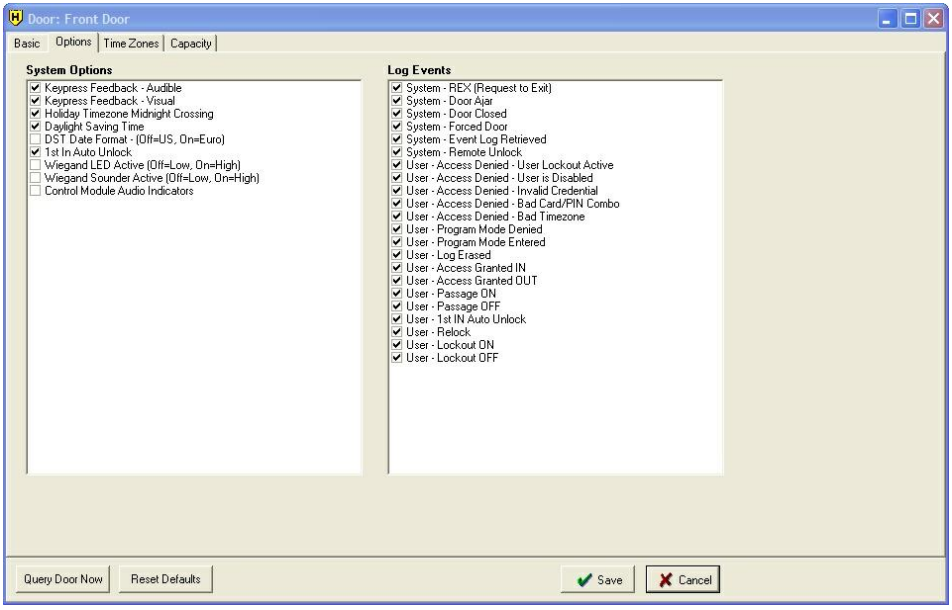


5. Select the **Controller Type**. The example below shows a Max 3 v1 controller and is used throughout the rest of this example. The options shown may differ, depending on the controller type. Also specify the **Controller Address**, if required by the specific controller type. The controller address is the door number that you must program into the controller, via the controller keypad. It is required to uniquely identify each door in the system. This number will be automatically filled by the software sequentially starting at an address of 1.

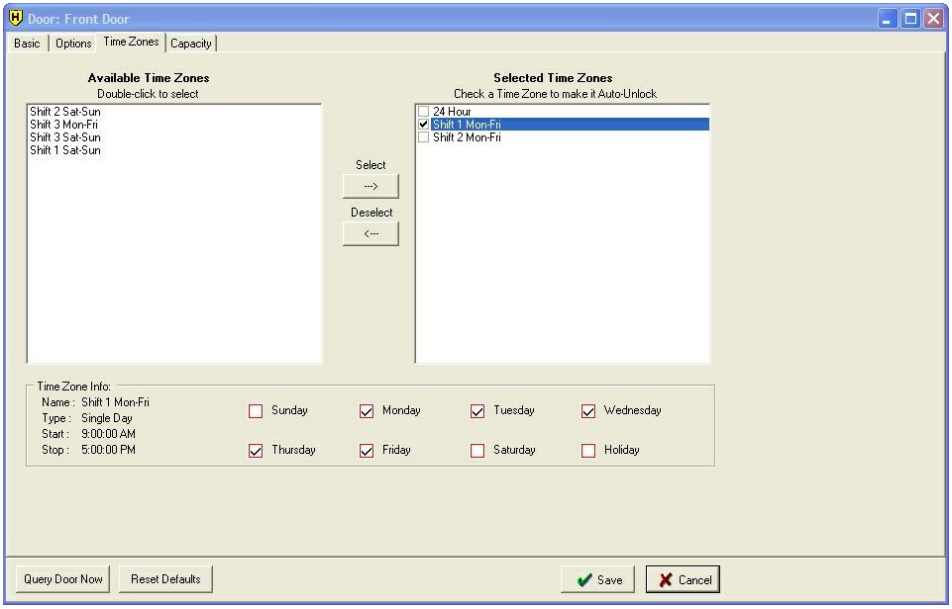


6. Modify any of the **System Parameters**, if you require settings different from the default values.

7. Select the **Options** tab to modify any System Options, as required. Options are enabled by checking the box next to the option and disabled by clearing the checkbox, unless otherwise specified next to the option. In addition, you can specify which Log Events you want the controller to record. By default, all log events are recorded, but if do not want an event to record, clear the checkbox next to the event. Keep in mind, the transaction log buffer in the controller works on a first-in, first-out basis, meaning, once it's full, the first event (oldest) is discarded making room for new events. Disabling an event is useful if you want to avoid filling up your transaction log with events that occur frequently, but are not important to you.



8. Select the **Time Zones** tab to assign time zones to the door. All available time zones, added through the Time Zones directory, are listed on the left. When you highlight a time zone, the details are displayed at the bottom of the screen. To add a time zone to the controller, either click on the Time Zone once to highlight it and click the Select button or double-click on the Time Zone. In either case, the Time Zone moves over the right-hand side, indicating that the Time Zone is assigned to that Door. You can assign up to eight (8) Time Zones to any one door controller. In addition, checking the box next to time zone designates that time zone as an **Auto-Unlock** time zone in that door controller.



9. Select Save to save the information to the database or select Cancel to discard all changes and return to the Doors directory.

NOTE: For details about the Max 3 v2 refer to the prox.pad plus, Max 3 v1 and Max 3 v2 section.

Common Door Settings Field/Button Descriptions

Name
Name of the door.

Site
Identifies the site to which door is being added. A site is a group of devices that share a common connection type and a common communications protocol.

Controller Type
Specifies the type of controller you have controlling this door.

Controller Address
Two-digit number that corresponds to the actual address programmed in this particular door controller.

Controller Serial Number
The ***Controller Serial Number*** is a unique ID assigned at the factory to this specific controller. This field is filled only after the software communicates with the controller and is not editable in the software. Some controllers such as the HC500, Hub+\Max, Max 2 v1, and Max 2 v2 do not get assigned a Serial Number, so this field is not visible for those controller types.

NOTE: The Controller Address field is not visible when a Handheld connected controller type is selected, such as the following controllers: prox.pad plus IR and LS2 \P.

Query Door Now
A quick way to check the online status of this individual door controller. Works ' online' with hardwired sites or currently connected Modem Sites.

NOTE: This feature cannot be performed on Handheld connected controllers.

Reset Defaults
Resets the default information for all fields of this door based upon the currently selected controller type.

Door System Options

"Options" usually have an ON/OFF value. Placing a checkmark in the box next to the options typically enables this feature. But there are some options that toggle between 2 choices.

Door System Parameters

"Parameters" usually have an numeric value denoting a count or a timer value. But some values may reference a single value of several options.

The following chart contains the list of features supported in all supported controller types. If a feature is supported it either contains a value (ie. "1-90 sec" for a timer or "8" for the number of time zones) or and "X" to indication the option is supported. If it's blank, then the feature is not supported by that controller type.

Feature	HC500	Hub+ Hub Max	Max 2 v1	Max 2 v2	LS2/P	prox. pad plus	Max 3 v1	Max 3 v2	prox.pad plus IR
Lock Timer	1-90 sec	1-90 sec	1-90 sec	1-90 sec	1-255 sec	1-255 sec	1-255 sec	1-255 sec	1-255 sec
Forced Door Timer	0-990 sec	0-990 sec	0-990 sec	0-990 sec	0-990 sec	0-990 sec	0-990 sec	0-990 sec	0-990 sec
Door Ajar Timer (Propped Door)	1-990 sec	1-990 sec	1-990 sec	1-990 sec	1-990 sec	1-990 sec	1-990 sec	1-990 sec	1-990 sec
Log Event Mask	n/a	X	X	X	X	X	X	X	X
Error Lockout Count	n/a	n/a	n/a	n/a	1-50 tries	1-50 tries	1-50 tries	1-50 tries	1-50 tries
Error Lockout Duration	n/a	n/a	n/a	n/a	1-255 sec	1-255 sec	1-255 sec	1-255 sec	1-255 sec
Audio Alerts	n/a	n/a	n/a	n/a	X	n/a	n/a	n/a	n/a
Keypress Feedback - Audible	X	X	X	X	X	X	X	X	X
Keypress Feedback - Visual	X	X	X	X	X	X	X	X	X
First In Auto Unlock Time Zones	n/a	n/a	X	X	X	X	X	X	X
Auto Unlock Time Zones	1	8	8	8	8	8	8	8	8
Auto-Entry Count	n/a	n/a	n/a		X	X	X	X	X

Feature	HC500	Hub+ Hub Max	Max 2 v1	Max 2 v2	LS2/P	prox. pad plus	Max 3 v1	Max 3 v2	prox.pad plus IR
Daylight Savings Time Auto Adjust (2007 Standard)	n/a	n/a	n/a	X	X	X	X	X	X
Daylight Savings Time Date Format	n/a	n/a	n/a	X	X	X	X	X	X
Lock Prior to Sleep	n/a	n/a	n/a	n/a	X	n/a	n/a	n/a	n/a
Card AND Code Programming	n/a	n/a	n/a	n/a	X	X	X	X	X
Aux Relays	n/a	n/a	n/a	n/a	n/a	n/a	n/a	X	n/a
Temporary Users	n/a	n/a	n/a	n/a	n/a	n/a	n/a	X	n/a
First-In Auto-Unlock by User	n/a	n/a	n/a	n/a	n/a	n/a	n/a	X	n/a

Door Feature and Parameter Descriptions

Lock Timer
Amount of time, in seconds, that the Lock output is activated (door unlocked) after a valid access occurs.

Forced Door Timer
This parameter specifies the amount, in seconds, that the Forced Door output is activated when a forced door condition occurs. If the value is set to 0, the output activates and remains that way until it is reset using a valid credential.

Door Ajar Timer **(Propped Door)**
This parameter specifies the amount of time, in seconds, that the door contacts can remain open after the door is unlocked for a valid reason, before the Door Ajar output is triggered. This timer starts once the door contacts are opened.

Log Events

This section contains the list of events (aka transactions) that the selected controller type supports. By default, all the events are selected, which means when any of the events occur at the controller they are recorded in the transaction log buffer. You must deselect the events you do not wish to record.

Error Lockout Count

This parameter specifies how many incorrect keypad PIN or incorrect Card attempts are allowed before the door controller will lock up and deny access to anyone for a specified amount of time specified in Error Lockout Duration.

Error Lockout Duration

The Error Lockout Duration specifies how may seconds a controller stays in Error Lockout before returning to normal operation. While in this mode, all keypad and card entries are denied.

Audio Alerts

Some controller's support audio alerts for both forced door and propped door (aka door ajar). This parameter lets you specify which local audio alerts are enabled. Enter one of the following values to set the desired functionality:

0 = Propped Door and Forced Door audio alerts are both disabled.
1 = Forced Door audio alert is enabled, Propped Door audio alert is disabled.
2 = Propped Door audio alert is enabled, Forced Door audio alert is disabled.
3 = Propped Door and Forced Door audio alerts are both enabled.

Keypress Feedback Audible

Audible Keypress Feedback refers to a short audible tone generated each time a controller key is pressed.

Keypress Feedback Visual

Visual Keypress Feedback refers to a short LED flash generated each time a controller key is pressed.

First-In Auto-Unlock

When First-In Auto-Unlock is enabled, an Auto-Unlock won't occur at it's prescribed time and will be deferred until the first person, who is allowed to trigger First-In, is granted access during an Auto-Unlock Time Zone.

Auto Entry Count

Auto entry means that you don't have to press the * (asterisk) key after you enter your keypad PIN. This count specifies the number of digits that will be buffered before a PIN lookup is performed. For example if you set this value to 4, then after you enter the 4th digit of your PIN, the controller automatically looks the PIN for validation. When this option is enabled, all PIN numbers must be the same number of digits.

Holiday Time Zone Midnight Crossing

This option applies to users that are assigned to a Time Zone that crosses the midnight boundary, such as 11PM to 7AM. If a user is assigned to this Time Zone, for example, that normally has access Monday through Friday, but Friday is a holiday. When this option is enabled, user's assigned to that Time Zone, would still have access after midnight on Thursday night and allowed to work through Friday morning. If you disable this option, however, users would not be allowed access after midnight Thursday and could not be granted access anytime on Friday.

Regarding Auto-Unlock Time Zone functionality, when this option is enabled, if your midnight-crossing time (11PM to 7AM Monday-Friday) is designated as an Auto-Unlock Time Zone the Auto-Unlock will remain active past midnight, even if Friday is a holiday. However, If the option is disabled, then at midnight on Thursday night, the door will automatically relock, because Friday is specified as a holiday.

Daylight Savings Time

This option lets the hardware auto adjust to Daylight Savings Time (dates are based on DST Date Format Option).

> **NOTE:** Because of the change in the Daylight Saving Time (DST) standard in 2007, existing controllers that previously supported the old dates should be set to not automatically adjust on the Spring-Forward or Fall-Back dates, since the dates were previously hard-coded into the controllers, and are no longer correct. Please refer to the manual that came with your controller to see if it supports the new Daylight Saving Time 2007. For controllers that don't support the new 2007 DST Dates, you must disable this option in the Door Settings screen, and you will need to change the time on the controllers via the controller's keypad twice a year on the Spring-Forward or Fall-Back dates, by performing an export with a device (either a DTD or a PDA running LS Link) that has the corrected Daylight Saving Time.

To positively determine if your controller supports DST 2007 format do one of the following:

1. **RECOMMENDED METHOD:** Perform a self test on the keypad 7890#123456*, if there is a yellow flash at the end of the beeping sequence, then the controller supports DST 2007, if there is no yellow flash at the end then it means DST 2007 is not supported.
2. Locate the firmware revision label on the microchip, then compare to the revision listed in the DST warning messages displayed within Hub Manager™ Professional.
3. You can retrieve the firmware revision using the DTD (***Utilities > Get Door Info***) or using LS Link (***Files > Action > Info***), then compare to the revisions listed in the warning messages.
4. The date code is found on the product packaging, then compare to the revisions listed in the warning messages.

***DST Format* (Daylight Savings Time)**

This option determines the DST Date Format that the controller uses.

Euro format:

- "Spring Forward" at 2:00 AM on the last Sunday in March and "Fall Back" at 3:00 AM on the last Sunday in October.

US Format

- DST prior to 2007: "Springs Forward" at 2:00 AM on the first Sunday in April and "Falls Back" at 2:00 AM on the last Sunday in October.
- DST 2007: "Springs Forward" at 2:00 AM on the second Sunday in March and "Falls Back" at 2:00 AM on the first Sunday in November.

Lock Prior to Sleep

This option applies to battery powered products only. Periodically, these controllers "wake up" and this option determines whether or not it attempts to send the lock signal before it goes back to "sleep." By default this option is disabled, but if you enable it, the controller will send a lock signal each time it goes back to "sleep."

> **Warning:** Enabling this feature will result in a shorter battery life. This feature should only be enabled at the request of a Technical Support representative.

Card AND Code Required for Programming at the Controller

This option specifies whether both Card **AND** Code credentials are required to enter programming mode via the controller's keypad.

Door Capacity

The ***Capacity*** tab on ***Door*** edit screen allows you to see the maximum capacity of the door, how many users are currently assigned to the door and how many available user positions are left. In addition, this screen shows a break down of all the Access Levels that this door is currently assigned to and how many users are assigned from each access level. This is helpful if you have reached the full door capacity, but you still want to add users to the door. Now you can review your Access Levels and see if everyone that is currently assigned to the door really needs access.

For example, if you attempt to add users to the "All Access" Access Level, which contains the "Front Door," but you discover that the maximum door capacity is reached, you can review the ***Capacity*** tab to see which Access Levels contain this door. When you review the door you see that there is an Access Level named "Shift 3 Crew" with 245 users, but you know these employees never use the "Front Door." You now know to edit the "Shift 3 Crew" access level and remove the "Front Door" from it to free up 245 user slots in the door.

Controller Type	User Capacity of Controller
HC500	500
Hub+\Max	500
Max 2 v1	1000
Max 2 v2	2000
LS2\P	2000
prox.pad plus	2000
Max 3 v1	2000
Max 3 v2	2000
prox.pad plus IR	2000

Time Zones

The ***Time Zones*** tab is where you select the Time Zones that you want to assign to a specific door. For most controllers, you can select up to 8 Time Zones.

NOTE: You must select at least one time zone when adding a door.

These Time Zones are used for two reasons:

- To specify when a user is allowed access.
- To specify an auto-unlock (or scheduled unlock) time period.

Auto-Unlock Time Zones

An Auto-Unlock Time Zone means the door will unlock at a scheduled time and relock again at a scheduled time. This feature is sometimes referred to as scheduled unlock. You can designate any number of the time zones assigned to a door as auto-unlock.

Use the following steps to create an Auto-Unlock Time Zone:

1. First add a time zone to the ***Time Zones*** directory located in ***Database > Time Zones***. See Time Zones for more information.
2. Next edit the door you want to auto-unlock (or add a new door), then select the Time Zones tab.
3. Now find the time zone on the left, under ***Available Time Zones***, that you want to assign as an auto-unlock. Double-click it to move it over to the right, so it appears under ***Selected Time Zones***.
4. Finally, check the box next to the time zone you just assigned to the door to make an auto-unlock time zone.

When the clock in the controller reaches the time zone start time, the door will automatically unlock and when the time zone end time is reached, the door will automatically lock. It will do this only on the days you selected when you first set up the time zone.

NOTE: If the ***1st In Auto Unlock*** option is enabled in this controller (on the ***Options*** tab), then the door won't automatically unlock when any auto-unlock time zone assigned to that door begins. The ***1st In Auto Unlock*** option means that the door does not auto-unlock until a valid user, assigned to that time zone, gains access. Once a valid user gains access, the auto-unlock time zone starts and the door remains unlocked until the time zone expires. This option is enabled by default, to provide a more secure environment, but if you want the door to automatically unlock by itself, then disable the ***1st In Auto Unlock*** option. If you are using a Max 3 v2 controller, and you want to use the ***1st In Auto Unlock*** option, you must enable the ***This User can trigger First In Auto Unlock Time Zones*** option for each user (on the ***Users*** edit screen) for each user you want to allow to trigger a 1st In auto-unlock

time zone. Refer to the First-In Auto-Unlock User Selection section under the prox.pad plus, Max 3 v1 and Max 3 v2 section for details.

6.6.1 HC500, Hub+\Max, Max 2 v1 and Max 2 v2

This chart helps identify which of these four controller types you have, based on the information that appears on the firmware label and any physical traits it has.

Controller Type	Info on the firmware label	Physical Identities
HC500	v2.x or greater	Plastic Single-Gang Box
Hub+\Max	v1.x P or greater	Plastic Single-Gang Box or Max Cabinet
Max 2 v1	v2.0 or v2.1	Max or MiniMax Cabinet
Max 2 v2	v2.2 or greater	Max or MiniMax Cabinet

6.6.2 prox.pad plus IR

The prox.pad plus IR controllers work in conjunction with a Handheld transfer device.

You can add both LS2\P and prox.pad plus IR controllers in the same access control system and on the same Site.

Basic Characteristics:

- 2000 Users
- 16 Single Date Holidays
- 16 Block Holidays
- 8 Time Zones
- Up to 8 Auto Unlock Time Zones
- 2000 Event Transaction Log Buffer
- Hard-wired power
- 1 Lock Relay (Form C), which can be used to control an external locking device such as a mag lock or electric strike
- 1 Auxiliary Relay (Form C), which can be assigned to one of the following functions: Alarm Shunt, Forced Door, or Door Ajar (Propped Door). The changing of this AUX relay output must be done through manual programming at the controller's keypad. See the controllers programming manual for the programming commands.
- Invalid Code Lockout Count
- Invalid Code Lockout Duration
- Option to require "Card AND Code" to Enter Programming Mode
- First In Auto Unlock
- Prox Antenna can be remoted from the controller, up to 10' away.
- User Types including: Emergency, Extended Unlock (for people who require a longer unlock time), Lockout, Single-Use, Passage and others.
- Option to use the Local Sounder for Forced Door or Door Ajar (propped door)

Communicating with a prox.pad plus IR Controller

The following steps detail how to communicate to the prox.pad plus IR controller.

1. Choose ***Communication > Import\Export Doors***, and select the doors you want to send data to. Some doors may already have a checkmark; this means that either data was added or modified that affected that specific door. When using a DTD, connect it to the PC and export to it, as though it were a controller. If you are using a Palm PDA, export first, then you must launch HotSync Manager and perform a HotSync with the PDA.
2. You then visit each controller with your Handheld device and communicate with the controller.

3. Remember, on the controller you must enter a Communications Unlock credential before you communicate to it with your Handheld device.
4. On the Handheld, select the ***Import/Export*** option. During this time new data is sent to the controller and any new transaction events in the controller, are retrieved.
5. Once you visit all the doors, you must return to the PC. If you are using a PDA connect it to the PC and perform a HotSync. In addition, go to ***Communications > Import/Export*** to perform an Import/Export to import the data into the software. If you are using a DTD connect it to the PC and go directly to ***Communications > Import/Export*** to perform an Import/Export to retrieve transaction event data.

6.6.3 prox.pad plus, Max 3 v1 and Max 3 v2

The prox.pad plus, Max 3 v1 and Max 3 v2 controllers work on an RS-485 network bus and cannot be placed on the same network bus as the HC500, Hub+, HubMax, Max II v1 or Max II v2 controllers, which use the RS-232 communication protocol. If you want to use both RS-232 and RS-485 controllers in the same access control system, then a separate Site must be created for each device group.

Common Features

The following list of features are common between the prox.pad plus, Max 3 v1 and Max 3 v2 products, unless otherwise noted:

- 2000 Users
- 16 Single Date Holidays
- 16 Block Holidays
- 8 Time Zones
- 8 Auto-Unlock Time Zones
- 2000 Event Transaction Log Buffer
- 1 Lock Relay
- 1 Alarm Shunt Relay (**Max 3 v1 and Max 3 v2 only**)
- 1 Forced Door Relay (**Max 3 v1 and Max 3 v2 only**)
- 1 Door Ajar Relay (**Max 3 v1 and Max 3 v2 only**)
- 1 Assignable Auxiliary Relay (can assign to operate as Alarm Shunt, Forced Door, Door Ajar, Panic, or Duress; **prox.pad plus only**)
- Invalid Code Lockout Count
- Invalid Code Lockout Duration
- Daylight Saving Time (DST) supports the 2007 Standard
- Option to require "Card AND Code" to Enter Programming Mode (**prox.pad plus only**)
- Timed Anti-Passback (**prox.pad plus only**)
- First-In Auto-Unlock
- Multiple User Types such as: Emergency, Extended Unlock (for people who require a longer unlock time), Lockout, Single-Use and others
- Fast Log Import Time (the software only imports new events from the controller)
- Controller Grants Access During Communications with Software (when exporting data or importing event logs)
- Assignable Local Sounder (can assign to operate as Forced Door or Door Ajar; **prox.pad plus only**)
- Network up to 64 prox.pad plus, Max 3 v1 and Max 3 v2 controllers on a single RS-485 bus (additional networks/sites may be added to the software as needed)
- TCP/IP Communications over a LAN/WAN network using the IEI SEG-1 or SEG-M

Max 3 v2 Features

The following list of features applies only to the Max 3 v2 controller:

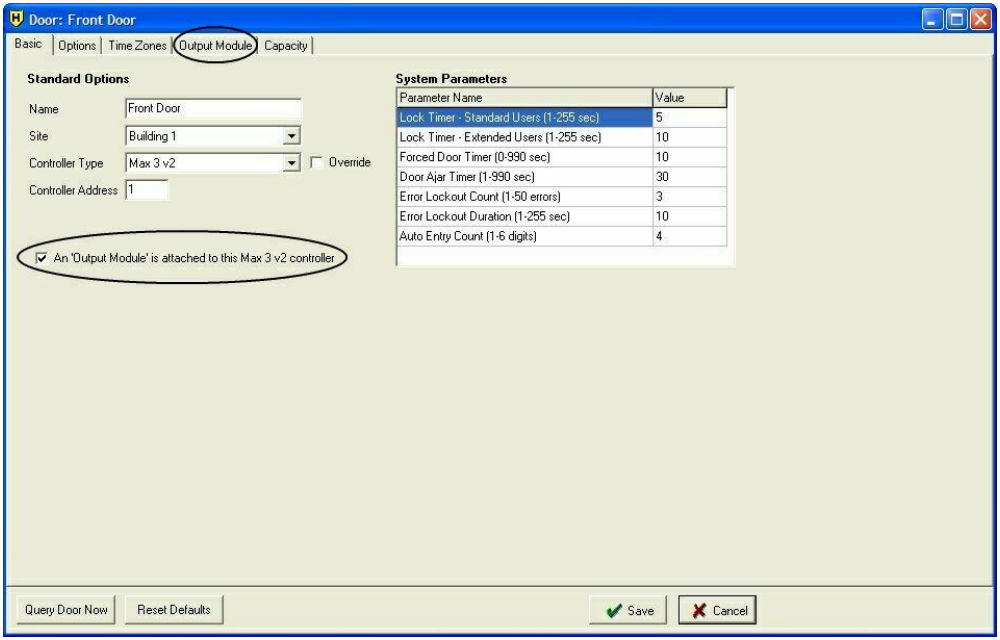
- Users Trigger Auxiliary Outputs (requires Max 3 Output Module)
- First-In Auto-Unlock Selectable by User
- Temporary\Expiring Users

Max 3 Output Module (Users Trigger Auxiliary Outputs)

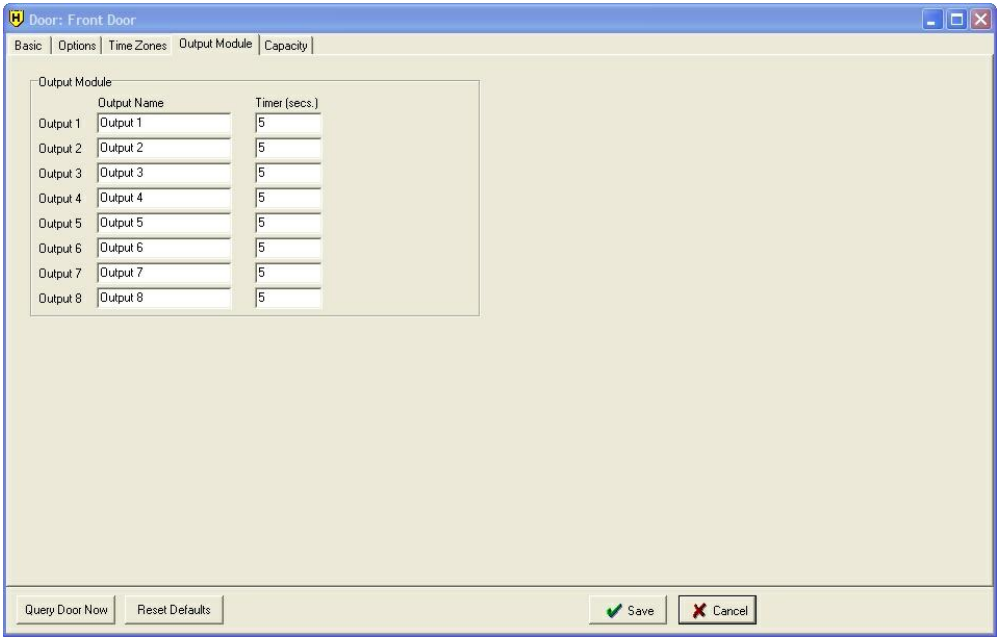
The Max 3 v2 controller type supports the Max 3 Output Module. The Max 3 Output Module contains eight individual auxiliary relays, referred to as outputs. Each output also has it's own individual timer. When you set up your access levels for users, you can assign these outputs. When an output is selected in an Access Level, any user assigned to that Access Level will trigger the output(s) when they are granted access.

This section discusses how to enable the output module features, name the outputs and set the output timers. In addition, step 3 discusses how to assign users to trigger auxiliary outputs by selecting the outputs when setting up an Access Level. For further details regarding Access Levels refer to the Access Levels section.

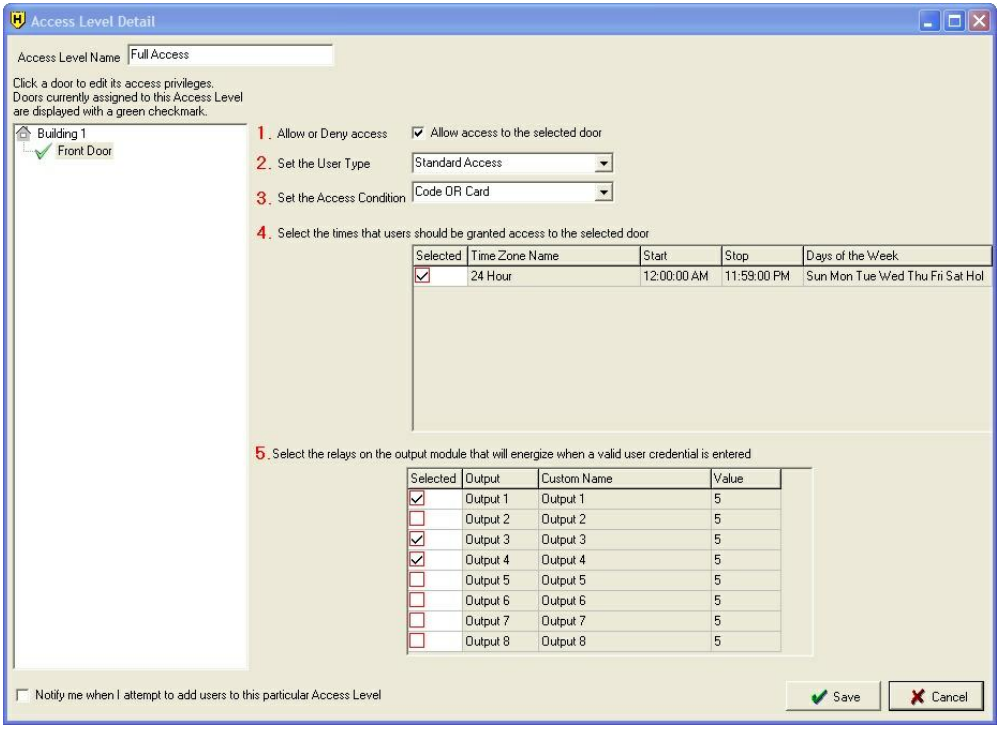
1. First you must enable the Output Module on the ***Basic*** tab on the ***Door*** edit screen. Check the box that says: "***An 'Output Module' is attached to this Max 3 v2 controller***." After checking the box, the ***Output Module*** tab appears at the top.



2. Next, select the ***Output Module*** tab. This screen is where you specify the name of your outputs and set the output timers. In the edit boxes below ***Output Name*** enter the custom names of each of the your outputs. The maximum number of characters is 30. Next to these edit boxes are the ***Timer*** value edit boxes. Here you enter how long you want the output to remain active. This value is entered in seconds from 1 to 65535 seconds. The default value for each timer is 5 seconds. To calculate the number of seconds in a minute, multiply the number of minutes by 60 (ie. 2 minutes x 60 = 120 seconds). If you want the the output to trigger for a certain number of hours, multiply the number of hours by 60, which gives you minutes, then multiply that number by 60 to give you seconds (ie. 8 hours x 60 = 480 minutes; then 480 minutes x 60 = 28800 seconds). In the timer field enter 28800.



3. As mentioned above, the next step is to assign the outputs to users, via an access level. Go to ***Database > Access Levels***, then click ***Add*** to add an access level. Once you select your Max 3 v2 door in the ***Access Level Detail*** screen and complete step 1, steps 2 through 5 are visible. Step 5 is where you select which outputs (auxiliary relays) activate when a user, belonging to this access level, is granted access. You can select any combination of the eight available outputs. Keep in mind, each access level is unique, which means you can have different output selections per access level. For further details regarding access levels refer to the Access Levels section.



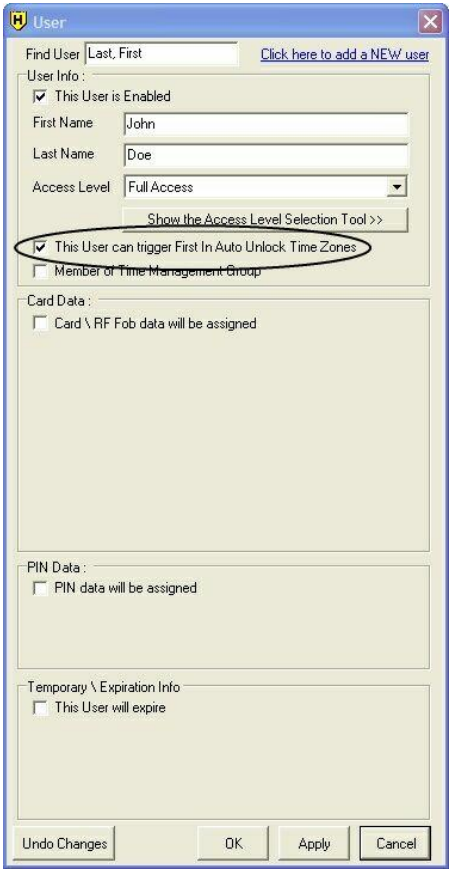
Auxiliary Relay Transaction Events

User - Aux Relay Changed: This event occurs each time a user, that is configured to activate an auxiliary relay, gains access.

System - Aux Relay Timed Expiration: This event occurs each time an auxiliary relay timer expires and the relay de-energizes.

First-In Auto-Unlock User Selection

The Max 3 v2 controller type contains a feature that requires you to specify which users can trigger a First-In Auto-Unlock time zone. The ***User*** edit screen contains a check box called ***This User can trigger First In Auto Unlock Time Zones***. When this box is checked, that specific user can trigger a First-In Auto-Unlock time zone when they are granted access. **By default, this check box is checked, so all users will trigger First-In Auto-Unlock**. If you do not want a particular user to trigger First-In Auto-Unlock, you must uncheck the box.



Please note, you must also have at least one Auto-Unlock time zone assigned to the door and the ***1st In Auto Unlock*** option must be enabled. To assign a time zone to a door and designate it as Auto-Unlock, go to ***Database > Doors***, and either ***Edit*** or ***Add*** a door. Then go to the ***Time Zones*** tab in the ***Door*** edit screen. The ***1st In Auto Unlock*** option is located on the ***Options*** tab in the ***Door*** edit screen. In addition, a user can only trigger a First-In Auto-Unlock when they are assigned to an Access

Level containing that particular time zone. For further details regarding Users, Doors and Access levels, refer to the Users, Doors and Access Levels sections. For addition details regarding Auto-Unlock refer to the Auto-Unlock Time Zones section of the Doors topic.

NOTE: This option only applies to users sent to Max 3 v2 controllers, although the check box is visible for all users. This check box has no affect on users sent to any other controller type.

Temporary\Expiring Users

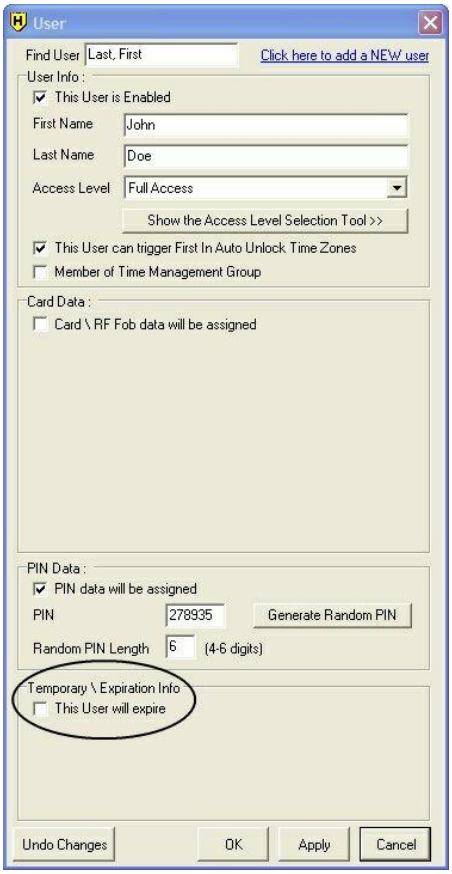
Another feature supported by the Max 3 v2 is temporary users, also known as expiring users. The Max 3 v2 supports a single temporary user option called ***Start and Stop Date***.

Start and Stop Date: The user has access between a fixed start and stop date.

The ***User*** edit screen contains a check box below ***Temporary\Expiration Info*** called "***This User will expire***." To designate a user as a temporary user, check this box, then choose the ***Expiration Type***, as discussed above. For further details regarding temporary users refer to the Users section.

NOTE: This option only applies to users sent to Max 3 v2 controllers, although the check box is visible for all users. This check box has no affect on users sent to any other controller type.

Please refer to the Tools > Options section for more details on an option that affects how Temporary Users will function in controllers that don't support Temporary Users.



6.6.4 LS2\P

The LS2\P controllers work in conjunction with a Handheld transfer device.

Basic Characteristics:

- 2000 Users
- 16 Single Date Holidays
- 16 Block Holidays
- 8 Time Zones
- Up to 8 Auto Unlock Time Zones
- 2000 Event Transaction Log Buffer
- Invalid Code Lockout Count
- Invalid Code Lockout Duration
- Option to require "Card AND Code" to Enter Programming Mode
- Auto Unlock as well as First In Auto Unlock

- User Types including: Emergency, Extended Unlock (for people who require a longer unlock time), Lockout, Single-Use, Passage and others.

Communicating with a LS2\P Controller

The following steps detail how to communicate to the LS2\P controller.

1. Choose ***Communication > Import\Export Doors***, and select the doors you want to send data to. Some doors may already have a checkmark; this means that either data was added or modified that affected that specific door. When using a DTD, connect it to the PC and export to it, as though it were a controller. If you are using a Palm PDA, export first, then you must launch HotSync Manager and perform a HotSync with the PDA.
2. You then visit each controller with your Handheld device and communicate with the controller.
3. Remember, on the controller you must enter a Communications Unlock credential before you communicate to it with your Handheld device.
4. On the Handheld, select the ***Import/Export*** option. During this time new data is sent to the controller and any new transaction events in the controller, are retrieved.
5. Once you visit all the doors, you must return to the PC. If you are using a PDA connect it to the PC and perform a HotSync. In addition, go to ***Communications > Import/Export*** to perform an Import/Export to import the data into the software. If you are using a DTD connect it to the PC and go directly to ***Communications > Import/Export*** to perform an Import/Export to retrieve transaction event data.

6.6.5 Door Wizard

The Door Level Wizard presents you with a step-by-step process for adding doors to the system. This wizard was created to allow you to create doors with the least amount of effort required. It will also help you to assign consistent settings to the doors you are creating.

Although this wizard may make it easier to add a single door to the system, because of the step by step nature of the wizard, the true benefits will be seen if, for example, you are adding 10 doors to 2 different sites (20 doors total). Adding 20 doors and setting up the options and Time Zones without the wizard takes approximately 240 mouse clicks, but with the Wizard it may only take 12 clicks, because what you are setting up for one door is only done once for all doors being created.

Initial Step - How many doors to add where to add them

- The initial choice you must make is whether or not you want to use the wizard to add multiple doors, and also if you want to add these doors to multiple sites. This Wizard was designed to allow a fast and efficient setup of many types of systems for different applications.

- Some of the content in the following steps may change due to the initial option you selected but the concept of that step is still the same.

Step 1 of 4 - Door Settings

- Step 1 is where you specify the number of doors (if applicable), and the site(s) to which the doors(s) are being added to.

Step 2 of 4 - Sites

- This step is where you select which Sites you want to add the Doors to. The Site list will only contains Sites that support the selected Door type.

Step 3 of 4 - Door Options

- This step is where you select which door options and log event masks to enable or disable. Any selections you make here will be applied to all the doors currently being added with the wizard.
- Any of the options of a door can be customized after the doors have been created.

Step 4 of 4 - Time Zone Selection

- This is where you specify what Time Zones will be assigned to these doors you are adding.
- Time Zones can be assigned, by placing a checkmark in the column labeled 'Selected' .
- Auto-unlock Time Zones can be specified, by placing a checkmark in the column labeled 'Auto Unlock'.
- Any of the Time Zone assignments of a door can be customized after the doors have been created.

Final Option For Multiple Doors

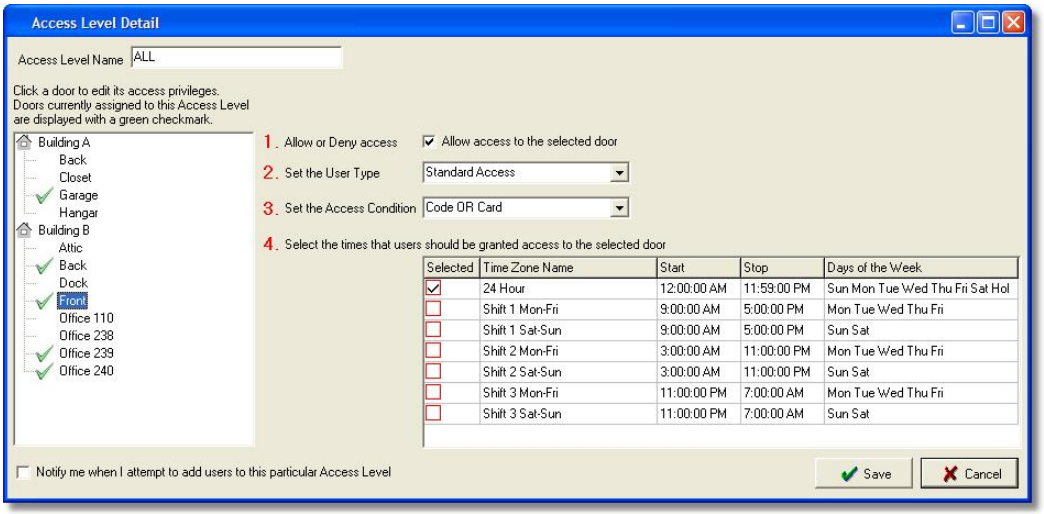
- If you chose to add multiple doors, the last option will ask how you want to name and number these doors.
- You can choose to let the wizard add all the doors now and give them names like 'Door 1' , 'Door 2', etc...
- You can also have the Wizard prompt you for the names (and possibly the controller addresses) one after the other.

6.7 Access Levels

The Access Level feature provides you with a powerful tool to quickly and efficiently maintain users in your system. This is especially important if you have a large system with a large number of users and various security requirements. When you create a new user, you assign the user to an Access Level, rather than directly to a door. An Access

Level defines which doors a user has access to, the type of user, the users access condition (ie. Code OR Card/Code AND Card) and the Time Zones in which the user has access. This simplifies administration because the Access Level contains all information about a user's access, allowing you to group like users together, rather than set up each user's access requirements individually.

This section requires special attention, because Access Levels are integral to the operation of the Hub Manager™ Professional software. Please ensure that you understand this section completely before you start adding or editing Access Level information. To select the Access Levels option, select ***Database > Access Levels***.



NOTE: You can assign users to an Access Level that has no doors assigned to it. A warning message appears asking if you are sure you want to do this, but you can choose to override the warning. This allows you to create an Access Level called NONE, for example, that has no doors assigned to it and then simply re-assign users to that Access Level. That user is now, in effect, disabled, because that user has access to no doors. Make sure you export after reassigning a user like this to ensure that the user is removed from the controllers.

Adding an Access Level

1. Select the ***Add*** button on the ***Access Levels*** screen to open the ***Access Level Detail*** screen.
2. Enter the name for the new Access Level in the ***Access Level Name*** field.
3. In the door list on the left, select a single door you want to include in this Access Level.
4. Once you select a door, section 1 ***Allow or Deny Access*** appears. Check the box labeled ***Allow Access to the selected door*** to open sections 2, 3 and 4. If

you are using a Max 3 v2 with an Output Module, section 5 also appears.

5. Next choose the user type from the ***Set the User Type*** drop down box. See the User Types section below for the definition of each type.
6. Now choose whether the user is ***Card AND Code*** or ***Card OR Code*** from the ***Set the Access Condition*** drop down list. When ***Card AND Code*** is selected, the user must enter both credentials at the door. When ***Card OR Code*** is selected, the user can enter either credential at the door.
7. Finally in section 4, check the box next to each Time Zone you want the users, assigned to this Access Level, to be allowed access. You can choose any number of available Time Zones for each door.

   NOTE: If you are using a Max 3 v2 controller, section 5 is where you select the outputs you want the users, assigned to this Access Level, to trigger when they enter a code/present a credential. For further details about assigning outputs to users in the Max 3 v2, refer to the prox.pad plus, Max 3 v1 and Max 3 v2 section.

8. Repeat steps 3-7 above for each door you want to include in the Access Level.
9. When you finished configuring the Access Level, click ***Save*** to save the data to database.

Access Level Detail Screen - Field/Button Description

Access Level Name

Enter the name or your Access Level here. Choose a name that helps you quickly recognize the settings.

Door Selection List

This is the area on the left side of the ***Access Level Detail*** screen that contains the list of doors currently in the system. When you click a door the current settings for that door are loaded and displayed.

NOTE: A green check mark next to the door name indicates the door has the ***User Type, Access Condition, and Time Zone*** defined. This helps you identify which doors are currently part of the Access Level you are editing.

Allow or Deny Access

After you select a door from the door selection list, this check box appears. Check the box to include the selected door in the Access level and to display the additional settings required for the Access Level. If you uncheck this box, all the settings for that door are removed and the door is no longer part of the Access Level.

Set the User Type

This drop down box contains the user types available in the selected door. A user type defines how the user's credential is processed when presented at the door. A typical user would be assigned as Standard Access, which means they simply allowed to gain access through the door. Other user types perform different functions. See the User Types section below for the definition of each type.

> **NOTE:** Refer to the Supported User Types section below for a list of user types supported by each controller type.

Set the Access Condition

The ***Access Condition*** drop down box contains two options, ***Code OR Card*** and ***Code AND Card***. If you select the ***Code OR Card*** option, users assign to the Access Level only require a single credential at the door. When you create the user, you can add both a code (PIN) and a card, but only one is required. If you select the ***Code AND Card*** option, users assign to the Access Level require both credentials at the door. In this case, you must add both a code (PIN) and a card to the user.

> **NOTE:** The ***Code AND Card*** option is not available for controllers that do not support the entry of multiple credentials.

Select the times that users should be granted access to the selected door

The Time Zone section is where you specify the times when a user is allowed access to the selected door. You can select up to a maximum of 7 Time Zones per door. Keep in mind that you can choose different Time Zones for each door in the Access Level.

Select the relays on the output module that will energize when a valid user credential is entered

This section is only available if the door you are editing is a Max 3 v2 controller with an Output Module. In this area the eight outputs available on the Output Module are displayed. Select the output that you want each user in this Access Level to trigger when they enter their credentials. Refer to the prox.pad plus, Max 3 v1 and Max 3 v2 section for additional details.

Notify me when I attempt to add users to this particular Access Level

If you enable this option a notification message will appear if you attempt to add a user to this Access Level. This may be useful to you if you want to be warned/alerted anytime you assign a user to an Access Level that has 24/7 access to all Doors in your system.

Save

The ***Save*** button saves current data to database.

Cancel

The ***Cancel*** button discards all edits and returns to ***Access Levels*** directory without saving data.

User Types

Com Unlock - Import \ Export (aka Communications Enable)

This user type is supported by Handheld connected controllers only. It is used to unlock (or enable) infrared communications in the controller so you can export data to it from a Handheld device or import transaction logs. This user type does not unlock the door.

Emergency

As the name implies, this user type is designed for use in emergency situations. An Emergency User is a special user that unlocks the door regardless of reason it is locked. This user overrides a Lockout User, meaning if the controller is in lockout mode an Emergency user can still gain access. In battery powered products, with the low voltage warning and inhibit features, standard user's are denied access when the low voltage inhibit warning is reached (ie. low battery). However, Emergency Users can still gain access after this threshold is reached. One other important item to note is the unlock timer. This user type uses the ***Lock Timer - Extended Users*** time, rather than the time for Standard Users.

> **NOTE:** The Emergency User type cannot be disabled via the User directory or the User edit screen. If you do disable a user in the software, the user will still gain access. An Emergency User in the Max 3 v2 controller has 24 hour access, regardless of the Time Zones assigned in the Access Level. In addition, this user type will not trigger a First-In Auto-Unlock Time Zone.

Extended Time

An Extended Time user type unlocks the door for a longer period of time than a standard user. The unlock time is set in the ***Lock Timer - Extended Users*** setting in the ***System Parameters*** section of the ***Door*** edit screen. This time is defaulted to 10 seconds. You must specify the time in each individual controller. You would use this user type for anyone that requires more time to get to the door after they've unlocked it.

Lockout

When a Lockout User enters/presents their credentials all other users are "locked out" and are denied access to the door. This applies to all users in the controller except the Master, Supervisor and Emergency users, which can't be locked out. To remove the lockout condition, either the lockout user who initiated the lockout or another lockout user must present their credential. The Lockout user is especially useful if a danger is identified in a particular room or area and you do not want anyone to enter until the danger is cleared. Please note, the state of the lock does not change when a Lockout code is entered (ie. the door doesn't unlock) because Lockout users cannot be used to gain access.

Passage (aka Toggle)

The Passage user type (also referred to as Toggle) acts much like an on/off switch. This means if the door is locked when you enter the credential, the door unlocks and remains in the unlocked state indefinitely. If the door is already unlocked, due to a previous Passage code, the door is re-locked when the credential is presented.

NOTE: Passage users do not function during active auto-unlock Time Zones.

Relock

This user type locks the door if the door is in an unlocked state for any reason, including an Auto-Unlock Time Zone, a Passage User or due to a long timed unlock. This feature is useful, for example, when a door is unlocked by an Auto-Unlock Time Zone but you need to relock the door before the scheduled lock time. Relock users can lock the door only, not unlock it.

Standard Access

Standard Access is the most common user type you will use in your system. The majority of the users in your system are everyday users that you simply want to momentarily unlock the door when they present their credential. When you set up an access level for these types of users, choose the Standard Access option. The unlock time for this user type is set in the ***Lock Timer - Standard Users*** setting in the ***System Parameters*** section of the ***Door*** edit screen. This time is defaulted to 5 seconds. You must specify the time in each individual controller.

Supported User Types

The chart below shows the User Types supported by each controller type and how many of each User Type is allowed in each controller type (up to the maximum user capacity of the specific controller type).

User Type	HC500, Hub+ \Max	Max 2 v1, Max 2 v2	LS2\P	prox.pad plus	Max 3 v1	Max 3 v2	prox.pad plus IR
Com Unlock - Import \ Export	N/A	N/A	No Limit	N/A	N/A	N/A	No Limit
Emergency	N/A	N/A	No Limit	No Limit	No Limit	No Limit	No Limit
Extended Time	N/A	N/A	No Limit	No Limit	No Limit	No Limit	No Limit
Lockout	N/A	N/A	No Limit	No Limit	No Limit	No Limit	No Limit
Master	1 (required)	1 (required)	1 (required)	1 (required)	1 (required)	1 (required)	1 (required)
Passage	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit
Relock	No Limit (not available in HC500)	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit
Standard	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit	No Limit
Supervisor	N/A	N/A	1 (required)	1 (required)	1 (required)	1 (required)	1 (required)

6.8 Access Level Wizard

The Access Level Wizard presents you with a step-by-step process to creating an Access Level that can be assigned to users. The wizard will help you to create consistent access privileges to the Doors you have selected. If you choose to apply all the settings you specify to every selected Door by leaving the default 'YES' option selected in steps 3, 4, and 5, every Door you selected in step 2 will be setup the exact same way.

Step 1 of 5 - Name the Access Level

- It is recommended that you chose a name that describes the type of people that will be assigned to this Access Level, such as 'Accounting Manager', 'Accounting Staff', 'Production Manager', 'Production Staff', 'All Access', or even 'Relock All'
- Anyone assigned to this Access Level will have the exact same access privileges as every other member of this Access Level.
- The name you assign can be changed at any time after the Access Level is created.

Step 2 of 5 - Door Selection

- This step is where you select which Doors the Users that are assigned to this Access Level will have access to.
- If this Access Level will have access to ALL Doors in the system, just leave 'YES' selected, otherwise choose 'NO' and select the appropriate Doors.

Step 3 of 5 - User Type Selection

- This is where you specify what action will occur when users assigned to this Access Level enter their valid credentials.
- If you want to assign the same User Type to all selected Doors leave the 'YES' option selected, otherwise select 'NO' and use the combo box in the right most column to make the appropriate user type selection for each Door.

Step 4 of 5 - Access Condition Selection

- This is where you specify what type of code or card combination is required of users assigned to this Access Level.
- If you know you have front ends/controllers that support only one type of credential input, you should select 'Code OR Card'.
- If you know you have front ends/controllers that support and require that both code and card credentials to be presented before access is granted, then you should select 'Code AND Card'.
- Only those Access Conditions that are supported by all device types will be displayed.
- If you want to assign the same Access Type to all selected Doors leave the 'YES' option selected, otherwise select 'NO' and use the combo box in the right most column to make the appropriate access condition selection for each Door.

Step 5 of 5 - Time Zone Assignments

- This is where you specify what Time Zones Users assigned to this Access Level will be granted access.
- By default, the 'YES' option is selected, and in the bottom grid, the wizard will only show Time Zones that appear in every one of the selected Doors from step 2. If this grid is empty, that means there isn't a common Time Zone that appears in every Door, and you must now select 'NO' because the Time Zone selections must be made for each individual Door.

- Select one of the Doors and the Time Zones assigned to that Door will appear at the bottom. If no Time Zones appear at the bottom that means a Time Zone was never assigned to that Door when it was created. You must now decide what you want to do. You can either go back to step 2 and deselect that Door, and then finish creating this access level, and add that Door afterwards.
- You could also decide to cancel adding this Access Level and go back and add the Time Zone to that Door and come back to the Wizard to re-create the Access Level. Either way, you will need to go to that Door and assign a Time Zone to it.
- Every selected Door from step 2 must have a time Zone selection made in Step 5.

6.9 Users

The ***Users Database,*** located in ***Database > Users***, is where you add people to your access control system. Within this database is the ***Users*** directory, which contains a list of all the users in your system, and is where you go to add, delete, edit, retire or disable users. In addition, you can batch load a group of users with the ***Add Group*** or ***User Import Wizard*** features. Each user contains several pieces of information including the user's name, access credential (such as a PIN and card), Access Level and a few other options. The following section discusses all the available options in detail.

Master User
Supervisor User
Users Directory Button Descriptions
Adding a User
User Edit Screen Field/Button Description
Access Level Selection Tool
Card Format
Proximity Card Fields
Enrollment Station
Raw Card Data
PIN Data (a.k.a. Keypad Code data)
Temporary\Expiring Users

Master User

NOTE: The master user's PIN must be changed prior to adding any users to the system. This ensures the default PIN of 1234 is not unintentionally sent to each controller.

- The Master User (aka Master Code) is a mandatory user that is required in every user database and always appears in the user list. This user is sent to every controller in the system and is always stored in user memory location 1 in the controller. The default access code (PIN) is 1234. This is also the default user contained in every controller from the factory.
- This user is not assigned to an Access Level because this user is sent to every controller in the system during export.
- You can use this PIN to access program mode in the controller, although this is not recommended when using software.
- This user also acts as a "Com Unlock - Import and Export" user, which is used to enable handheld communications when using a LS2\P and prox.pad plus IR controller.

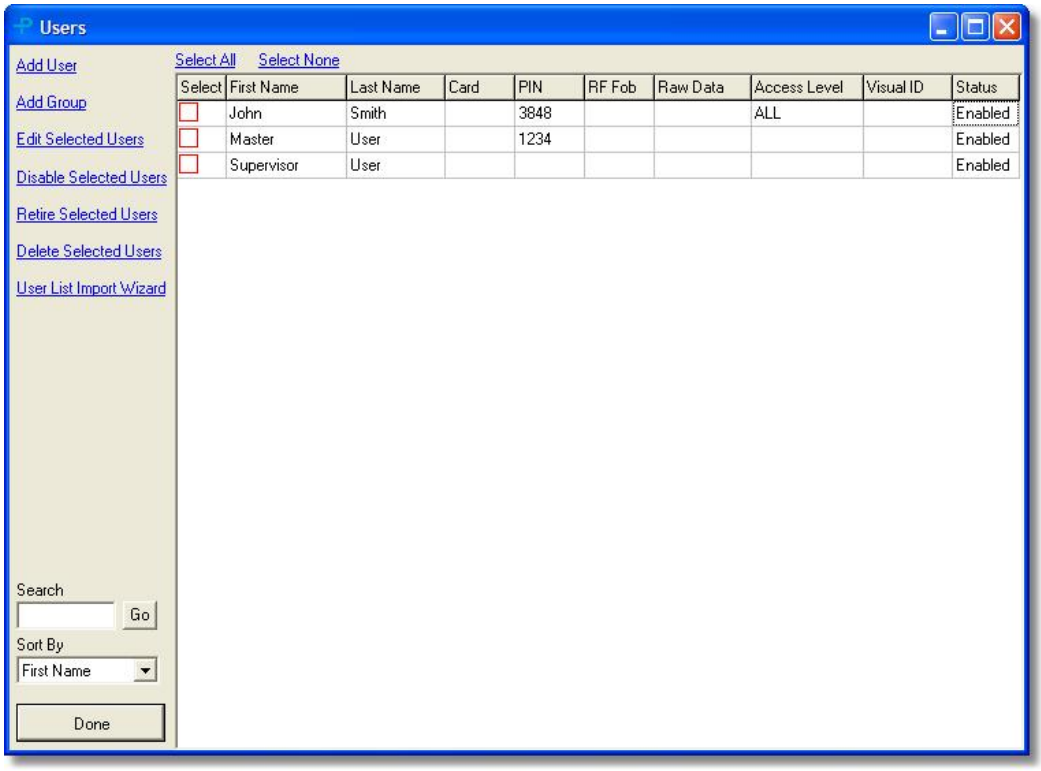
NOTE: The Master Code should not be used to gain access to any battery powered controllers. Using this code type to gain access will reduce the controller battery life, since it also enables communications and keeps the controller powered up for 60 seconds.

Supervisor User

- The Supervisor User (aka Supervisor Code) is a mandatory user that is required in every user database and always appears in the user list. IEI recommends that you add a supervisor PIN, even if you don't plan to use it.
- By default, this user's PIN is empty. As soon as you define a PIN for this user, this user is sent to every controller in the system, that supports this user type, during export. This user is always stored in user memory location 2 in the controller. This user is not sent to controller's that do not support the supervisor user. Refer to the Support User Types Chart in the Access Levels section for a list of support user types.
- This user is not assigned to an Access Level, because this user is automatically sent to every controller in the system, that supports this user type, during export.
- You can use this PIN to access program mode in the controller, although this is not recommended when using software.
- This user also acts as a "Com Unlock - Import and Export" user, which is used to enable handheld communications when using a LS2\P and prox.pad plus IR controller.

Users Directory Field/Button Descriptions

Below is a screenshot of the ***Users*** directory. Following the image is a description each of the options available on this screen.



Selecting Users

There are four buttons(***Edit Selected Users***, ***Disable Selected Users***, ***Retire Selected Users*** and ***Delete Selected Users***) in the ***Users*** directory that require you to select a single user or multiple users. The following list contains all the possible ways to select users, prior to using these buttons.

- Check a single box next to a user's name and click the desired button.
- Check the box next to the name of multiple users and click the desired button.
- Check a single box next to a user's name, then use the up or down arrow on your keyboard to select multiple, adjacent users.
- Click the ***Select All*** option at the top of the user list to select all the users in the list.
- Click the ***Select None*** option to de-select all selected users.

NOTE: You can also double-click on a single user to edit a user.

Add User

Click the ***Add User*** button to add a single user.

Add Group

Click the ***Add Group*** button if you want to add a group of users with common properties. See the Add User Group section for more details.

Edit Selected Users

To edit a single user, check the box next to a single user's name then click ***Edit Selected Users*** button. You can then change any of the user's information. To edit multiple users at once, select the users you want to edit by using one of the methods described above, then click the ***Edit Selected Users*** button. When editing multiple users you can only change options that are common to all users, such as ***Access Level***, ***This user is enabled*** option, ***Member of Time Management Group***, **This User can Trigger First In Auto Unlock Time Zones** option or ***Temporary/ Expiration Info*** option. All other options including ***First Name***, ***Last Name***, ***Card Data*** or ***PIN Data*** can not be edited.

Disable Selected Users

Disabling a user means that the user will be sent to all controllers in the system, that they have access to in their Access Level, but the user will be denied access at the controller when they present their credential. You would use this feature, for example, when you want to temporarily disable a user because they are going on vacation or taking an extended leave, but you want to assure that their credentials can't be used to gain access.

To disable a single user, check the box next to a single user's name then click the ***Disable Selected Users*** button. To disable multiple users at once, select the users you want to disable by using one of the methods described above, then click the ***Disable Selected Users*** button.

You can also disable a single user, by editing the user and uncheck the ***This User is Enabled*** checkbox, a shown in the image below. If you want to reactivate the user, edit the user, then check the ***This User is Enabled*** checkbox.

There is an alternate way to disable a user by creating an Access Level called "NO ACCESS" that has access to no doors in the system. You can then simply assign the user you want to disable to this "NO ACCESS" Access Level, which will deny the user access, because there are no doors selected in the access level. When you want to enable the user, you can simply change the Access Level for that user to the original Access Level the user was assigned to and then export again.

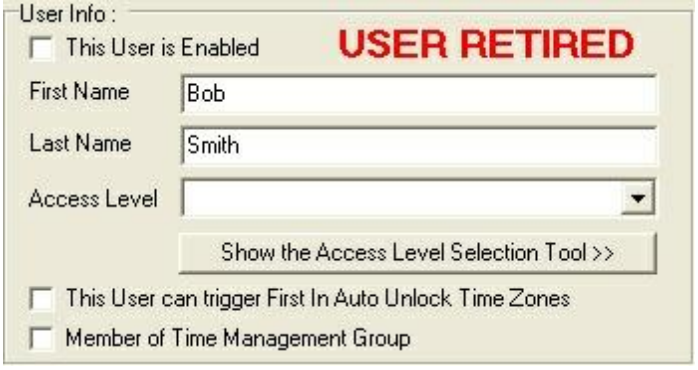
If you find that you also want to see events that record this particular user trying to gain access when they should have been on vacation, you can simply create an access level that mirrors that access level this user was originally assigned to, but you don't assign any Time Zones to the doors. Now when this user attempts to access the building, an event is generated and stored in the controller that says 'Access Denied - Bad Time Zone'.

Retire Selected Users

Retiring a user means that the user will not be sent to any door controllers in the system, but the user will remain in the database. In addition, when you retire a user, the PIN or card data that was assigned to the user is removed from that user and is now available for use by any other new or existing user in the system. You would use this feature when you want to permanently remove a user from all the controllers in the system, but you want them to remain in the database so you can view their entire transaction log history in the log filter report. When a user is retired, all the user's events that occurred prior to retiring the user remain in the transaction log filter report. The ***Retire Selected Users*** option is an alternative to the ***Delete Selected Users*** option, which permanently deletes a user from the database, including all events associated with that user.

To retire a single user, check the box next to a single user's name then click the ***Retire Selected Users*** button. To retire multiple users at once, select the users you want to retire by using one of the methods described above, then click the ***Retire Selected Users*** button.

After you retire a user, it says ***USER RETIRED*** in the ***User Info*** section when you edit that user. If you want to reactivate the user, edit the user, then check the ***This User is Enabled*** checkbox. Next you have re-enter all the user data, as discussed in the Adding a User section below.



Delete Selected Users

Deleting a user means that the user is completely removed from the database. All events associated with his user are no longer displayed in the log filter report. In addition, the PIN or card data that was assigned to the user is removed from that user and is now available for use by any other new or existing user in the system. If you still want a user's events to appear in the transaction log filter report, then it is recommended that you choose to '***Retire Selected Users*** option instead of deleting the user.

To delete a single user, check the box next to a single user's name then click the ***Delete Selected Users*** button. To delete multiple users at once, select the users you want to delete by using one of the methods described above, then click the ***Delete Selected Users*** button.

User Import Wizard

The User Import Wizard option lets you add users to the database by importing the user names from an external list, using a simple step-by-step procedure. After adding users, you must export to your door controllers.

***Search* Edit Box**

Use the ***Search*** edit box to search the user list for a certain word, such as a user's name. To search, type in the text you want to search for, then click the ***Go*** button.

Go

The ***Go*** button is used when searching for a word entered into the ***Search*** text box.

Sort By

The ***Sort By*** drop down box allows you to sort the user list by any column at the top of the user list, such as the ***First Name***, ***Last Name*** or ***PIN***. To sort the user list, click on the down arrow next to ***Sort By***, then choose an item in the list. The user list will then automatically re-sort itself based on your selection.

Done

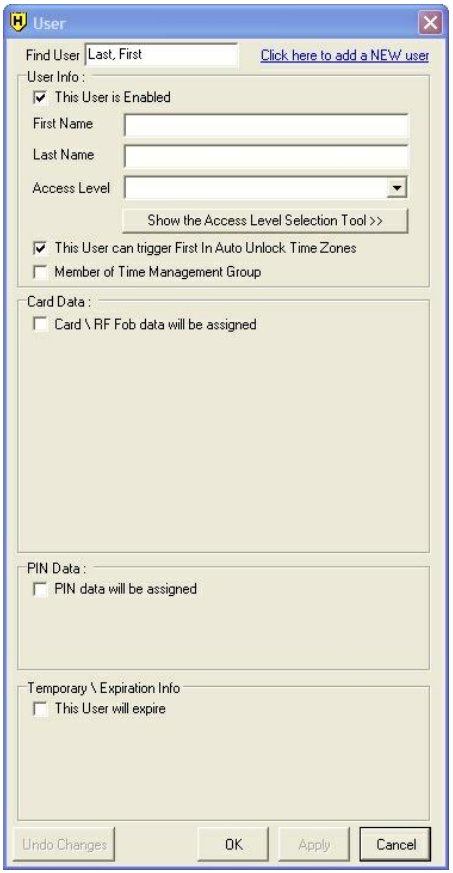
To close the ***Users*** directory, click the ***Done*** button.

Adding a User

This section discusses how to add a user to the system. See the User Edit Screen Field Button/Description section below for detailed descriptions of each field in the ***User*** edit screen.

NOTE: The Master User's PIN must be changed prior to initially adding any users to the system.

1. Click the ***Add User*** button on the ***Users*** directory screen to open the ***User*** edit screen.



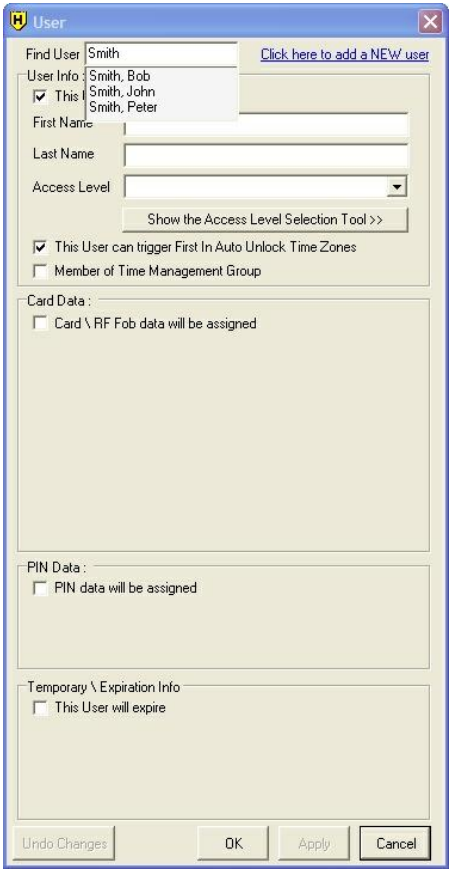
2. Enter the user's ***First Name***, ***Last Name*** and select an ***Access Level***.
3. Choose either ***Card Data***, ***PIN Data*** or both by checking the box next the option. Enter the required data.

4. Select ***Apply*** to save the settings. To cancel adding this particular user, select the **Cancel** button.
5. To close the ***User*** edit box click the ***OK*** button. If you want to add another user with similar properties, select the ***Click here to add a NEW user*** option at the top of the screen.

User Edit Screen Field/Button Description

Find User

Use this option to search for an existing user in the database directly from the ***User*** edit screen. To use this feature, just type the name of an existing user in Last Name, First Name format. As you start typing the last name of the user, the software searches for users that match what you've typed. As soon as a user is found that matches, that user record is automatically loaded. If more than one user matches what you've typed then a drop down list is displayed with all the matching users, as shown below.



Click here to add a NEW user

Use this feature to add another user, with similar properties as the previous user, without closing the ***User*** edit screen. When you select this option, only the unique fields such as ***First Name***, ***Last Name***, ***Visual ID***, ***Card Number*** (if assigned) and ***PIN*** (if assigned) are cleared, while all other non-unique fields such as ***Access Level***, ***This user is enabled*** option, ***Member of Time Management Group***, **This User can Trigger First In Auto Unlock Time Zones** option and ***Temporary/Expiration Info*** option settings remain unchanged. This allows you to add multiple users with common settings, without re-entering the same data over and over again.

This User is Enabled

This checkbox is used to either enable or disable this particular user. Disabling a user means that the user will be sent to all controllers in the system, that they have access to in their Access Level, but the user will be denied access at the controller when they present their credential. If a disabled user attempts to gain access, a transaction log event of "User - Access Denied - User Disabled" is generated in LS2 \P, Max 3 v1, Max 3 v2, prox.pad plus IR or prox.pad plus controllers and an event of "User - Access Denied - Bad Time Zone" in Secured Series Controllers controllers.

First Name

Enter the user's first name here. (30 character max)

Last Name

Enter the user's last name here. (30 character max)

Access Level

This drop down box contains a list of all the available Access Levels in the system. The Access Level also contains the Auxiliary Output settings when using the Max 3 v2 controller type. Select the Access Level you want to assign to the user.

Show the Access Level Selection Tool

Selecting this button expands the ***User*** edit screen to display the ***Access Level Selection Tool***. This tool is designed to help you select the best Access Level for the user you are adding. Simply select the doors, in the area labeled ***Door Selection***, that you want to add a user to. As you select door on the left, the Access Levels containing only the selected doors are displayed in the area on the right, labeled ***Matching Access Levels***. When you see the Access Level you want to assign this user to, just double-click that Access Level. Your selection will then appear in the ***Access Level*** drop down box.

See the Access Level Selection Tool below for more information.

This User can Trigger First In Auto Unlock Time Zones

The ***User*** edit screen contains a feature that allows you to specify which users can trigger a First-In Auto-Unlock time zone. When this box is checked, that specific user can trigger a First-In Auto-Unlock time zone when they are granted access. You must check this box for each user that you want to trigger First-In Auto-Unlock. If you do not check this box, then the user will not trigger First-In Auto-Unlock and is simply granted access.

NOTE: This box is checked by default for all Users and must be unchecked if this User is not to trigger First In Auto Unlock Time Zones.

Please note, you must also have at least one Auto-Unlock time zone assigned to the door and the ***1st In Auto Unlock*** option must be enabled. To assign a time zone to a door and designate it as Auto-Unlock, go to ***Database > Doors***, and either ***Edit*** or ***Add*** a door. Then go to the ***Time Zones*** tab in the ***Door*** edit screen. The ***1st In Auto Unlock*** option is located on the ***Options*** tab in the ***Door*** edit screen. In addition, a user can only trigger a First-In Auto-Unlock when they are assigned to an Access Level containing that particular time zone. For further details regarding Users, Doors and Access levels, refer to the Users, Doors and Access Levels sections.

NOTE: This option only applies only to users sent to Max 3 v2 controllers. This option has no affect on users sent to any other controller type, regardless of the check box setting. In addition, this option has no affect on Master, Supervisor or Emergency user types. These User types will not trigger First In Auto Unlock Time Zones.

Member of Time Management Group
When this option is enabled, the user is included in the Time Management report.

NOTE: The Time Management Report requires that both ***User - Access Granted In*** and ***User - Access Granted Out*** events are generated. This is required so that the report can calculate how long the user was 'In' the building. The ***User - Access Granted Out*** event is not supported by all controller types, especially LS2\P products. Without the ***User - Access Granted Out*** event, you can only calculate the ***gross time*** between the first ***User - Access Granted IN*** event and the last ***User - Access Granted IN*** event. Please refer to the Doors section for further details about enabling transaction events.

Card \ RF Fob data will be assigned
Enabling this option displays the options related to card data, such as the card format and card number. Disabling this option clears all data and hides all the options related to this type of credential. Refer to the sections below entitled Card Format, HID Proximity, Enrollment Station and Raw Data for further details.

PIN data will be assigned

Enabling this option displays the options related to PIN data (aka User Code). Disabling this option clears all data and hides all the options. Refer to the PIN Data section below for further information.

Temporary\Expiration Info

A temporary/expiring user has access during a specified period of time and when that time period ends, the user access expires and no longer has access. Enabling this option displays the temporary\expiring user options, which allows you to specify when the user has access. The details of this options are discussed below in the Temporary\Expiring Users section.

NOTE: This option only applies to users sent to the Max 3 v2 controller type. All other controller types do not support temporary/expiring users.

Undo Changes

The ***Undo Changes*** button is inactive (grayed-out) until you make any changes to a user while editing or when you start adding a new user, at which point the button becomes active. You would use this button typically when you are editing a user and accidentally changed some user information and want to revert back the original data. When you click the button, it resets all the data in the ***User Info***, ***Card Data***, ***PIN Data and Temporary / Expiration Info*** sections to their previous values, before you made any changes, without closing the ***User*** edit screen.

OK

The ***OK*** button permanently saves the currently opened user data, closes the ***User*** edit screen and returns you to the ***Users*** directory.

Apply

The ***Apply*** button is inactive (grayed-out) until you make any changes to a user while editing or when you start adding a new user, at which point the button becomes active. This button is similar to the ***OK*** button, as it permanently saves all of the changes you make, except when clicked it does not close the ***User*** edit screen. This feature is useful if you want to add or edit several users in a row, but you want to remain on the ***User*** edit screen without returning to the ***Users*** directory each time. After clicking the ***Apply*** button, you can then use the ***Find*** feature to search for an existing user you want to edit or use the ***Click here to add a New User*** feature to add a new user.

Cancel

The ***Cancel*** button discards any edits made to the currently displayed user, closes the ***User*** edit screen, then returns you to the ***Users*** directory.

Access Level Selection Tool

The ***Access Level Selection Tool*** is designed to help you select an Access Level for the user you are adding, by finding an existing Access Level that matches your requirements for the new user. In addition, if there are no access levels that meet your requirements, this tool allows you to add a new Access Level directly from this screen. This eliminates the need for you to exit the ***User*** edit screen and search through your Access Levels to find one that suits you.

Simply select the the door(s), in the area labeled ***Door Selection***, that you want to add a user to. As you select door on the left, the Access Levels containing only the selected doors are displayed in the area on the right, labeled ***Matching Access Levels***. When you see the Access Level you want to assign this user to, just double-click that Access Level. Your selection will then appear in the ***Access Level*** drop down box.

Below is a detailed description of each function in the ***Access Level Selection Tool***.

Find Door

The ***Find Door*** section allows you to search for a specific door. Just type the name of the door you are looking for to highlight the matching door in the ***Door Selection*** list. This is useful if you have a large number of doors in the list.

Door Selection

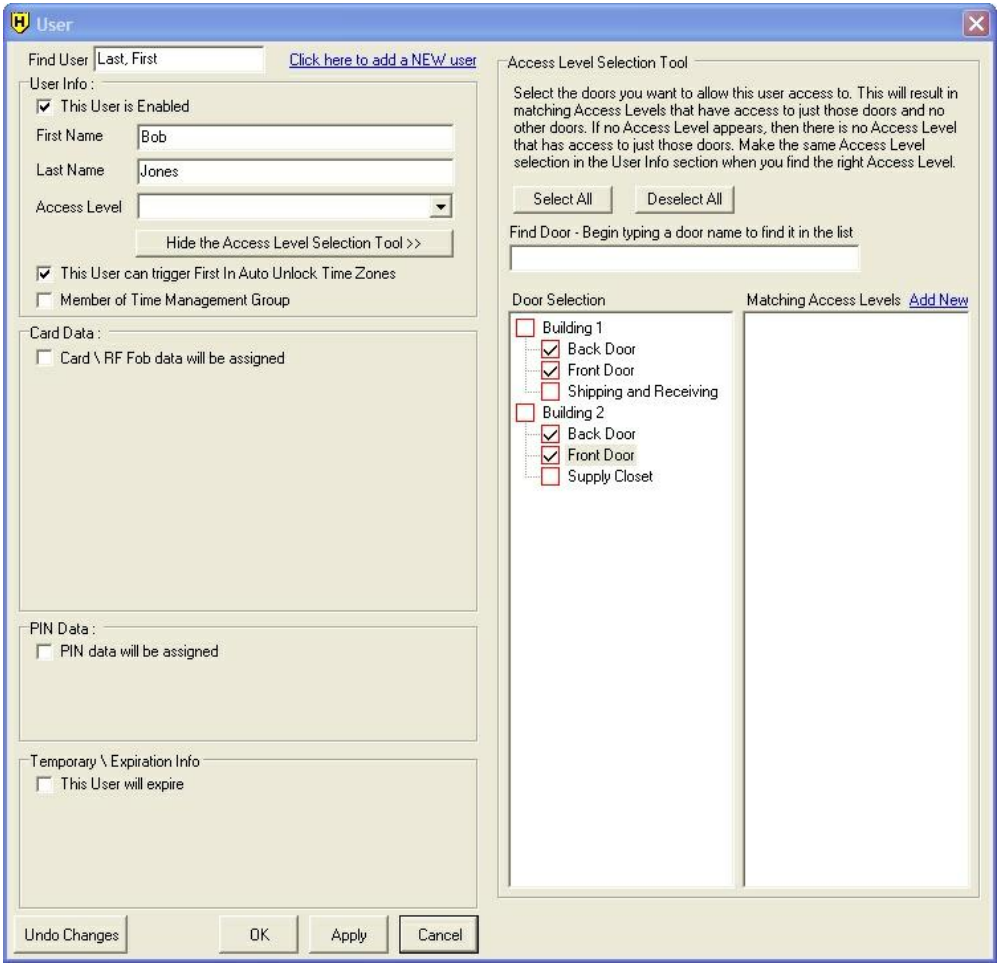
The ***Door Selection*** area shows all the doors currently in the system. This is where you select which doors you want the user to have access to. When you select doors, the available access levels containing all the selected doors is shown in the ***Matching Access Levels*** area on the right. If there are no Access Levels that match your selection then the ***Matching Access Levels*** remains blank. Now you would use the ***Add New*** feature described below.

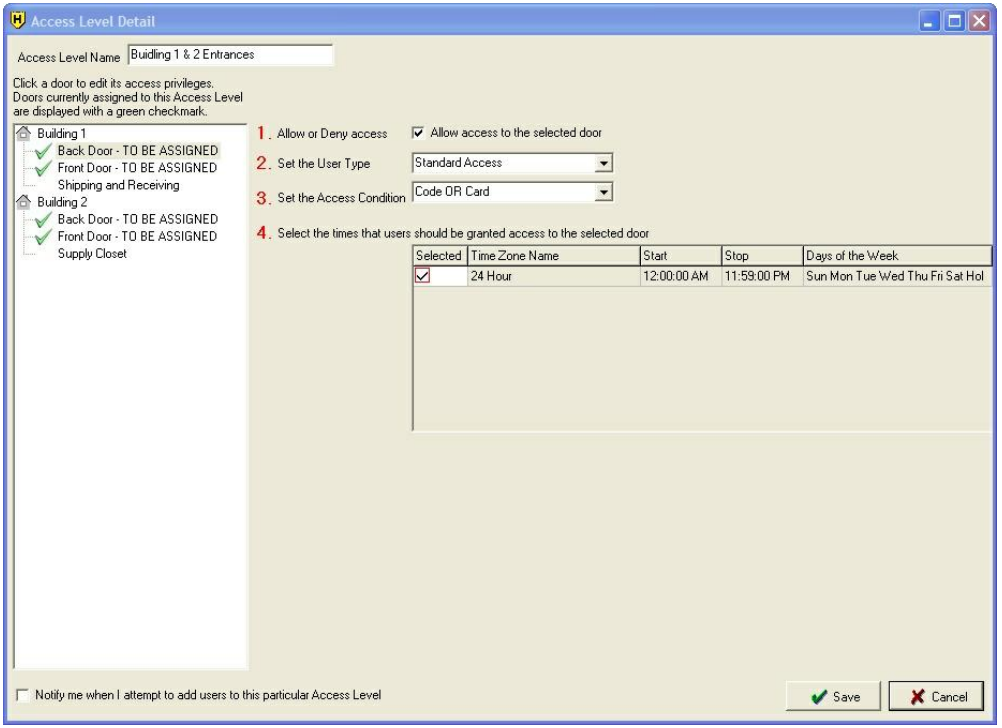
Add New

As mentioned above, if there are no Access Levels that match your selection then the ***Matching Access Levels*** remains blank. In this situation, use the ***Add New*** feature, which allows you to create an Access Level directly from the ***Access Level Selection Tool*** screen. To create the new Access Level, leave the desired doors selected, then click on ***Add New*** to open the ***Access Level Detail*** screen. Next to each door you had selected is the text ***TO BE ASSIGNED***, indicating these are the doors you intend to add to the Access Level.

Example:

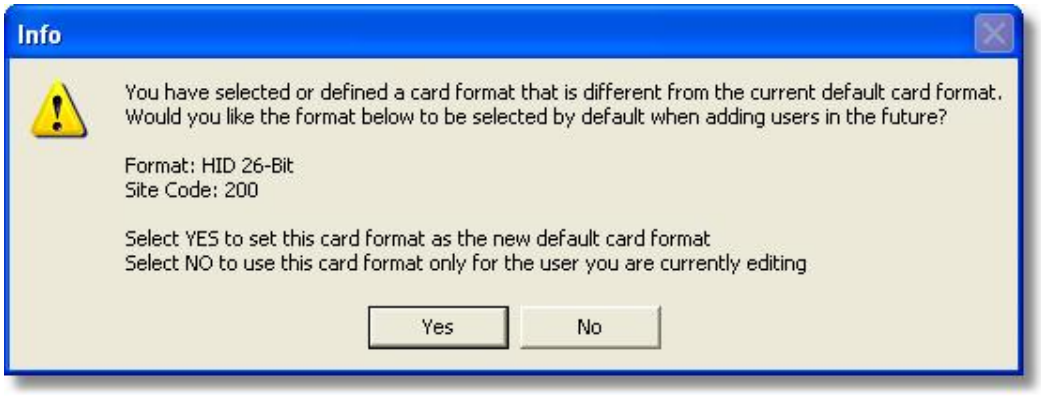
In the following example, the Operator has selected the Front Door and Back Door in both Buildings 1 and 2. In the ***Matching Access Levels*** section you can see that nothing is displayed, because there is currently no Access Level that has access to only those doors, as shown in the image below. Now when the operator clicks on ***Add New***, the ***Access Level Detail*** screen opens. Next to each door that was selected is the text ***TO BE ASSIGNED***. Now set up the Access Level to include these doors. Refer the Access Levels section for further details.





Card Format

When adding a new user, you may notice the ***Card Format*** and supporting data fields are pre-filled with default data. This occurs because an Operator was previously asked if they wanted to set a specific default card format for all future user additions, as seen in the screenshot below. This message appears when you save the first user to the system. Directly after installation, there is no defined default card format yet, so the first user you add, you must select a ***Card Format***. After this point, if you choose to set that format as the default format, you will no longer need to select a card format when you add additional users, since it's already selected for you. This is simply a time saver for you so you don't need to select a card format each time you add a user. Since most systems use the same format card for every user, you typically only need to enter the card number.



When you select either an HID or AWID format, you must enter the site code before you can save the user. If you decide to save this card format and site code as the new default, then you do not need to enter the site code again.

Card Format

Here you must specify what type of credential you are assigning to the user. The term card is used to represent the type of data entered into this field for this user. It can be data of a known HID proximity card format, or the data for an RF Fob (radio frequency fob) supplied by IEI. Some card formats explained in this manual may not be available in all controllers supported by this software.

Card Format Name	Default Site Code	Site Code Editable?
Prox 26-Bit HID	NONE	YES
Prox 26-Bit HID - IEI	11	YES
Prox 26-Bit AWID	NONE	YES
Prox 26-Bit AWID - IEI	11	YES
Prox 34-Bit HID	NONE	YES
Prox 35-Bit HID Corporate 1000	NONE	YES
Prox 36-Bit AWID	NONE	YES
Prox 36-Bit AWID - IEI	11	YES
Prox 37-Bit HID (no site code)	NONE	NO
Magnetic Stripe (ABA Track II)	n/a	n/a
Dallas Touch Chip	n/a	n/a
Enrollment Station (HID)	n/a	n/a

If you have a proximity card format that is not shown in the list of card formats above, or you have a custom card format, it is possible to have a custom card format add-on file created by International Electronics, Inc. and sent to you. After you install this add-on file on the PC running Hub Manager™ Professional, you then have the option

of selecting this new format from the ***Card Format*** list. You can then enter the card PIN into the software without using an Enrollment Station. This does require that you know the exact bit designations of that particular card format, including all parity bits, card number location and site code location within the format.

NOTE: If you are using a Motorola Proximity Card reader or a Wiegand Keypad Front End with a Secured Series Hub controller, then you must select the ***Card Format*** named ***Magnetic Stripe***. In addition, if you are using Motorola Cards, you will likely need to place a "7" in front of the card number that you enter into the ***Card Number*** field.

Visual ID **(not required)**
A text field (50 characters max.) that allows you to enter the visual identifier of the credential you are assigning to this user. This is helpful if the credential has printing on it that is not information related to the data encoded on the credential. It can be used as a way to identify the owner of a lost credential if it is found.

This field can also be used to store data for any purpose that you wish that is unrelated to the card data, such as entering the employee number, or license number of that user. This could help you to sort the User directory by the data entered into the Visual ID field.

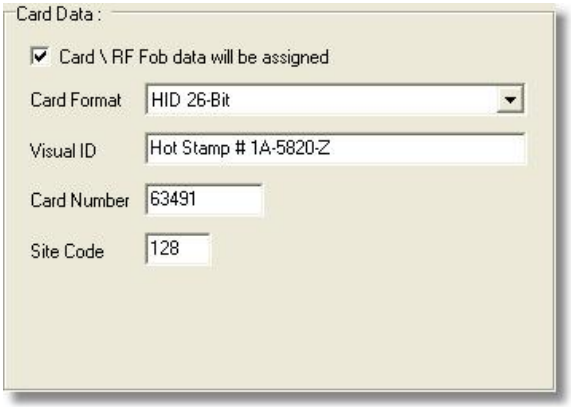
Proximity Card Fields

Card Number
This field stores proximity card number, typically this is the number printed on the card, but sometimes the hot stamp is just a reference number and is not the card number (refer to ***Visual ID*** above). The length and range of a card number varies based on the particular format selected.

Site Code (if applicable to the selected proximity format)
This field is only visible if the card format selected requires the operator to define the Site Code of the proximity card.

Group Code (if applicable to the selected proximity format)
This field is only visible if the card format selected requires the operator to define the Group Code of the proximity card.

Corp. Code (if applicable to the selected proximity format)
This field is only visible if the card format selected requires the operator to define the Corporate Code of the proximity card.



NOTE: If you know that the Site, Group or Corporate Codes are part of the data format you have selected, but these fields are not visible, then these fields may be predefined, unchangeable and should not be displayed (potentially for security reasons).

Enrollment Station

The Enrollment Station is a device used to enroll HID format proximity cards (up to 40 bits). This device connects to the PC using a USB or serial COM port connection. It allows you to read the raw card data directly from an HID proximity card and store it in the database so you can export it to the door controller. This is helpful if you do not know the exact format of the HID proximity cards you want to assign to a user. The raw data received by the Enrollment Station is the exact data the controller reads from an HID proximity card when presented to a card reader. It then uses this data to determine whether or not a user is allowed access through the door.

Use the following steps to enroll a card into the database using the Enrollment Station:

1. Select Enrollment Station as the ***Card Format***.
2. Specify the ***Com Port*** the Enrollment Station is connected to (if not already defined)
3. Select the ***<<<Get Card Data From Enrollment Station>>>*** button.
4. Present the card to the proximity antenna of the Enrollment Station.
5. After presenting the card, the Enrollment Station reads the raw data, imports it and displays it in the ***Raw Data*** field. In addition, the message ***Enrollment Successful*** is displayed. You can now save the user.

NOTE: The Enrollment Station format can also be used to enter the raw data from a proximity card with an unknown format, even if you don't have an Enrollment Station. To do this, you must get the raw data off the card by enrolling the card into your controller through the card reader, then importing the door settings (refer to the Import Door Settings section). When the data is imported, copy down the raw card data stored in the user location you programmed the card into and enter that exact data into the ***Raw Data*** field. This method does not apply to LS2\P or prox.pad plus IR products.

Raw Card Data

Raw data is the actual data that is stored in the controller. This raw data has no particular format. It can be comprised of HID proximity card data, RF Fob Data, enrollment station data or some other type of input device, but none of the parameters of those formats are specified in the raw data. It is up to the controller to capture the data that it received and see if a match can be found. Since the controller does not know the origin of the card data, it is able to store card data for any 40 bit (or less) HID card format. Because the controller does not know the format of the data it has no way to perform Site Code, Group Code, Corporate Code verification.

PIN Data (a.k.a. Keypad Code data)

A user PIN (Personal Identification Number) is the actual keypad code used to gain access through the door.

PIN data will be assigned

Check this box to open the ***PIN Data*** options and assign a PIN to the user.

PIN

You can enter a custom PIN in this edit box. This number is the actual keypad PIN (code) used to gain access through the door.

Generate Random PIN

The ***Generate Random PIN*** button generates a random PIN for the user. The number of digits is set in the ***Random PIN Length*** Edit Box.

Random PIN Length
The ***Random PIN Length*** Edit Box contains the number of digits used when creating a random PIN, when you click the ***Generate Random PIN*** button. You must enter a number between 4 and 6 digits.

Temporary\Expiring Users

NOTE: This option only applies to users sent to the Max 3 v2 controller type. All other controller types do not support temporary/expiring users. In addition, the master or supervisor users can't be programmed as temporary users.

The Max 3 v2 supports one type of temporary/expiring users. It's called ***Start and Stop Date***.

Start and Stop Date: The user has access between a fixed start and stop date.

This type allows you to specify a date range when a user will be granted access. This type of user will not be granted access prior to the specified start date or beyond the specified stop date. If the user attempts to gain access in either case, the door will deny access and generate an access denied log event. The user can only gain access between the start and stop date. It is possible for the start and stop date to be the same date. You would do this when you only want the user to have access for a single day.

This temporary user type has a limit of 500 unique temporary access intervals. An access interval is the term used to describe a single temporary time interval when a temporary user is allowed access. This means you can't have more than 500 users set to more than 500 different temporary access intervals. You can, however, assign multiple users to a single access interval by using the ***Copy Temp settings from another user*** button, which allows you to copy the settings from another user. If you do select a start and stop date that happens to match another user, the software will recognize this and automatically use the same access interval, rather than create a new one.

If you know you are not going to exceed 500 users in your system, then you can use any ***Start Date*** and any ***Stop Date*** combination you want, without worrying about exceeding this limit.

NOTE: Any time zone and holiday restrictions defined in the user's access level still apply.

To configure a user for ***Start and Stop Date***, follow these steps:

1. Check the box next to the ***This User will expire*** option.
2. Click the arrow in the ***Expiration Type*** drop down box and select ***Start and Stop Date;*** If you want the user to have the same settings as another user, click the ***Copy Temp settings from another user*** button and skip steps 3 and 4.
3. Click the arrow in the ***Start Date*** drop down box, to display a calendar, and select the start date.
4. Click the arrow in the ***Stop Date*** drop down box, to display a calendar, and select the stop date.
5. Click ***Apply*** to save the changes.

NOTE: If this user is exported to multiple controllers, each controller contains the same Start and Stop Dates, which means when the stop date has passed, every controller in the system will deny this user access.

Below are few examples how to reduce the number of access intervals used in a controller:

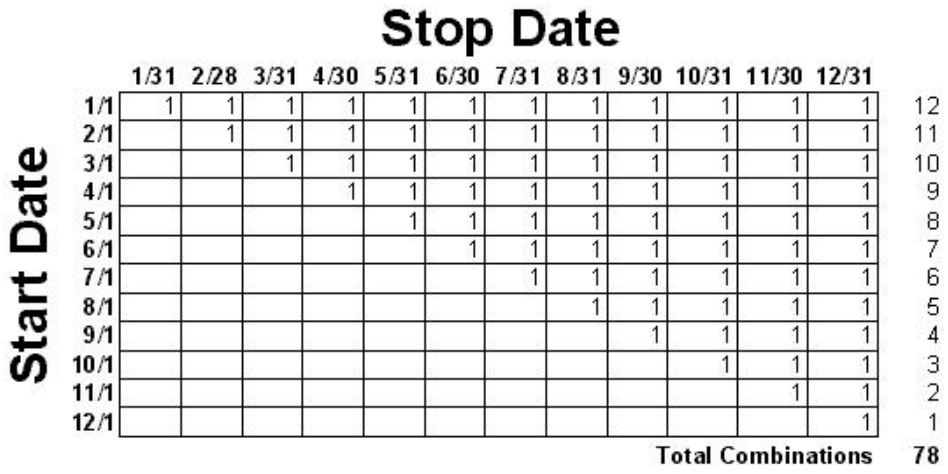
Example 1: If you are issuing memberships, where your customers typically renew their membership each month, then try to specify a start date that begins on the first day of each month and a stop date that ends on the last day of each month. In this case you only use 12 of the 500 unique access intervals (within a given 12 month period), as shown in the following chart.

Month	Start Date	Stop Date
January	1/1	1/31
February	2/1	2/28
March	3/1	3/31
April	4/1	4/30
May	5/1	5/31
June	6/1	6/30
July	7/1	7/31
August	8/1	8/31
September	9/1	9/30
October	10/1	10/31
November	11/1	11/30
December	12/1	12/31

Example 2: If you issue memberships quarterly (3 months at a time), then follow the same principal, where the start date is the first day of the month in each quarter and the stop date is the last day of the month in each quarter. in this case you only use 4 of the unique access intervals, as shown in the following chart.

Quarter	Start Date	Stop Date
Quarter 1	1/1	3/31
Quarter 2	4/1	6/30
Quarter 3	7/1	9/30
Quarter 4	10/1	12/31

Example 3: The following example shows how to issue memberships that allow any number of months. For this to work, you must always start on the first day of any month and stop on the last day any month. In this situation you only use 78 of the total 500 possible unique access intervals (within a 12 month period). The following chart shows all the possible start and stop dates in 12 month period. As you can see, they add up to 78 unique access intervals.



Copy Temp settings from another user

As mentioned in the previous sections, this option allows you copy the temporary settings of another user. When you click this button a list of all temporary users appears, showing the ***Expiration Type*** and the settings for each user. To select a user, simply double-click the user to copy the settings.

Temporary Users exported to controllers that do not support Temporary Users

If one or more of the controllers in your system does not support temporary users, it is still possible to export any temporary users to those controllers. This option is located in ***Tools > Options > General Options*** and is called ***Temporary Users will function in controllers that don't support Temporary Users***.

Checkbox Enabled (checked): Temporary users are exported to all controllers, in which case the temporary users do not expire, but can gain access and function indefinitely.

Checkbox Disabled (unchecked): Temporary users are exported to all controllers, but these users can not gain access. Any attempt to gain access with these users result in a log event of "User - Access Denied - Bad Time Zone."

6.9.1 User Import Wizard

The User List Import Wizard is a lot like the Add User Group function but with the added capability to import a user's First Name, Last Name, Keypad PIN, Card Number, and a Custom text field from a CSV file. This is useful if you have an existing list of names located in another system such as a Human Resources personnel file, and you wish to save time when adding a large group of users without having to type the names of each user that is added to the Hub Manager™ Professional database.

If the user names and data you have are in a third party database system such as a Human Resources database, then review the documentation or help file of that program for information referring to 'Exporting Data to a CSV file'.

This wizard will allow you to import up to 20,000 names from a CSV file.

Required CSV File Format

- The CSV name file that you are importing must be in the following format:
  Field 1: First Name
  Field 2: Last Name
  Field 3: Keypad PIN
  Field 4: Card Number programmed onto card
  Field 5: Visual ID (typically refers to the hot stamp number printed on an access card, but can be any text you want to import)
- The CSV file shouldn't have a header row.
- The CSV file shouldn't have any carriage returns.
- If a field such as "Keypad PIN" is being imported, then that field must be filled for each and every user being imported using the CSV file.
- Each field shouldn't be more than 30 characters long. If any field is more than 30 characters, that field will be truncated to the first 30 characters.
- Any apostrophes will be removed.
- Here is a sample of the required CSV file format:
  John,Smith,827163,23862,License Plate - LA-647
  Jim,Jones,291737,295,License Plate - 28W-E59

Recommended Preparation of the Hub Manager™ Professional database before CSV File Import

Although it is possible to import a name list of up to 20,000 and create these users without assigning them to an Access Level, it is highly recommended that you assign an Access Level to each of the users you are adding.

If you are importing 1000's of names and do not assign an access level, afterwards you will have to edit each of these users individually, requiring 1000's of keystrokes. But this may be the option you want if you prefer to bring in the entire list and then assign the Access

Level to the users.

The wizard will warn you to not create users without an Access Level assigned.

If you do not know for sure where each and every user will be granted access, you can always create an empty Access Level that has access to no doors assigned initially. You can then add the group of people that will most likely have the exact same access privileges, and modify the Access Levels privileges afterwards.

Try not to add groups of users larger than 1,998 in this manner (1,998 users + 1 Master Code + 1 Supervisor Code), since most controller's don't support more than that number of users.

Step 1 - Open CSV File

Step 1 of the wizard prompts you to specify the CSV file where the names are located.

1. Select the ***Open CSV File*** button and browse to where you have stored the CSV file containing the user names. If the list is Imported successfully you will receive a message 'File Read OK'.
2. Select ***Next*** to continue.

The import function will check for and announce to you any duplicate first and last name combinations within the CSV file as they are being imported.

Step 2 - Add Users

Step 2 is where the users are actually added to the database

You may select: a block of Users, individual Users one at a time, or all Users in the list. You may use any combination of these selection tools, you can deselect a user by removing the check in the checkbox next to the User name, or by clicking the 'Uncheck All' button and starting again.

Selecting a Block of Users by Selecting One from the List

To select a block of Users using the list, first select the User name at the top of the block to be selected, then hold down Shift and select the bottom User name of the block. This will select all User names in between the top and bottom User names you selected.

Selecting a Block of Users by Specifying the Number of Users to Select

To select a specified number of Users:

1. Select the starting user name anywhere in the list.
2. Enter the number of User names you want to select in the edit box labeled 'Select X Users' (where X is the number of Users you want to select).
3. Select the button labeled 'Select X Users'.

4. The Wizard will now select the X number of Users below the User you selected in Step 1.

This is useful if you have imported 1,000 names and you only want to select the first 300 names, or some subset of names in the middle of the list.

Selecting a Block of Names by Selecting the Individual Names

If you only have a small number of names to select, you can simply select the individual names from the list.

Assigning Card Data

During the add sequence you may either: auto generate and assign sequential card numbers or not assign card data at all. If there was data in the Card data field of the CSV file, then that data will be assigned to the user being added.

If you are using the Card data in the CSV file, then you must not specify a starting sequential card number.

Assigning Code PIN Data

During the add sequence you may either: auto generate and assign random 4, 5, or 6 digit PIN numbers or not assign PIN data at all. If there was data in the Keypad PIN data field of the CSV file, then that data will be assigned to the user being added.

Assigning Visual ID Data

If data is found in the Visual ID field of the CSV file then that data will be used during the import process. The Visual ID field is a custom text field and can be used for any data you may have, such as the Hot Stamp of the access card, license plate number, employee ID number, etc…

Card Formats

See Users for an explanation of the different card formats and card format options available.

Assigning Access Levels

Choose the Access Level you want to add the users to. You can also choose to not assign the users to an Access Level at this time.

NOTE: If you choose to not assign users to an Access Level, you will need to edit each user individually afterwards.

Adding Users

After you have specified the Card Format, Card data, PIN data, and the Access Level to be assigned to the selected users. Select the Add button to start adding these users to the system.

Before attempting to add any users, the wizard will analyze the selected Access Level to make sure you are not trying to exceed the capacity of any door assigned to that Access Level. For example: if you have an Access Level named "All Doors" that has access to a controller with a capacity of 2,000 users and 1,800 users are already assigned to this controller and you attempt to add 700 more users, you will get a warning that the capacity of this door has been exceeded by a certain number of users, in this case 500.

Cancel the addition, and go back and edit the list to remove those 500 people that do not need access to this particular door. You will have to decide which of these 700 users have the greatest priority on getting access to this door. If you require that ALL of the 700 people have access, you may be able to upgrade to a door controller that has a higher user capacity if one is available or you may have to exit the Wizard and go back into the main program and go to that door and select the 'Capacity' tab and see the breakdown of how users are assigned to this door, and make some changes.

Refer to the Doors section for details.

6.9.2 Add User Group

This feature allows you to add a **batch** of users with common traits and/or sequential card numbers.

1. Select the **Add Group** button on the Users screen. The Add Users Group screen displays.
2. Enter the information in the add group fields as required.
3. Select **Add** to save the user data to the user database. To cancel the addition of a group of Users, select the **Cancel** button.

NOTE: Before you can start adding new users, Hub Manager™ Professional requires that you edit the PIN of "Master User". This is done to reduce the chances that you unknowingly send the default Master Code of "1234" to the controllers.

Field/Button Description

Number of Users to Add

Specifies the number of users being added during this process.

Member of Time Mgt. Group

Lets you assign Time & Management status to this user.

Triggers 1st In Auto Unlock Time Zones

When this box is checked, the User can trigger a First-In Auto-Unlock time zone when they are granted access. See the Users section for more details.

Access Level

Specifies the access level for these users.

Generate Sequential Card

Checkbox that specifies that a card credential will be assigned to the users being added.

Card Format

Specifies the format of the cards you are adding.

First Sequential Card Number
Specifies the card number for the first sequential card being added for this group.

Site Code, Group Code, Corp Code
This is where you define the Site, Group, or Corporate code required by the HID prox cards you are adding sequentially, dependant upon which card format you have selected. You are required to know the exact site code of these cards you are adding in your access control system. If you do not know the site code, you may have to use the 'Enrollment Station' option and add these users one at a time using the standard Add User feature.

Generate Random PIN
Checkbox that specifies that a random PIN will be assigned to the users being added.

PIN Length
Specifies the length of the random PIN number.

NOTE: For more details on the fields above refer to the section that discusses Users.

6.10 Holidays

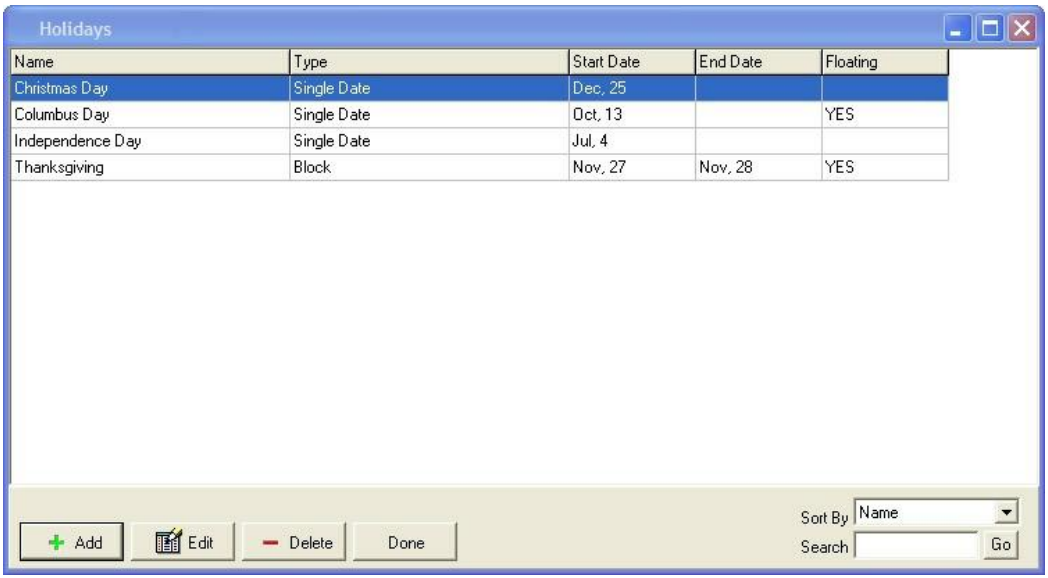
Holidays are used to determine when a user is allowed access. When you set up a Time Zone, you must specify whether or not the Time Zone applies to holidays. If a person normally has access from 9 AM to 5 PM, Monday through Friday, but Thursday is a holiday, do you still want the user to have access? If the facility is closed for the day, you may want to deny access to the majority of your users on that day. In this case, do not select the holiday check box in the Time Zone. You may still want some users, like managers, to have access on the holiday. In this case, select the holiday check box for the manager's Time Zone only. For more details about defining Time Zones refer to the Time Zones section.

A holiday is defined by specifying the month and day of the holiday. Holidays can be either a ***Single Date*** for holidays that are only a single day or ***Block*** holiday for multi-day events. When you set up your holidays you have to specify which type you want to use. The year is not included in your holiday definition, making the holiday year-independent, which means they only apply to the current year. Hub Manager™ Professional has the option of designating a holiday as a floating holiday for holidays that fall on a different date each year. Refer to the Floating Holiday Option below. You can define up to 16 ***Single Date*** holidays and/or 16 ***Block*** holidays.

All defined Single Date holidays are sent to all controllers in the system. All defined Block holidays are only sent to controllers in the system that support Block Holidays. Secured Series Controllers controllers do not support Block holidays. LS2\P, Max 3 v1, Max 3 v2,

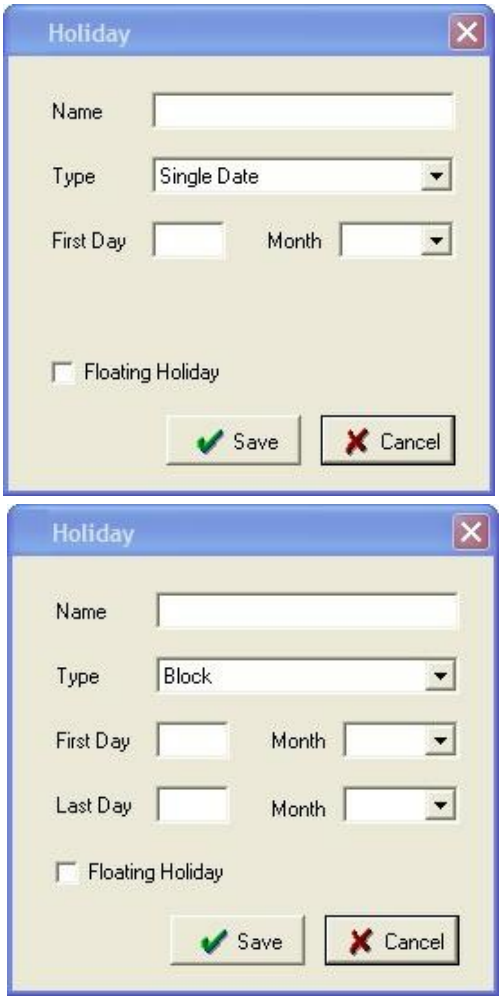
prox.pad plus IR and prox.pad plus controllers do support Block Holidays.

To use the Holidays option, select ***Database > Holidays*** to open the Holidays directory, shown below.



Adding a Holiday

1. Select the ***Add*** button on the ***Holidays*** directory to open the ***Holiday*** edit screen.



2. Enter the name of the holiday in the ***Name*** field.
3. Select the ***Type*** of holiday you want to create. You have two options here called ***Single Date*** or ***Block***. The ***Single Date*** option means your holiday is a single day event. Enter the day and month of the holiday. A ***Block*** holiday is a multi-day event, such as a school vacation. For this option, you must enter the first day and month of the holiday and the last day and month of the holiday. Since the year is not specified, the start date must precede the end date within a single calendar year.
4. If you are adding a floating holiday, check the ***Floating Holiday*** check box. Refer to the Floating Holiday Option below for details.
5. Select ***Save*** to save the holiday to the database.

Floating Holiday Option

A floating holiday is defined as a holiday that does not occur on a fixed date each year. For example, Columbus Day was on October 13, 2008, but in 2009 it occurs on October 12th. You must check this box for each holiday you want to define as a floating Holiday.

When this box is checked for any holiday, the software then knows the database contains at least one floating holiday. The first time the software is run in a new year the software displays a message that reminds you that the database contains a floating holiday. You should then review your holiday list and adjust any that occur on a new date. For quick reference, the ***Holiday*** directory has a column called ***Floating***. If a holiday is a floating holiday, then this column contains the word ***YES***. Once you've adjusted the dates for your floating holidays, you must export the data to your controllers. The warning message won't be displayed again, until the following year.

Chapter 7: Communications

7.1 Communications Menu

The ***Communications*** menu contains most of the options that allow you to send data to a controller or import data from a controller.

Select ***Communications*** from the main menu to display the drop-down menu, which contains the following items:

Import Door Settings
Import\Export Doors
Network Query
System Dashboard

7.2 Security Chip

The Security Chip is a small microchip that must be installed into the controller that has a Controller Address of 1 in Secured Series Controllers hardware networks so that exporting and/or importing from the PC software can be performed. Each separate network of Secured Series Controllers controllers must have a controller with an address of 1 and that controller must contain a security chip.

Those controller types that require a security chip are: HC500, Hub+\Max, Max 2 v1 and Max 2 v2.

7.3 Import Door Settings

The ***Import Door Settings*** feature imports and displays the complete user data and door settings of any physically connected (com port, modem, or TCP/IP) door controller to the Hub Manager™ Professional computer. This is useful if you need to retrieve the information stored in a door controller for troubleshooting or if you lose you database and you don't have the information stored anywhere else. You can then view, print or save this information to a space delimited text file. This imported information is stored separately from the central Hub Manager™ Professional databases in a text file and cannot directly overwrite any data in the Hub Manager™ Professional database. If you did lose your database, you would then need to re-enter your data.

NOTE: The Import Door Settings can not be performed on Handheld connected controllers.

1. First go to ***Database > Sites*** and select the site containing the door from which you want to retrieve data. Click the ***Connect*** button and exit the screen.
2. Then go to ***Communications > Import Door Settings*** from the Hub

Manager™ Professional main menu to access the ***Import Door Settings*** feature.
3. Select the door controller from the drop down list.
4. To begin the import, click the ***Start*** button.
5. When complete the data appears on the screen
6. You can now either print the data or save it to a file. To print the data to you printer select ***Print***. To save the data to a file select ***File***.
7. Now click the ***Print*** button. If you are printing it to hardcopy, then a standard printer dialog opens. If you are saving it to a file, then a standard save file dialog appears.
8. When finished, click the ***Cancel*** button to close the screen.

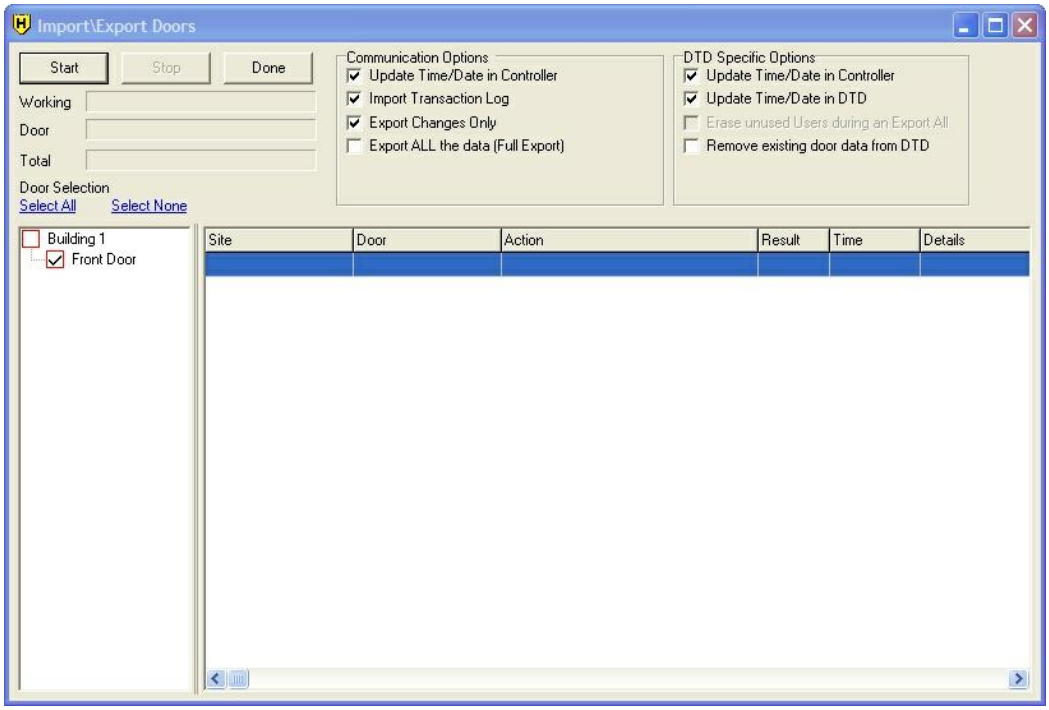
7.4 Import\Export Doors

The Import\Export Doors option on the Communications menu is where you send data to your door controllers and import the transaction logs. During the export process Hub Manager™ Professional automatically connects to each site and depending on the connection type, the software will attempt to communicate to your door controllers.

To import or export to your door controllers follow these steps:

1. Select ***Communications > Import\Export Doors*** from the main menu to open the ***Import/Export Doors*** screen.
2. When you first enter the screen any doors that are known by the database to contain changes will automatically have a checkmark next to the door name. If no doors are selected when this screen is opened, then this means that Hub Manager™ Professional believes that all changes were sent to the controllers in a previous export.
3. Make any additional door selections (if required).
4. Verify the correct ***Communications Options*** and ***DTD Specific Option*** (if you are using a DTD) are selected for the operation you are trying to perform.
5. Click the ***Start*** button to execute the communications process.

NOTE: For PDA connected sites, you must run HotSync after the import/export process is complete. This will move the data files from the PC to the PDA.



Field/Button Description

Working
This progress bar shows detailed progress for the current door.

Door
This progress bar shows the overall progress of the individual door currently being communicated with.

***Total* Progress bar**
This progress bar shows the total progress for all the selected doors.

Door Selection
To include a door in the import/export process, place a check mark next to a door name. If a door already has a check mark next to it when you enter this screen, it means that changes were made to the data contained in that door since the last export. For this reason, you usually don't need to select the doors you want to export to, since the program automatically select the doors for you. If there are additional doors you want to include in your export, select them and if there are doors that are already checked that you don't want to include, uncheck them.

Select All
Click this to select all the doors in the ***Door Selection*** list.

Select None
Click this to de-select all the doors in the ***Door Selection*** list.

Start\Stop
These buttons start or stop the import/export process. After selecting ***Start***, only the ***Stop*** button is available until the Import\Export process is complete.

Done
This button closes the ***Import\Export Doors*** screen and returns you to the main screen.

Communication Options

Update Time/Date in Controller **Checkbox**
If this option is enabled, then the current time and date of the PC is sent to your door controllers when you you start the import/export process. This option does not apply to PDA connected controller, since PDA is responsible for updating the controller's time and date. To update the time and date with DTD, you must select that option under the ***DTD Specific Options*** (see below).

> **NOTE:** If your door controller does not support the 2007 DST date format, then you must perform this operation when daylight saving time occurs in both the spring and fall via the controller's keypad. You must also remember to disable the Daylight Saving Time option in the door options screen, so the time doesn't automatically change on the wrong date.

Import Transaction Log
If this option is enabled, then the transaction log of the selected door controllers is imported and placed into the Hub Manager™ Professional database.

> **NOTE:** It is recommended that you select one of the export options when performing an 'Import Transaction Log' from a DTD. This ensures that the PC and DTD are properly synchronized.

Export Changes Only
If this option is enabled, then only the changes since the last successful export are sent to the selected door controllers. Using this option results in a faster export time.

Export ALL the data (Full Export)
Enabling this option results in the longest possible export time, but this

guarantees that all data in the door controller is overwritten and matches the data in the software exactly. This option is recommended for new door controllers, if you replace or re-locate a door controller, or if you erase (default) the memory of an existing door controller.

DTD Specific Options

Update Time/Date in Controller

If this option is enabled, then the current time and date of the DTD is sent the next time you visit the selected controllers with the DTD.

> **NOTE:** If your door controller does not support the 2007 DST date format, then you must perform this operation when daylight saving time occurs in both the spring and fall via the controller's keypad. You must also remember to disable the Daylight Saving Time option in the door options screen, so the time doesn't automatically change on the wrong date.

Update Time/Date in DTD

This option synchronizes the real time clock in the DTD with the current clock of the PC.

Erase unused Users during an Export All

This option is enabled only after the ***Export All the data (Full Export)*** option is enabled. Enabling this option results in a longer export time between the PC and DTD (no more than 49 seconds per door) and between the DTD and the controller (no more than 127 seconds per door), but also results in a highly secure system. Enabling this option guarantees that any hidden codes or cards in the controller, that the PC's database does not know about, are deleted. These hidden codes or cards may have been manually programmed at the controller itself, or via another DTD or could be previous data that was in the controller prior to installing it. Disabling this option means that it is possible for a hidden code or card to exist in the controller without you realizing it.

You should enable this option the first time you export to a door controller or any time you receive a message warning you about a potential security risk due to the ***Program Mode Entered*** flag in the controller. Any door you add to the system will display a security risk warning message until you perform a full export to the controller with this option enabled.

Remove existing door data from DTD

Enabling this option erases existing data that is on the DTD prior to an Import or Export operation and ensures that you have enough space for the selected doors, by deleting any other doors that are already on the DTD but aren't part of the current export process. The additional time it takes to perform this erase operation

is relative to the amount of door data files currently on the DTD but it takes approximately 1 second to delete each data file on the DTD. The erase operation only applies to door export data. Any transaction log import data that is currently on the DTD is not removed.

This option only removes existing doors from sites that have at least one door selected in the ***Door Selection*** list at the time you perform the import/export. Enabling this option does not delete doors from the DTD that are part of other sites.

You would typically only use this option if you have more doors in your system than the DTD can hold.

If you wish to completely erase the DTD's memory, go to the DTD Site Settings screen and use the button labeled ***Erase DTD Memory***.

7.5 Network Query

The Network Query feature is used to scan (or poll) each door address of the currently connected site and display the online\offline status of each controller. Once the process is started, the program searches the network of controllers for each door address starting at door 1. You can use this feature to test communications to each controller in your system when you first set up a system or if you need to troubleshoot communications issues.

Network Query Process

NOTE: You cannot use the Network Query feature for Handheld connected controllers.

1. Prior to using the ***Network Query*** feature, all your door controllers must be physically connected and each must be addressed with a unique door address.
2. After you've opened Hub Manager™ Professional, go to ***Database > Sites*** to open the ***Sites*** directory.
3. Select the site you want to query and click the ***Connect*** button. Click the ***Done*** button to exit the screen.
4. Select ***Communications > Network Query*** from the main menu to display the Network Query screen.
5. Place a check mark in the ***Add new found doors*** box. This box tells the software to automatically add each new unknown door it detects during the query process. Each time the software finds a new door controller, it prompts you with a door settings screen to confirm the name and door settings before adding it to the database. If you've already added all your doors to the database or if you are troubleshooting a previously working system, then you do not need to use this option.
6. Press ***Start*** to begin the network query.

7. The program then polls each door address for the site, starting at address 1. Each controller's network status starts with a blue question mark next to each door location, which indicates the software hasn't attempted to query that controller yet. As the operation continues and each door controller location is polled, the fields (described below) are populated as each door is found.

NOTE: If you want to query just a single door, go ***Database > Doors***, open that door for editing and select the ***Query Now*** button.

Field/Button Description

Current Site
This field identifies the current site you are connected to and are attempting to query.

Add new found doors
This box tells the software to automatically add each new unknown door it detects during the query process. Each time the software finds a new door controller, it prompts you with a door settings screen to confirm the name and door settings before adding it to the database.

Start\Stop
These buttons start and stop the network query process.

Done
The ***Done*** button closes the Network Query screen and returns to the main screen.

Found
When the Network Query finds a door controller, it fills in this field with what it found.

Name
This is the name of your door controller.

Expected
This field contains the controller type the Network Query expects to find. It uses the controller type you selected when you added the door.

Description of Network Query Icons

Black Check Mark
A black check mark indicates the query found a door controller.

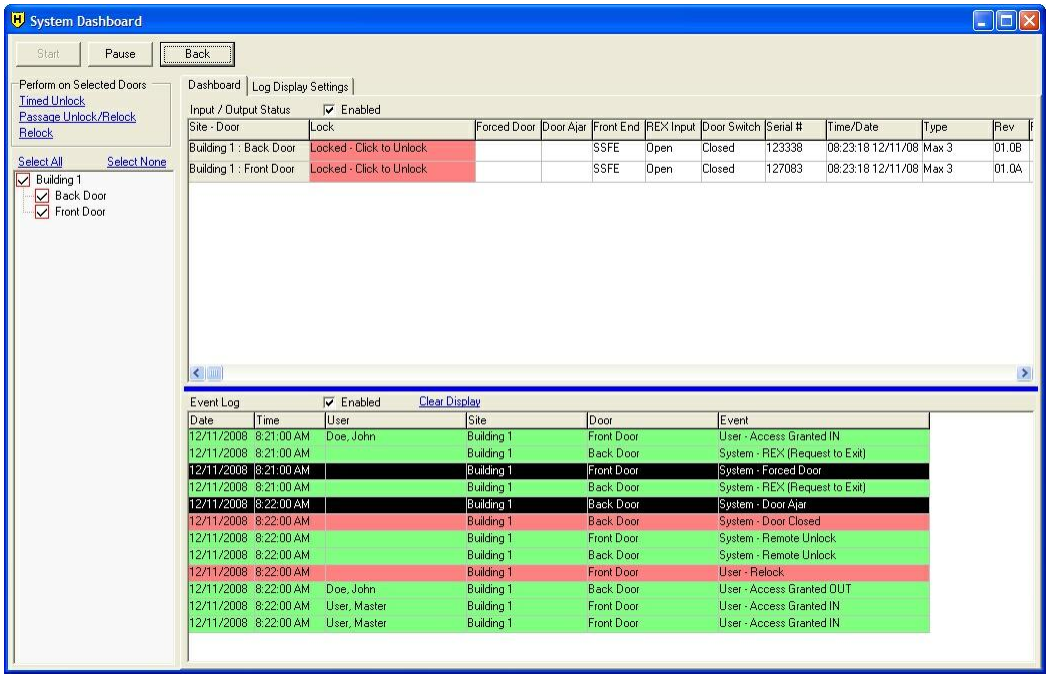
Red "X"
A red "X" means the query did not find a door controller with that door address.

Blue Question Mark
A blue question mark indicates the software hasn't attempted to query that door address yet.

7.6 System Dashboard

The ***System Dashboard*** option, on the ***Communications*** menu, shows the live door status for each Max 3 v1 and Max 3 v2 door you select on this screen. Currently, these are the only two controllers that support this feature, so any other controller types in the system are not shown on this screen. The top portion of the screen shows status of the relays, inputs, and time and date. The lower portion shows live updates of events occurring at the door. The dashboard polls (or retrieves data) each door one at a time for status and updates the screen as quickly as possible. Keep in mind, if you have a large number of doors there can be a slight delay before each door is updated. In addition to door status, you can unlock the door remotely using the ***Timed Unlock*** and ***Passage Unlock*** (toggle) features. You can also relock the door using the ***Relock*** feature.

To access ***System Dashboard*** select ***Communications > System Dashboard*** from the main menu. Only Max 3 v1 and Max 3 v2 controller types will appear. By default, all controllers are selected and status monitoring and event log retrieval begins automatically when the screen opens. If you don't want to see status for every door, just de-select the doors you don't want to see. After you've finished your selection, you must press the ***Start*** button again.



Dashboard Field/Button Descriptions

Start

By default, the ***Start*** button is already selected when you enter the screen. There are only two reasons live monitoring will stop and require you to click the ***Start*** button:

- If at any point you de-select or select a door, live monitoring stops.
- When you click the ***Pause*** button, live monitoring stops.

Pause

The ***Pause*** button suspends the live monitoring process. The ***Input/Output Status*** and ***Event Log*** monitoring will not update while the dashboard is paused. To re-start the process you must click the ***Start*** button.

Back

Clicking the ***Back*** button exits System Dashboard and returns you to the main screen.

Timed Unlock

When you select this option the selected doors unlock for the specified time duration set for each individual door, which is defined in the door settings screen. It operates the same as a standard user. This feature is temporarily disabled while System Dashboard is paused. If System Dashboard is paused, clicking ***Timed Unlock*** will

automatically start updating data again.

NOTE: If the ***First-In Auto-Unlock*** option is enabled in a door controller when you use the Timed Unlock feature, the door will go into Auto-Unlock mode, which unlocks the door for the duration of the Auto-Unlock Time Zone.

Passage Unlock
Use this option to permanently change the state of the lock relay for all the selected doors. It operates the same as a passage (aka toggle) user. If the door is locked, it will unlock and remain unlocked and if it's already unlocked due to passage mode, it will relock the door. To relock a door in passage mode, you can also use the ***Relock*** function. This feature is temporarily disabled while System Dashboard is paused.

Relock
Selecting this option locks the selected doors, regardless of why those doors are unlocked. This is useful if you need to lock down your entire system for an emergency. This option has no effect on doors that are already locked. This feature is temporarily disabled while System Dashboard is paused.

Input/Output Status Enabled
You can disable this option (uncheck the box) so System Dashboard does not retrieve door status updates. You would disable the option if you only wanted to retrieve event log updates. An additional benefit is that the log events are retrieved much faster, since it's only getting log data.

Event Log Enabled
You can disable this option (uncheck the box) so System Dashboard does not retrieve log event data. You would disable the option if you only wanted to retrieve input/output door status. An additional benefit is that the status is retrieved much faster, since it's not getting log data. The log events are still in the controller, they are just not displayed here. You can retrieve them later by either enabling this option or importing them using the import/export feature.

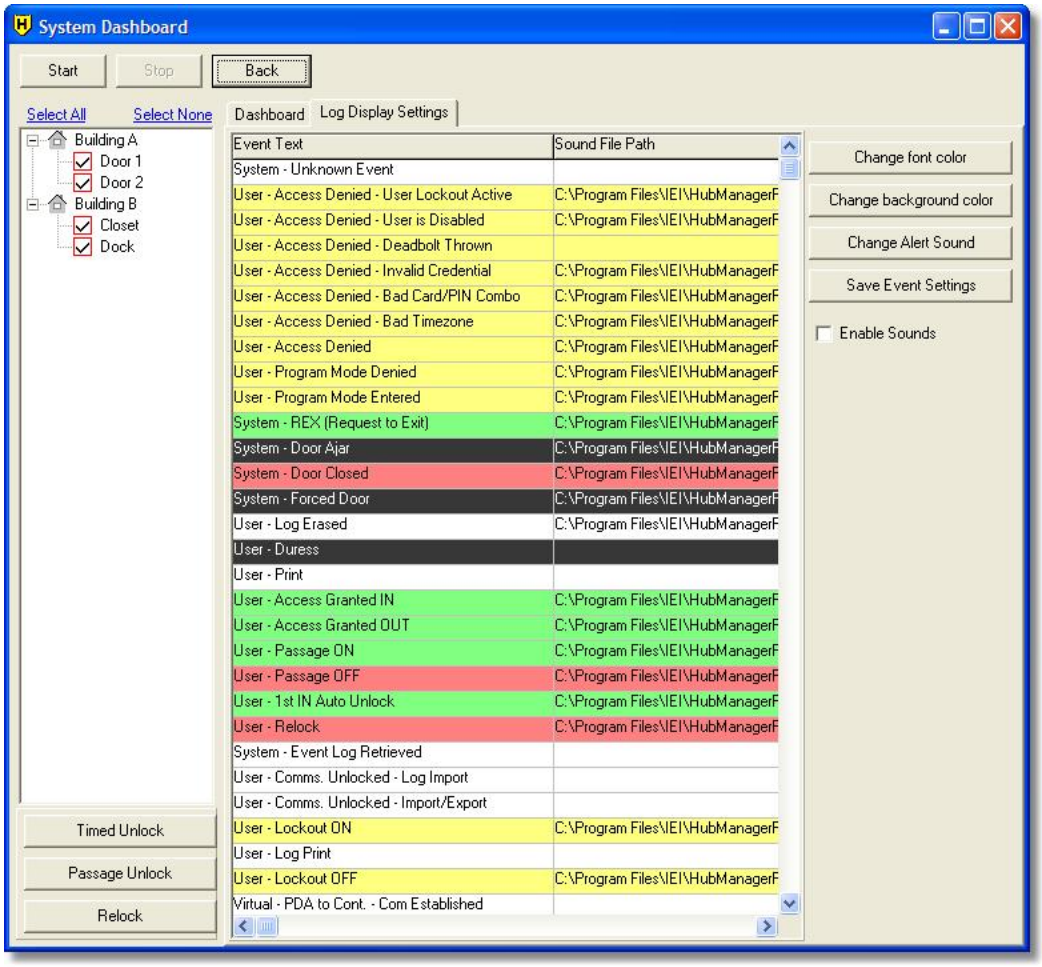
Clear Display
Selecting this option simply clears all the log events from the Event Log grid. It does not affect the events that are stored in the database.

Log Display Settings Field/Button Descriptions

The Log Display Settings tab allows you to customize what happens when specific Log Events occur on one of the selected doors. You can customize the font color, background color and alert sound. The most common events are pre-configured with color and sound.

By default:

- Yellow events are minor warnings
- Black events are actions that should be responded to
- Green events are actions that unlocked the door
- Red events are actions that locked the door



Change Font Color

This button allows you to change the font color of the ***Event Text***. First select the event you want to change, then click the ***Change font color*** button. The standard color picker appears. Choose the color you want, then click ***OK***.

Change Background Color

This button allows you to change the background color of the ***Event Text***. First select the event you want to change, then click the ***Change background color*** button. The standard color picker appears. Choose the color you want, then click ***OK***.

Change Alert Sound

This option allows you to specify the sound file that is played when each specific event is displayed in the Event Log. Only WAV sound files are supported. To have no sound play, simply select and delete the text in the ***Sound File Path*** column next to that specific event.

Save Event Settings

You must select this button to save any changes you make to the color or sound settings.

Enable Sounds

If this option is enabled, an associated sound file is played when each event type occurs. If enabled, the default sound is the spoken event text. To change the sound that plays when an event occurs, select the event, then select the ***Change Alert Sound*** button. A standard "Browse to File" option appears. Only WAV sound files are supported. Enabling sounds may slow down how fast events are displayed in the dashboard, since the sound file must be played before another event is displayed. This option should be disabled if you want the fastest possible Event Log update.

Chapter 8: Tools

8.1 Tools Menu

The ***Tools*** drop-down menu contains the following items.

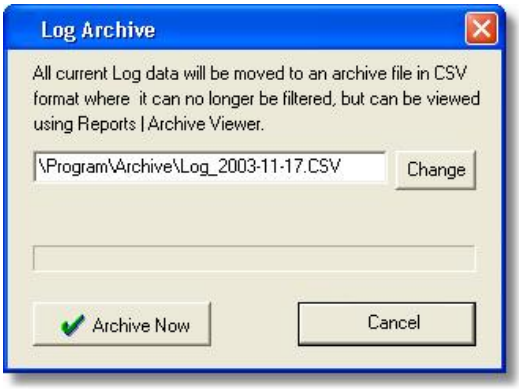
Log Archiving
Audit Archiving
Database Backup/Restore
Database Conversion Utility
Run Com Port Test
Scheduled Log Import
Table Initialization
Indexing
Application Initialization
Options

8.2 Log Archiving

The ***Log Archiving*** feature is used to backup your log event data to an archive folder. It removes the data from your working database and saves it to a CSV file to a location of your choice. You should only use this feature if you no longer want to view the data within the Hub Manager™ Professional reports or if you would rather view the data in a CSV file.

Log Archives can only be viewed later within Hub Manager™ Professional using the ***Reports > Archive Viewer*** tool, but you can no longer use any of the filtering features available within Hub Manager™ Professional.

1. Select ***Tools > Log Archiving*** from the Hub Manager™ Professional main menu to access the ***Log Archiving*** feature.



2. By default, the file is saved to the archive folder in the Hub Manager™ Professional folder structure and is named ***LOG_YEAR-MONTH-DAY.CSV***. If you want to put the file in a different location or you want to change the file name, click the ***Change*** button.
3. Click the ***Archive Now*** button. When complete, a message pops up confirming the operation. When you click ***OK***, you are returned the main screen.

8.3 Audit Archiving

The ***Audit Archiving*** feature is used to backup your audit data, which is a log of all the activity perform by operators within Hub Manager™ Professional, to an archive folder. It removes the data from your working database and saves it to a CSV file to a location of your choice. You should only use this feature if you no longer want to view the data within the Hub Manager™ Professional reports or if you would rather view the data in a CSV file.

Audit Archives can only be viewed later within Hub Manager™ Professional using the ***Reports >*** ***Archive Viewer*** tool.

1. Select ***Tools > Audit Archiving*** from the Hub Manager™ Professional main menu to access the Audit ***Archiving*** feature.

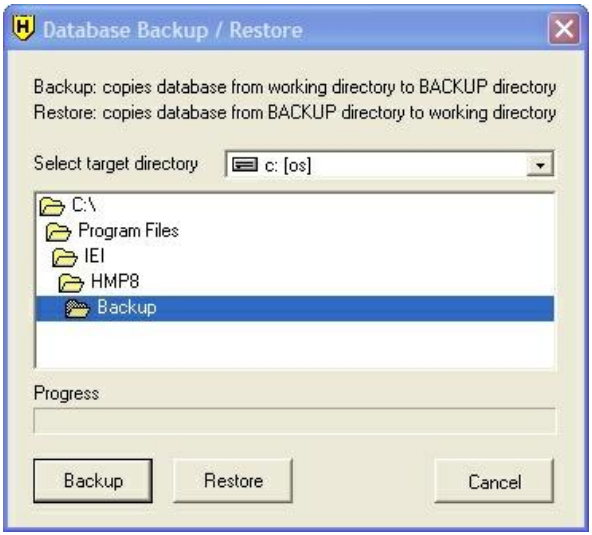
2. By default, the file is saved to the archive folder in the Hub Manager™ Professional folder structure and is named ***Audit_YEAR-MONTH-DAY.CSV.*** If you want to put the file in a different location or you want to change the file name, click the ***Change*** button.
3. Click the ***Archive Now*** button. When complete, a message pops up confirming the operation. When you click ***OK***, you are returned the main screen.

8.4 Database Backup/Restore

Backup Database

The Database Backup option makes a backup (copy) of the Hub Manager™ Professional database and places it in the specified folder.

1. Select ***Tools > Database Backup/Restore*** from the Hub Manager™ Professional main menu to access the Database Backup/Restore option. The Database Backup/Restore screen displays.
2. By default, the backup is stored in the Backup folder in the Hub Manager™ Professional folder structure, but you can store it any place you like.
3. Select the ***Backup*** button to begin the backup procedure.
4. A new folder is created in the selected backup location and that is where the database backup is placed. The name of this new folder has the current date/ time stamp in the following format. Year, Month, Day, Hour, Minute, Second (sometimes noted as YYYY-MM-DD-HH-NN-SS). This method allows you to easily identify when a specific backup was created and also enforces not overwriting an existing backup.



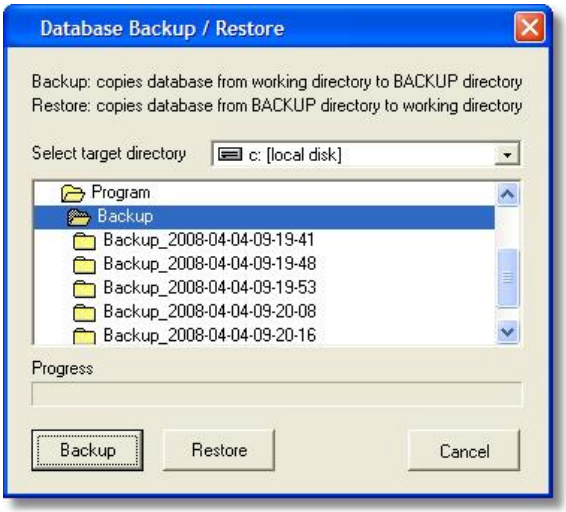
Restore Database

The Database Restore option lets you restore from a specific backup of a Hub Manager™ Professional database.

WARNING: The Restore procedure will erase any data currently in the Hub Manager™ Professional database.

1. Select ***Tools > Database Backup/Restore*** from the Hub Manager™ Professional main menu to access the Database Backup/Restore option. The Database Backup/Restore screen displays.
2. Browse to the folder that contains the backup of the database you want to restore from. If you have created multiple backups, then you may need to scroll to the folder that has the date/time stamp of the day you created the backup, in the following format: Year, Month, Day, Hour, Minute, Second (sometimes noted as YYYY-MM-DD-HH-NN-SS). The folder with the most current date/time stamp is located at the bottom since that is how Microsoft Windows numerically sorts file and folder names.
3. Select the ***Restore*** button to begin the restore procedure from the selected folder.

NOTE: If you attempt to restore from a database backup that was created with a previous major version of Hub Manager™ Professional, the software instructs you to instead use the Database Conversion Utility.

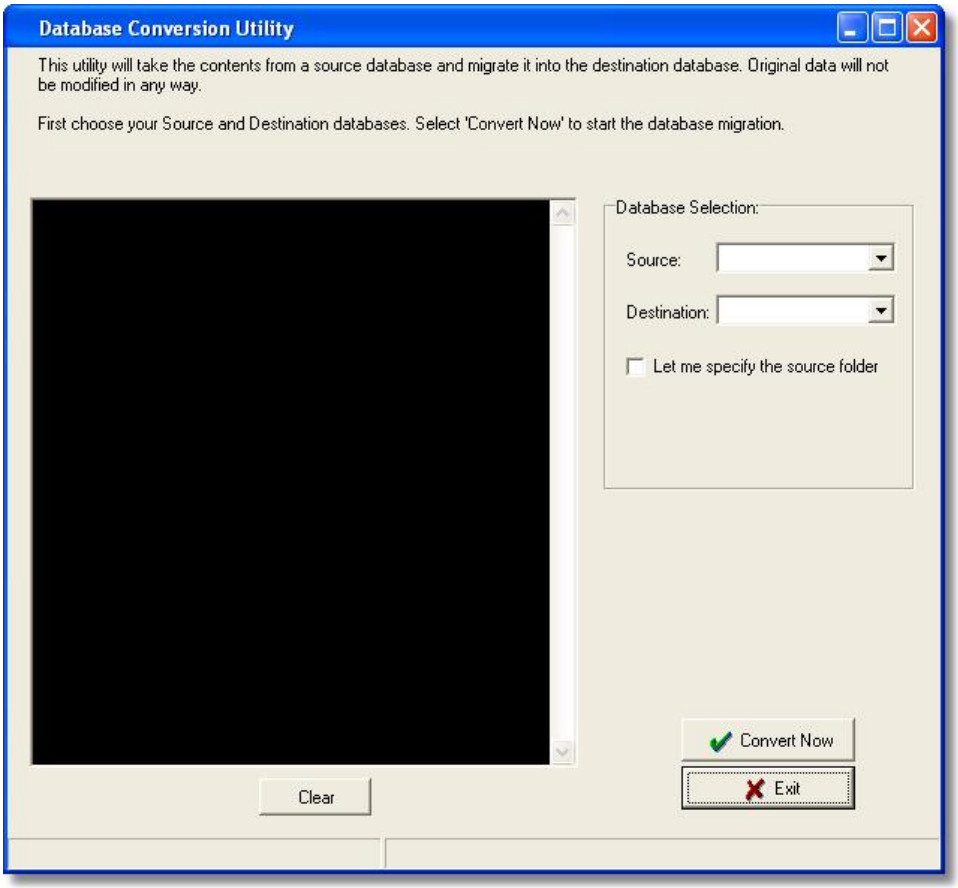


8.5 Database Conversion Utility

WARNING: Performing this data migration function will overwrite any existing data you may have stored in Hub Manager™ Professional. If you have any data in Hub Manager™ Professional that you need to save, perform the Backup function under the Tools menu, and select a folder that is outside the Hub Manager™ Professional folder structure.

This utility is provided to allow you to migrate a prior version of Hub Manager™ Professional v1, v2, v3, v4, v5, v6, or v7 database into Hub Manager™ Professional v8.

1. Launch the utility by going to ***Tools > Database Conversion Utility***.
2. The Database Conversion Utility screen appears (see image below).



3. Specify version you are converting from in the ***Source*** drop down list.
4. Specify the new version of Hub Manager™ Professional you are converting to in the ***Destination*** drop down list.
5. The source data is not modified in any way; it is merely copied and re-formatted appropriately into the destination database.
6. At the end of the data conversion, open the new version of Hub Manager™ Professional and go to ***Database > Import\Export Doors***. Before doing anything, make sure the ***Export ALL the data (Full Export)*** option is enabled and disable (uncheck) the ***Import Transaction Log*** option. You must also verify all the doors in your system are selected.
7. Now click the ***Start*** button to export to you door controllers. This ensures that you database is fully synchronized with your hardware.
8. When complete you can import the transaction log.

Converting a Database from a Custom Folder

There is also an option to let you browse to a custom source folder and convert that database into the destination database. This is useful if you are installing Hub Manager™ Professional v8 on a new PC and you want to migrate data from a previous version that is located on a different PC. Refer to the Upgrading section for additional details about transferring data between two PC's.

1. Select the Source database version from the ***Source*** drop down list.
2. Select Hub Manager™ Professional version 8 in the ***Destination*** selection.
3. Enable the check box labeled ***Let me specify the source folder***.
4. Click the ***Browse to Database*** button.
5. When browse dialog box appears, locate the folder you copied the database to. Once you've located the database, select it, then click the ***Convert Now*** button.
6. When complete click the ***Exit*** button.

Converting a data when you are using System Manager

If you used System Manager to create multiple systems, then you must follow these instructions in order to convert the databases of those Systems.

1. Launch Hub Manager™ Professional v8 and use System Manager to create one NEW System for each of the prior version Systems you want to convert. These new systems can be created in the same System Repository folder you used in the previous version of software, but you will need to assign a unique name for each of the new systems you create. Placing a "v8" at the end of the new System name will help you to identify between the old and new systems more easily.
2. Launch the prior version of Hub Manager™ Professional.
3. Launch Hub Manager™ Professional v8.
4. In the prior version of software use System Manager to open one of the OLD systems that you want to convert from.
5. In Hub Manager™ Professional v8 use System Manager to open one of the NEW systems you want to convert the old data into.
6. In Hub Manager™ Professional v8 launch the conversion utility by going to ***Tools > Database Conversion Utility***.
7. Select the prior database version in the ***Source*** drop down list.
8. Select Hub Manager™ Professional v8 as the ***Destination*** database.
9. Select ***Convert Now***. This will convert the database from the old system into the new system.
10. Go to System Manager in both the prior software and in Hub Manager™ Professional v8 and close the open system.
11. Repeat Steps 4-10 as needed.

8.6 Run COM Port Test

NOTE: If you are using Handheld connected controllers, it is not necessary to perform the COM Port Test, but you could follow steps 1 - 3 below to determine if the COM port assigned to the Handheld device exists or is already in use.

About the COM Port Test Program

This program tests the availability of your computer's COM ports 1 - 12, and also determines if these ports can be used for communications via the supplied connectors.

Running the COM Port Test

This program tests the availability of your computer's COM ports (serial communications ports), and also determines if these ports can be used for communications via the supplied connectors. IEI recommends that you run this program; it can also be selected and run separately. There are two parts to this procedure (testing without the loopback connector and testing with it), and both parts must be performed.

1. Start the COM Test program in one of two ways: (a) **Start > Programs > Hub Manager™ Professional v8 > Com Port Test**, or (b) from the Hub Manager™ Professional v8 Main Menu, ***Tools > Run COM Port Test*** to open the COM Port Test screen.
2. Click the ***Start Test*** button. This message then displays: ***Please make sure the loopback connector is NOT installed and select OK to continue or CANCEL to stop testing***.
3. Ensure that the supplied loopback connector is not connected to any of the COM ports on your computer. Then click ***OK***. The program conducts the first part of the COM test by looking for all available COM ports. The COM ports and the current status of each port is displayed on the screen and the following message appears: ***Please connect the loopback connector to your computer's COM port. Click OK to continue***.
4. Now connect the loopback connector to your computer's COM port (the loopback connector has both a female DB9-pin and DB25 connector; connect to your PC using the appropriate side) , then select ***OK*** to continue or ***Cancel*** to stop testing.
5. If the COM port test is successful, the following message appears: ***The test connector has been found at COM Port: x. Please record this information and select the same COM port for use in your program***.
6. If the test is not successful, there could be one of several problems: no COM ports are available, available COM ports are being shared with other devices or any available COM ports are not working correctly. Contact your computer dealer as you may need to add another COM port.
7. Record the COM port information safely as instructed and then select ***OK***.
8. Review the COM Port Test Results screen, then select ***Close***.

Running the COM Port Test using the IEI RS-232 to RS-485 Converter or the IEI USB to Serial Converter

You can also perform the loopback test using the IEI RS-232 to RS-485 converter and the IEI USB to Serial converter.

If you are using the IEI RS-232 to RS-485 converter:

1. Connect the converter to the PC COM port using the 6-foot cord and DB25 or DB9 connector. Do not power up the converter.
2. Follow the steps in the procedure above.
3. When you reach step 4 in the procedure above place the jumper J2 on the converter on both pins, then continue with remainder of the procedure.

If you are using the IEI RS-232 to RS-485 converter:

1. Connect the converter to the PC USB port using the 6 USB cable. Plug the 5-conductor wire harness into the converter.
2. Follow the steps in the procedure above.
3. When you reach step 4 in the procedure short the blue and green wire on the wire harness together, then continue with remainder of the procedure.

8.7 Scheduled Log Import

The Scheduled Log Import option lets you specify the time of day the import will be performed, the number of days between the automatic imports, and start date parameters. The automatic importing of the Transaction Log data will be performed on all door controllers in all sites.

NOTE: You must log out from but NOT exit the Hub Manager™ Professional program for the automatic importing of transaction logs to occur. If an operator is logged in when the scheduled import is set to start, then a prompt displays asking the Operator if the import should be performed. The Operator must select YES for the import to be performed, otherwise the import will not start.

NOTE: The delay period is how many days you want to lapse before another scheduled log import will occur.

NOTE: With Handheld connected controllers such as the LS2\P and prox.pad plus IR, the Scheduled Log Import feature will simply attempt to import any new Transaction Log data that may have already been placed onto the PC during a HotSync with a PDA running LS Link. This can be helpful if you have a person, such as a tour guard, that is responsible for regularly visiting the door controllers with the PDA and collecting the Transaction Logs, and only HotSync's the PDA with the managers PC and leaves. With Scheduled Log Import enabled, Hub Manager™ Professional will

automatically import those new transaction events into the database, without the need for the manager to remember to perform that action before generating a Transaction Log report. This helps keep newly generated reports, that the manager creates, as up to date as possible.

1. Select ***Tools > Scheduled Log Import*** from the Hub Manager™ Professional main menu to access the Scheduled Log Import program. The Scheduled Log Import screen displays.
2. Enable the ***Use scheduled log import*** checkbox to enable this feature.
3. Enter the desired parameters and select the ***OK*** button.

See also : Logout, Scheduled Log Import Errors, Scheduled Log Import Reminder

8.8 Scheduled Log Import Reminder

See also Scheduled Log Import

If you are logged into Hub Manager™ Professional when the Scheduled Log Import is set to run automatically, a message box will appear asking you if you want to run the import now.

If you had intended for the scheduled log import to run automatically without any user intervention, you must log out of Hub Manager™ Professional using ***System > Logout***.

Forcing you to logout is done as a safety precaution so that the software can be left running and set to import logs automatically, but not be left in a vulnerable "logged in" state where someone may be able to see sensitive information such as access codes.

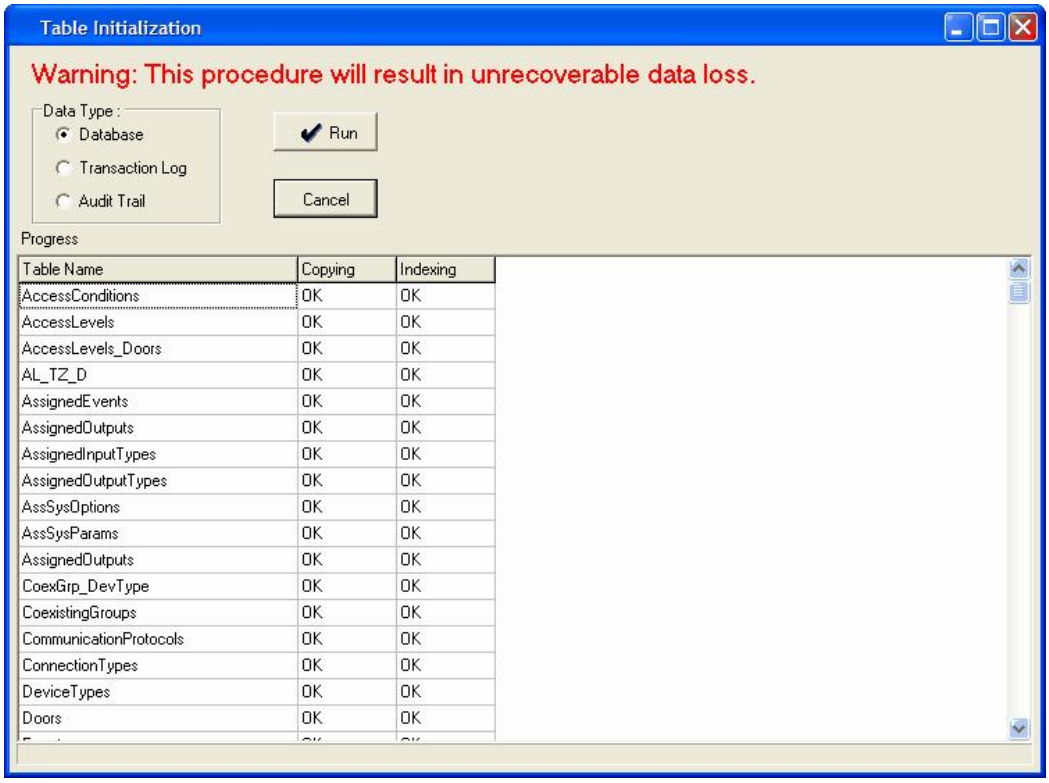
8.9 Table Initialization

WARNING: THIS PROCEDURE RESULTS IN UNRECOVERABLE DATA LOSS!!!

The Table Initialization option erases all the existing data from the Hub Manager™ Professional program's databases. You can select from several types of initialization:

Database - all operator entered data, including all users and door settings
Transaction Log - just the transaction log data
Audit Trail - just the operator audit trail

1. Select ***Tools > Table Initialization*** from the Hub Manager™ Professional main menu to access the Table Initialization program.



2. Select the type of initialization desired,
   - ***Database*** - Erases all data in all tables, excluding the Transaction Log and Audit Trail
   - ***Transaction Log*** - Erases just the Transaction Log table
   - ***Audit Trail*** - Erases just the Audit Trail
3. Select the ***Run*** button. A confirmation prompt displays.
4. Select ***Yes*** or ***No*** to reply as appropriate. If you select ***Yes***, the program performs the specified database initialization, displaying the results under the Copying and Indexing columns as shown in the previous example.

8.10 Application Initialization

The Application Initialization option defaults the program's parameters back to an "Out of Box" state. Using this option in conjunction with the "Total Database Initialization mode returns all databases and programs settings to the default "out-of-box" settings. It would be the equivalent of deleting all databases and reinstalling the Hub Manager™ Professional software.

The parameters and settings that are reset include, but are not limited to:

- disables System Manager and associated settings.
- defaults the Report Writer path, password, and options.
- disables Auto Login.
- removes custom support contact info.
- removes the default card format setting.
- removes all memory of custom screen size and position of the screens opened in Hub Manager™ Professional.

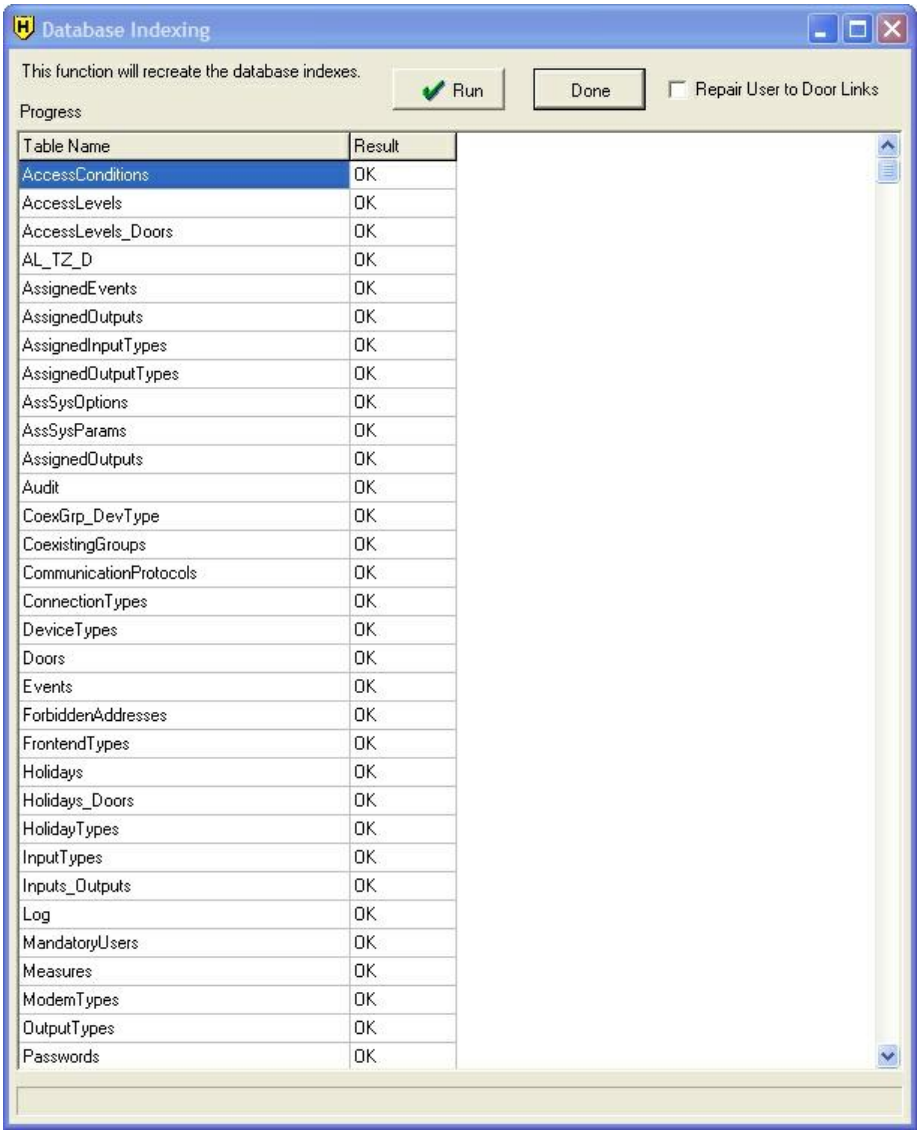
1. Select ***Tools > Application Initialization*** from the Hub Manager™ Professional main menu to access the Application Initialization program. A confirmation prompt displays.
2. Select ***OK*** or ***Cancel*** to reply as appropriate. If you select ***OK***, the program resets all application settings to the default values and then displays a prompt at the end (not shown).
3. Select ***OK***.

8.11 Indexing

The Indexing option indexes the Hub Manager™ Professional program's databases. Indexing reorganizes all the records in each database so that user access is faster and more efficient. Running this option is not usually necessary. No data is modified during this process.

1. Select ***Tools > Indexing*** from the main menu to access the Indexing feature and display the Indexing screen.
2. Select the ***Run*** button to continue indexing. Once you click ***Run***, the program performs the indexing procedure and a confirmation prompt displays when the process is complete. The results of the indexing process is displayed under the ***Results*** column.
3. Select the ***Done*** button to return to the main menu.

NOTE: If you ever receive an Indexing error within Hub Manager™ Professional, perform the Indexing option to resolve the issue.



Repair Users to Door Links Option

This option is used to repair reporting issues with users and doors. If you see users assigned to doors in your ***Assignment Reports***, but they do not appear as part of the same doors in the doors database report, the you know you have a database issue. In this case, check the box next to ***Repair User to Door Links*** option and click ***Run***. The indexing process will then repair this issue.

8.12 Options

Report Writer

These options relate to the creation of the Report Writer database.

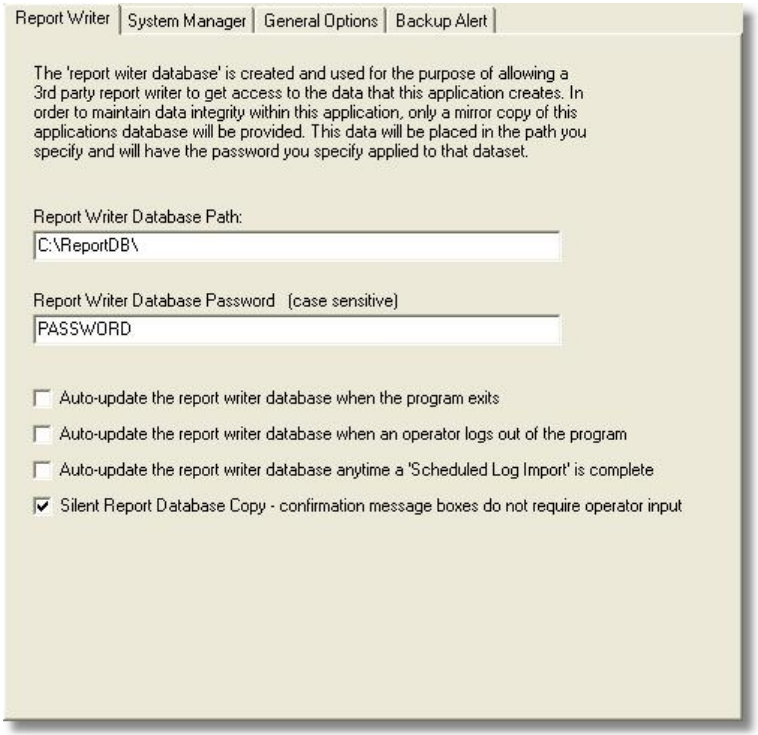
The 'Report Writer Database Copy' feature creates an exact copy of the current database that Hub Manager™ Professional is working from. The copy is made in order to allow a 3rd party report writing program such as Crystal Reports to access the data for the purpose of creating custom reports. This allows the Hub Manager™ Professional database to maintain data integrity, by not allowing access to the actual data, and at the same time, give the data to an outside source.

Report Writer Database Path
This is where the database copy will be stored.

Report Writer Database Password
This is the password that will be required to open the database copy within the 3rd party report writer.

Auto-Update Options
Specifies when the database copy will be updated. Selecting all 3 will keep the database copy up to date.

Silent Report Database Copy
Enabling this option stops any messages from prompting the operator to select OK or Cancel to the copying procedure.



System Manager

See section System Manager for a detailed description of the System Manager options

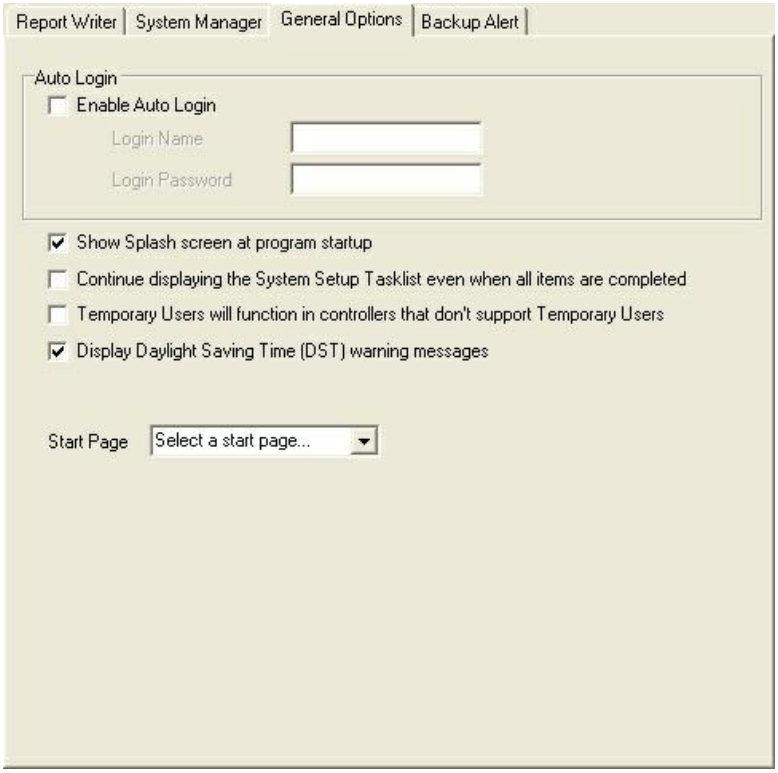
Backup Alert

The Backup Alert is a feature that will prompt you to perform a backup of the data if you have not performed a backup in the time period that you specify. The backup alert will occur at the time you log into a system. If on a given day, you choose to decline backing up, you will not receive any more prompts that day, but you will receive the backup alert prompt each time you log into that particular system on each subsequent day until a backup is performed.

The delay period can be set from 1 - 365 days.

General Options

The ***General Options*** tab contains several options. Below the screenshot is a detailed explanation of each option.



Auto Login

Enabling this option will cause the program to automatically attempt to log you in using a name and password you specify, whenever the login is displayed.

NOTE: This option should only be used if you are not worried that an unauthorized person will sit at your computer and attempt to access the Hub Manager™ Professional database and access codes. If you think there is a chance of this, then this option should be disabled immediately.

Show Splash screen at program startup

Disabling this option will cause the splash screen to not show when the program is launched, thereby creating a slightly faster startup.

Temporary Users will function in controllers that don't support Temporary Users

When this option is enabled, users set up as temporary/expiring users are exported to controllers that do not support the temporary user feature, but they will be allowed to gain access indefinitely (ie. they won't expire). If you disable this option, which is the default state, users are still exported to controllers that do not support the temporary user feature, but they won't be allowed access at all. For more information regarding Temporary/Expiring Users refer to the Users section.

Continue displaying the System Startup Tasklist even when all items are completed

Enabling this option will cause the System Startup Tasklist to always remain visible, even when completed, which may be a helpful reminder of what needs to be added.

Display Daylight Saving Time (DST) warning messages

When this option enabled, the Daylight Saving Time warning message is displayed when the software is launched. By default this option is enabled.

Start Page

This option allows you to select which page automatically opens when you successfully log into Hub Manager™ Professional. By default, the Main Screen is displayed.

- Users
- Log Filter Report
- System Dashboard
- Import/Export To Doors
- Main Screen

Chapter 9: Reports

9.1 Reports Menu

Select ***Reports*** from the Hub Manager™ Professional menu to display the following options.

Log Filter
Time Management
Misc. Log Reports
Assignment Reports
Database
Audit
Archive Viewer
Generate Data for External Report Writer
Scheduled Log Import Errors

9.2 Printer Options

Printing to Monitor, Printer, or File

In each report you have a choice of where you want to print the data: ***Monitor***, ***Printer*** or ***File***. The ***Monitor*** option means, the data is printed, or displayed, directly to you PC monitor for viewing. When you choose ***Printer***, the data is printed to a printer available through your PC. The ***File*** option uses the format for importing text files into Microsoft Excel.

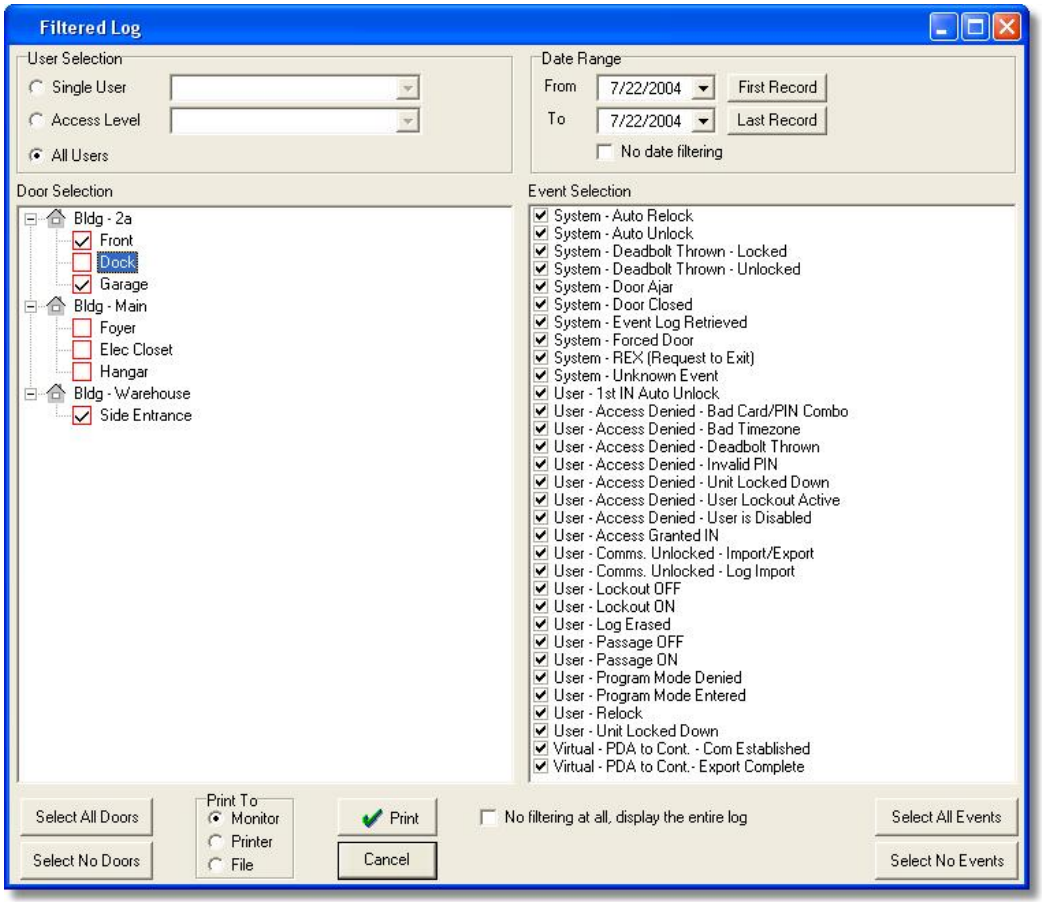
NOTE: To use this feature, you must have a printer driver installed. If you are not using a printer connected to you PC and you do not have a printer driver installed, you must add an ASCII printer driver from your Windows CD-ROM. Typically, the Generic / Text Only printer driver can be used.

9.3 Log Filter

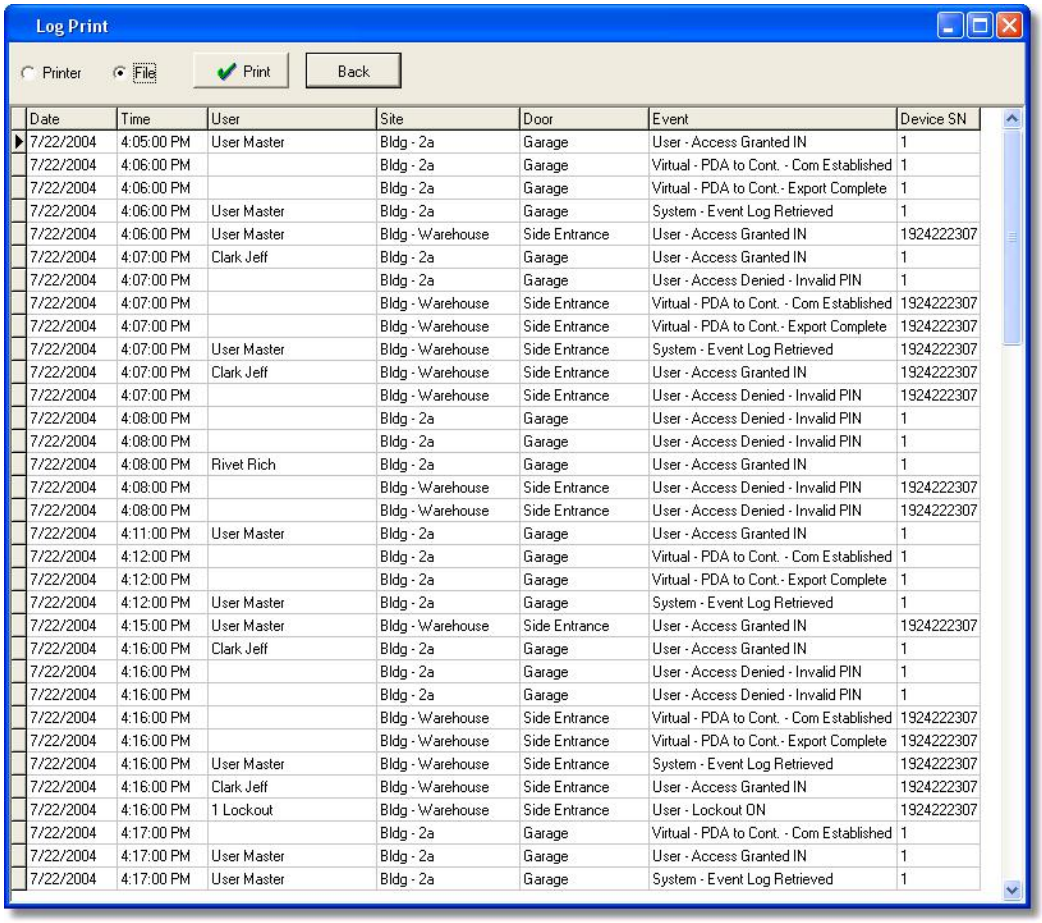
The Log Filter report contains details of the transaction logs generated at the door controllers. You can modify the contents by selecting different parameters.

Only those events that are supported by the selected door types will be displayed on the right.

1. Select ***Reports > Log Filter*** from the Hub Manager™ Professional main menu. The Filtered Log screen displays (see the following screen shot).



2. Specify the information to appear on the report on the Filtered Log screen. Enter the Users to be included in the report, specify the ***From*** and ***To*** date range, select the door to be included in the report; and check the desired events on the right-hand side (or use the "All" buttons). Only the events that match all the criteria will be displayed in the report.
3. Specify the desired output device for the report (on the bottom left of the screen): ***Monitor*** (screen), ***Printer***, or ***File***; if you select ***File***, you must enter a name for the file in the ***Filename*** field. ***Monitor*** is the default choice. Select the ***Print*** button to print the report.



Date	Time	User	Site	Door	Event	Device SN
7/22/2004	4:05:00 PM	User Master	Bldg - 2a	Garage	User - Access Granted IN	1
7/22/2004	4:06:00 PM		Bldg - 2a	Garage	Virtual - PDA to Cont. - Com Established	1
7/22/2004	4:06:00 PM		Bldg - 2a	Garage	Virtual - PDA to Cont.- Export Complete	1
7/22/2004	4:06:00 PM	User Master	Bldg - 2a	Garage	System - Event Log Retrieved	1
7/22/2004	4:06:00 PM	User Master	Bldg - Warehouse	Side Entrance	User - Access Granted IN	1924222307
7/22/2004	4:07:00 PM	Clark Jeff	Bldg - 2a	Garage	User - Access Granted IN	1
7/22/2004	4:07:00 PM		Bldg - 2a	Garage	User - Access Denied - Invalid PIN	1
7/22/2004	4:07:00 PM		Bldg - Warehouse	Side Entrance	Virtual - PDA to Cont. - Com Established	1924222307
7/22/2004	4:07:00 PM		Bldg - Warehouse	Side Entrance	Virtual - PDA to Cont.- Export Complete	1924222307
7/22/2004	4:07:00 PM	User Master	Bldg - Warehouse	Side Entrance	System - Event Log Retrieved	1924222307
7/22/2004	4:07:00 PM	Clark Jeff	Bldg - Warehouse	Side Entrance	User - Access Granted IN	1924222307
7/22/2004	4:07:00 PM		Bldg - Warehouse	Side Entrance	User - Access Denied - Invalid PIN	1924222307
7/22/2004	4:08:00 PM		Bldg - 2a	Garage	User - Access Denied - Invalid PIN	1
7/22/2004	4:08:00 PM		Bldg - 2a	Garage	User - Access Denied - Invalid PIN	1
7/22/2004	4:08:00 PM	Rivet Rich	Bldg - 2a	Garage	User - Access Granted IN	1
7/22/2004	4:08:00 PM		Bldg - Warehouse	Side Entrance	User - Access Denied - Invalid PIN	1924222307
7/22/2004	4:08:00 PM		Bldg - Warehouse	Side Entrance	User - Access Denied - Invalid PIN	1924222307
7/22/2004	4:11:00 PM	User Master	Bldg - 2a	Garage	User - Access Granted IN	1
7/22/2004	4:12:00 PM		Bldg - 2a	Garage	Virtual - PDA to Cont. - Com Established	1
7/22/2004	4:12:00 PM		Bldg - 2a	Garage	Virtual - PDA to Cont.- Export Complete	1
7/22/2004	4:12:00 PM	User Master	Bldg - 2a	Garage	System - Event Log Retrieved	1
7/22/2004	4:15:00 PM	User Master	Bldg - Warehouse	Side Entrance	User - Access Granted IN	1924222307
7/22/2004	4:16:00 PM	Clark Jeff	Bldg - 2a	Garage	User - Access Granted IN	1
7/22/2004	4:16:00 PM		Bldg - 2a	Garage	User - Access Denied - Invalid PIN	1
7/22/2004	4:16:00 PM		Bldg - 2a	Garage	User - Access Denied - Invalid PIN	1
7/22/2004	4:16:00 PM		Bldg - Warehouse	Side Entrance	Virtual - PDA to Cont. - Com Established	1924222307
7/22/2004	4:16:00 PM		Bldg - Warehouse	Side Entrance	Virtual - PDA to Cont.- Export Complete	1924222307
7/22/2004	4:16:00 PM	User Master	Bldg - Warehouse	Side Entrance	System - Event Log Retrieved	1924222307
7/22/2004	4:16:00 PM	Clark Jeff	Bldg - Warehouse	Side Entrance	User - Access Granted IN	1924222307
7/22/2004	4:16:00 PM	1 Lockout	Bldg - Warehouse	Side Entrance	User - Lockout ON	1924222307
7/22/2004	4:17:00 PM		Bldg - 2a	Garage	Virtual - PDA to Cont. - Com Established	1
7/22/2004	4:17:00 PM	User Master	Bldg - 2a	Garage	User - Access Granted IN	1
7/22/2004	4:17:00 PM	User Master	Bldg - 2a	Garage	System - Event Log Retrieved	1

NOTE: The Log Filter report is best printed in landscape format so that all the data in all columns will fit.

No date filtering

Enabling this option will cause the report to disregard any date filter you may have entered. This will allow you to see the entire contents of the transaction log, and can be helpful if events were imported with wrong time\date data that may have accidentally been outside the range of the date range criteria, and therefore causing those events to not be displayed in the report. The report will be sorted by date and time.

No filtering at all, display the entire log

Enabling this option will cause the report to disregard any filter you may have entered, including users, access levels, doors, events, or date range. This will allow you to see the entire contents of the transaction log, and can be helpful if events were imported

with data that may have accidentally been outside the range of the filter criteria. The report will be sorted by date and time.

First Record \ Last Record

These buttons search the Log Table for the oldest or newest events and set the From and To filters to those respective dates.

If the operator selects the 'First Record' or 'Last Record' buttons and there are no records in the Log table at all then a message will be displayed 'There are no records in the log table to sort. You must import a log first.'

"Unknown User ID"

There is an event that may appear in your Log Filter Report that says 'Unknown User ID: X' (where X is a user location reference). There are a few reasons that this event will be generated by Hub Manager™ Professional.

1. Regardless of the controller type, this event is generated if someone were to go into programming mode manually at the controller and try to add a user code for the purpose of 'hiding' it because they are trying to breach the security system. The reference number that is assigned to this event in this case will be the user location that the code was assigned to during manual programming. For example if someone tried to hide a code in user location 2000 of the controller, if someone attempted to use this user code to gain access, after the log was imported, an event would be displayed as 'Unknown User ID: 2000 Access Granted - IN'. If you see this 'Unknown User' event and your system has been up and running for some time, and you know you have imported logs from this door previously, then the chances are good that someone has manually programmed a user into the controller. To remove this user, you should perform a full export to this controller, by enabling the ***Export ALL the data (Full Export)*** checkbox in the Import\Export Doors screen.

2. Regardless of the controller type, any user generated events that occurred before Hub Manager™ Professional had exported user data to this controller will cause 'Unknown User ID' events to occur. This is because all user created events of these device types are tagged with an ID of the user that was used to trigger that event. When Hub Manager™ Professional exports user data to the controllers, it assigns a unique 'User ID' that it knows and is not present on new or defaulted controllers. If you see one of these 'Unknown User ID' events during your initial Log Import from either of these device types, you can dismiss it. Because these events occurred before the program and controller were synchronized. If you have already exported to this controller, then any subsequent Log Imports will not generate this 'Unknown User ID' event, except for the other reasons that this event may be generated as noted in this section.

3. This 'Unknown User ID' can also occur if you were to install a controller that had previous transaction log event data in the controllers event buffer memory. To stop this event from occurring on newly installed controllers, whether it be new or used, erase all system data as well as defaulting the log data. The programming commands for most of your controllers would be to enter programming mode and enter 46# 00000# 00000# * * to delete system data and also 76# 00000# 00000# * * to delete transaction log data. Always refer to the programming manual that came with the controller for the commands.

9.4 Time Management

The Time Management report is used to calculate how long a user was inside the protected area during a given time period. This report allows you to select a few different parameters to generate your reports, such as a single user, access level, time management group. In addition, Hub Manager™ Professional offers three types of reports called ***Detailed Daily Report***, ***Summarized Daily Report*** and a ***Summary Report***. Prior to running a report, you must also select a date range for which you'd like to see activity. All these options are discussed in detail below.

> **NOTE:** The ***Time Management Report*** requires controllers that support both User IN and User OUT events. Every controller can generate User IN events but not all controllers can generate a User OUT event, especially self contained locks. To find out if a specific controller can generate an OUT event, go to the ***Options*** tab of the ***Door*** settings screen and look in the ***Log Events*** list for an entry labeled ***User - Access Granted OUT***. If this entry is not there, then this particular controller type does not support OUT events.

Each report contains the terms ***Gross Time*** and ***Clear Time***. Below is the definition of these terms, including an example.

> ***Gross Time*** is defined as the total amount of time from the first IN event of the day to last OUT event of the day, including any time between IN and OUT events throughout the course of the day. For example, if John Doe comes to work (IN) at 9AM, goes (OUT) to lunch at Noon, and returns (IN) at 1PM, then leaves for the day (OUT) at 5 PM, the gross time is 8 hours. This is the total time between arriving (IN) at 9AM and leaving (OUT) at 5PM, including the 1 hour for lunch. This feature is not designed to work with 3rd Shift Workers that cross over the midnight boundary.

> ***Clear Time*** is defined as the total amount of time, from first IN event of the day to the last OUT event of the day, excluding any time between IN and OUT events through the course of the day. For example, if John Doe comes to work (IN) at 9AM, goes (OUT) to lunch at Noon, and returns (IN) at 1PM, then leaves for the day (OUT) at 5 PM, the clear time is 7 hours. This is the total time arriving (IN) at 9AM and leaving (OUT) at 5PM, minus the 1 hour for lunch. If Hub Manager™ Professional does not see an

opposing IN or OUT event for a user an error is printed on the report for that day, such as the term Missing in the OUT event column. In this case, the clear time is not calculated properly due to the missing event.

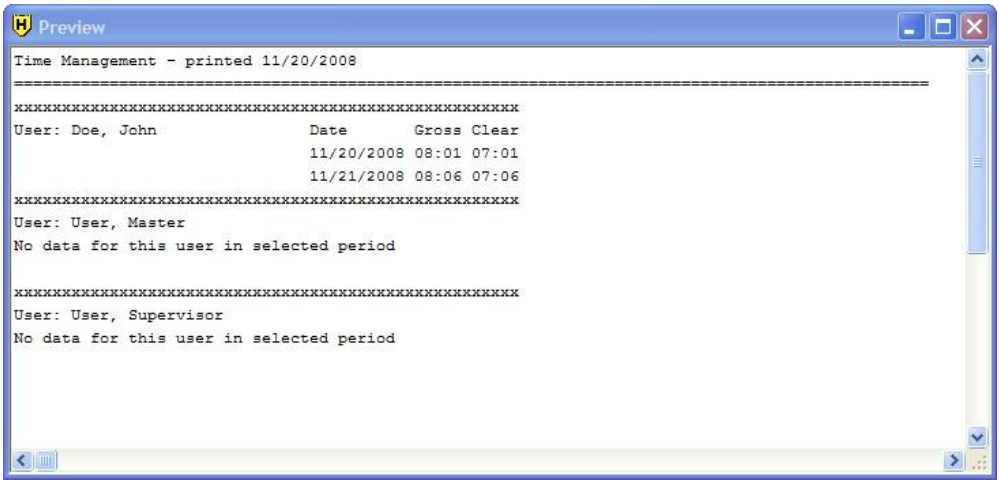
There are three types of Time Management reports you can generate using Hub Manager™ Professional. Below is a detailed description of the each type and a sample report.

Detailed Daily Report

This report shows a detailed daily activity report for each user selected, in the ***User Selection*** section, during the specified ***Date Range***. The example below shows two days of activity for a single user.

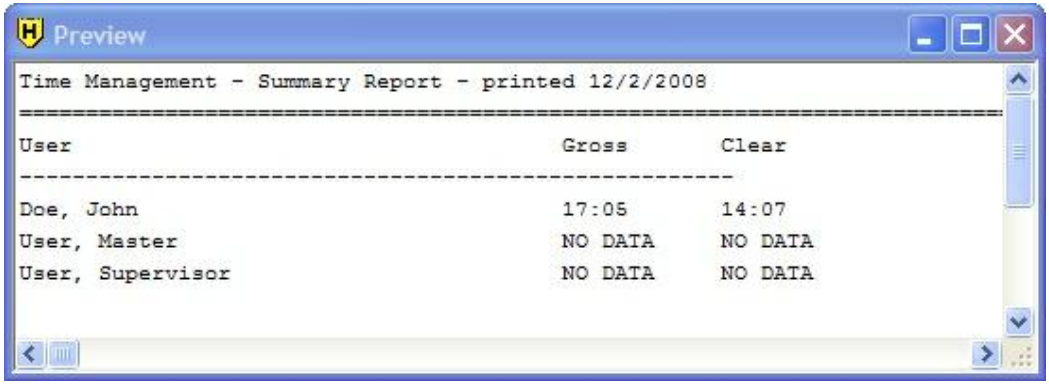
Summarized Daily Report

This report shows a summarized daily activity report for each user selected, in the ***User Selection*** section, during the specified ***Date Range***. This report only shows the ***Gross*** and ***Clear*** time for each day. The example below shows two days of activity for a single user.



Summary Report

This report shows a summary of total ***Gross*** and ***Clear*** time for each user in the system for the selected ***Date Range***. The example below shows the activity for a single user.

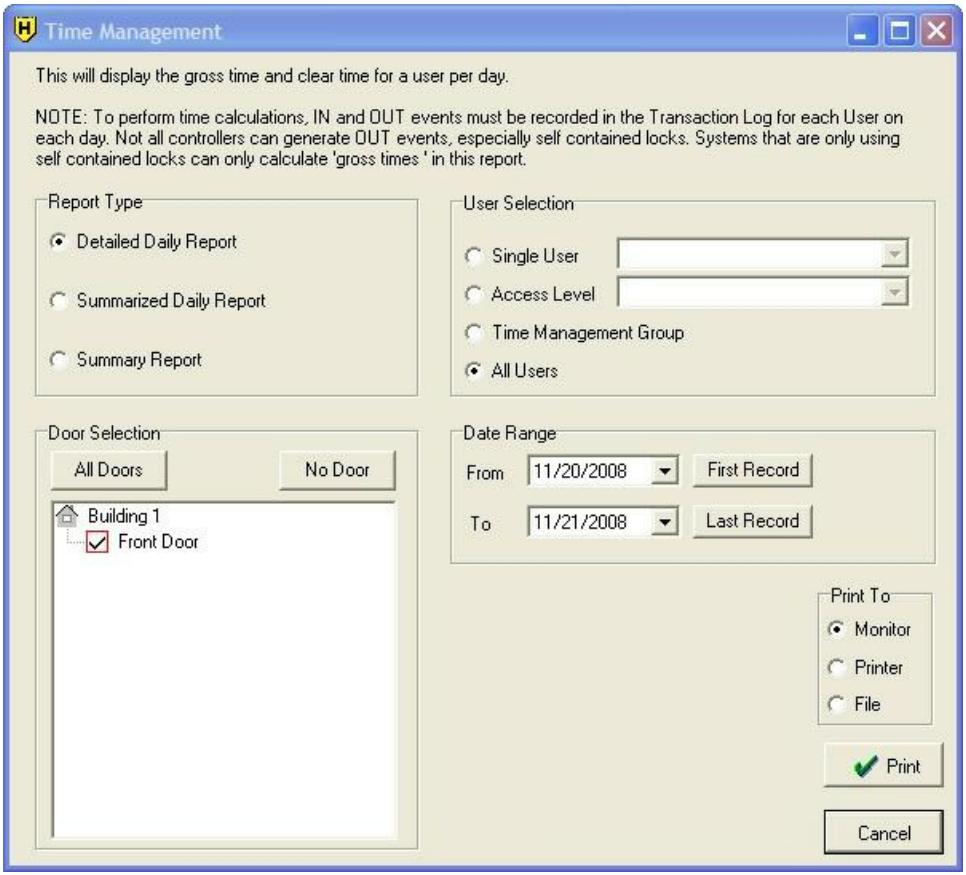


Printing a Time Management Report

The steps below describe how to print a Time Management report.

1. Select ***Reports > Time Management*** from the main menu to display the ***Time Management*** screen.
2. Specify the users you want to include in your report from the ***User Selection*** area. You can choose only one option from the following choices: ***Single User***, ***Access Level***, ***Time Management Group*** or ***All Users***.

3. In **Door Selection**, choose the doors you want to include in your report.
4. Choose the desired ***Date Range*** for which you want to show activity.
5. Choose the ***Report Type*** you want to generate. As mentioned above, you can choose from: ***Detailed Daily Report***, ***Summarized Daily Report*** or a ***Summary Report***
6. Before you print your report, you must select the output device you want to print to. You have three choices under ***Print To: Monitor*** (to display on your computer screen), ***Printer***, or ***File***. If you select ***File***, you must enter a file name in the ***File name*** field. ***Monitor*** is selected by default.
7. Finally to print the report, click the ***Print*** button in the lower right portion of the screen.

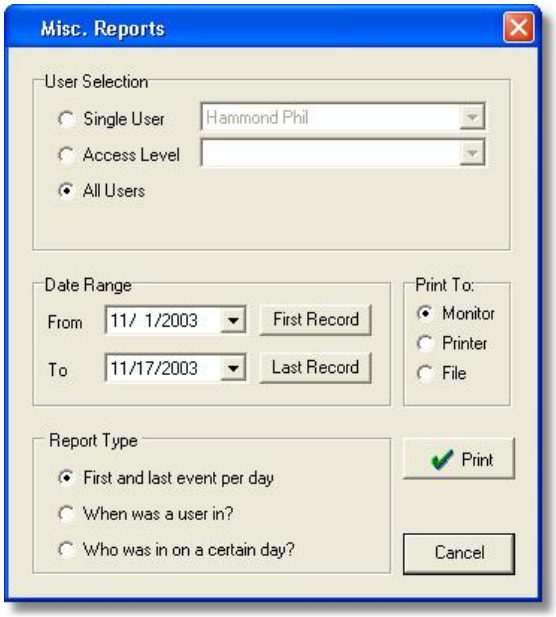


9.5 Misc. Log Reports

The Misc. Log Reports can show:

- The first and last event that occurred each day.
- What days a particular User was granted access.
- Who was granted access on a particular day.

1. Select ***Reports > Misc. Log Reports*** from the Hub Manager™ Professional main menu. If data is present, the Misc. Log Reports screen displays.
2. Specify the information to appear on the report on the Misc. Log Reports screen. Enter your ***User Selection*** choice, the appropriate ***Date Range***, ***Report Type***, and the ***Print To*** output device for the report: ***Monitor*** (screen), ***Printer***, or ***File***. If you select ***File***, you must enter a name for the file in the ***Filename*** field. ***Monitor*** is the default choice.
3. Select the ***Print*** button to print the report.



9.6 Assignment Reports

The Assignment Reports screen allows you to select from 4 different report types. Each report type allows you to select the individual items that you want to include in the report. Report types include:

- Show the Access Levels that contain the selected doors.
- Show the Users assigned to each door.
- Show the Doors each User can access.
- Show the Users assigned to each Access Level.

To use this reporting tool, perform the following:

1. Select ***Reports > Assignment Reports*** from the Hub Manager™ Professional main menu to show the Assignment Report selection screen.
2. In the section of the screen labeled ***Report Types***, select which report type you want to generate.
3. Select the items you want to include in the report. Options that are specific to that report type are discussed in the following sections that describe the individual report types.
4. Specify the ***Print To*** output device for this report: ***Monitor*** (screen), ***Printer***, or ***File***.
5. Select the ***Print*** button to print the report to the selected output. If you selected ***File***, you will be prompted to enter a name for the file in the ***Filename*** field.

Show the Access Levels that contain select doors

This report type can be helpful when you are adding users, and you have a large number of Access Levels. Simply select the doors on the left that you wish to add a user to. Each time you select or deselect a door on the left, Access Levels that contain all the selected doors will be displayed on the right.

Door Selection

Select the doors that will be displayed in the report.

Matching Access Levels

Displays the Access Levels that contain all the selected doors and also comply with the "Access Level Filtering" selection.

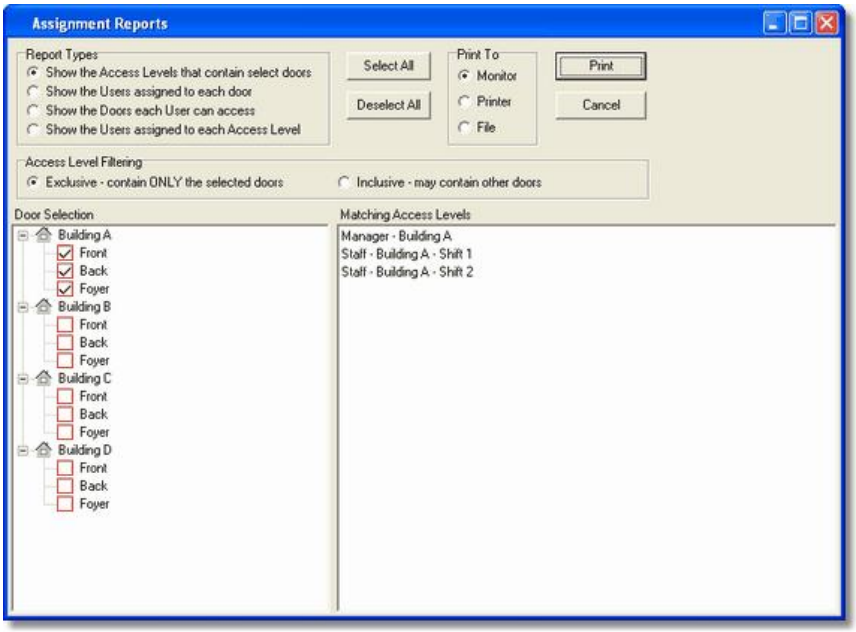
Access Level Filtering

Exclusive

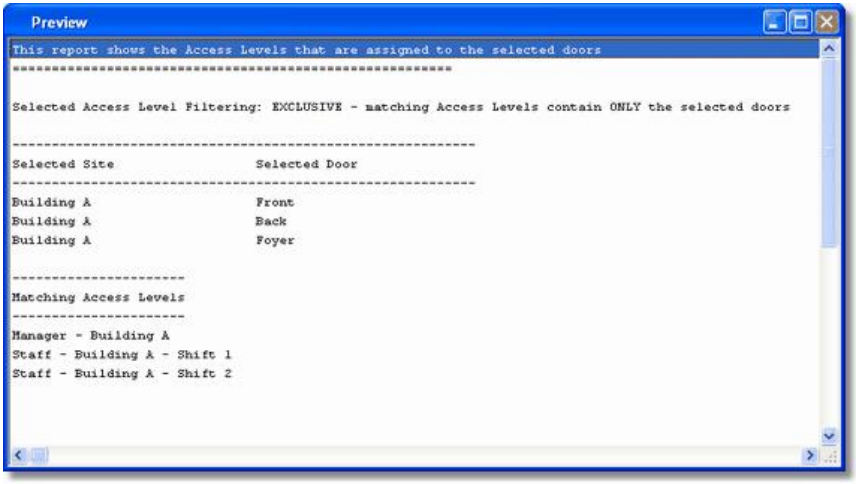
Displays matching Access Levels that grant access to ONLY the selected doors and no other doors.

Inclusive

Displays matching Access Levels that grant access to all the selected doors, but may also grant access to other doors.



Door Selection Screen



Print Report to Monitor

Show the Users assigned to each door

This report displays the users that are assigned to each of the selected doors. You have the option to not display particular data in the report, which can help you to distribute this report but still maintain security.

Door Selection

Select the doors that will be displayed in the report.

Show these items in the user report

PIN Data

Disabling this option will cause the PIN field to be replaced with an "X" (if that field contains data). If PIN data is disabled, then all the data in the PIN fields will be replaced by an X

Card Data

Disabling this option will cause the Card data fields to be replaced with an "X" (if any of those fields contain data).

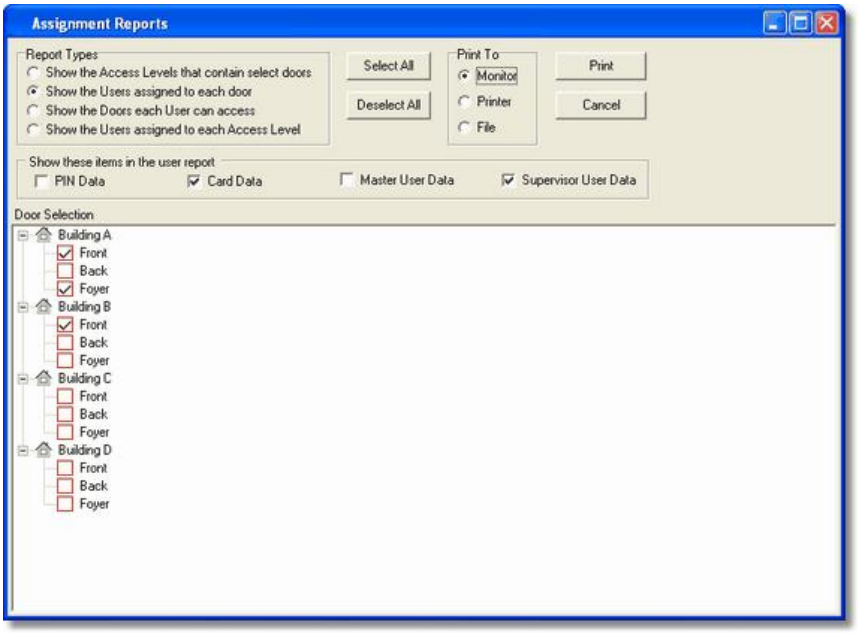
> **NOTE:** If you include either PIN data or Card Data in this report, and the report is printed to a hard copy or saved to a file, be sure to keep the report in a secure location, since data in that report could potentially be used to gain access.

Master User Data

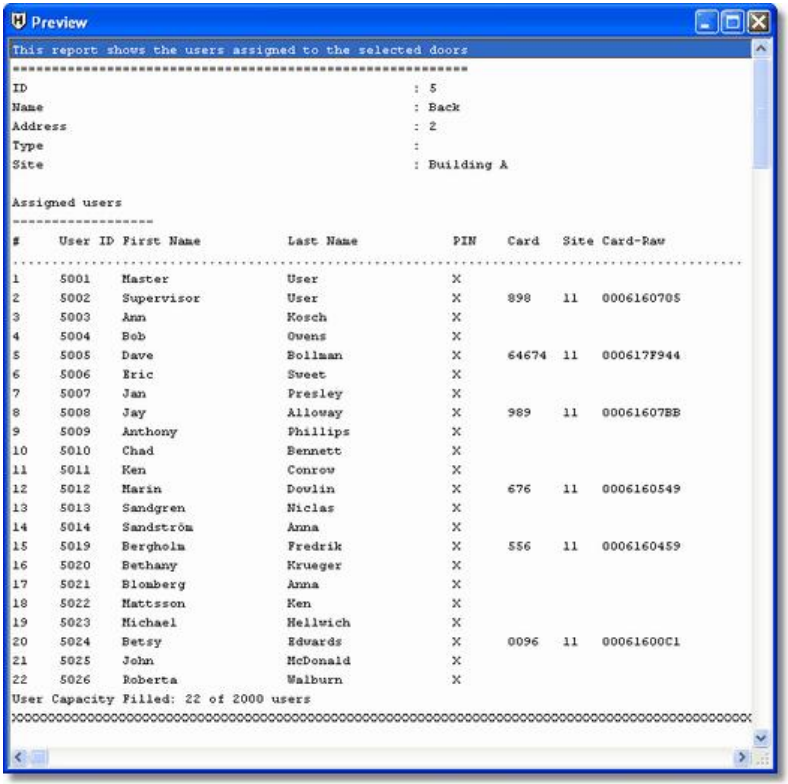
Disabling this option will cause the PIN and Card data fields of the Master User to be replaced by an "X" (if any of those fields contain data). This can be helpful if you want to distribute this report to someone but you do not want that person to be able to enter programming mode manually.

Supervisor User Data

Disabling this option will cause the PIN and Card data fields of the Supervisor User to be replaced by an "X" (if any of those fields contain data). This can be helpful if you want to distribute this report to someone but you do not want that person to be able to enter programming mode manually.



Door Selection Screen



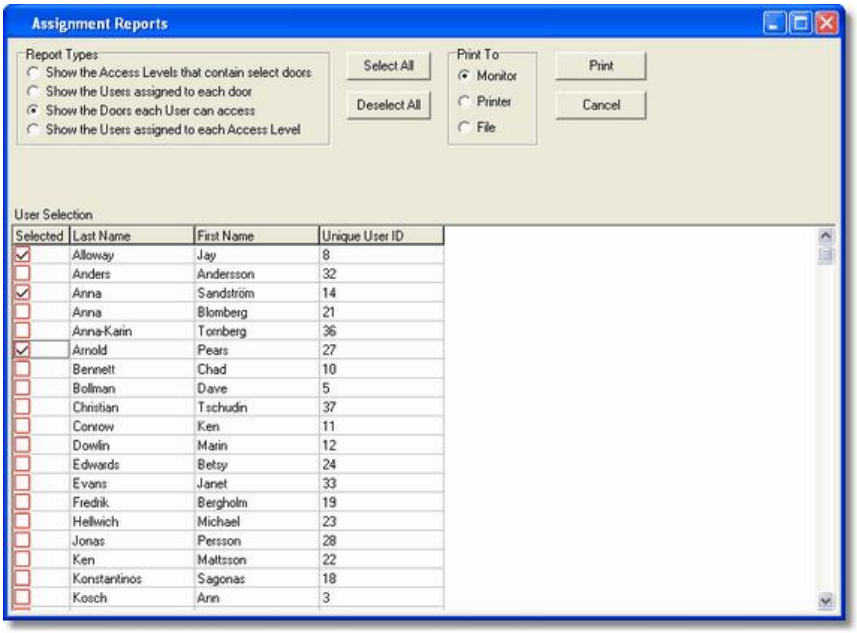
Print Report to Monitor

Show the Doors each User can access

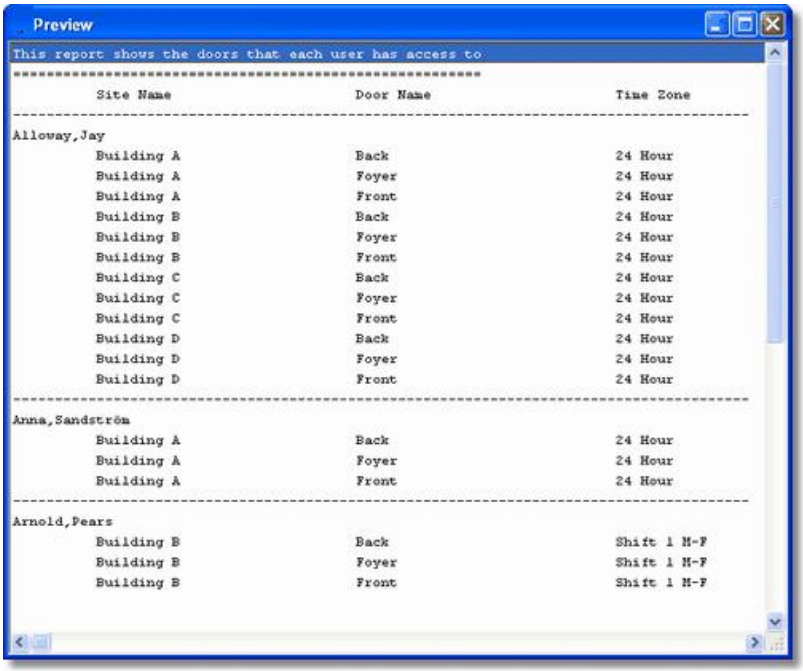
This report will display the Doors and Time Zones that each of the selected users can access. This report can help you decide if the Access Level you have assigned to this user is the best choice, based upon the doors that user has access to.

User Selection

Select the Users you want to include in this report.



User Selection Screen



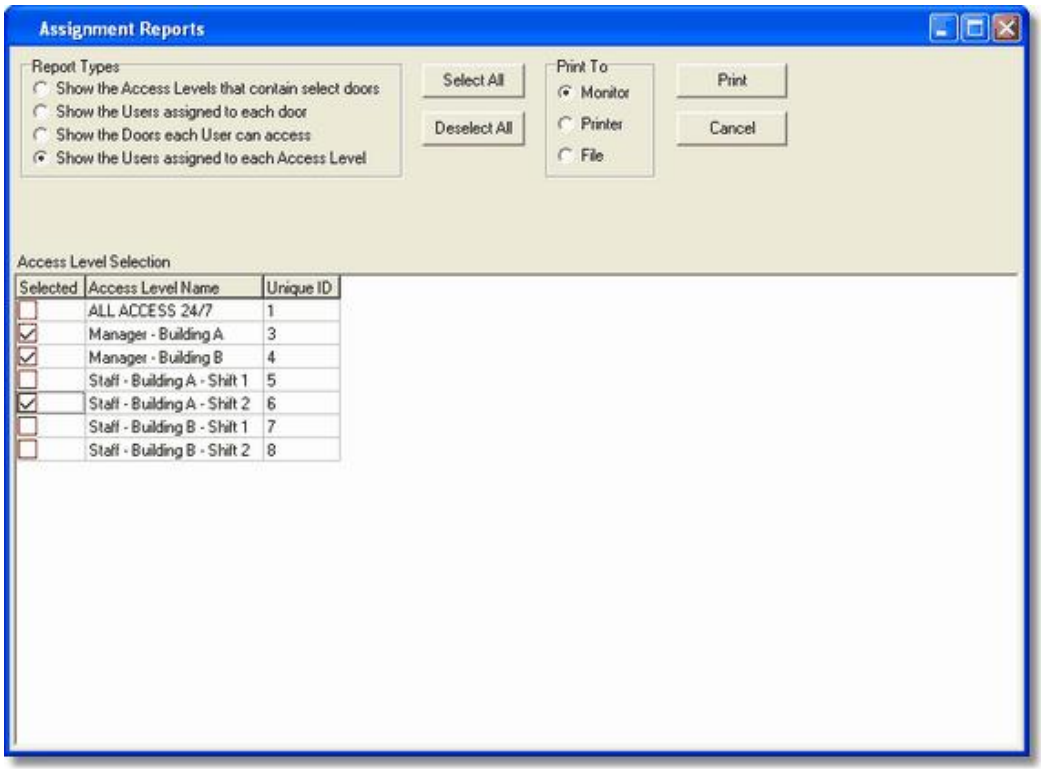
Print Report to Monitor

Show the Users assigned to each Access Level

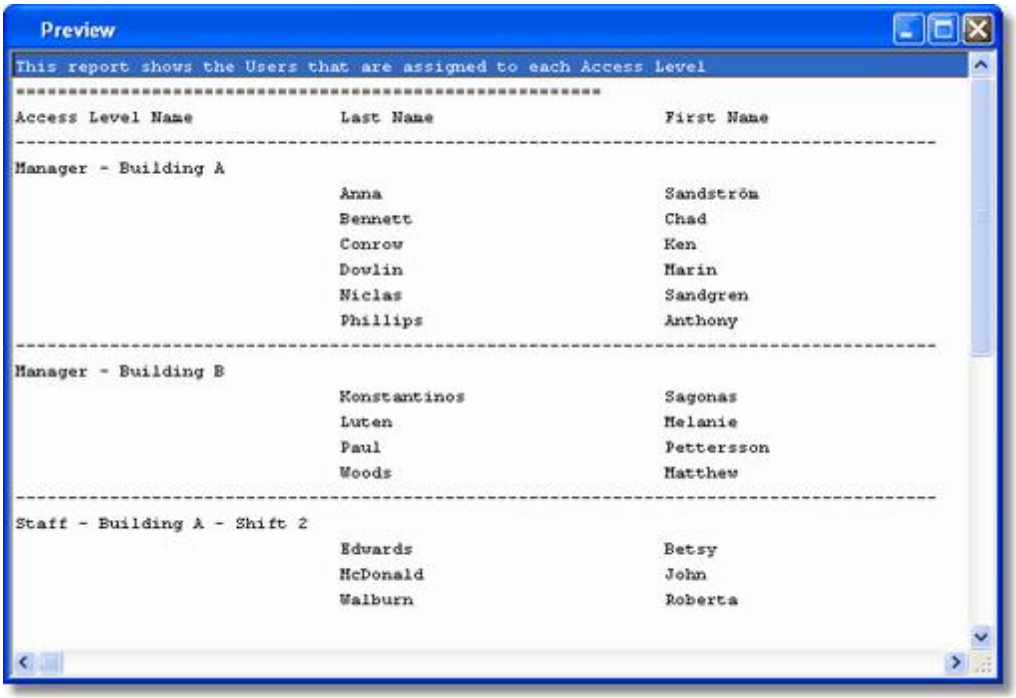
This report will display all the Users that are assigned to each of the selected Access Levels.

Access Level Selection

Select the Access Levels you want included in the report.



Access Level Selection Screen



Print Report to Monitor

9.7 Database

The Database report shows all programmed items within a certain database. Simply select the type of Database report you would like to generate.

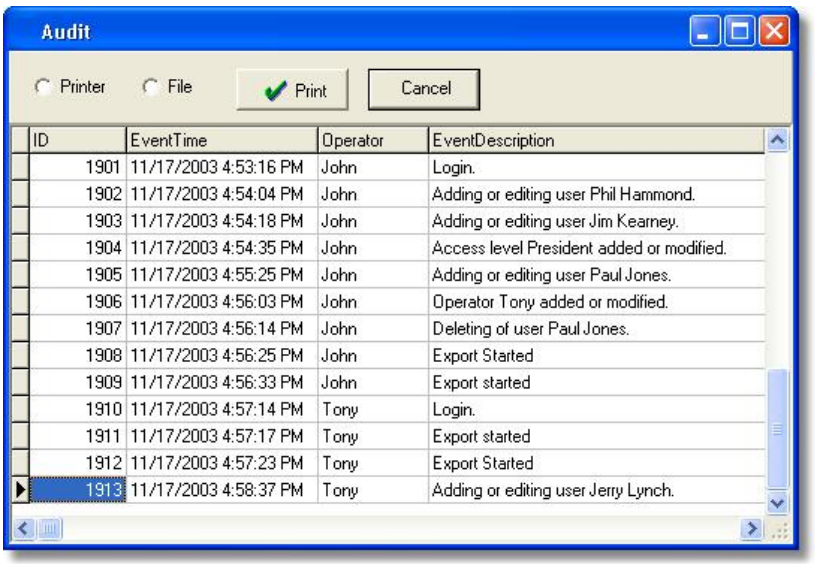
1. Select ***Reports > Database*** from the Hub Manager™ Professional main menu. The Database screen displays.
2. Specify the information to appear on the report on the Database screen. You can select the contents of these databases: ***Time Zones***, ***Sites***, ***Doors***, ***Access Levels***, ***Users***, and ***Holidays***.
3. Specify the desired output device for the report: ***Monitor*** (screen), ***Printer***, or ***File***; if you select ***File***, you must enter a name for the file in the ***Filename*** field. ***Monitor*** is the default choice.
4. Select the ***Print*** button to print the report.


Print of Databases
Database Selection
Timezones
Sites
Doors
Access Levels
Users
Holidays
Print To
Monitor
Printer
File
Print
Cancel

9.8 Audit

The Audit report contains a listing of operator activity, database modifications, and times of the activity.

1. Select ***Reports > Audit*** from the Hub Manager™ Professional main menu. The Audit screen displays. All Audit Trail data displays on the monitor.
2. If you want to save this data to a file or print a hardcopy, then specify the desired output device for the report: ***Printer***, or ***File***; if you select ***File***, you must enter a name for the file in the ***Filename*** field.
3. Select the ***Print*** button to print or save the report.

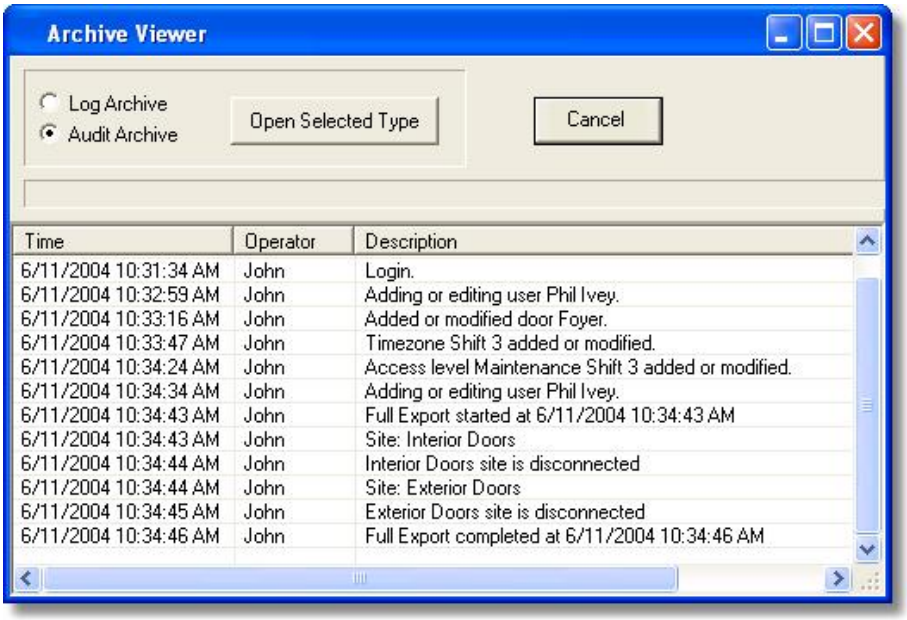


ID	EventTime	Operator	EventDescription
1901	11/17/2003 4:53:16 PM	John	Login.
1902	11/17/2003 4:54:04 PM	John	Adding or editing user Phil Hammond.
1903	11/17/2003 4:54:18 PM	John	Adding or editing user Jim Kearney.
1904	11/17/2003 4:54:35 PM	John	Access level President added or modified.
1905	11/17/2003 4:55:25 PM	John	Adding or editing user Paul Jones.
1906	11/17/2003 4:56:03 PM	John	Operator Tony added or modified.
1907	11/17/2003 4:56:14 PM	John	Deleting of user Paul Jones.
1908	11/17/2003 4:56:25 PM	John	Export Started
1909	11/17/2003 4:56:33 PM	John	Export started
1910	11/17/2003 4:57:14 PM	Tony	Login.
1911	11/17/2003 4:57:17 PM	Tony	Export started
1912	11/17/2003 4:57:23 PM	Tony	Export Started
1913	11/17/2003 4:58:37 PM	Tony	Adding or editing user Jerry Lynch.

9.9 Archive Viewer

The Archive Viewer report permits you to open either Log or Audit archives for viewing. For more information on archiving, see Log Archiving and Audit Archiving.

1. Select ***Reports > Archive Viewer*** from the Hub Manager™ Professional main menu. The Archive Viewer screen displays.



2. Specify the desired type of Archive report, ***Log Archive*** or ***Audit Archive*** and select the ***Open Selected Type*** button. A Select Archive screen displays. Select the Log or Audit file you wish to view. You can navigate to the desired directory using standard Windows techniques.
3. To print these files, open them in another program that can read .CSV files such as Microsoft Excel.

9.10 Generate Data for External Report Writer

This option will start the Report Writer Database Copy. See ***Tools > Options*** for details on the Generate Report Database option.

9.11 Scheduled Log Import Errors

The Schedule Log Import Errors report presents a list of recorded error events with a description for each. These are errors that occur during the scheduled importing of transaction logs. The program operates in this fashion because logs can be imported even if an operator is not present, and this report allows you to determine if any errors occurred during the automated Scheduled Log Import process.

Select ***Reports > Scheduled Log Import Errors*** from the main menu. The system processes your request for this report and then displays the results. After viewing the errors, the errors are moved into the Audit Trail log.

Chapter 10: Help

10.1 Help

The electronic Help file is context sensitive. This means, for example, that if you press F1 while the Access Levels Edit screen is open in Hub Manager™ Professional, the Help file opens to the topic that describes Access Levels.

10.2 Online Support

Online Support is available but you must contact a Technical Support Representative prior to using this feature.

10.3 Check for Updates

iUpdate is a feature that checks for and installs any updates that are found for the Hub Manager™ Professional software. No sensitive information is sent during this process.

NOTE: This feature requires an active internet connection.

1. Upon selecting this option from the Hub Manager™ Professional main menu ***Help > Check for Updates***, the program attempts to establish a connection with the update server located on the internet.

NOTE: If a Windows Security Alert is displayed, choose ***Unblock*** to allow the update program access to the update server located on the internet.

2. If the server is found then any available updates are displayed.

3. Select ***Next*** to start downloading and installing the updates. You may be required to run the update again, depending which pieces need updates.

4. When all updates are complete you will receive a final message stating that all components are up to date and Hub Manager™ Professional will restart.

10.4 Check for Custom Updates

This option checks for special updates that are distributed on an individual basis. In order to use this feature you need the Custom Update Information provided to you. This information includes the iUpdate server, login name and password.

No sensitive information is sent during this process.

NOTE: This feature requires an active internet connection.

1. When you select this option from the Hub Manager™ Professional main menu ***Help > Check for Custom Updates***, the program asks you for the Server IP Address, Login Name, and Login Password.
2. iUpdate then attempts to establish a connection with the specified update server located on the internet.
3. Any available updates are displayed. Select ***Next*** to start the download process.
4. Hub Manager™ Professional will restart when the download and installation process is complete.

10.5 Upgrading Hub Manager™ Professional

This section discusses how to upgrade to Hub Manager™ Professional v8 from a previous version of the product.

Upgrading to Hub Manager™ Professional v8 on the same PC

If you are currently using Hub Manager™ Professional v1, v2, v3, v4, v5, v6, or v7 on your PC and want to convert to Hub Manager™ Professional v8 that is installed on the same PC, then follow these instructions.

1. If you haven't already done so, install Hub Manager™ Professional version 8 onto your PC. Refer to the installation section for details.
2. Run Hub Manager™ Professional version 8 on your PC and login.
3. Once the program is open, you must convert the database to the new version. Go to ***Tools > Database Conversion Utility***. Refer to the Database Conversion Utility section of this manual.

Upgrading to Hub Manager™ Professional v8 from another PC

If you are currently using Hub Manager™ Professional v1, v2, v3, v4, v5, v6, or v7 on one PC and want to convert to Hub Manager™ Professional v8 that is installed on different PC, then follow these instructions.

1. Open Windows Explorer on your old machine: ***Start > Programs > Accessories > Windows Explorer***.
2. Next browse to the Hub Manager™ Professional database folder:

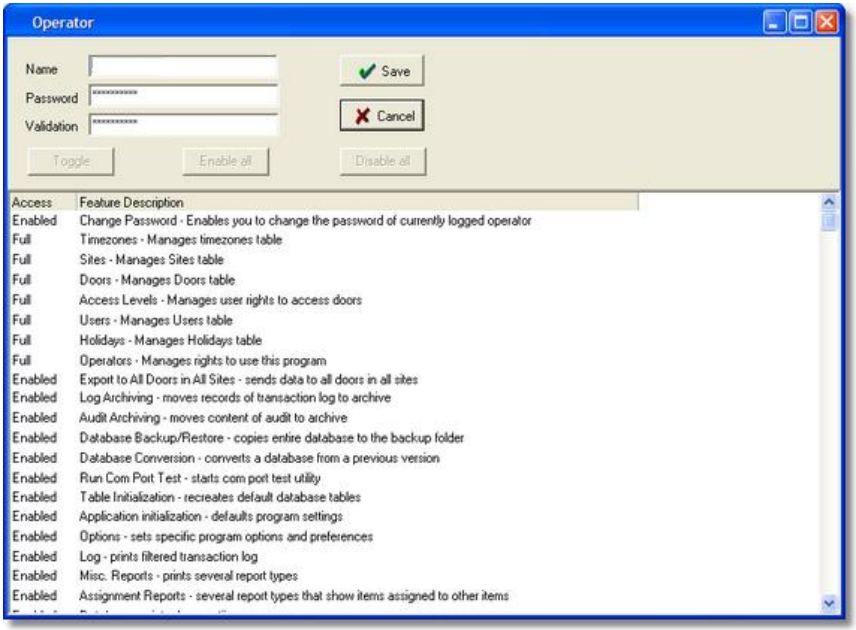
   C:\Program Files\IEI\HubManagerProX\Program\Database (where X is the Major version of the software)

3. Now copy the entire Database folder onto some form of removable media (CD, USB Flash Drive) or to a network drive that is accessible from your new PC.
4. If you haven't already done so, install Hub Manager™ Professional v8 onto your new PC. Refer to the installation section for details.
5. Run Hub Manager™ Professional v8 on your new PC and login.
6. Once the program is open, select ***Tools > Database Conversion Utility***. Refer to the Database Conversion Utility section of this manual.
7. In the Conversion Utility, select the version of Hub Manager™ Professional database you are converting from in the ***Source*** selection. Select Hub Manager™ Professional v8 in the ***Destination*** selection.
8. Check the option called ***Let me specify the source folder*** and click the ***Browse to Database Folder*** button.

9. When browse dialog box appears, locate the folder you copied the old database to. If you placed in on removable media, insert it and browse to it. Once you've located the database, select it, then click the ***Convert Now*** button.
10. When complete click the ***Exit*** button. The upgrade process is now complete.

10.6 About

This screen contains information about the Hub Manager™ Professional program. This is also the screen where you can edit the ***Support Contact Information***, that appears in the lower right of the main screen. In order to edit these fields, you must log in to the program using the Hub Manager™ Professional administrator login name and password. This login was initially named HUBMAN, but may have been changed. If you have more than one login operator in the system and you are not sure which one is the Administrator, it is easy to recognize. Assuming your login has full access rights to the operator database, if you open each operator in the list, the Administrator operator has the ***Toggle***, ***Enable All*** and the ***Disable All*** buttons disabled (the text appears gray, as shown below).



If you log in with this operator and go to ***Help > About***, you can edit the ***Support Contact Information***.

The Administrator Operator always has FULL access to all areas of the program. The options can not be edited, and this operator can never be deleted.

see also:

Obtaining Technical Support

10.7 Glossary

Auto Unlock: An Auto-Unlock Time Zone means the door will unlock at a scheduled time and relock again at a scheduled time. This feature is sometimes referred to as scheduled unlock. When the clock in the controller reaches the time zone start time, the door will automatically unlock and when the time zone end time is reached, the door will automatically lock. It will do this only on the days you selected when you first set up the time zone.

Card Number: The card number is the electronic code contained in an access card or other access credential stored in the card field that is used to perform an action on a door controller. The card number is read electronically by a card reader. (This definition also applies to Magnetic (ABA Track II) cards, Proximity cards, RF Fobs and Dallas Touch Chips.)

Code Number: The access number that the user enters on a keypad to gain access to a door. It can be 1 to 6 digits in length. The longer the code, the greater the security. It only takes 9 attempts to find a 1-digit code.

Code PIN: Same as Code Number.

COM Port: This is a serial communication port or a USB port on a personal computer through which the Hub Manager™ Professional software communicates.

DB9: This is a 9-pin connector that is shaped like an elongated "D"; it can be found on the back of a computer.

DB25: This is a 25-pin connector that is shaped like an elongated "D"; it can be found on the back of a computer.

Door: In this manual, the term door is used synonymously with the term controller, Door Controller, or Door Control Module. When referring to "Door Status"what is really being said is "Controller Status."

Export: The action of sending Door Settings information from the Hub Manager™ Professional software to the controllers.

Forced Door Alarm: This is the programmable feature in a controller whereby the Forced Door relay located in the controller is activated for a specified time when the controller detects that a locked door has been forced open. NOTE: This requires that a door position detection device has been properly installed.

Handheld: This is a generic term used to describe a PDA or DTD handheld device.

Import: The action of retrieving information from the controller network into the Hub Manager™ Professional software.

Keypress Feedback: This is a feature of the controller whereby a yellow LED light is flashed or a sonalert device is beeped (depending on installed equipment) with each keypress on a keypad.

Log: Short for Transaction Log. The log is a list of recorded events for a particular door.

Master Code: This code is used to enter programming mode on a controller. It is located in User #1. The name of User #1 is defaulted to "Master User".

Operator: Person responsible for managing the access control system using Hub Manager™ Professional and System Manager software.

PIN: Acronym for Personal Identification Number. See Code Number.

System Dataset (aka Dataset or System): A 'System Dataset' is a compressed zip file that stores all the data that is related to that particular System, currently including (but not limited to) the complete contents of the following folders: Archive, Backup, Database, Gateway, DTD, Maps, PDAFiles, Print, and ReportDB.

System Manager: System Manager is a program that is responsible for accessing the System Repository and loading System datasets onto the local PC. System Manager also sends that same dataset back to the System Repository.

System Repository (aka Repository, or Repository folder): A 'System Repository' is a folder that can store any number of System Datasets. Any number of System Repository folders can be created based upon your security needs. All systems stored in that repository can be accessed by any installation of System Manager that has network privileges to see that particular System Repository folder.

Chapter 11: Obtaining Technical Support

11.1 Obtaining Technical Support

Should you experience any difficulty installing or operating the Hub Manager™ Professional software, please contact your installer or contact IEI at 800-343-9502.

The installer information can be found in the bottom right corner of the Hub Manager™ Professional main screen, or go to ***Help > About***.

Chapter 12: Copyright Information

12.1 Copyright Information

Index

- 2 -

24 Hours 131

- A -

About 261
Access Condition 162
Access Level Selection Tool 183
Access Level Setup 162
Access Levels 162
Add User 179
Add User Group 198
Administrator 15
Application Initialization 227
Archive Viewer 254
Archiving 216
Assigned Doors 77
Assignment Reports 245
Audit Archiving 217
Audit Trail Report 254
Auto Configuration 209
Autorun 6
Auto-Unlock Time Zone 148
Auxiliary Outputs 152

- B -

Backup Alert 230
Batch Load Users 198
Block Holiday 200

- C -

Capacity 134
Card 172
Card Format 172, 186
Change Login Password 71
Check for Custom Updates 259
Check for Updates 257
Com Port 83
Com Port Test 223
Communications
  Export Data to Doors 205
  Import Door Settings 204
  Import Transaction Log 205
  Network Query 209
  System Dashboard 211
  Update Time/Date 205
Connect 77
Connection
  DTD 85
  LAN 106
  Modem 127
  PDA 83
  Serial 83
Connection Type 77
  Parameters 77
Contact Information 261
Controller Status 209
Conversion Utility 220
Copyright Information 266
Corporate Code 172
Crystal Reports 256
Crystal Reports Compatibility 230

- D -

Data Conversion 220
Data Transfer Device 77

Database 73
Access Levels 162
Doors 134
Holidays 200
Menu 73
Operators 73
Sites 77
Time Zones 131
Users 172
Database Backup\Restore 218
Database Conversion Utility 220
Database Printing 252
Date Setting 205
Deselect Door 162
Device Group 77
Device Type
HC500 149
Hub+\Max 149
LS2\P 160
Max 2 v1 149
Max 2 v2 149
Max 3 v1 152
Max 3 v2 152
prox.pad plus 152
prox.pad plus IR 150
Secured Series Controllers 149
DHCP 106, 113, 117
Disconnect 77
Door
Address 134
Device Type 134
Log Event Mask 134
Name 134
Site 134
System Options 134
System Parameters 134
Time Zones 134
Door Settings 134
Door Wizard 161
Doors
Door Type 134
Type 134
DTD 77
DTD Printer Utility 6
Dynamic IP Address 106, 113, 117

- E -

Emergency User 162
Enrollment Station 172, 189
Event
Unknown User ID 236
Event Log 205
Events 205
Exit 72
Expiring Users 152, 172
Export data to Doors 205
Export Time/Date 205
Extended Unlock User 162
External Tools 223

- F -

First-In Auto-Unlock 152
Floating Holiday 200
Foreword 2

- G -

Generate Data for External Report Writer 256
Glossary 263
Go To Assist 257
GoToAssist 257
Group 198
Group Code 172

- H -

HC500 149
Help 1
About 261
Check for Custom Updates 259
Check for Updates 257
Help 257
HID Cards 172
HID Prox Cards 172
Holidays 200
Hub+\Max 149

- I -

Import Door Settings 204
Import Log 205
Indexing 228
Indexing error 228
Initial Setup 23
Installation
PC Software 6
PDA Software 6
IP Address 106, 113, 117
iUpdate 257, 259

- L -

LAN 106
Live Event Log 211
Live Log Settings 211
Live Status 211
Lockdown User (Panic) 162
Lockout User 162
Log 205
Log Archiving 216
Log Filter 236
Log Importing 205
Login 15, 70
Logout 70
LS Link 160
LS2\P 160

- M -

Main Menu 28
Manual Conventions 2
Master Code 172
Master User 162, 172
Max 2 v1 149
Max 2 v2 149
Max 3 v1 152
Max 3 v2
Auxiliary Outputs 152
Expiring Users 152
First-In Auto-Unlock 152
Max 3 v2 Output Module 152
Temporary Users 152
Max 3 v2 Output Module 152
Menu
Database 73
Tools 216
Menu System 28
Midnight Crossing 131
Migrating Data 220
Misc. Log Reports 244
Modem 127
Multiple databases 50
Multiple Systems 50

- N -

Name List Import 195
Navigating through the Program 28
Network Query 209

- O -

Online Support 257
Online Updates 257, 259
Operator 70, 71
  Audit Trail Report 254
Operator Wizard 76
Operators 73
Options 230
Overview
  Converting data 220
  General Overview 15
  Initial Setup 23
  Menu System 28
  PDA Software 35
  Running the software 30
  Uninstall 47

- P -

Palm OS Software 6, 35
Panic User 162
Passage User 162
Password 70
PDA 77
PDA Application 83
PDA Software 6, 35
PIN 172
PIN Data 190
Print to File 235
Print to Monitor 235
Printer 235
prox.pad plus 152
prox.pad plus IR 150

- Q -

Query Now 209

- R -

Random PIN 172
Raw Card Data 190
Raw Data 172
Relock 162
Remote Relock 211
Remote Unlock 211
Report Writer 230
Reports
  Archive Viewer 254
  Assignment Reports 245
  Audit 254
  Database Printing 252
  Generate Data for External Report Writer 256
  Log Filter 236
  Misc. Log Reports 244
  Scheduled Log Import Errors 256
  Time Management 240
RS232 - RS485 Converter 83
Run Com Port Test 223
Running the software 30

- S -

Scheduled Log Import 71, 72, 224
Scheduled Log Import Errors 256
Scheduled Log Import Reminder 225
Scheduled Unlock 148
Secured Series Controllers 149
Security chip 204
SEG 106, 113, 117
Sending Data to a Door 205

Serial 83
Serial Converter 83
Settings
Door 134
Setup 23
Setup Wizards 161, 169, 195
Single Use 162
Site Code 172
Site Wizard 82
Sites 77
Static IP Address 106, 117
Supervisor Code 172
Supervisor User 162, 173
System 50
Change Password 71
Exit 72
Login 70
Logout 71
System Manager 50
System Dashboard 211
System Dataset 50
System Manager 230
Clear System List 50
Close System 50
Create System 50
Define Existing Repository 50
Delete System 50
Emergency Override 50
Open System 50
Rename System 50
System Repository 50
Systems
Multiple 50

- T -

Table Initialization 226
Tecnincal Support 265
Temporary Users 152, 172
Time Management 172, 240
Time Setting 205
Time Zone Selections 162
Time Zones 134
TimeZones 131
Tools
Application Initialization 216, 227
Audit Archiving 216, 217
Backup Alert 230
Database Backup/Restore 216
Database Backup\Restore 218
External Tools 216
Indexing 216, 228
Log Archiving 216
Options 230
Report Writer 230
Run Com Port Test 216, 223
Scheduled Log Import 216, 224
Scheduled Log Import Reminder 225
System Manager 230
Table Initialization 216, 226
Transaction Log 205
Transaction Log Importing 205
Type 162

- U -

Uninstall 47
Unknown User ID Event 236
Updates 257, 259
Upgrading 260
User Name List Import 195
User Type 162
Extended Unlock 162
Lockdown (Panic) 162
Lockout 162
Master 162
Passage (Toggle) 162
Standard 162

User Type 162
Supervisor 162
Toggle (Passage) 162
Users 172
Add Batch of Users 198
Add Group of Users 198

- V -

Visual ID 172

- W -

Walkthrough 30
Warning Messages
User Capacity Exceeded 195
Warranty 2
Windows Logon 15
Wizards 82, 161, 169, 195
Access Level 169
Door 161
Site Wizard 82
User Import Wizard 195