Doors™ for use with Windows™
Access Control Software

Users Guide v2.1
# Table of Contents

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Doors™</td>
<td>9</td>
</tr>
<tr>
<td>The Host Computer</td>
<td>11</td>
</tr>
<tr>
<td>System Requirements</td>
<td>11</td>
</tr>
<tr>
<td>COMTEST Serial Port Test</td>
<td>12</td>
</tr>
<tr>
<td>The Loop-Back Plugs</td>
<td>12</td>
</tr>
<tr>
<td>Starting COMTEST In Windows 95</td>
<td>12</td>
</tr>
<tr>
<td>Starting COMTEST In Windows 3.11</td>
<td>12</td>
</tr>
<tr>
<td>Running COMTEST</td>
<td>12</td>
</tr>
<tr>
<td>If the Host Computer Fails COMTEST</td>
<td>14</td>
</tr>
<tr>
<td>If the Host Computer Passes COMTEST, but there are Still Problems</td>
<td>14</td>
</tr>
<tr>
<td>Setting the Host Computer Date and Time</td>
<td>15</td>
</tr>
<tr>
<td>Setting the Date and Time in Windows '95</td>
<td>15</td>
</tr>
<tr>
<td>Setting the Date and Time in Windows 3.11</td>
<td>15</td>
</tr>
<tr>
<td>Software Installation</td>
<td>17</td>
</tr>
<tr>
<td>Upgrade Installation</td>
<td>17</td>
</tr>
<tr>
<td>Backing Up in Windows 95</td>
<td>17</td>
</tr>
<tr>
<td>Backing Up in Windows 3.11</td>
<td>17</td>
</tr>
<tr>
<td>New Installation</td>
<td>17</td>
</tr>
<tr>
<td>To Install Doors using Windows 95</td>
<td>17</td>
</tr>
<tr>
<td>To Install Doors using Windows 3.11</td>
<td>18</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>19</td>
</tr>
<tr>
<td>Low System Resources</td>
<td>19</td>
</tr>
<tr>
<td>Verifying System Resources in Windows 95</td>
<td>19</td>
</tr>
<tr>
<td>Verifying System Resources in Windows 3.11</td>
<td>19</td>
</tr>
<tr>
<td>Missing DLL Files</td>
<td>19</td>
</tr>
<tr>
<td>To Copy the Missing DLL Files in Windows 95</td>
<td>20</td>
</tr>
<tr>
<td>To Copy the Missing DLL Files in Windows 3.11</td>
<td>20</td>
</tr>
<tr>
<td>Recovering an Original Doors Installation</td>
<td>20</td>
</tr>
<tr>
<td>Recovery Using Windows 95</td>
<td>20</td>
</tr>
<tr>
<td>Recovery Using Windows 3.11</td>
<td>21</td>
</tr>
<tr>
<td>Deleting a Backed Up Doors Installation</td>
<td>21</td>
</tr>
<tr>
<td>Deleting Using Windows 95</td>
<td>21</td>
</tr>
<tr>
<td>Deleting Using Windows 3.11</td>
<td>21</td>
</tr>
<tr>
<td>Users Guide</td>
<td>23</td>
</tr>
<tr>
<td>Users Guide Conventions</td>
<td>24</td>
</tr>
<tr>
<td>Windows Conventions</td>
<td>25</td>
</tr>
<tr>
<td>On-Line Help</td>
<td>25</td>
</tr>
</tbody>
</table>
The Order of Operation 25

Logging On the Doors Program 25
Setup and Verify Network Communication 25
Set Communication Parameters 25
Auto-Config 25
Set Time 26
Perform Smart Update 26
Get Controller Status 26
Begin Database Programming 26
Setup Operators 26
Setup Time Zones 26
Setup Doors 26
Setup Access Groups 26
Setup Cards 26
Setup Monitor Windows 26
Download Information to the Network 27

System Operation 27
Advanced Features 27

Logging On 29
Starting the Doors Program 29
Starting the Program in Windows 95 29
Starting the Program in Windows 3.11 30
System Logon 30
Network Update 31

Introducing the Doors Desktop 33
The Desktop 33
The Tool Bar 34
On-Line Help 34
Exiting a Doors Window 35
Exiting in Windows 95 35
Exiting in Windows 3.11 35

Setup/Verify Network Communication 37
Set Communication Parameters 37
Set the COM Port 37
Set the Communication Speed 38
Set the Modem Parameters 39
Save the Communication Parameters 39
Auto-Config 39
Successful Auto-Config 41
Failed Auto-Config 41
Set Controller Time and Date 42
Network Update – Default Parameters 43
Get Controller Status 45
Get Status For All Controllers 45
Get Status For One Controller 47

Database Programming 49
Setup Operators 49
  Editing the Default Operator 49
  Creating a New Operator 50

Setup Time Zones 53
  Day-Shift Time Zone Example 53
  Janitorial Shift Time Zone Example 56
  Grave Shift Time Zone Example (Crossing Midnight) 57
  Holiday Schedules 58
  Display/Edit a Time Zone 60
  Delete a Time Zone 61

Setup Doors/Controllers 63
  Set Controller Dial-Out Parameters 63
    Enable Controller Dial-Out 63
    Set the Dial-Out Threshold Percentage 64
    Disable Controller Dial-Out 64
  Assign a Door Name 65
  Assign a Door Class 66
  Disable/Enable a Reader 67
  Set a Door Unlock Time 68
  Set a Door Open Time 69
  Set an Unlock/Lock Time Zone 70
  First Person In 71
  Alarm Output 72

Setup Access Groups 75
  Create a New Access Group 75
  Edit an Existing Access Group 80
    Add/Remove a Door from the Access Group 81
    Change the Time Zone on an Access Group Door 82
  Delete an Access Group 84

Setup Cards 87
  Card Enrollment – Dialog Box Method 87
    Enroll Tab 87
    Block Enrollment by Card Number Range 87
    Enrolling by Presenting to a Reader 90
    Card Data Tab 91
      Entering Card Data for a Cardholder 92
      Editing Card Data for a Cardholder 94
      Voiding a Card 94
      Deleting a Card 96
  More Card Data 97
  Preferences 98
  Personal Setup 99
  Personal 101
Card Enrollment – Spreadsheet Method 103
  Enrolling Cards 103
  Entering Card Data for a Cardholder 104
  Voiding Cards 107
  Deleting Cards 109
  Sorting Data 110
  Block Copying Data 111
  Personal Data Fields 113
  Editing Cardholder Data 114
  Resizing Columns and Rows 116
    To Resize a Column 116
    To Resize a Row 116
  Printing Cardholder Data from the Spreadsheet (Quick Print) 116

Setup Monitor and Events 117
  Enable/Disable Auto-Collection 117
  Configure Event Monitoring Windows 118
    Naming Event Monitoring Windows 118
    Message Text Strings 119
    Message Text String Definitions 121
  Assigning Events to be Monitored 126
    Save to File 128
  Controller Reports Events 130

Update the Network 133

System Operation 135
  Locking, Unlocking, and Updating Doors 135
    Lock Doors 136
      Lock All Doors 136
      Lock All Doors in a Door Class 136
      Lock a Single Door 137
    Unlock Doors 138
      Unlock All Doors 138
      Unlock All Doors in a Door Class 139
      Unlock a Single Door 140
    Timed Unlock 140
      Timed Unlock All Doors 140
      Timed Unlock All Doors in a Door Class 141
      Timed Unlock a Single Door 142
    Update Doors 142
      Update All Doors 142
      Update All Doors in a Door Class 143
      Update a Single Door in a Door Class 144
  Monitor and Collect Events from the Controllers 147
    Verifying Communication Status 147
    Starting Monitoring 147
    Collecting Events 148
    Stopping Monitoring 148
Create Event Reports 149
  Quick Search Event Report 149
  Clear all Fields 149
  Select Doors 150
  Select Cardholders 151
  Select Events 152
  Select Dates 152
Generate Report Output 153
  View Report on Screen 153
  Print Report 154
  Save Report to File 154
Power Search Event Reports 155
  Field Type and Field Value 156
  Boolean Operators 157
  Boolean Links 159
  Power Search Example 160
  Generate the Report 163
Library Tab 163
  Save a Search Expression 164
  Get a Search Expression 164
Options Tab 165
  Reverse Order of Sort 165
  Save Card ID Numbers in the Report File 166
Identify an Unknown Card 167
  ID by Reading the Card 167
  ID by Entering the Internal Number 168
  ID by Entering the Card Number 168
Disconnect from the Access Control Network 169
Window Management 169
  Cascading Windows 169
  Tiling Windows 170
  Tiling Windows Horizontally 170
  Arranging Icons 171
  Cycling Windows 172
Retrieving the Software Revision and Logged Operator 172

System Maintenance 175
  Secure Storage of Source Disks 175
  Periodic Doors Software Backup 175
    In Windows 95 175
    In Windows 3.11 175
  Archiving the Event Logs 176
    In Windows 95 176
    In Windows 3.11 176
  Generating Reports from an Archived Event Log 177
Advanced Features 179
  Multiple Site Control 179
  Enable Sites 179
  Enter Site Configuration Information 181
    Assign a Site Name 182
    Enter the Site Address 182
    Site Number 182
    Site Personal Identification Number (PIN) 182
    Site Phone Number 183
    Site Modem Initialization String 183
    Site Global Secure Time 184
    Site Global Unlock Enable 184
    Site Comment 184
  Adding a New Site 185
  Changes in Database Entry and Program Operation 186
    Cardholder Spreadsheet Changes 186
    Access Group Changes 187
      For a New Access Group 187
    Update Site 189
    Select a Site 189
    Quick Search Reports by Site 190
    Power Search Reports by Site 191
I/O Control 193
  I/O Configuration 193
  Link Configuration 194
    Link Parameters 195
    I/O Link Example 197
  Manual Output Control 202

Appendix 203
  Database Field Field Definitions 205
    Data Format in Single Site Mode – Using the Cardholder’s Name 206
    Data Format in Single Site Mode – Using the Cardholder’s Card Number 207
    Data Format in Multiple Site Mode – Using the Cardholder’s Name 208
    Data Format in Multiple Site Mode – Using the Cardholder’s Card Number 209
Glossary 211

Index 215
Introduction to Doors™

Doors™ for use with Windows™ is a software program that configures and manages an access control system utilizing Keri Systems' PXL-250 Tiger Controllers or PXL-100 Smart Entry Controllers.

Doors is a fully functional Windows program, making full use of all popular Windows features such as resizing and relocating windows, drag-and-drop functions, multiple windows open simultaneously, background operation, and "real-time" operation. Doors operates under Windows 3.11, Windows 95, or Windows NT.

Doors provides the operator with a user-friendly interface for defining system parameters, managing card and transaction files, setting timing functions, and preparing reports. For operators who are familiar with spreadsheet programs (such as Microsoft Excel™), many operations can be performed in spreadsheet format, with simple sorting, block, and copy functions. A wizard provides the operator a step-by-step walk-through procedure for creating Access Groups (a method for associating access doors with time periods of operation). An extensive on-line help file places assistance at the operator's fingertips.

A dedicated PC is not needed to run Doors. The PC is only needed for entering and uploading information to the controllers, downloading information from the controllers, or for real-time system monitoring. Doors uses a proprietary communications protocol to automatically check all controllers on the network and configures itself according to the connected hardware, greatly simplifying the system setup procedure.

Doors is capable of managing a single site via a direct connect line or a modem, and is capable of managing up to 255 remote sites, each via modem. Remote multiple site management features automatic dial-up of remote sites, global and site specific card enrollment, global and site specific event reporting, and configurable automatic downloads of events from controllers.

The Doors software can handle:

- Up to 32 system operators, each with password protection and configurable privileges.
- Up to 32 time zones, each with 4 start/stop intervals.
- 3 holiday schedules, each with up to 32 definable holiday dates.
- An unlimited number of Access Groups (subject to available hard disk space).
- Up to 6 sortable user definable text fields for individual cardholder information in addition to last name, card number, access group, and department group fields.
- Up to 255 sites.
- Up to 128 controllers per site.
- Up to 128 doors (one per controller), or up to 256 doors (two per controller) if using optional Satellite boards with every controller.
- Up to 6,400 cards/cardholders.
This page is intentionally left blank.
The Host Computer

System Requirements

For proper operation of the Doors access control software, the host computer operating the software must meet the following requirements.

- PC compatible computer using a Pentium-90 or faster microprocessor
- minimum of 16 MB of system RAM\(^{(1)}\)
- 520 KB of free, conventional memory
- VGA color monitor with VGA graphics card
- 3.5 inch floppy disk drive
- keyboard
- mouse or other pointing device
- 20 MB of hard disc space
- COM port\(^{(2)}\) with a 16550 UART to support an external modem or a direct RS-232 serial connection, or an internal 9600 baud (or faster) modem
- one of the following operating systems:
  - Windows 3.11\(^{(3)}\) with MS-DOS 6.2 (or greater)
  - Windows 95
  - Windows NT

NOTES

\(^{(1)}\) The larger the number of cards being enrolled, the larger the system RAM should be to efficiently handle the card database.

\(^{(2)}\) Since all communication between controllers and the Doors software is done through the host computer's COM port, Doors cannot work if the host computer's COM port is not working correctly. Keri Systems cannot be held responsible for host computer COM port or hardware problems. With the Doors software package, Keri Systems, Inc. provides a simple COM port test that can verify basic operation of the COM port. Please refer to the COMTEST Program section below for instructions on operating the program.

\(^{(3)}\) This must be the Windows 3.11 upgrade version and not the older Windows 3.0 or 3.1 versions. There are features and improvements made in the 3.11 revision that the Doors program needs for proper operation. To determine which revision of Windows is on a host computer, click on the Help/About pull-down menu in the main program window. A text box will appear listing a variety of information regarding the host computer, including the revision of the Windows software. If necessary, contact Microsoft or a computer software vendor for operating system upgrades.
COMTEST Serial Port Test

The Keri Systems, Inc. COMTEST program is a simple program. It is designed to send a string of characters out the host computer's COM port output and see if they are echoed back to the host computer's COM port input.

It is not designed to determine if the COM port has more serious problems such as conflicts with other devices on the host computer. For these types of problems, troubleshooting by a computer technician is required.

The Loop-Back Plugs

To use the COM Test utility program, unplug the connection made from the access control system to the host computer's COM port. Plug in the correct loop-back plug. The loop-back plug routes the output signal from the serial port back to the input signal. Two plugs are provided – one with 9 pins and one with 25 pins. Virtually every serial COM port will use one of these two plugs.

Starting COMTEST In Windows 95

1. Open the Windows Explorer program.
2. Locate the COMTEST.EXE program. For a default software installation, the program can be found in the "kerisys\doors\utils" subdirectory.
3. Double-click on the COMTEST.EXE program icon, or click on the COMTEST.EXE icon and then click on the File ⇒ Run pull-down menu option.
4. Skip to the Running COMTEST section below.

Starting COMTEST In Windows 3.11

1. Open the FILE MANAGER program.
2. Click on the File ⇒ Run pull-down menu.
3. Click on the Browse button and locate the COMTEST.EXE program. For a default software installation, the program can be found in the "kerisys\doors\utils" subdirectory.
4. Click on the Run button.

Running COMTEST

1. When the program begins, the following screen will appear.

   KERI SYSTEMS INC. COMM TEST UTILITY

   Plug in the Keri Loopback Test plug before starting the test.

   Type C to set COM port
   Type T to test COM port
   Use icon in upper left to quit the program

   PORT: COM2
   STATUS: Untested
2. Press the letter C. The following screen will appear.

KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested

Enter 1 = COM1, 2 = COM2, 3 = COM3, 4 = COM4

3. Press the number corresponding to the COM port the host computer is using for communication with the access control network (in this example, 2 was pressed). The following screen will appear.

KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested

4. Press the letter T. The following screen will appear.

KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Untested

Testing, please wait . . .
5. The COM port test takes just a few seconds. When complete, if the COM port has passed the test it is able to send and receive data. The following screen will appear.

   KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Passed

6. If the COM port has failed the test, the following screen will appear (the error message will vary depending upon what type of error was detected).

   KERI SYSTEMS INC. COMM TEST UTILITY

Plug in the Keri Loopback Test plug before starting the test.

Type C to set COM port
Type T to test COM port
Use icon in upper left to quit the program

PORT: COM2
STATUS: Failed

An error has occurred <type of error>
Press any key to continue

7. To rerun the COMTEST, press any key to return to the beginning of the program.

8. To exit the program, either click on the box in the upper-right corner of the COMTEST window, or click on the Windows icon in the upper-left corner of the program window and a pull-down menu will appear. In the menu, click on Close.

9. Remove the loop-back plug from the serial port and reinstall the communication cable.

If the Host Computer Fails COMTEST
If the host computer failed COMTEST, there is a basic problem in transferring data through the COM port. A computer technician should examine the computer.

If the Host Computer Passes COMTEST, but there are Still Problems
Some COM port problems are beyond the scope of this COM test program. These types of problems tend to involve several devices within the computer that are trying to use the same resources within the computer, each device affecting the others. A computer technician should examine the computer to resolve these kinds of problems.
Setting the Host Computer Date and Time

To ensure that the date and time assigned to events on the access control system are correct, the date and time kept by the host computer should be checked for accuracy. Part of the controller configuration process, later in this manual, will be to set the time and date of the controllers to match that of the host computer.

Setting the Date and Time in Windows '95

The Windows Help file provides instructions on setting the date and time.

2. Click on Help and a help topics window will appear.
3. Click on the Index tab and in the first field type Date/Time. This will automatically search for and highlight the Date/Time help entry.
4. Click on the display button and a list of hyperlinks to the instructions for setting the date and time will appear.

Setting the Date and Time in Windows 3.11

The Windows Help file provides instructions on setting the date and time.

1. Double-click on the Main window icon to open the Main window.
2. Double-click on the Control Panel icon to open the Control Panel.
4. Click on the Contents menu option and a list of selections will appear.
5. Under the "How to . . ." heading, click on Change the System Date and Time.
6. A window will appear with instructions for setting the date and time.
Software Installation

This section covers upgrading an existing Doors software installation, performing a brand-new installation, troubleshooting some basic installation problems, and deleting an old software installation. For a brand-new installation, please skip to the New Installation section below.

Upgrade Installation

If you have an original revision of the Doors software and you're upgrading to a new revision, you should make a complete copy of the original Doors installation into a backup location for recovery if there is an issue with the new software installation. You must perform this step before installing the new revision of Doors as the installation process will overwrite critical files in the original revision making recovery of the original revision impossible.

Backing Up in Windows 95

1. Open the Windows EXPLORER program.
2. Click on the "kerisys" folder icon (typically c:).
3. Click on File ⇒ New ⇒ Folder, or right-click the mouse, scroll down the displayed list of available commands, and click on New ⇒ Folder.
4. Enter a name for the backup folder (such as "backup").
5. Locate and click on the "kerisys\Doors" folder and then click on Edit ⇒ Copy.
6. Click on the "backup" folder.
7. Click on Edit ⇒ Paste. All files in the "kerisys\Doors" folder will be copied to the "kerisys\backup" folder.
8. When the copy process is complete, skip to the New Installation section below for instructions on the new installation of Doors software.

Backing Up in Windows 3.11

1. Enter the FILE MANAGER program.
2. Locate and click on the "Doors" directory and then click on FILE ⇒ COPY. A prompt box will appear asking for a destination path.
3. Click in the text box within the prompt box and type the name of the destination path (such as "c:\kerisys\backup") into which the backup copy can be saved.
4. Click on the Copy button. All files in the "kerisys\Doors" folder will be copied to the "kerisys\backup" folder.
5. When the directory copy process is complete, skip to the New Installation section below for instructions on the new installation of Doors software.

New Installation

A new installation of the Doors software requires 20 MB of free space on the hard disc drive for program and database storage.

To Install Doors using Windows 95

1. Insert Disk 1 into the host computer's floppy disk drive.
2. Click on the Windows Start button.
3. In the start menu, click on the RUN button. A run window appears on screen.
4. Click in the "Open:" text box and type a:\winstall.exe.
5. Click on the OK button. Program installation now begins.
6. A text window appears with the README.TXT file for the Doors software. Please read
the README.TXT file for late-breaking information regarding this revision of Doors
software. When you are finished reading, click on the File ⇒ Exit pull-down menu or
click on the box in the upper-right corner of the window.
7. The installation program will then verify that the host computer has at least 20 MB of
available space before allowing the file copying process to begin.
8. The installation program will request a directory name into which the software should be
loaded. The Doors program uses “kerisys\doors” as the default directory path for
installing software. If another directory path is desired, click in this text field and enter
that path now. If this installation is an upgrade to an existing installation and the existing
installation is in a different directory path, enter that directory path now.
9. Click on the OK button.
10. The installation program will request an icon name. The default icon name is Doors. If
desired, enter a more descriptive name at this time (perhaps a name including the
software revision).
11. Click on the OK button.
12. A number of files will be copied to the host computer. When disk 1 is complete, the
installation program will prompt for disk 2. Remove disk 1, insert disk 2, and click the
OK button.
13. A few more files will be copied to the host computer. When the installation is complete,
an “Installation Successful” banner will appear. Remove disk 2.
14. Click on the OK button and the Doors software is now ready for use.

To Install Doors using Windows 3.11

1. Insert Disk 1 into the host computer's floppy disk drive.
2. Open the Main window.
3. Open the FILE MANAGER program.
4. Click on the File ⇒ Run pull-down menu.
5. Click in the text box and type a:\winstall.exe.
6. Click on the OK button. Program installation now begins.
7. A text box will appear with the README.TXT file for the Doors software. Please read
the README.TXT file for late-breaking information regarding this revision of Doors
software. When you are finished reading, click on the File ⇒ Exit pull-down menu or
click on the box in the upper-right corner of the window.
8. The installation program will then verify that the host computer has at least 20 MB of
available space before allowing the file copying process to begin.
9. The installation program will request a directory name into which the software should be
loaded. The Doors program uses “kerisys\doors” as the default directory path for
installing software. If another directory path is desired, click in this text field and enter
that path now. If this installation is an upgrade to an existing installation and the existing
installation is in a different directory path, enter that directory path now.
10. Click on the OK button.
11. The installation program will request an icon name. The default icon name is Doors. If
desired, enter a more descriptive name at this time (perhaps a name including the
software revision).
12. Click on the OK button.
13. A number of files will be copied to the host computer. When disk 1 is complete, the
installation program will prompt for disk 2. Remove disk 1, insert disk 2, and click the
OK button.
14. A few more files will be copied to the host computer. When the installation is complete,
an “Installation Successful” banner will appear. Remove disk 2.
15. Click on the OK button and the Doors software is now ready for use.
Troubleshooting

The following section provides information on correcting two basic program installation/operation problems and for recovering an original saved installation.

Low System Resources

Sporadic problems in operating the Doors software can be due to an inadequate amount of the host computer's resources being available for use by the Doors software. The greater the number of programs open concurrently, the less the amount of system resources available for any one program. Doors needs approximately 65% of the computer system's resources free for proper operation.

Verifying System Resources in Windows 95

1. Click on the Start button on the Task Bar. A menu of selections will appear.
2. Click on Settings ⇒ Control Panel.
3. When the Control Panel window appears, double-click on the System icon.
4. When the System Properties window appears, click on the Performance tab.
5. A list of system performance status values will appear; one of which is the system resources value.
6. The system resources value should be above 65% to ensure proper operation of the Doors program. If it is not, close other unneeded programs to release the system resources they are using.
7. When you have finished viewing the system performance values, click on the OK button or click on the  box in the upper-right corner of the window.
8. If closing programs does not release enough system resources, close all programs, re-boot the host computer, and then start the Doors program. This will release all system resources for reallocation.

Verifying System Resources in Windows 3.11

1. In the Program Manager window, click on Help ⇒ About.
2. A list of information about this Windows installation will appear. One of the items listed is the system resources value.
3. The system resources value should be above 65% to ensure proper operation of the Doors program. If it is not, close other unneeded programs to release the system resources they are using.
4. When you have finished viewing the installation information, click on the OK button or click on the  box in the upper-right corner of the window.
5. If closing programs does not release enough system resources, close all programs, re-boot the host computer, restart Windows, and then start the Doors program. This will release all system resources for reallocation.

Missing DLL Files

Sporadic problems with the screens and buttons in the Doors software in older Windows 3.11 installations can be due to two files that are required for proper operation of the Doors software but are missing from the Windows installation. In Windows 95 use WINDOWS EXPLORER and in Windows 3.11 use FILE MANAGER to verify these two files exist in the "Windows/System" directory.

CTL3D.DLL
CTL3DV2.DLL
If these files do not exist, they may be copied from Disk 1 of the Doors installation disks. Perform the following steps to copy these files to your Windows/System directory.

**To Copy the Missing DLL Files in Windows 95**

1. Exit the Doors program.
2. Insert Doors installation disk number 1 into the floppy disk drive.
3. Start the WINDOWS EXPLORER program.
4. Click on the floppy disk drive icon, typically a:\.
5. When its file directory appears, click on theCTL3D.DLL file. This file name should now be highlighted.
6. Hold down the CTRL key and click on the CTL3DV2.DLL file. Both file names should now be highlighted.
7. Click on Edit ⇒ Copy, or click on the right mouse button, scroll down the displayed list of available commands, and click on Copy.
8. Scroll down the list of folders and locate the "windows\system" directory. Click on the "windows\system" directory.
9. Click on Edit ⇒ Paste, or click on the right mouse button, scroll down the displayed list of available commands, and click on Paste.
10. Restart the Doors program and the DLLs will be applied to the program.

**To Copy the Missing DLL Files in Windows 3.11**

1. Exit the Doors program.
2. Insert Doors installation disk number 1 into the floppy disk drive.
3. Double-click on the Main window icon and then double-click on the FILE MANAGER program.
4. Click on the floppy disk drive icon, typically a:\.
5. When its file directory appears, click on the CTL3D.DLL file in the right-side of the window. This file name should now be highlighted.
6. Hold down the CTRL key and click on the CTL3DV2.DLL file. Both file names should now be highlighted.
7. Click on File ⇒ Copy, or click on the right mouse button, scroll down the displayed list of available commands, and click on Copy.
8. Click on the hard disk drive icon, typically c:\.
9. When its file directory appears, scroll down the list of folders in the left-side of the window and locate the "windows\system" directory. Click on the "windows\system" directory.
10. Click on File ⇒ Paste, or click on the right mouse button, scroll down the displayed list of available commands, and click on Paste.
11. Restart the Doors program and the DLLs will be applied to the program.

**Recovering an Original Doors Installation**

At times following an upgrade installation, it can become necessary to restore the original installation of Doors software. Restoration is simply a matter of copying the original installation back over the new installation.
Recovery Using Windows 95
1. Open the WINDOWS EXPLORER program.
2. Locate and click on the backup folder and then click on EDIT ⇒ COPY.
3. Click on the folder to which the original installation should be restored (typically c:\kerisys\doors).
4. Click on EDIT ⇒ PASTE, or click on the right mouse button, scroll down the displayed list of available commands, and click on Paste.
5. When the folder copy process is complete, the original revision of Doors software has been restored and is ready for use.

Recovery Using Windows 3.11
1. Enter the FILE MANAGER program.
2. Locate and click on the backup directory and then click on FILE ⇒ COPY. A prompt box will appear asking for a destination path.
3. Click in the text box within the prompt box and type the name of the destination path (typically c:\kerisys\doors) into which the original installation should be restored.
4. Click on the OK button.
5. When the directory copy process is complete, the original revision of Doors software has been restored and is ready for use.

Deleting a Backed Up Doors Installation
If the new installation has been operating correctly for an extended period of time and if disc storage space is at a premium, the backed up installation can be deleted.

Be sure the new installation is working to your satisfaction before deleting the backed up installation. Once deleted, the backed up installation cannot be recovered.

Deleting Using Windows 95
1. Open the WINDOWS EXPLORER program.
2. Locate and click on the backup folder and then click on FILE ⇒ DELETE.
3. A file deletion confirmation window will appear. Click on the Yes button.
4. At some point during the file deletion process a prompt box will appear asking if executable files should be deleted. Click on the Yes to All button.
5. When the file deletion progress window disappears, the original installation has been deleted and disc storage space has been recovered.

Deleting Using Windows 3.11
1. Open the FILE MANAGER program.
2. Locate and click on the backup folder and then click on EDIT ⇒ DELETE.
3. A file deletion confirmation window will appear. Click on the Yes button.
4. When the file deletion progress window disappears, the original installation has been deleted and disc storage space has been recovered.
Users Guide

_Doors_ is designed to make the access control system configuration and operation as simple as possible. This is done by breaking the configuration and operation processes into logical sections. Each section is responsible for a specific operation; whether it is entering information regarding how some aspect of the system is to be used or physically performing some operation.

The Users Guide is written for the novice user, learning how to navigate the Doors software menus and how to use the commands within the menus. The Users Guide presents the configuration and operation process in a recommended order of implementation. An operator can configure the system in almost any order, but the order described in the Users Guide provides the most sequential and complete path for the first time installer and for a new installation. Generally speaking, each section of the Users Guide builds upon what has been completed in the previous section.

To present this information, the Users Guide provides "real-world" examples of a new installation for a small company in an order that logically builds a complete access control database. By using real-world examples, this Users Guide will reveal the extensive power and simplicity of the Doors software.

The scenario for these real-world examples consists of a small building with 4 controllers controlling 5 doors. Figure 1 provides a floor-plan of this building. Access control will be provided for three exterior doors and for two interior doors. The people working in this building have a variety of jobs: manufacturing, stockroom, sales, technical, janitorial, management, so the time of access and area of access requirements differ depending upon the personnel.

Older revisions of Doors software and controller firmware do not have all the features described in this Users Guide. This Users Guide is written to describe the capabilities of the current Doors software and controller firmware, and might not accurately reflect the capabilities of previous software/firmware revisions.
Users Guide Conventions

There are certain conventions the Users Guide follows for presenting information and for indicating when an operator needs to perform an action on the computer.

Folder or directory names are identified in the text as "folder/subfolder."

Locating an item under a pull-down menu is identified as Menu Option ⇒ Sub-Menu Option.

Program names are identified in all UPPER-CASE.

Information to be typed by an operator is identified in Boldface.

If a button is clicked to perform an operation, the button icon is displayed or the button name is shown in Boldface.
Operation notes are shown in *italics*. These are things of which to be aware while using the Doors software.

⚠️ Items that require special attention or that can dramatically affect the access control network are prefaced with a caution sign.

**Windows Conventions**

*Doors* is a fully compliant *Windows* program; providing complete operability in *Windows* and allowing its program window to be opened, closed, resized, and multi-tasked as any other *Windows* compliant program. Please refer to the help file within the *Windows* operating system for information on working in *Windows*.

**On-Line Help**

To assist the end user there is a "point-and-tell" on-line help file in the *Doors* software. Once in the help file, simply point and click on a menu option, command, or selection and a description of that item is displayed. To call-up the help file when in the *Doors* program,

Click on the Help/Contents pull-down menu or click on the button on the *Doors* tool bar (see the Tool Bar section under *Introducing the Desk Top*) to open the help file.

**The Order of Operation**

This section provides a summary of the major sections in the order that they are presented in the Users Guide.

**Logging On the *Doors* Program**

Each operator has a unique log on password that allows the *Doors* program to identify the operator logging on to the program and to track the actions the operator takes while logged on.

**Setup and Verify Network Communication**

The setup and verify network communication section describes the process for configuring the *Doors* operating parameters to meet those of the host computer and then verifying that basic communication is indeed happening between host computer and all the controllers on the access control network.

**Set Communication Parameters**

Four tasks are performed to set the *Doors* communication parameters.

1. Set the program’s COM port to match the host computer.
2. Set the program’s communication speed.
3. Set the remote phone number (for remote access via modem).
4. Restart the program to configure *Doors* with the communication parameters.

**Auto-Config**

The *Doors* program polls the access control network and receives information identifying which controllers are communicating on the network. It then inserts this information into the appropriate databases within the *Doors* program.
Set Time

The Doors program then needs to synchronize the time/date between the host computer and all controllers so that all events can be tracked correctly.

Perform Smart Update

The Doors program downloads default operating information to the access control network.

Get Controller Status

The Doors program polls the access control network and receives information regarding controller/door configuration. It then inserts this information into the appropriate databases within the Doors program. This is the quickest way to verify that all controllers/doors are recognized by the access control system.

Begin Database Programming

Database programming is where the day-to-day operating parameters for the access control system are entered.

Setup Operators

The setup operators commands allow for the creation of system operators and the assignment of operator privileges. It is the operators that will be performing the work: creating the databases required by the Doors software to do its job and monitoring the access control network once everything has been downloaded to the network.

Setup Time Zones

The setup time zones commands allow an operator to create the various daily time periods and holiday time periods to be applied to access groups, the auto unlock/lock door function, and for input/output operations.

Setup Doors

The setup doors commands allow an operator to define the configuration and operation parameters for all the controllers/doors on the access control network.

Setup Access Groups

The setup access groups commands allow an operator to combine time zones and doors into a superset of information that is applied to cardholders. In conjunction with time zones, access groups allow an operator to define which doors an employee is allowed to use at what times.

Setup Cards

The setup cards commands allow an operator to enroll cards into the system and enter cardholder information, and to void cards from the system. Each cardholder has a card that identifies that individual to the access control network. When a cardholder presents a card to a reader requesting access, information associated with the card is compared to information in the databases stored at the controller to determine if that cardholder should be allowed access through that door.

Setup Monitor Windows

The setup monitor window commands allow an operator to configure up to three different monitoring windows to allow filtered, real-time tracking of events on the access control network.
Download Information to the Network
The download information to the network command allows an operator to download information from the program database to the access control network. This information is used by the controllers in the network to run the access control system.

System Operation
The system operation commands allow an operator to manually, immediately perform specific functions such as:

- unlock and lock doors
- monitor and collect events from controllers
- override regularly programmed door controls
- create and view event reports

Advanced Features
The Doors program is capable of several advanced features that expand the program’s capabilities. These features include:

- Remote communication with one or more access control networks via modems.
- I/O control – the linking of input events to drive output responses (i.e. an input connected to a vibration sensor on a window that is linked to an alarm output so that a broken window will sound an alarm).
Logging On

The first step is to start the Doors program and log onto the system. In normal operation, the log on process identifies to the software which operator is entering the program. With this identification, the program is able to limit the operator’s actions to those that operator has been approved to perform.

Starting the Doors Program

For both Windows 95 and Windows 3.11, there are several ways to start the Doors program. The easiest, most common methods are described below.

Starting the Program in Windows 95

1. From the Windows 95 Task Bar.
   - Click on the Start button. A pop-up menu of commands appears.
   - Click on the Programs menu option. A pop-up menu of program folders appears.
   - Click on the Kerisys program folder. A pop-up menu of programs appears.
   - Click on the Doors program icon.
   - The program now begins.

2. Using WINDOWS EXPLORER.
   - Run the WINDOWS EXPLORER program.
   - Locate the DOORS.EXE program (it is typically found under the "\kerisys\doors" folder.
   - Either double-click on the DOORS.EXE program icon or click on the File ⇒ Open pull-down menu.
   - The program now begins.

3. Using WINDOWS EXPLORER to create a Windows desk top shortcut.
   - Run the WINDOWS EXPLORER program.
   - Locate the DOORS.EXE program (it is typically found under the "\kerisys\doors" folder.
   - Click on the DOORS.EXE program icon. It should now be highlighted.
   - Either click on the File ⇒ Create Shortcut menu option or right-click on the DOORS.EXE program icon, scroll down the list of menu options, and select the Create Shortcut option.
   - A new file is created titled "Shortcut to Doors.exe".
   - Click on the "Shortcut to Doors.exe" icon and then click on either File ⇒ Copy or right-click on the "Shortcut to Doors.exe" icon, scroll down the list of menu options, and select the Copy option.
   - Close the WINDOWS EXPLORER program and click on the main Windows desk top.
   - Right-click the mouse, scroll down the list of menu options, and select the Paste option. The new icon for the Doors program will be placed on the desk top.
   - This icon will now appear on the desk top every time the Windows program is entered. Simply double-click on the icon to start the Doors program.
**Starting the Program in Windows 3.11**

1. Run the program from the Doors program group.
   - Locate the Doors program group on the main window.
   - Double-click on the Doors program group icon. A window will open with icons for all the programs within the Doors program group.
   - Locate the DOORS.EXE program icon.
   - Double-click on the DOORS.EXE program icon.
   - The program now begins.

2. Using FILE MANAGER.
   - Run the FILE MANAGER program.
   - Locate the DOORS.EXE program (it is typically found under the "kerisys\doors" subdirectory.
   - Either double-click on the DOORS.EXE program listing or click on the File ⇒ Open pull-down menu.
   - The program now begins.

**System Logon**

Once the program begins, it will prompt for an operator Logon (see Figure 2). This is an identifying name and password for the operator entering the program. The first time the program is entered, the default Logon information must be used. Until changed, the default password provides access to everything in the Doors program. Later in the Doors configuration process, each authorized operator is assigned identifying names and passwords.

![Logon Screen](image)

Figure 2 – Logon Screen

To logon the program:

1. Click in the Name box, type **Keri** and press **ENTER**.
2. Click in the Password Box, type **Keri**. Asterisks will appear in the password box instead of letters so that someone looking over your shoulder during Logon cannot steal your password.
3. Press **ENTER** or click on the **OK** button.

The program will now verify the user name and password. If both are correct, the Logon window disappears allowing access to the Doors program. If either are incorrect, the user name and password fields are cleared and the Logon window remains. To leave the Logon process and return to Windows, for Windows 95 click on the **X** box in the upper-right corner of the Logon window, for Windows 3.11 click on the File ⇒ Exit pull-down menu option.
NOTE: The operator name and password are both case sensitive. That is, the program differentiates between UPPER CASE and lower case in both the operator name and password. Please keep this in mind when creating operator names and passwords for your operators, and when entering your operator name and password to log onto the program.

Network Update

The first time the program is started a "Network Update" window appears (see Figure 3). The Network Update window indicates first-time communication between the Doors program and the access control network has not yet been made.

![Network Update Screen](image)

Figure 3 – Network Update Screen

In the future, whenever starting the program, this window appears if a change has been made to any Doors database that has not yet been sent out to the access control network. This window serves as a reminder that changes in the database are not physically implemented in the access control network until they have been uploaded to the network.

Click on the OK button to enter the Doors desk top.
This page is intentionally left blank.
Introducing the *Doors* Desktop

Every task in *Doors* is begun from the desktop. Navigating the desktop is simply a matter of using the mouse to point and click on items, and entering appropriate information when needed.

The Desktop

There are eight fields on the *Doors* desktop (see Figure 4).

![Doors Desktop Diagram](image)

**Figure 4 – The Doors Desktop**

1. **Window Title Bar** – On the left side of the title bar is the name of the program operating the window; on the right side are the *Windows* control boxes for minimizing or maximizing the window and for immediately closing the program (refer to *Windows*’ online help for detailed information on using these boxes).

2. **Menu Bar** – A list of the pull-down menus in the *Doors* program is displayed on the menu bar. The menu bar is used for accessing all programming and configuration tasks. Future chapters in this manual provide all the details for using all the commands in the menu bar. Each pull-down menu option has an underlined letter. To quickly access a menu option, press the ALT key followed by the underlined letter. Sub-menus also have underlined letters and can be accessed in a similar manner. For example, to access the Setup ⇒ System pull-down menu option press **ALT S S**.

3. **Tool Bar** – The tool bar is a collection of tool buttons for the most used functions in the *Doors* program. Clicking on a tool button immediately opens a function’s window. A summary of what functions are available on the tool bar appears in the Tool Bar section below.

4. **Task Field** – When a task is begun by a selection from the menu bar or the tool bar, a window will appear within this field to manage whatever is necessary to perform this task. Multiple task windows can be open simultaneously within the task field. Each window in the task field will have its own title bar identifying the window. The title bar of the active task in the task field is highlighted.
5. Status/Help Box – The status/help box provides a short description of the active task in the task field.

6. Monitor Indicator Box – The monitor indicator box displays if a system monitor is enabled, meaning real-time data collection is being done by the Doors program of events from the access control network.

7. Date Box – The date box displays the date kept by the host computer.

8. Time Box – The time box displays the time kept by the host computer.

The Tool Bar

The tool bar is a collection of tool buttons for the most used functions in the Doors program (see Figure 5). Clicking on a tool button immediately opens a function’s window. Placing the mouse cursor on top of a tool button displays the name of that button beside the mouse cursor.

![Figure 5 – The Tool Bar](image)

On-Line Help

On-line help is built into the Doors program. To access on-line help, click on the on the tool bar or click on Help ⇒ Contents. A new window appears providing brief descriptions of every feature in the Doors program. On-line help places assistance for using the Doors program at your fingertips.

Once in on-line help, simply "point and click" on the item you have a question about. If the item is nested under a pull-down menu, click on the menu item and follow your way down the menu tree until you locate the item. Once you’ve found the item, click on it and a brief description will appear.

When finished, for Windows 95 click on the box in the upper-right corner of the help window. For Windows 3.11, click on File ⇒ Exit pull-down menu option.
NOTE: When using on-line help, you may consider resizing the Doors program window to take up half of the computer screen and then resizing the on-line help to take up the other half of the computer screen. This allows you to jump back and forth between the program and the on-line help, tracking down assistance for nested items.

Exiting a Doors Window

Whenever changes are made to the data in a window, these changes must be saved by clicking on the button before exiting the window, or the data is lost and must be re-entered. Once saved, the access control network must be updated with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

Exiting in Windows 95

Click on the File ⇒ Exit pull-down menu option or click on the box in the upper-right corner of the window to exit any window in the program at any time.

Exiting in Windows 3.11

Click on the File ⇒ Exit pull-down menu option to exit any window in the program at any time.
This page is intentionally left blank.
Setup/Verify Network Communication

The Setup/Verify Network Communication section describes the process for configuring the Doors communication parameters to meet those of the host computer and then verifying that basic communication is indeed happening between the host computer and all the controllers on the access control network.

Set Communication Parameters

The following tasks are described in this section. All four tasks must be performed to properly set the communication parameters.

- Set the COM port.
- Set the communication speed.
- Set the modem parameters (if the access control network requires modems for remote access).
- Save the communication parameters and restart the program to configure Doors.

Set the COM Port

The COM port that is used for communication between the host computer and the access control network must be identified.

1. Click on the Setup ⇒ System pull-down menu or click on the button on the tool bar.
2. The first time the Setup menu is entered (and every time until system configuration is complete) the Setting Up The System window will appear as a reminder that system configuration needs to be performed (see Figure 6).

![Figure 6 – Setting Up The System Reminder](image)

3. Click on the button. The Setup/System window appears (see Figure 7).
4. Click on the **System Configuration** tab. The System Configuration window appears (see Figure 8).

![System Configuration Window](image1)

**Figure 8 – System Configuration Window**

5. Use the pointing device and click on the COM port radio button (1, 2, 3, or 4) corresponding to the COM port that will be used for communication between the host computer and the access control network.

**Set the Communication Speed**

6. Verify the communication speed is set at 9600. If it is not, click on the **9600** radio button.

![Setup System Window](image2)
NOTE: The other communication speed options are reserved for future applications. If a different communication speed is selected, the Doors program might not communicate correctly.

7. If this is a direct connect connection using a cable between the host computer and the master controller in the access control system, skip to the Save the Communication Parameters section below.

Set the Modem Parameters

8. If this is a modem connection, the modem parameters must be entered.
9. Click in the "PC Phone Number" field, and enter the phone number for the modem attached to the host computer. For example, type 555-1111.
10. If the site should be assigned a PIN, click on the "PIN Number" (Personal Identification Number) field and enter the PIN to be used for the remote site. This is an optional field.

NOTE: Once a PIN has been assigned to a site, an operator must know that site’s PIN to be able to access that site. This is an extra security measure to ensure that an operator has authorization to access any given site.

11. Click on the "Modem Init String" field and enter the modem initialization string for the PC's modem. As the modem initialization string differs per modem type and manufacturer, refer to the modem's manual for the initialization string.
12. Click on the "Remote Site Phone Number" field and enter the phone number for the modem attached to the master controller at the remote site. For example, type 555-9999.

Save the Communication Parameters

13. When all information is entered/verified, click on the button and the new configuration information is saved to a configuration file. If the new communication parameters are not saved before clicking any other button or exiting the setup communication parameters window, the data entered is lost and must be re-entered.
14. Now the Doors program must be exited and restarted for the new communication parameters to take effect. To exit the Doors program use your pointing device and click on the File ⇒ Exit pull-down menu option. Now start the Doors program per the instructions in the Logging On section above. The new communication parameters now take effect and the program is ready to communicate with the access control network.

Auto-Config

The Auto-Config command is used to automatically retrieve controller/door configuration information from the access control network and insert that information into the appropriate databases within the Doors program.

1. Click on the Setup ⇒ System pull-down menu or click on the button on the tool bar.
2. Click on the Controllers tab. The Setup/System window appears (see Figure 9).
Figure 9 – Auto-Config System Controllers

3. Per the instructions in the Start-Up Checklist, the PXL-250 Quick Start Guide, or the PXL-250 Technical Reference, ensure the access control network has been powered on properly.

4. Click on the button. The Net Communication window appears as communication is being established.

Figure 10 – Connecting to the Network

5. Once communication has been established, the Autoconfiguration window appears indicating data is being transferred from the network to the host computer.
Successful Auto-Config

1. When all data is received by the host computer, the System/Setup/Controllers window displays the configuration information for all responding controllers on the access control network.

Failed Auto-Config

1. If the host computer cannot establish communication with the access control network, the Network Error window appears.
2. Click on the button and the Autoconfig Error window appears.

![Autoconfig Error Window](image)

Figure 14 – Auto-Config Error

3. Click on the button.
4. Verify the following items.

- The communication parameters in the "System Configuration" tab are correct.
- The Doors program was restarted to recognize the communication parameters.
- The communication connections are fully operational (COM port and modems as applicable).
- If the previous three suggestions do not resolve the problem, please refer to the PXL-250 Troubleshooting and Diagnostics reference document (Keri part number 01841-001) to verify controller and cabling operations.

**Set Controller Time and Date**

The set time and date command is used to synchronize the time and date between the host computer and all the controllers on the access control network. Before synchronizing the host computer and the controllers, look at the date and time listed at the bottom of the Doors window. This is the date and time of the host computer. Be sure these values are correct. If they are not correct, change them per the instructions given in the Setting the Host Computer Date and Time section above. If they are correct, perform the following steps.

1. Click on the Setup ⇒ System pull-down menu or click on the icon on the tool bar. The Setup/System window appears.
2. Click on the Controllers tab. The Controllers window appears (see Figure 15).
3. Click on the button. After a brief pause, the Set Network Time And Date window appears.

![Figure 15 – Controllers Window: Set Time Button](image)

Figure 15 – Controllers Window: Set Time Button

4. The time and date kept by all controllers now matches that of the host computer. Click on the button.

![Figure 16 – Setting Network Time and Date](image)

Figure 16 – Setting Network Time and Date

Network Update – Default Parameters

The Doors software now needs to download default operating parameters to all controllers on the access control network.

1. Click on the icon on the tool bar. A series of windows similar to Figure 17 will appear as the program collects the default database parameters to be sent to the access control network.
2. Once all parameters are collected, the host computer connects to the access control network (if it isn’t already connected). The Net Communication window appears as the connection is made (see Figure 18).

3. Once the connection is made a series of windows similar to Figure 19 appears indicating data is being transferred from the host computer to the access control network.

NOTE: Once the update process has begun, please be patient. The update process can take anywhere from several seconds to several minutes depending upon the amount of information to be updated and the number of controllers receiving information.

4. When these windows disappear, the access control network has received all default operating parameters and is ready for basic operation.
Get Controller Status

The get controller status command allows an operator to verify that all controllers/doors are recognized and to verify that the configuration information reported by the controller is correct.

Get Status For All Controllers

1. Click on the Setup ⇒ System pull-down menu or click on the button on the toolbar.
2. Click on the Controller Status tab. The Controller Status window appears (see Figure 20).

3. Click on the button. All controllers are polled for their configuration and status, and this information is entered into the Controller Status spreadsheet (see Figure 21).
Figure 21 – Received Controller Status

4. Each line of this spreadsheet corresponds to a controller/door. Verify the information displayed in the spreadsheet matches the configuration of the installed controllers. The following list describes the fields in the spreadsheet that should be verified at this time.

**Door Name**
A descriptive text name for the door (this field should be blank as the door name is assigned later in the database programming process).

**Address**
The address of each controller recognized by the network and each door recognized by the controller. There should be a line item in the spreadsheet for every controller/door in the access control network. The addresses listed should match the addresses programmed into each controller on the access control network.

**Online**
Indicates if the controller is ONLINE (the host computer is able to communicate with the controller) or OFFLINE (the host computer is not able to communicate with the controller).

**Cltr Type**
- If the field displays a PXL-250, this indicates the controller is a PXL-250 without a satellite board, capable of single-door control.
- If the field displays an SB-293D, this indicates the controller is a PXL-250 with a satellite board that is configured to support two-door control, and has 6 inputs and 2 outputs.
- If the field displays an SB-293X, this indicates the controller is a PXL-250 with a satellite board that is configured to support 8 inputs and 4 outputs.
- If the field displays a PXL-100, this indicates the controller is a PXL-100 smart controller.

**ROM Rev**
Displays the revision of the firmware ROM on the controller.
RAM Config
Displays the size of the RAM on the controller (the size of the RAM directly controls the number of cards that can be programmed into the controller and the number of events that can be stored by the controller).

Events
Displays the number of events currently stored in the controller.

Cards In Use
Displays the number of cards programmed into the controller (this field should be blank as the card programming process is done later in the database programming process).

Date
Displays the date kept by the controller when controller status was requested.

Time
Displays the time kept by the controller when controller status was requested.

The remaining fields in the Controller Status spreadsheet are not valid until the access control database has been completely configured and downloaded to the controllers. The remaining fields relate to either the performance of the controller over time or to controller/door programming information that is done later in the database programming process. At this time, they all have initial or default values.

Get Status For One Controller
If work has been performed on one controller in the access control network (such as replacing or resetting the controller, changing the firmware, or changing the controller’s configuration), that one controller can be polled for its status. Polling one controller saves time by not polling the status of the other controllers in the access control network.

1. Click on the Setup ⇒ System pull-down menu or click on the button on the tool bar.
2. Click on the Controller Status tab. The Controller Status window appears (see Figure 20).
3. Scroll up and down the list of controllers and locate a controller for which status is needed. Click in the Address cell for that controller (see Figure 20).
4. Click on the button. The selected controller is polled for its configuration and status, and this information is entered into the Controller Status spreadsheet (see Figure 21).
5. Verify the information displayed in the spreadsheet matches the configuration of the controller. Refer to the above list for explanations of the fields in the spreadsheet that should be verified at this time.
This page is intentionally left blank.
Database Programming

The database programming section describes the process for entering the day to day operating parameters for the access control network. This section describes the following operations.

- Setup Operators
- Setup Time Zones
- Setup Doors
- Setup Access Groups
- Setup Cards
- Setup Monitor Windows

Setup Operators

This section describes the process for creating system operators and assigning operator privileges.

It is the operators who will be performing the work, creating the databases required by the Doors software to do its job and monitoring the system once everything has been downloaded to the controllers. Every operation performed by an operator has an operator identification number attached to it. This allows for tracking of operator performed changes.

Since the default operator has access rights to every operation, anyone who knows the default operator name and password could have complete programming access. Keri Systems recommends, at a minimum, changing the default password to protect your access control network.

Editing the Default Operator

1. Click on the Setup ⇒ Operators pull-down menu. The Setup Operators window appears (see Figure 22).

![Setup Operators Window](image)

Figure 22 – Setup Operators Window
2. As recommended above, the default operator will be edited and assigned to the system supervisor. The supervisor will need the ability to perform any and every action within the Doors program. Leave every radio button option on Yes so that the supervisor will have full access to all program options.

3. Double-click in the "Name" field. The "Keri" name is highlighted. Type a descriptive name for the operator being assigned Operator Number 1 (the default operator). For this example, type Sys Supervisor.

NOTE: There is a 15 character maximum for the operator name.

4. Double-click in the "Password" field. For the Password, enter a string of characters or numbers, 4 characters minimum to 8 characters maximum, case sensitive (that is, the program does keep track of upper-case versus lower-case characters). The password should be something easily remembered by the operator, but not easily guessed by unauthorized personnel. For this example, type AbCd1234.

5. To ensure that the password entered is correct, it must be entered again in the "Retype Password" field. The characters entered into the "Retype Password" field must exactly match the Password field. If not, the password is rejected (see Figure 20) and the program will prompt you to re-enter them. Double-click in the "Retype Password" field. For this example, again type AbCd1234.

![Password Error](image)

Figure 23 – Password Error

6. Click on the button to save these changes. If the operator changes are not saved before clicking any other button or exiting the setup operators window, the data entered is lost and must be re-entered.

Creating a New Operator

The following list are the feature operation rights available for assignment to an operator (refer to Figure 22). Each operator must be created and saved, one-at-a-time.

**Setup Cards**
Identifies if an operator is allowed to perform the Setup Cards commands: enrolling, entering data, voiding, deleting, assigning access groups, or to have Read Only access to review this information.

**Setup Doors**
Identifies if an operator is allowed to perform the Setup Doors commands: entering or editing the parameters by which a door/controller operates, or to have Read Only access to review this information.
Setup Timezones
Identifies if an operator is allowed to perform the Setup Timezone commands: creating or editing Timezones and Holiday schedules, or to have Read Only access to review this information.

Setup Access Groups
Identifies if an operator is allowed to perform the Setup Access Group commands: creating or editing access groups (specifically associating timezones with doors), or to have Read Only access to review this information.

Setup Monitor
Identifies if an operator is allowed to modify a Monitor window (a window that views events on the access control network as they happen), or to have Read Only access to review this information.

Setup Operators
Identifies if an operator is allowed to create new operators.

Operate Doors
Identifies if an operator is allowed to manually lock and unlock doors using program commands and to perform complete database updates of selected controllers on the access control network.

Start Monitor
Identifies if an operator is allowed to start the event monitoring process.

Stop Monitor
Identifies if an operator is allowed to stop the event monitoring process.

Start Monitor #1, #2, #3
Identifies which of the three definable event monitors an operator may open.

Card Reports
Identifies if an operator is allowed to generate Card reports (this feature is not yet available).

Door Reports
Identifies if an operator is allowed to generate Door reports (this feature is not yet available).

Event Reports
Identifies if an operator is allowed to generate Event reports (summaries of events that have occurred on the access control network).

Exit Program
Identifies if an operator is allowed to exit the Doors program, returning to the operating system.

NOTE: Exiting the program does not end the access control process. Once all information is entered and uploaded to all controllers, the controllers manage access by themselves and the Doors program is only needed for uploading changes to the controllers or downloading event information from the controllers.

Depending upon the assignment choice, each Operator assignment is set to one of these three values.
NO
The operator does not have operation rights.

YES
The operator does have operation rights.

RO
The operator has read-only operation rights – the operator can view, but not make any changes to this operation.

Do a little pre-planning before assigning operator operation rights.

• Determine how many operators are needed to cover operation of the access control system.
• Determine the requirements and responsibilities of these operators.
• Use the above list and determine which operators should have which responsibilities.

1. Click on the buttons to scroll up and down the list of available operator slots and locate an operator slot that is unassigned (there are 32 operator slots).
2. Assign an operator name and password.
3. For each operator option on the screen, click on the radio button that corresponds to the operator’s responsibilities being granted for that option (NO, YES, RO).
4. Click on the button to save these changes. If the operator changes are not saved before clicking any other button or exiting the setup operators window, the data entered is lost and must be re-entered.
5. Repeat this process for each operator to be assigned.
Setup Time Zones

The setup time zones section describes the process for defining the daily and holiday access time periods to be applied to doors in access groups and to automatic door locking/unlocking control. A time zone is defined as the hours-of-the-day when an employee is granted access to a secure area.

Up to 32 time zones can be defined. For each day-of-the-week and for up to three holiday schedules, there are four separate start/stop periods that can be programmed. This provides maximum flexibility in setting time zone work schedules for the cardholders using the access control system.

This section provides examples of time zones for a day-shift employee, a janitorial employee, a grave-shift employee, and one holiday schedule.

Before defining time zones, take some time and map out all the time zone usage possibilities for the site. Consider the variety of access hours for employees and customers, and consider special requirements such as janitorial personnel (may require late night access), service/repair personnel (may require all hours access), supervisory/management staff (may require extended hours access), and shift personnel (first/day, second/swing, third/grave, flex).

NOTE: All time values used and stored by the Doors program are in 24-hour format. For example: midnight is stored as 00:00 hours, 8 A.M. is stored as 08:00 hours, noon is stored as 12:00 hours, 6 P.M. is stored as 18:00 hours, and 11:30 P.M. is stored as 23:30 hours.

NOTE: The use of descriptive names when naming time zones and access groups can make the report viewing process easier, but keep in mind that time zones and access groups tend to be assigned similar names. It can be helpful to use TZ and AG as a prefix or suffix when assigning names to make the distinction between time zone and access group easier.

Day-Shift Time Zone Example

The instructions in the section create a time zone that is designed for a day-shift employee, eligible to work an 8 hour shift at any time within the day-shift time zone.

1. Create a list of the days-of-the-week and the hours-of-the-day when an access group should allow access for this time zone.

   • Monday through Friday – 06:00 to 20:00 hours
   • Saturday – 08:00 to 18:00 hours
   • Sunday – no access allowed
   • Holidays – 08:00 to 12:00 hours

2. Click on Setup ⇒ Timezones or click on the icon on the tool bar. The Setup Timezones window appears (see Figure 24).
The following is a list of the fields in the time zone window.

**Timezone Tab**
Displays the day-of-the-week / hours-of-the-day spreadsheet window.

**Holiday One, Two, Three Tabs**
Displays the holiday date/holiday name spreadsheet windows.

**Day-of-the-Week – Start/Stop Spreadsheet**
The access time period information is entered into these cells.

**New Button**
Clears the spreadsheet in preparation for new data entry.

**Save Button**
Saves the spreadsheet information.

**Delete Button**
Deletes the time zone named in the "Timezone Names" field, removing its information from the time zone database.

**Keys Field**
Identifies three pre-defined cell values: Always, Never, and Unused. Click on a cell and type the first letter of the key word (A, N, U). An Always cell always allows access on that day-of-the-week. A Never cell never allows access on that day-of-the-week. An Unused cell (used on the holiday schedules only) indicates that holiday schedule is undefined.

3. Click on the button. The day-of-the-week start fields and the time zone name field are cleared and the Cleared Time Zone window appears (see Figure 25).
4. Following the day-shift parameters given above, no access is allowed on Sunday. Double-click in the Sunday Start1 cell and type N. The "Never" key appears in the cell setting this time segment to never allow access on Sunday.

5. Double-click in the Monday Start1 cell and type 06:00.

**NOTE:** When you double-click in a cell, a spinner icon appears. If you click on the hour side of the time (00:00), you can use the spinner to advance the hours forward or backward to select the desired hour. If you click on the minute side of the time (00:00), you can use the spinner to advance the minutes forward or backward to select the desired minute. You may find this method easier to set the time instead of directly typing the information into the cell.

6. Double-click in the Monday Stop1 cell and type 20:00.

7. Repeat steps 5 and 6 for the Tuesday through Friday Start 1 cells and Stop1 cells.

8. Double-click in the Saturday Start1 cell and type 08:00.

9. Double-click in the Saturday Stop1 cell and type 18:00.

10. Double-click in the Hol1 Start1 cell and type 08:00.

11. Double-click in the Hol1 Stop1 cell and type 12:00.

12. Click in the "Timezone Names" field and type Day Shift.

13. For this example, the time zone window should appear identical to Figure 26. Any discrepancies can be corrected by clicking on the cell or field and making the correction.
14. Once everything has been verified as correct per the time zone list, click on the button. If the time zone is not saved before clicking any other button or exiting the time zone window, the data entered is lost and must be re-entered.

15. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Janitorial Shift Time Zone Example**

The instructions in this section create a time zone that is designed for an janitorial staff employee, eligible to work a four hours a night, three times a week.

1. Create a list of the days-of-the-week and the hours-of-the-day that an access group should have access for this time zone. The following list describes this janitorial shift time zone.
   
   - Sunday, Tuesday, and Thursday – 18:00 to 22:00 hours

2. Click on Setup ➔ Timezones or click on the icon on the tool bar. The Time Zone window appears (see Figure 24).

3. Click on the button. The day-of-the-week start fields and the time zone name field are cleared and the Cleared Time Zone window appears (see Figure 25).

4. Following the janitorial shift parameters given above, no access is allowed on Monday, Wednesday, Friday, and Saturday. Double-click in the Monday Start1 cell and type N. The "Never" key appears in the cell setting this time segment to never allow access on Monday. Repeat this step for the Wednesday, Friday, and Saturday Start1 cells.

5. Double-click in the Sunday Start1 cell and type 18:00.

6. Double-click in the Sunday Stop1 cell and type 22:00.

7. Repeat steps 5 and 6 for the Tuesday and Thursday Start 1 and Stop1 cells.

8. Click in the "Timezone Names" field and type Janitorial Shift.

9. The time zone window should appear similar to Figure 27. Any discrepancies can be corrected by clicking on the cell or field and making the correction.

![Figure 27 – Janitorial Shift Time Zone](image-url)
10. Once everything has been verified as correct per the time zone list, click on the button. If the time zone is not saved before clicking any other button or exiting the time zone window, the data entered is lost and must be re-entered.

11. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

### Grave Shift Time Zone Example (Crossing Midnight)

The instructions in the section create a time zone that is designed for a graveyard shift employee, eligible to work from 11:30 P.M. to 7:30 A.M. Monday/Tuesday through Friday/Saturday.

The grave shift time zone is unique in that it starts in one day-of-the-week and ends in the next day-of-the-week. To accommodate this, the time zone uses both the Start1/Stop1 and Start2/Stop2 cells to cover the split in access times Tuesday through Friday.

1. Create a list of the days-of-the-week and the hours-of-the-day that an access group should have access for this time zone. The following list describes this grave shift time zone.

   - Monday – 11:30 to Tuesday – 07:30 hours
   - Tuesday – 11:30 to Wednesday – 07:30 hours
   - Wednesday – 11:30 to Thursday – 07:30 hours
   - Thursday – 11:30 to Friday – 07:30 hours
   - Friday – 11:30 to Saturday – 07:30 hours

2. Click on Setup ⇒ Timezones or click on the icon on the tool bar. The Time Zone window appears (see Figure 24).

3. Click on the button. The day-of-the-week start fields and the time zone name field are cleared and the Cleared Time Zone window appears (see Figure 25).

4. Following the grave shift parameters given above, no access is allowed on Sunday. Double-click in the Sunday Start1 cell and type \(N\). The "Never" key appears in the cell setting this time segment to never allow access on Sunday.

5. Double-click in the Monday Start1 cell and type \(23:30\). Double-click in the Monday Stop1 cell and type \(00:00\). Monday access is limited to the hours between 23:30 and 00:00.

6. Double-click in the Tuesday Start1 cell and type \(00:00\). Double-click in the Tuesday Stop1 cell and type \(07:30\). Double-click in the Tuesday Start2 cell and type \(23:30\). Double-click in the Tuesday Stop2 cell and type \(00:00\). Tuesday access is split between 00:00 to 07:30 (to cover the end of the shift that began on Monday) and 23:30 to 00:00 (to cover the beginning of the shift on Tuesday).

7. Repeat step 6 for Wednesday through Friday.

8. Double-click in the Saturday Start1 cell and type \(00:00\). Double-click in the Saturday Stop1 cell and type \(07:30\). Saturday access is limited to the hours between 00:00 and 07:30.

9. Click in the “Timezone Names” field and type Grave Shift.

10. The time zone window should appear similar to Figure 28. Any discrepancies can be corrected by clicking on the cell or field and making the correction.
11. Once everything has been verified as correct per the time zone list, click on the button. If the time zone is not saved before clicking any other button or exiting the time zone window, the data entered is lost and must be re-entered.

12. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Holiday Schedules**

Holidays are treated as if they are just another day of the week. This allows holidays to have access time periods applied to them. Three holiday schedules are available for definition. This allows certain holidays to have different access times than others do. For example, on holidays such as Presidents’ Day or Martin Luther King’s birthday government offices are closed but many businesses remain open; on holidays such as Christmas or Thanksgiving virtually all business and government offices are closed. An access control network might need to assign holiday access times differently for these two types of holidays.

Before defining holiday schedules, take some time and map out all the holiday possibilities for the site. Consider the relative importance of the holiday and determine if multiple holiday schedules are required.

**NOTE:** Certain holiday dates change from year-to-year (i.e. Easter or Thanksgiving). Operators should review and update the holiday schedules prior to the beginning of a new year to ensure proper holiday coverage.

The following is an example of a possible holiday schedule.

1. Create a list of the holiday names and dates that should be applied to time zones. This list can crossover to the following year.
2. Click on Setup ⇒ Timezones or click on the 🕒 icon on the tool bar. The Time Zone window appears (see Figure 24).

3. Click on the Holiday One tab. The Holiday One window appears (see Figure 29).

![Figure 29 – Holiday One Entry Window](image)

4. Click on the Dates/1 cell and type **01/01/1998**. Click on the Names/1 cell and type **New Year’s Day**.

**NOTE:** When you double-click in a cell, a spinner icon will appear. If you click on the month side of the date (00/00/00), you can use the spinner to advance the month forward or backward and select the desired month. If you click on the day side of the date (00/00/00), you can use the spinner to advance the day forward or backward and select the desired day. If you click on the year side of the date (00/00/00), you can use the spinner to advance the year forward or backward and select the desired year. You may decide to use this method to set the date instead of directly typing the information into the cell.

5. Working down through the spreadsheet, repeat step 4 for each holiday on the above list.

6. When complete, the holiday one schedule should appear similar to Figure 30. Any discrepancies can be corrected by clicking on the cell or field and making the correction.
7. Once everything has been verified as correct per the holiday list, click on the button. If the holiday one schedule is not saved before clicking any other button or exiting the holiday window, the data entered is lost and must be re-entered.

8. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Display/Edit a Time Zone**

The following instructions explain how to review or edit the contents of a time zone.

1. Click on Setup ⇒ Timezones or click on the icon on the tool bar. The Time Zone window appears (see Figure 24).
2. Click on the arrow in the Timezone Names field. A list of all saved time zones is displayed.
3. Scroll up and down the list until the desired time zone is located.
4. Click on that time zone name and the time zone is displayed in the spreadsheet.
5. Review the data displayed. If any edits need to be made, click in the cell needing editing and type the new value for that cell.
6. Once edits have been made, click on the button. If the edits are not saved before clicking any other button or exiting the time zone window, the data entered is lost and must be re-entered.
7. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).
Delete a Time Zone

If a time zone becomes unneeded it can be deleted.

1. Click on Setup ⇒ Timezones or click on the icon on the tool bar. The Time Zone window appears (see Figure 24).
2. Click on the arrow in the Timezone Names field. A list of all saved time zones is displayed.
3. Scroll up and down the list until the desired time zone is located.
4. Click on that time zone name and the time zone is displayed in the spreadsheet.
5. Review the data displayed and verify this is the time zone to be deleted.
6. Click on the button and the time zone spreadsheet is cleared.
7. Once the deletion has been performed, click on the button. If the deletion is not saved before clicking any other button or exiting the time zone window, the deletion does not take affect and the time zone remains in the system.
8. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

NOTE: Once deleted, a time zone is not recoverable. If a time zone was deleted by mistake, it must be recreated.

NOTE: If a time zone is in use by the access control network, the Doors program will not allow it to be deleted. Review all access groups to ensure all references to the time zone to be deleted have been changed.
This page is intentionally left blank.
Setup Doors/Controllers

The setup doors/controllers section describes how to configure doors and controllers on the access control network. The following operations are performed in this section.

- set controller dial-out parameters
- assign a descriptive door name
- assign a door class
- enable/disable the reader associated with a door
- set a door’s unlock time
- set a door’s open time
- set a door’s unlock/lock time zone
- set a door’s first person in value
- set a door’s alarm output mode

Set Controller Dial-Out Parameters

The dial-out parameters define if a controller is allowed to automatically dial the host computer and upload its contents to the host computer when the controller’s event memory reaches a defined percentage of being full.

NOTE: These instructions configure the controller for dialing out, but the Doors software must also be configured to receive this information. This is done in the Enable/Disable Auto-Collection section found later in this user’s guide. Both steps must be done for proper uploading of information from a controller to the host computer/Doors software.

NOTE: When a controller dials the host computer to upload the contents of its buffer, it will only try to dial-out once. If it is not successful in making the connection with the host computer, it will not try again. It will wait for the next time the host computer connects with the controller and then will upload the contents of its buffer. If the buffer has filled prior to the host computer making contact with the controller, the oldest events in the buffer may be lost as the newest events overwrite the oldest events.

Enable Controller Dial-Out

1. To set the controller dial-out parameters, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Controllers tab. The Controllers window appears (see Figure 31).

![Controller Parameters](image)

Figure 31 – Controller Parameters
2. Scan down the controller addresses column and locate a controller that should have permission to dial the host computer.

3. Scan across that controller’s row in the spreadsheet and locate the **Dialout Enable** button. If the button is Red/OFF, controller dial-out is disabled.

4. To enable controller dialout, click on the **Dialout Enable** button. It will change color from red to green and the text in the "Threshold Percent" column should change color from grey to black. When this text is black, it is editable.

**Set the Dial-Out Threshold Percentage**

1. The default value for how full the controller’s memory should be before dialing out, is 80%. If this value should be changed (to 60%, for example), click in the corresponding "Threshold Percent" cell and type 60 (see Figure 32). When the controller’s event memory reaches 60% of full, the controller will dial the host computer and upload the contents of its event memory.

![Figure 32 – Enabled Controller Dial-out Parameters](image)

2. Once changes have been made, click on the **SAVE** button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

3. Now update the access control network with the new information. Click on the **Update** button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Disable Controller Dial-Out**

1. To set the controller dial-out parameters, click on the Setup ⇒ System pull-down menu or click on the **Controllers** tool bar button. Then click on the **Controllers** tab. The Controllers window appears (see Figure 28).

2. Scan down the controller addresses column and locate a controller that should have permission to dial the host computer.

3. Scan across that controller’s row in the spreadsheet and locate the **Dialout Enable** button. If the button is Green/ON, controller dial-out is enabled.

4. To disable controller dialout, click on the **Dialout Enable** button. It will change color from green to red and the text in the "Threshold Percent" column should change color from black to gray. When this text is gray, it is not editable.
5. Once changes have been made, click on the button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this user’s guide).

Assign a Door Name

The door name parameter allows an operator to assign a descriptive name to a door on the access control system. When monitoring system activity or reviewing event reports, it can be easier to follow a string of events if the door associated with the events has a descriptive name.

1. To assign a door name, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. The Setup Doors window appears (see Figure 33).

![Figure 33 - Setup Doors Tab - Part 1](image)

2. Scan down the controller/door addresses column and locate a door to be named.
3. Click on the "Door Name" cell corresponding to the selected controller/door address.
4. Type a descriptive name for that door. For example, based on the information given in Figure 1 in the Users Guide section, for controller C001/Door D1, type Emergency Exit.
5. Based on the remaining information in Figure 1, the following information can be entered.
   - C002/D1 – Front Door
   - C003/D1 – Manufacturing Door
   - C003/D2 – Stockroom Door
   - C004/D1 – Back Door
6. The resulting window should look similar to Figure 34.
7. Once changes have been made, click on the button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

8. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Assign a Door Class**

Door classes allow an operator to classify doors so that door commands can be performed on all doors within that class. Using the example from Figure 1 in the Users Guide section, this access control network could have three door classes: exterior doors, interior doors, and emergency doors.

With these classifications in place, an operator can perform commands on door classes such as manually locking/unlocking all doors within the door class or performing a complete database update of all controllers within the door class.

Before assigning door classes, take some time and map out all the door class possibilities for the site. Consider how doors with similar access responsibilities can be grouped together.

1. To assign a door class, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. Building off the previous section, the window found in Figure 34 appears.
2. Scan down the door name and controller/door address columns and locate a door to be assigned a door class.
3. Click on the "Door Class" cell corresponding to the selected controller/door.
4. Type a descriptive door class title for that door. For example, based on the information given in Figure 1 in the Users Guide section, for controller C001/Door D1-Emergency Exit, type Emergency Doors.

**NOTE:** In the door class cell is a drop-down arrow . If you click on the arrow, a list with all available selections will appear. Once a number of selections has been entered, you may decide to use this method to make a selection instead of directly typing the information into the cell.
5. Based on the remaining information in Figure 1, the following information can be entered.

- C002/D1-Front Door – **Exterior Doors**
- C003/D1-Manufacturing Door – **Interior Doors**
- C003/D2-Stockroom Door – **Interior Doors**
- C004/D1-Back Door – **Exterior Doors**

6. The resulting window should look similar to Figure 35.

![Figure 35 – Assigning Door Classes](image)

7. Once changes have been made, click on the **Save** button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

8. Now update the access control network with the new information. Click on the **Update** button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**NOTE:** In the door class cell is a drop-down arrow. If you click on the arrow, a list with all available selections will appear. Once a number of selections has been entered, you may decide to use this method to make a selection instead of directly typing the information into the cell.

**Disable/Enable a Reader**

The reader enabled button allows an operator to disable/enable a reader. In normal operation, a reader is enabled to allow cards to be read and processed by the controller. However, there may be times when a reader must be disabled. For example, to temporarily disable a door to prevent access.

**NOTE:** Even if a reader is disabled, egress is still allowed through Request to Exit commands, and the door is still monitored for forced openings.

1. To enable/disable a reader, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. Building off the previous section, the window found in Figure 35 appears.
2. Scan down the door name and controller/door address columns and locate the reader to be disabled.
3. Locate the "Reader Enabled" column and click on the ON button corresponding to the selected controller/door. The ON button will toggle to OFF and its color will change from green to red. For example, locate the "Stockroom Door - Reader Enabled" cell and click on the ON button.

4. The resulting window should look similar to Figure 36.

![Figure 36 – Disabling/Enabling a Reader](image)

5. Enabling a reader is simply the opposite of disabling a reader. Locate the reader to be enabled. Click on the OFF button corresponding to the selected controller/door. The OFF button will toggle to ON and its color will change from red to green. For example, locate the "Stockroom Door - Reader Enabled" cell and click on the OFF button. The window should again appear similar to the window in Figure 35.

6. Once changes have been made, click on the button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

7. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

### Set a Door Unlock Time

The door unlock time is the number of seconds the controller holds the door lock relay in the unlocked position to allow ingress or egress. A timer with this value begins counting once the card is presented to the reader. When the timer ends, the door lock relay resets to the locked position; the default time is 5 seconds (if a door status switch is used, the door lock also resets once the door is opened).

1. To set a door’s unlock time, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. Building off the previous section, the window found in Figure 35 appears.

2. Scan down the door name and controller/door address columns and locate the door to have an unlock time assigned.

3. Locate the "Unlock Time" column and click on the cell corresponding to the selected controller/door. Type the desired unlock time; the existing value will be overwritten. For example, a back door may need to stay unlocked longer than other doors. Locate and click on the "Back Door - Unlock Time" cell and type 15. This will set the unlock time for this door to 15 seconds.
NOTE: If you double-click in the cell, a spinner icon will appear. If you click on the spinner icon, you can use the spinner to advance the time forward or backward and select the desired time. You may decide to use this method to set the time instead of directly typing the information into the cell.

4. The resulting window should look like Figure 37.

![Figure 37 – Set the Door Unlock Time](image)

5. Once changes have been made, click on the button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**NOTE:** The unlock/lock time zone is valid on holidays as well as days-of-the-week. Any door assigned a unlock/lock time zone that includes a holiday schedule will be automatically unlocked and locked on the dates in that holiday schedule.

**Set a Door Open Time**

The door open time is the number of seconds a door can be held open for ingress or egress before the controller generates a door held alarm. The default time is 20 seconds.

1. To set a door's open time, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. Building off the previous section, the window found in Figure 37 appears.

2. Scan down the door name and controller/door address columns and locate the door to have an open time assigned.

3. Locate the "Open Time" column and click on the cell corresponding to the selected controller/door. Type the desired open time; the existing value will be overwritten. For example, a back door may need to stay open longer than other doors. Locate and click on the "Back Door - Open Time" cell and type **60**. This will set the unlock time for this door to 60 seconds.
NOTE: If you double-click in the cell, a spinner icon will appear. If you click on the spinner icon, you can use the spinner to advance the time forward or backward and select the desired time. You may decide to use this method to set the time instead of directly typing the information into the cell.

4. The resulting window should look similar to Figure 38.

![Figure 38 – Set the Door Open Time](image)

5. Once changes have been made, click on the button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Set an Unlock/Lock Time Zone**

The unlock/lock time zone allows an operator to assign a time zone to a door for the automatic unlocking and locking of that door based on the time zone. For example, a time zone can be created for use by a front door used by customers. The unlock/lock time zone would unlock the front door at the beginning of the time zone and lock it at the end of the time zone.

1. To set a door’s unlock/lock time zone, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. Building off the previous section, the window found in Figure 38 appears.
2. Scan down the door name and controller/door address columns and locate the door to have an unlock/lock time zone assigned.
3. Locate the "Unlock/Lock Time Zone" column and click on the cell corresponding to the selected controller/door (depending upon the size of the window displayed on the screen, you might need to use the scroll bar to bring the remaining columns into view).
4. Click on the arrow and a list of available time zones will appear. Scroll up and down this list and locate the desired time zone. For example, if a "Customers" time zone has been created allowing access between 08:00 and 17:00 (8 A.M. and 5 P.M.), click on the Customers time zone.
5. The resulting window should look similar to Figure 39.
6. Once changes have been made, click on the  button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

7. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**First Person In**

First Person In (FPI) allows an operator to determine if a door should be automatically unlocked when the unlock/lock time zone begins, or if the door should not unlock until after a person presenting a valid card arrives.

FPI can be used wherever employees may be delayed in arriving at a secured site (perhaps due to inclement weather). This ensures that at least one access-granted employee is in the building before the unlock/lock time zone is allowed to unlock the door for general ingress/egress. The default value is ENABLED meaning a door will not be unlocked for general ingress/egress until a valid card has been presented within the unlock/lock time zone.

There are four alternate values that may be selected:

- ENABLED 15
- ENABLED 30
- ENABLED 45
- ENABLED 60

These alternate values allow a controller to "look ahead" 15, 30, 45, or 60 minutes. If an employee presents a valid card during the look ahead period, the door will unlock and allow that employee access (but still will not unlock for general access until the time specified by the unlock/lock time zone). This allows access for an employee who arrives to work early. If this feature is used, the operator should select a time that best suits the security needs of the site.

*NOTE: This feature is only available if a time zone other than Never is selected.*
1. To set a door’s FPI value, click on the Setup ⇒ System pull-down menu or click on the tool bar button. Then click on the Doors tab. Building off the previous section, the window found in Figure 39 appears.

2. Scan down the door name and controller/door address columns and locate the door to have an FPI value assigned.

3. Locate the "First Person In" column and click on the cell corresponding to the selected controller/door (depending upon the size of the window displayed on the screen, you might need to use the scroll bar to bring the "First Person In" column into view).

4. Click on the arrow and a list of FPI values will appear. Scroll up and down this list and locate the desired FPI value. For example, employees are allowed access at the front door up to 60 minutes early to prepare for the day’s tasks. Click on the "ENABLED 60" FPI value.

5. The resulting window should look similar to Figure 40.

![Figure 40](image)

Figure 40 – Set the First Person In Value

6. If desired, select the "Never" time zone to disable FPI for any door.

7. Once changes have been made, click on the button. If the changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

8. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Alarm Output**

Alarm Output allows an operator to select the alarm annunciation mode of the alarm out relay. There are 4 options.

1. Disabled – regardless of the alarm condition, the alarm output relay associated with the door will not be used.
2. Door Forced – the alarm output relay associated with the door will activate only when the door is forced open.
3. Door Held Open – the alarm output relay associated with the door will activate only when the door is held open beyond the door open time period.
4. Both Door Forced and Door Held Open – the alarm output relay associated with a door will activate whenever the door is either forced open or is held open beyond the door open time period.
When a door alarm is activated it will remain on until the alarm condition is corrected; a
forced door must be closed and a door held open must be closed.

1. To set a door’s alarm output value, click on the Setup ⇒ System pull-down menu or click
on the tool bar button. Then click on the Doors tab. Building off the previous
section, the window found in Figure 40 appears.
2. Scan down the door name and controller/door address columns and locate the door to
have an alarm output value assigned.
3. Locate the "Alarm Output" column and click on the cell corresponding to the selected
controller/door (depending upon the size of the window displayed on the screen, you
might need to use the scroll bar to bring the "Alarm Output" column into view). For
example:
   • The front door and back doors need to be monitored for both door forced and door open
     conditions.
   • The emergency exit and stockroom doors need to be monitored for just the door forced
     condition.
   • The manufacturing door needs to be monitored for just the door held open condition.
4. For each door, click on the arrow and a list of alarm output values will appear. Scroll
   up and down this list and locate the desired alarm output value.
5. The resulting window should look similar to Figure 41.

![Figure 41 – Set the Alarm Output Value](image)

6. Once changes have been made, click on the button. If the changes are not saved
   before clicking any other button or exiting the system setup window, the data entered is
   lost and must be re-entered.
7. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network
   section found later in this users guide).
Setup Access Groups

The setup access groups section provides the instructions for creating access groups. Access groups combine time zones and doors into a superset of information that is applied to cardholders – basically when and where cardholders are granted access. Each door can be assigned a unique time zone, or any number of doors can be assigned the same time zone.

To be granted access to a secure door, a cardholder must meet the criteria of the access group. The cardholder must be at a door that accepts members of that access group and it must be during a time zone that allows that cardholder access.

*Doors* uses a *Windows* convention called a Wizard to create an access group. In this application, the access group wizard is a sequential set of windows that requests information from the operator and then creates the access group. This section provides examples for creating a new access group, editing an existing access group, and deleting an access group.

**NOTE:** Along with the three access group examples provided below, several other access groups may be used in this Users Guide providing building access for all three shifts, stockroom access for all three shifts, janitorial access, and all access.

Create a New Access Group

This section uses an example to describe the process for creating a new access group. In this example, the day shift staff needs access to the front, back, and manufacturing doors during the day shift time zone.

1. To create a new access group, click on the Setup ⇒ Access Groups pull-down menu or click on the tool bar button. The Create and Edit Access Groups window appears (see Figure 42).

![Create and Edit Access Groups - Entry Window](image)

Figure 42 – Create and Edit Access Groups - Entry Window

2. Click on the button and the Edit Access Group window appears (see Figure 43).
3. Click on the **NEW** button. This will clear any information that may be stored in the access group fields.

4. Click on the **Next** button and the Select Doors window appears (see Figure 44).

5. The Select Doors window in Figure 41 displays all doors recognized by the system. Click on the doors to be included in this access group. For this example, click on the **Back Door**, **Front Door**, and **Manufacturing Door** icons. The window should look similar to Figure 45.
NOTE: Selected doors can be differentiated from unselected doors by the appearance of the door icon. Selected doors stand out from the window and their door names are written in black text. Unselected doors appear to recede into the window and their door names are written in grey text.

6. Click on the Next button and the Assign Timezones window appears (see Figure 46).

7. The selected door icons should appear in this window. If a door icon is missing or an unwanted door icon is in the window, click on the Back button to return to the previous window and make the necessary changes.

8. Click on the Back Door icon. A time zone list window appears in the middle of the Assign Timezones access group window (see Figure 47).
9. Scroll up and down the time zone window and locate the **Day Shift** time zone.

10. Click on the **Day Shift** time zone and then click on the button. The time zone list window disappears.

11. Repeat steps 8 through 10 for the Front Door and the Manufacturing Door.

12. When complete, the access group window should look similar to Figure 48.

13. Click on the button and the Save Access Group window appears (see Figure 49).
14. Click in the "Access Group Names" field and type a descriptive name for this access group. For this example, type **Building Access - Day**. The window should look similar to Figure 50.

15. Click on the **SAVE** button. If the new access group is not saved before clicking any other button or exiting the setup access group window, the data entered is lost and must be re-entered.

16. Now update the access control network with the new information. Click on the **Update the Network** button on the tool bar (for details on the update process refer to the **Update the Network** section found later in this users guide).
Edit an Existing Access Group

This section describes the process for editing an existing access group. In this example, two changes to a Janitorial Access access group will be made: access to the stockroom will be removed and the time zone assigned to the front door will be changed from Day Shift to Janitorial Staff.

1. To edit an access group, click on the Setup ⇒ Access Groups pull-down menu or click on the tool bar button. The Create And Edit Access Groups window appears (see Figure 51).

Figure 51 – Create And Edit Access Groups

2. Click on the button and the Edit Access Group window appears (see Figure 52).

Figure 52 – Edit Access Group

3. Click on the arrow in the "Access Group Names" field and a list of available access groups will appear. Scroll up and down this list and locate the desired access group for editing. For example, click on the "Janitorial Access" time zone and that access group is entered into the "Access Group Names" field (see Figure 53).
4. Click on the button and the Select Doors window appears showing that the Back Door, Front Door, Manufacturing Door, and Stockroom Door are all selected, and that the Emergency Exit is not selected (see Figure 54).

Add/Remove a Door from the Access Group

1. For this example, to delete a door from the access group, click on the Stockroom Door icon. This will remove the door from the access group. The door icon will change and appear to recede into the window, and the door name text will change from black to grey. The window will change to appear similar to Figure 55.

2. Should a door need to be added to the access group, click on that door icon. This will add the door to the access group. The door will change and appear to stand out from the window, and the door name text will change from grey to black.
Figure 55 – Access Group Edited Doors

3. Click on the button and the Assign Timezones window appears (see Figure 56).

Figure 56 – Access Group Time Zones for the Edited Doors

4. The correct door icons should now appear in this window. If a wanted door icon is missing or an unwanted door icon is in the window, click on the Back button to return to the window in Figure 55 and make the necessary changes.

Change the Time Zone on an Access Group Door

1. For this example, refer to Figure 56. To change the time zone on an access group door, click on the door to be changed.

2. Click on the Front Door icon. A small, time zone list window will appear in the middle of the Assign Timezones window (see Figure 57).
Figure 57 – Assigning Time Zones to Doors in the Access Group

3. Scroll up and down the time zone window and locate the Janitorial Staff time zone.

4. Click on the Janitorial Staff time zone and then click on the OK button. The time zone list window will disappear and the window should look similar to Figure 58.

Figure 58 – Edited Time Zone on Front Door Access Group

5. Click on the Next button and the save Access Group window appears (see Figure 59).
6. Click on the **SAVE** button. If the edited access group is not saved before clicking any other button or exiting the setup access group window, the data entered is lost and must be re-entered.

7. Now update the access control network with the new information. Click on the **Update** button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

## Delete an Access Group

This section describes the process for deleting an access group. For this example, an access group named Emergency Access will be deleted.

1. To delete an access group, click on the Setup ⇒ Access Groups pull-down menu or click on the tool bar button. The Create and Edit Access Groups window appears (see Figure 60).

![Figure 60 – Access Group - Entry Window](image)

---

October 1998 01821-001
Page 84 Revision 2.1
2. Click on the button and the Edit Access Group window appears (see Figure 61).

![Figure 61 – Edit Access Group](image1.png)

3. Click on the arrow in the "Access Group Names" field and a list of available access groups will appear. Scroll up and down this list and locate the desired access group for deleting. For this example, click on the "Emergency Access" time zone and that access group is entered into the "Access Group Names" field (see Figure 62).

![Figure 62 – Selected Access Group for Deletion](image2.png)

4. Click on the button. The access group is removed from the system.

5. Click on the button. If the edited access group is not saved before clicking any other button or exiting the setup access group window, the data entered is lost and must be re-entered.
6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

*NOTE: If an access group is in use by the access control network, the Doors program will not allow it to be deleted. Review all cardholder/access group assignments to ensure all references to the access group to be deleted have been changed.*
Setup Cards

The setup cards section provides the instructions for enrolling access control cards and managing the database for these cards. Each person to be granted access to secured areas will have a card that identifies that person to the access control system.

Through the cards setup menu, an operator can enroll, void, and delete cards; assign cards to cardholders; enter and edit cardholder information; and apply access groups to card holders. There are two methods for working with the card database: through dialog boxes or through a spreadsheet. Each method accomplishes the same tasks.

The dialog box method allows an operator to enter all cardholder data through a series of "fill-in-the-blank" type windows. The spreadsheet method allows an operator to enter all cardholder data into a spreadsheet. Work with the method that feels the most comfortable to you.

**Card Enrollment – Dialog Box Method**

The dialog box method allows an operator to enter all cardholder data through a series of "fill-in-the-blank" type windows. There are six possible windows (accessed through tabs in the Setup ⇒ Cards window) used to enter enroll a card and enter cardholder information, starting with card enrollment and continuing through cardholder data entry.

**Enroll Tab**

Commands within the enroll tab create a database entry for each card enrolled into the access control system. There are two ways to enroll cards: block enrollment by card number range and by card presentation to a reader.

**Block Enrollment by Card Number Range**

Block enrollment by card number range is best used when there is a large quantity of sequentially numbered cards (referring to the external number etched on the body of the card). Cards do not have to be on hand when enrolled through the number range process. Five cards will be enrolled in this example.

*NOTE: Block enrollment by number range is valid for "K" series Keri proximity cards – Keri part numbers KC-10 and KC-10X and "K" series Keri proximity key tags – Keri part numbers PKT-10 and PKT-10X (identified by a leading "K" on the card's external number printed on the body of the card). Block enrollment by number range is not yet available for "W" series Wiegand cards or key tags (identified by a leading "W" on the card’s external number printed on the body of the card), or "C" series cards or key tags (used by older Keri Systems products).*

*NOTE: When block enrolling a large number of cards, Keri recommends enrollment in several medium sized-blocks (up to 1,000 cards) instead of one large block. The database download times for several medium sized-blocks is shorter than that of one large block and the risk of losing download information to a power outage or computer glitch is reduced.*

1. To enroll cards, click on the Setup ‰ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.
2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Enroll tab. In the enroll window, locate the Enroll Type field (see Figure 63).

![Figure 63 – Enrolling by Card Number Range, Dialog Box Method](image)

4. The enroll type field has two radio buttons: Enter Range and Read Cards. Click on the **Enter Range** radio button. The resulting window should look similar to Figure 63.

5. Locate the Internal Number Range field. Click in the **FROM** field. Enter the card number for the first card in the range of cards to be enrolled. The card number is the second set of digits printed on the body of the card (the *nnnnnnnn* digits, see Figure 64). The card number can be anywhere from 5 digits long to 8 digits long. For this example, the entire number of the first card is K1757 187491; the card number is 187491. Type **187491**.

![Figure 64 – Proximity Card Number](image)

**NOTE:** Block enrollment by number range is valid for "K" series Keri proximity cards (identified by a leading K on the card’s external number etched on the body of the card). This is a sample K-series external number: Kdddd nnnnnnn. It is the last set of digits that should be entered as the external number. Block enrollment by number range is not yet available for "W" series Wiegand cards.
6. Locate the Internal Number Range field. Click in the TO field. Enter the card number for the last card in the range of cards to be enrolled. The card number is the second set of digits printed on the body of the card (the nnnnnnnn digits, see Figure 10-2). The card number can be anywhere from 5 digits long to 8 digits long. For this example, the entire number of the last card is K1757 187495; the card number is 187495. Type 187495. The resulting window should look similar to Figure 65.

![Image of the window showing Enrolling by Card Number Range, Before Saving]

Figure 65 – Enrolling by Card Number Range, Before Saving

7. Click on the button. If the card enrollment information is not saved before clicking any other button or exiting the card enrollment window, the data entered is lost and must be re-entered.

8. The card numbers are moved from the internal number range field to the card number range field. Through an automatic translation process each card’s internal identification number is calculated and entered into the internal number range field. The resulting window should look similar to Figure 66.

![Image of the window showing Enrolling by Card Number Range, After Saving]

Figure 66 – Enrolling by Card Number Range, After Saving
9. Examine the value displayed in the Cards Enrolled field. The cards enrolled field displays the number of cards successfully enrolled during this card enrollment session. This number should match the number of cards you have enrolled.

10. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Enrolling by Presenting to a Reader**

Enrolling by card presentation to a reader is best used when there is only a few cards to enroll or the cards are not in sequential order. The cards must be on hand to be presented to a reader for enrollment. Two cards will be enrolled in this example.

1. To enroll cards, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Enroll tab. In the enroll window, locate the Enroll Type field (see Figure 67).

![Figure 67 – Enrolling by Presenting to a Reader, Dialog Box Method](image)

4. The enroll type field has two radio buttons: Enter Range and Read Cards. Click on the Read Cards radio button. The resulting window should look similar to Figure 67.

5. Click on the button. If the Doors program is not connected to the access control network, the program will automatically connect.

6. The "A" reader on the master controller is used for reading cards being enrolled. The reader’s LED toggles between amber and red to indicate it is ready for enrolling cards.

**NOTE:** The reader/controller is not available for any other use during the card enrollment process – any attempts to use a door associated with the master controller will be denied until card enrollment is complete and can disrupt the card enrollment process.
7. Present the first card to the enrollment reader. The reader will provide one short beep to indicate a successful read has been performed.

*NOTE:* If the Doors program is unable to enroll a card, the reader will provide one long beep and an error message window will be displayed providing a brief description of the problem with the card being enrolled. Click on the OK button to acknowledge the error message, correct the problem, and continue card enrollment.

8. Present the second card to the enrollment reader. Again the reader will provide one short beep. The card enrollment window should look similar to Figure 68.

![Figure 68 – Enrolling by Presenting to a Reader, Cards Presented](image)

9. Once all cards have been presented for enrollment, click on the button to put the enrollment reader back into regular service.

10. Click on the SAVE button. If the card enrollment information is not saved before clicking any other button or exiting the card enrollment window, the data entered is lost and must be re-entered.

11. Examine the value displayed in the Cards Enrolled field. The cards enrolled field displays the number of cards successfully enrolled during this card enrollment session. This number should match the number of cards you have enrolled.

12. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Card Data Tab**

The card data tab allows an operator to enter or edit personal data for each card/cardholder database entry. It also allows an operator to void or delete a card/cardholder. This example will demonstrate entering information for one cardholder, editing an information field for that cardholder, voiding a cardholder, and deleting a cardholder.
Entering Card Data for a Cardholder

1. To enter cardholder card data, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Card Data tab. The Card Data window appears (see Figure 69).

4. Click on the buttons to scroll up and down the list of cards available and locate the card to which data should be entered. For this example, scroll up and down the list until card number 187491 is displayed in the card number field (see Figure 70).
NOTE: All block enrolled cards will have entries for both the internal number and card number. The internal number is the card’s internal identification number – the number actually read from the card and processed by a reader. The card number is the number etched on the body of the card (entered during block enrollment). Cards enrolled by presenting to a reader will only have a value in the internal number field; the card number field will be set to 0. The actual external number can be entered by an operator if desired.

5. Click in the Last Name field and enter the cardholder’s last name. For this example, type *Adams*.
6. Click in the First name field and enter the cardholder’s first name. For this example, type *John*.
7. Click in the Middle name field and enter the cardholder’s middle name or initial. For this example, type *Q*.
8. Locate the Card Status field and click in the Active box. This activates the card for the cardholder. The time that the card was activated is entered as the Enroll Date and Time.
9. If the Card Number field displays a "0," the actual card number can be entered. Click in the Card Number field and type the card’s number (the last 6 digits etched on the body of the card, see Figure 61).
10. Locate the Access Group field and select an access group to be assigned to this cardholder. Click on the * and a list of the available access groups will appear. For this example, select the Building Access - Day access group.
11. The resulting window should look similar to Figure 71.

![Figure 71 – Entered Cardholder Data](image)

12. Click on the *button. If the cardholder data is not saved before clicking any other button or exiting the card data window, the data entered is lost and must be re-entered.

13. Now update the access control network with the new information. Click on the *button on the tool bar (for details on the update process refer to the *Update the Network* section found later in this users guide).
Editing Card Data for a Cardholder

1. To edit cardholder card data, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Card Data tab (information for a cardholder should be in the window).

4. Click on the buttons to scroll up and down the list of cards and locate the card to be edited. For this example, scroll up and down the list until cardholder John Q Adams is displayed in the name fields (see Figure 71).

5. Double-click in the Middle name field. All data within the field is highlighted. Enter the cardholder’s entire middle name. For this example, type Quincy.

6. The resulting window should look similar to Figure 72.

![Figure 72 – Edited Cardholder Name](image)

7. Click on the button. If the edited card cardholder data is not saved before clicking any other button or exiting the card data window, the data entered is lost and must be re-entered.

8. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

Voiding a Card

The void feature allows an operator to remove a cardholder from the access control database without removing the card from the database. A voided card can then be reassigned to a new cardholder while maintaining the history of who has held the card in the past. In this example, cardholder James K Polk will be voided from the access control database.
1. To void a card/cardholder, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Card Data tab (information for a cardholder should be in the window).

4. Click on the buttons to scroll up and down the list of cards and locate the card to be voided. For this example, scroll up and down the list until cardholder James K Polk is displayed in the name fields (see Figure 73).

![Figure 73 – Preparing to Void a Card](image)

5. Click on the button. The current date and time is entered into the void date and time fields, and the card status is changed to inactive (the active box is not checked). The void window should look similar to Figure 74.
6. Click on the button. If the voided card/cardholder data is not saved before clicking any other button or exiting the card data window, the void command is not applied to the database and must be redone.

7. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

Deleting a Card

The delete feature allows an operator to remove a card from the access control database, erasing all database references to that card and its cardholders. A card that has been deleted from the database must be re-enrolled if it is to be reused in the access control system.

1. To delete a card/cardholder, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Card Data tab (information for a cardholder should be in the window).

4. Click on the buttons to scroll up and down the list of cards and locate the card to be deleted. For this example, scroll up and down the list until cardholder James K Polk is displayed in the name fields.

5. Before deleting a card, it must be voided. Perform the void operation as described in the Voiding a Card section above.

6. Once the card has been voided, click on the button. A deletion confirmation window appears (see Figure 75).
7. Click on the button. The card/cardholder entry in the database is now removed.

8. Click on the button. If the deleted card/cardholder data is not saved before clicking any other button or exiting the card data window, the delete command is not applied to the database and must be redone.

9. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**More Card Data**

The more card data tab allows an operator to assign a department group to a cardholder. A department group is a method of cardholder identification based on the department for which a cardholder works, i.e. Engineering, Janitorial, Management, Manufacturing, Sales, Stockroom. By using this field, cardholder data can be sorted by department groups, displaying all members of a given group when in the cards spreadsheet view.

In this example, the Management department group will be assigned to cardholder John Quincy Adams.

1. To assign a department group for a card/cardholder, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Card Data tab (information for a cardholder should be in the window).

4. Click on the buttons to scroll up and down the list of cards and locate the card to which data should be entered. For this example, scroll up and down the list until cardholder John Quincy Adams is displayed in the name fields.

5. Click on the More Card Data tab. The window should look similar to Figure 76.
6. Locate the **Dept Groups** field and click on the arrow. A list of existing department groups is displayed.

7. Scroll up and down the list. If the desired department group name is in the list, click on that name. If the desired department group name does not exist, click in the **Dept Groups** field and type the name of the department group. For this example, click in the field and type **Manufacturing**.

8. Click on the **SAVE** button. If the department group name is not saved before clicking any other button or exiting the more card data window, the data entered is lost and must be re-entered.

9. Now update the access control network with the new information. Click on the **UPDATE** button on the tool bar (for details on the update process refer to the **Update the Network** section found later in this users guide).

**Preferences**

The preferences tab allows an operator to disable the card number and department group functions if they are not to be used in the access control database (the default value for these functions is to be enabled). The department group function is found under the more card data tab. The card number function is found under the card data tab.

*NOTE: If the card number function is disabled, the field is still used by the Doors software during block card enrollment, but is not used by any other part of the program.*

1. To change a preference for the card database, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment dialog box window is active.
3. Click on the **Preferences** tab. The resulting window should look similar to Figure 77.

![Figure 77 – Selecting Card Database Preferences](image)

**NOTE:** The keypad number function seen in Figure 77 is not functional. It is for a feature in development.

4. If the box beside the preference options has a check mark, the option is enabled; if there is not a check mark, the option is disabled.

5. To change a preference option, click on the **box** beside the option. Every time the box is clicked, it changes state between on and off.

6. Click on the **SAVE** button. If the configuration option changes are not saved before clicking any other button or exiting the preferences window, the preference options are lost and must be re-entered.

7. Now update the access control network with the new information. Click on the **button** on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Personal Setup**

The personal setup tab allows for the creation of up to six separate personal data categories to be designated for cardholder data entry. Examples of fields that may be created are automobile license plate number, home telephone number, spouse’s name, demographic information.

When a personal data category is created, a sixth tab, the Personal tab, will be added to the Setup/Cards window. The actual personal data for each cardholder is entered in the personal tab. In this example, a personal data category will be created for entering cardholder home telephone numbers.
1. To change a preference for the card database, click on the Setup ⇒ Cards pull-down menu or click on the  tool bar button. A card enrollment window appears and these two icons appear on the tool bar .

2. Click on the  tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the Personal Setup tab. The resulting window should look similar to Figure 78.

![Personal Setup Window](image)

Figure 78 – Personal Setup Window

4. Click in the small box beside Field 1. A check mark will appear in the box, activating the field for assignment.

5. Click in the large box beside Field 1. Use the backspace and delete keys on the keyboard to erase the "FIELD 1" text within the box.

6. Now type in the name to be designated to this field. For this example, type **Home Telephone Number**. The resulting window should look similar to Figure 79.
7. Click on the \( \text{SAVE} \) button. If the personal data field changes are not saved before clicking any other button or exiting the personal setup window, the changes are lost and must be re-entered.

8. Now update the access control network with the new information. Click on the \( \text{UPDATE NETWORK} \) button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Personal**

Once personal data fields have been created in the personal setup tab, the personal tab appears in the Setup/Cards window. The personal tab allows an operator to enter personal information regarding the cardholder into the fields created in the personal setup tab.

Based on the personal setup field created in the Personal Setup section above, this example will enter a home telephone number for cardholder John Quincy Adams.

1. To enter personal data for a card/cardholder, click on the Setup \( \Rightarrow \) Cards pull-down menu or click on the \( \text{Enroll} \) tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the \( \text{Ensure Active} \) tool bar button to ensure the card enrollment dialog box window is active.

3. Click on the \( \text{Card Data} \) tab (information for a cardholder should be in the window).

4. Click on the \( \text{Prev} \) \( \text{Next} \) buttons to scroll up and down the list of cards and locate the card to which data should be entered. For this example, scroll up and down the list until cardholder John Quincy Adams is displayed in the name fields.

5. Click on the \( \text{Personal} \) tab. The window should look similar to Figure 80.
6. Click on the **Home Telephone Number** field and type the telephone number. For this example, type **800-555-1212**. The resulting window should look similar to Figure 81.

7. Click on the **SAVE** button. If the personal data entries are not saved before clicking any other button or exiting the personal data window, the changes are lost and must be re-entered.

8. Now update the access control network with the new information. Click on the **UPDATE NET** button on the tool bar (for details on the update process refer to the **Update the Network** section found later in this users guide).
Card Enrollment – Spreadsheet Method

The spreadsheet method allows an operator to enter cardholder data directly into a spreadsheet. The spreadsheet creates a row for each enrolled card, and either has database columns for every card parameter.

Enrolling Cards

Cards are enrolled by presenting them to an enrollment reader attached to the master controller. You must have the cards for enrollment on-hand for enrollment. Two cards will be enrolled in this example.

NOTE: For block enrollment of a large number of cards, please refer to the Block Enrollment by Card Number Range section.

1. To enroll cards, click on the Setup ⇒ Cards pull-down menu or click on the tool bar button. A card enrollment window appears and these two icons appear on the tool bar.

2. Click on the tool bar button to ensure the card enrollment spreadsheet window is active. The Setup Cards window appears (see Figure 82).

3. Click on the button. If the Doors program is not connected to the access control network, the program will automatically connect.

4. The "A" reader on the master controller is used for reading cards being enrolled. The reader’s LED toggles between amber and red to indicate it is ready for enrolling cards.

NOTE: The reader/controller is not available for any other use during the card enrollment process – any attempts to use a door associated with the master controller will be denied until card enrollment is complete and may disrupt the card enrollment process.
5. Present the first card to the enrollment reader. The reader will provide one short beep to indicate a successful read has been performed.

**NOTE:** If the Doors program is unable to enroll a card, the reader will provide one long beep and an error message window will be displayed providing a brief description of the problem with the card being enrolled. Click on the button to acknowledge the error message, correct the problem, and continue card enrollment.

6. Present the second card to the enrollment reader. Again the reader will provide one short beep. The card enrollment window should now look similar to Figure 83.

```
Figure 83 – Enrolling Cards
```

7. Once all cards have been presented for enrollment, click on the button to put the enrollment reader back into regular service.

8. Click on the button. If the card enrollment information is not saved before clicking any other button or exiting the card enrollment window, the data entered is lost and must be re-entered.

9. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Entering Card Data for a Cardholder**

Data can now be entered or edited for all cards displayed in the spreadsheet. Newly enrolled cards will display an internal card number, but have blank cells for all other spreadsheet values in that card’s row.

For this example, refer to Figure 83 above and locate the row corresponding to the card/internal card number for which data should be entered. For this example, locate internal card number 607656760. Cardholder information for James K Polk will be entered into this row.
Last Name
The cardholder’s last name is entered in this cell.

1. Click on the Last Name cell for this row.
2. Type Polk.

First Name
The cardholder’s first name is entered in this cell.

1. Click on the First name cell for this row.
2. Type James.

Middle Name
The cardholder’s middle name or initial is entered in this cell.

1. Click on the Middle name cell.
2. Type K.

Internal Number
The internal number value was entered when the card was enrolled. It is the card’s internal identification number, read from the card when the card was presented to the enrollment reader. This field cannot be edited.

Card Number
The card number refers to the number printed onto the body of the card (see Figure 11-3). The card number is the second set of digits printed on the body of the card (the mnnnnnnn digits, see Figure 84). The card number can be anywhere from 5 digits long to 8 digits long. For this example, the entire number of this card is K1757 211774; the card number is 211774.

1. Click on the Card Num cell for this row.
2. Reading from the card, type 211774.

Figure 84 – Proximity Card Number

NOTE: The Card Number is an optional field. A card number does not have to be entered; it is not required for program operation.

Access Group
An access group must be assigned to the cardholder. The access group defines through which doors and at what time-of-the-day and day-of-the-week a cardholder will be granted access.

1. Locate the Access Group cell. Click on the and a list of the available access groups appears. Scroll up and down this list and find the access group to be assigned to this cardholder.
2. For this example, click on Building Access - Day.
Based on entries made so far, the cards spreadsheet should look like Figure 85.

![Spreadsheet screenshot](image_url)

**Figure 85 – Entering Cardholder Data, Part 1**

Depending upon the size of the computer's screen, more of the spreadsheet may be displayed than is shown in Figure 85. If any portion of the spreadsheet is not displayed a scroll bar will appear across the bottom of the spreadsheet. For the following spreadsheet column descriptions, ensure all the columns to the right of the access group column are displayed by clicking on the until the Void Time column appears.

**Department Group**

A department group is a method of cardholder identification based on the department for which a cardholder works, i.e. Engineering, Janitorial, Management, Manufacturing, Sales, Stockroom. By using this field, cardholder data can be sorted by department groups, displaying all members of a given group. Instructions for sorting data is provided later in this section.

1. Locate the Department Group cell. Click on the and a list of the available department groups appears. Scroll up and down this list and find the department group to be assigned to this cardholder.
2. If an appropriate department group can be found, click on the Department Group name.
3. If an appropriate department group cannot be found, a new one can be entered. For this example a new department group will be entered. Click in the Department Group cell and type Management.

**On/Off**

The On/Off cell makes a card active or inactive. When a card is first enrolled, the card is inactive. A card must be made active to be read by readers.

Inactivate a card when the cardholder goes on vacation or takes a leave-of-absence and should not have access during this period. This can prevent an unauthorized person from taking that card and gaining access to a secured area. When the cardholder is due to return, activate the card and access will be granted again.

1. To activate a card, locate the On/Off cell. It should be OFF and the cell should be highlighted in red.
2. Click on the cell; it will turn red and be OFF.
Enroll Date and Time
When a card is activated for the first time, the date and time of activation is automatically entered into the Enroll Date and Enroll Time cells of the spreadsheet. These cells are not editable.

Based on the last set of entries, the second half of the cards spreadsheet should look similar to Figure 86.

![Figure 86 – Entering Cardholder Data, Part 2](image)

Saving the Card Data

1. Click on the **SAVE** button. If the card data is not saved before clicking any other button or exiting the card spreadsheet window, the changes are lost and must be re-entered.

2. Now update the access control network with the new information. Click on the **Update Out** button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

Voiding Cards
The void cards feature allows an operator to remove a cardholder from the access control database without removing the card from the database. A voided card can then be reassigned to a new cardholder while maintaining the history of who has held the card in the past. In this example, cardholder James K Polk will be voided from the access control database.

1. Scroll up and down the list of available cardholders and locate James K Polk.
2. Click on the **Last Name** cell, or any cell on that cardholder row (see Figure 87).
3. Click on the button. The card is inactivated and the void date and time is entered into the spreadsheet (see Figure 88). This card will not be accepted by any reader/controller in the access control system.

4. Click on the button. If the voided card is not saved before clicking any other button or exiting the card spreadsheet window, the changes are lost and must be re-entered.

5. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).
Deleting Cards

The delete cards feature allows an operator to remove a cardholder from the access control database, erasing all database references to that card and its cardholders. A card that has been deleted from the database must be re-enrolled if it is to be reused in the access control system. In this example, cardholder James K Polk will be deleted from the access control database.

1. Scroll up and down the list of available cardholders and locate James K Polk.
2. Click on the Last Name cell, or any cell on that cardholder row (see Figure 89).

![Figure 89 – Selecting a Card to Delete]

3. Click on the button. A deletion confirmation window will appear (see Figure 90).

![Figure 90 – Deletion Confirmation]

4. Click on the button. The card/cardholder entry in the database is now removed.
5. Click on the button. If the deleted card is not saved before clicking any other button or exiting the card spreadsheet window, the changes are lost and must be re-entered.
6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this user's guide).
Sorting Data

The sort data button allows an operator to display the data in the spreadsheet in a desired order (always from A to Z or from lowest to highest number). For example, sorting by last name places all cardholders in alphabetical order. Sorting by department group places all cardholders in alphabetical department group order. Sorting by card number places all cardholders in numeric card number order. Keri recommends sorting the data in the spreadsheet so that information is grouped in a manner that makes it easy to find desired information.

The following spreadsheet fields can be sorted.

- Last Name
- Internal Num
- Card Num
- Access Group
- Dept Group
- On Off
- Enroll Date
- Void Date

In this example, a sort by last name will be performed.

1. Click on the top of the Last Name column. The entire column is highlighted (see Figure 91).

![Figure 91 – Preparing to Sort Cardholder Data]

2. Click on the button. All data in the spreadsheet is now reorganized in alphabetical order by last name (see Figure 92).
Block Copying Data

The Block and Copy buttons allow an operator to select a data cell for copying to other data cells. This can be helpful when enrolling a large number of cards where a set of cells will all have the same information. When enrolling the entire card set for the day shift, the access and department groups for the entire card set would be the same. To minimize data entry, enter the information for the first cardholder and then copy it to the remaining cardholders. The following fields can be block copied.

- Card Num
- Access Group
- Dept Group
- On Off

In this example, the access group will be copied from one day shift cardholder to three new day shift cardholders.

1. Click on the cell from which data should be copied.
2. Click on the \texttt{COPY} button (see Figure 93).
3. There are three ways to block select the cells to which data is copied. Use the method you find easiest (see Figure 94).
   - Click and hold on the first cell to copy and then drag the mouse down to the last cell to copy.
   - Click on the first cell, hold the Shift key down, and click on the last cell.
   - Hold the Ctrl key down and one-at-a-time click on the cells to be copied. This method is best used when receiving cells are not in sequential order.

4. Click on the button. All copyable data will be transferred (see Figure 95).
5. Click on the button. If the copied data is not saved before clicking any other button or exiting the card spreadsheet window, the changes are lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Personal Data Fields**

An operator can assign up to six personal data fields which are added to the cards spreadsheet. These data fields are used for information such as an automobile license plate, home telephone number, spouse’s name, demographic information. The field assignment process is a part of the Personal Setup tab found in the Card Enrollment – Dialog Box Method section. Please refer to this section for information on creating a personal data field.

Once a personal data field is created, a column is added to the cards spreadsheet and cardholder data can then be entered. For this example, a personal data field has been created for a home telephone number and added to the end of the spreadsheet. A telephone number will be added for John Q Adams.

1. Locate John Q Adams in the spreadsheet.
2. If necessary, use the scroll bar and scroll left and right across the spreadsheet to locate the Home Telephone Number cell.
3. Click on the Home Telephone Number cell. The window should look similar to Figure 96.
4. Type the cardholder’s telephone number, **800-555-1212**. The resulting window should look similar to Figure 97.

5. Click on the button. If the personal data is not saved before clicking any other button or exiting the card spreadsheet window, the changes are lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Editing Cardholder Data**

Editing cardholder data is simply a matter of locating the cell requiring editing and entering the new information. In this example the middle name field for John Q Adams will be changed to Quincy.
1. Locate John Q Adams in the spreadsheet.
2. If necessary, use the scroll bar and scroll left and right across the spreadsheet to locate the middle name cell.
3. Click on the Middle name cell. The window should look similar to Figure 98.

```
<table>
<thead>
<tr>
<th>Last Name</th>
<th>First</th>
<th>Middle</th>
<th>Internal Num</th>
<th>Card Num</th>
<th>Access Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adams</td>
<td>John</td>
<td>Q</td>
<td>87691833</td>
<td>211774</td>
<td>Building Access - Day</td>
</tr>
<tr>
<td>Hamilton</td>
<td>Alexander</td>
<td></td>
<td>20866602</td>
<td>187493</td>
<td>Building Access - Grave</td>
</tr>
<tr>
<td>Jefferson</td>
<td>Thomas</td>
<td></td>
<td>204163752</td>
<td>187495</td>
<td>Building Access - Stockroom</td>
</tr>
<tr>
<td>Lincoln</td>
<td>Abraham</td>
<td></td>
<td>137054009</td>
<td>187481</td>
<td>Manager Access</td>
</tr>
<tr>
<td>Madison</td>
<td>James</td>
<td></td>
<td>204174369</td>
<td>187494</td>
<td>Building Access - Swing</td>
</tr>
<tr>
<td>Washington</td>
<td>George</td>
<td></td>
<td>202050219</td>
<td>187492</td>
<td>Total Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1007847434</td>
<td>Building Access - Day</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>607656760</td>
<td>Building Access - Day</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>403376811</td>
<td>Building Access - Day</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 98 – Editing a Cell

4. Type Quincy. The new information overwrites the existing information (see Figure 99).

```
<table>
<thead>
<tr>
<th>Last Name</th>
<th>First</th>
<th>Middle</th>
<th>Internal Num</th>
<th>Card Num</th>
<th>Access Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adams</td>
<td>John</td>
<td>Quincy</td>
<td>87691833</td>
<td>211774</td>
<td>Building Access - Day</td>
</tr>
<tr>
<td>Hamilton</td>
<td>Alexander</td>
<td></td>
<td>20866602</td>
<td>187493</td>
<td>Building Access - Grave</td>
</tr>
<tr>
<td>Jefferson</td>
<td>Thomas</td>
<td></td>
<td>204163752</td>
<td>187495</td>
<td>Building Access - Stockroom</td>
</tr>
<tr>
<td>Lincoln</td>
<td>Abraham</td>
<td></td>
<td>137054009</td>
<td>187481</td>
<td>Manager Access</td>
</tr>
<tr>
<td>Madison</td>
<td>James</td>
<td></td>
<td>204174369</td>
<td>187494</td>
<td>Building Access - Swing</td>
</tr>
<tr>
<td>Washington</td>
<td>George</td>
<td></td>
<td>202050219</td>
<td>187492</td>
<td>Total Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1007847434</td>
<td>Building Access - Day</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>607656760</td>
<td>Building Access - Day</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>403376811</td>
<td>Building Access - Day</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 99 – Edited Cell

5. Click on the [SAVE] button. If the edited cell data is not saved before clicking any other button or exiting the card spreadsheet window, the changes are lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).
Resizing Columns and Rows

If a cell is too small to display all the data in the cell, the spreadsheet’s columns and rows can be resized by dragging a column or row boundary to the desired size.

While within the cells of the spreadsheet, the mouse cursor looks like a small cross ⬤. When the mouse cursor hits a resizeable column or row boundary it will change to ✱ for a column and ⬦ for a row.

To Resize a Column

1. Locate the right boundary for a column. The mouse cursor will change to ✱.
2. Click, hold and drag the mouse to the left of the window to make the column smaller, and to the right to make the column larger.
3. Release the mouse button and the new column size is set.

To Resize a Row

1. Locate the bottom boundary for a row. The mouse cursor will change to ⬦.
2. Click, hold and drag the mouse to toward the top of the window to make the row smaller, and to the bottom to make the row larger.
3. Release the mouse button and the new row size is set.

Printing Cardholder Data from the Spreadsheet (Quick Print)

Selected sequential rows from the spreadsheet can be printed if desired. Because of the number and width of columns required for each card/cardholder, printing cardholder data typically requires two to three sheets of paper to display all the information for each card/cardholder.

1. Locate the first row to be printed.
2. Click on a cell in that row that is block copyable (the Block button becomes active when a block copyable cell is clicked).
3. Click on the Block button.
4. There are three ways to block select the rows to be printed. Use the method you find easiest.
   - Click and hold on the first row and then drag the mouse down to the last row.
   - Click on the first row, hold the Shift key down, and click on the last row.
   - Hold the Ctrl key down and click on the first row and then the last row.
5. On the menu bar, click on File ⇒ Print.
6. The highlighted data rows are now printed.
Setup Monitor and Events

The setup monitor and events commands allow an operator to perform four tasks.

- auto-collection of events from the controller
- configuration of up to three event monitor windows
- selecting which events to track and which to ignore in the monitor windows
- selecting which events to be saved and which to ignore in the controllers

1. To access the setup monitor and events commands, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the Monitoring Options tab. The Setup Monitor window appears (see Figure 100).

Figure 100 – Setup Monitor and Events Window

Enable/Disable Auto-Collection

The Auto-collection on buffer full option allows an operator to define if the host computer is allowed to receive event information from the controller’s event memory buffer when the controller’s buffer becomes full. This ensures that as new events are received, the oldest events are not deleted to make room for the new events. If the controller’s buffer reaches the buffer limit, the controller uploads its buffer contents to the host computer, clearing the buffer.

NOTE: These instructions configure the Doors software for receiving information from the controller, but the controller must also be configured to transmit this information. This is done in the Set Controller Dial-Out Parameters section found earlier in this users guide. Both steps must be done for proper uploading of information from a controller to the host computer/Doors software.

1. To enable auto-collection, click on the box beside the "Auto-collection if buffer full warning" message. When the box has a check-mark, auto-collection is enabled (see Figure 101).
2. To disable auto-collection, click on the box beside the “Auto-collection if buffer full warning” message. When the box does not have a check mark, auto-collection is disabled (see Figure 100).

3. Click on the button. If the auto-collection information is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

4. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**NOTE:** Even with auto-collection enabled, it is possible (but unlikely) to lose events during the upload process if new events are recorded by the controller faster than it can upload existing events to the host computer. To prevent this, change the controller Threshold Percentage value from its default of 80% to a lower value (see the Set the Dial-Out Threshold Percentage section in this users guide).

**NOTE:** When a controller dials the host computer to upload the contents of its buffer, it will only try to dial-out once. If it is not successful in making the connection with the host computer, it will not try again. It will wait for the next time the host computer connects with the controller and then will upload the contents of its buffer. If the buffer has filled prior to the host computer making contact with the controller, the oldest events in the buffer may be lost as the newest events overwrite the oldest events.

### Configure Event Monitoring Windows

Event monitoring allow an operator to configure up to three windows which display filtered, real-time events occurring on the access control system. This allows an operator to create custom monitoring windows, each dedicated to monitoring specific types of events.

There are two processes involved in configuring event windows: naming the windows and assigning the events to be tracked by the windows.

### Naming Event Monitoring Windows

The View One Name, View Two Name, and View Three Name fields allow an operator to assign a descriptive name of up to 32 characters for each of the three monitor screens. In this example, the view three name field will be named for monitoring door access events.

1. Click in the **View Three Name** field.
2. Delete the MONITOR VIEW 3 name in the field (use any combination of backspaces, deletes, and highlighting and deleting to clear the text out of the field).
3. Type **Door Access Events**. The resulting window should look similar to Figure 101.
4. Click on the \( \text{SAVE} \) button. If the naming event monitoring information is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

5. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Message Text Strings**

There are 87 possible events that can be tracked. Each event is identified by a message text string that is a brief description of the event generated by the controller when the event occurs. These strings can be edited; an operator can change the message that is displayed when an error occurs. This allows an operator to create a more descriptive error string to make report reviewing easier. In this example, the "Op Pulsed Door" message text string will be renamed to "Temporary Door Unlock."

1. To access the message text strings, click on the Setup \& Monitor and Events pull-down menu.
2. Click on the Messages tab. The Messages window appears (see Figure 102).
3. Use the scroll bar at the right side of the window to scroll up and down the entire list of event messages and locate the "Op Pulsed Door" message text string.

4. Click in the cell and type **Temporary Door Unlock** (see Figure 103).

5. Click on the button. If the message text change is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).
NOTE: When changing message text fields, the operator must be cautious that the intent of
the error message (the event that occurred to generate the message) is not changed when a
new string is defined. Otherwise other operators may misinterpret the redefined event
message.

Message Text String Definitions

Access Denied
Reported whenever an invalid card is presented to a door/controller in an attempt to gain
access to a controlled area.

Access Granted
Reported whenever a valid card is presented to a door/controller, which then grants the
cardholder access to a controlled area.

Access Group Changed
Reported whenever an operator changes access group data.

Access Group Deleted
Reported whenever an operator deletes an access group.

All Doors Locked
Reported whenever an operator performs a Global Lock command, locking all doors in the
access control network.

All Doors Unlocked
Reported whenever an operator performs a Global Unlock command, unlocking all doors in
the access control network.

APB Violation
Reported whenever a card was used twice-in-a-row at a door in an attempt to gain access to a
secured area without first leaving that area. This prevents a cardholder from using a valid card
to enter a controlled area and then passing that card back for another person to use to enter
that area.

Auto-Collect Flag Off
Reported whenever an operator disables a controller’s buffer full/automatic dial-in feature.

Auto Lock Restored
Reported whenever an operator restores/enables a controller/door’s automatic locking feature.

Auto Lock Suspended
Reported whenever an operator suspends/disables a controller/door’s automatic locking
feature.

Autoconfig Performed
Reported whenever an operator performs the auto-configuration command, polling all
controllers for information used to create the controllers database.

Card File Changed
Reported whenever an operator changes card file or cardholder data.

Card Report Created
Reported whenever an operator requests a card report to be generated for review or printing.
Connect Refused - PIN
Reported whenever an operator’s attempt to log into a remote site was refused by the site’s master controller because the operator did not enter the correct personal identification number (PIN) for the site.

Connect Refused - Site
Reported whenever an operator’s attempt to log into a remote site was refused by the site’s master controller because the operator does not have the authorization to access the site.

Ctlr Cold Reset
Reported if a cold reset (power cycling off and then on) occurs at a controller.

Ctlr Com Failure
Reported if communication with a remote site’s master controller was lost unexpectedly.

Ctlr Com Restored
Reported whenever communication with a remote site’s master controller is made.

Ctlr Did Not Respond
Reported if a command is sent to a remote site’s master controller, but the controller does not respond, acknowledging it received the command.

Ctlr Event Threshold
Reported by a controller whenever that controller reaches its event buffer threshold and it needs to transfer/clear data from its buffer.

Ctlr Hard Reset
Reported if a hard reset (someone physically resetting the controller) occurs at a controller.

Ctlr Internal Error
Reported if a controller has an unidentifiable internal error.

Ctlr IO File Changed
Reported whenever an operator changes controller IO data definitions.

Ctlr Key DB Corrupt
Reported if a controller’s keypad database (used for secondary verification of a cardholder) is corrupt, invalidating its data.

Ctlr Memory Corrupted
Reported if a controller’s RAM memory is corrupted, disrupting controller operation.

Ctlr Self Test Failed
Reported if a controller’s self-test fails.

Ctlr Warm Reset
Reported if a controller’s “watch-dog” timer expires (indicating the controller might be hung).

Ctlr/Door File Changed
Reported whenever an operator changes controller/door configuration information.

Daylight Savings Off
Reported when the controller’s clock disables the one-hour time change for daylight savings time.
Daylight Savings On
Reported when the controller’s clock enables the one-hour time change for daylight savings time.

Door Closed
Reported whenever a door closes following a valid access request.

Door Forced Open
Reported if a door has been forced open without a valid access request having been made.

Door Locked
Reported whenever a controller locks a door.

Door Locked by Op
Reported whenever a controller is locked by an immediate lock command issued by an operator.

Door Not Opened
Reported if a door is not opened within the Unlock Time following a valid access request.

Door Opened
Reported whenever a door is opened following a valid access request.

Door Opened Too Long
Reported if a door is held open beyond the Open Time following a valid access request.

Door Report Created
Reported whenever an operator requests a door report to be generated for review or printing.

Door Unlocked
Reported whenever a controller unlocks a door.

Door Unlocked by Op
Reported whenever a controller is unlocked by an immediate unlock command issued by an operator.

Doors Disconnected
Reported if a door/controller is disconnected from the access control network.

Dual Access Denied
Reported whenever an invalid card is presented to a door/controller in dual-door configuration in an attempt to gain access to a controlled area.

Dual Access Granted
Reported whenever a valid card is presented to a door/controller in dual-door configuration, which then grants the cardholder access to a controlled area.

Event Report Created
Reported whenever an operator requests a event report to be generated for review or printing.

Events Collected
Reported whenever events are collected from a controller’s buffer.
Global Secure Lock
Reported whenever a controller is locked by an global secure lock command issued by an operator.

Global Unlock Off
Reported whenever an operator disables the global unlock command.

Global Unlock On
Reported whenever an operator enables the global unlock command.

Holiday List Changed
Reported whenever an operator changes holiday list names or dates.

Host Com Failed
Reported if a controller loses communication with the host computer.

Input Point Off
Reported whenever an input point on a controller changes state from active to inactive.

Input Point On
Reported whenever an input point on a controller changes state from inactive to active.

Interphone
Reported whenever a remote site attempts to dial-in to a host computer or a host computer attempts to dial-out to a remote site.

Link Active
Reported whenever a communication link is established between the host computer and the master controller at a remote site.

Link File Changed
Reported whenever an operator changes controller IO link data definitions.

Monitor File Changed
Reported whenever an operator changes any of the three system monitor window definition.

Monitor Started
Reported whenever an operator starts any of the three system monitor windows.

Monitor Stopped
Reported whenever an operator stops any of the three system monitor windows.

Net Connect Accepted
Reported whenever an operator’s request to connect to a remote site is accepted by the remote site’s master controller.

Net Connect Made
Reported whenever the host computer connects to a remote site.

Net Connect Request
Reported whenever an operator makes a request to connect to a remote site.

Net Disconnected
Reported whenever a remote site disconnects from the host computer.
Op Added Site
Reported whenever an operator adds a new remote site to the access control database.

Op Deleted Site
Reported whenever an operator deletes a remote site from the access control database.

Op Did Smart Update
Reported whenever an operator performs a smart update (uploading only database values that have changed since the last update).

Op Did Update
Reported whenever an operator performs a complete update (uploading all database information).

Op Locked Door
Reported whenever an operator performs an immediate lock door command.

Op Modified Site
Reported whenever an operator modifies/changes any of the operating parameters for a site.

Op Pulsed Door
Reported whenever an operator pulses a door lock (temporarily unlocking the door to allow momentary, immediate entrance).

Op Restored Output
Reported whenever an operator restores/enables an output point.

Op Set Network Time
Reported whenever an operator performs the set time command, synchronizing the time and date tracked by all the controllers to the time and date tracked by the host computer.

Op Turned Output On
Reported whenever an operator manually turns on an output point.

Op Turned Output Off
Reported whenever an operator manually turns off an output point.

Op Unlocked Door
Reported whenever an operator performs an immediate unlock door command.

Operator File Changed
Reported whenever an operator changes an operator definition.

Operator Logged Off
Reported whenever an operator logs off the access control software.

Operator Logged On
Reported whenever an operator logs on the access control software.

Output Point Off
Reported whenever an operator manually turns off an output point.

Output Point On
Reported whenever an operator manually turns on an output point.
Panel Armed
Reported whenever a controller/reader has been activated.

Panel Disarmed
Reported whenever a controller/reader has been inactivated.

Panel Tamper
Reported whenever a controller’s tamper switch has changed state, indicating someone has opened the controller’s enclosure.

Request to Exit
Reported whenever a controller receives a request to exit signal.

Timezone Changed
Reported whenever an operator changes a time zone definition.

Timezone Deleted
Reported whenever an operator deletes a time zone.

Unknown Event
Reported if an event has occurred on the access control system that is not recognized by the controller firmware or by the access control software.

Unknown Key
Reported if an attempt was made to access a secure area with a card that is not recognized by the site’s access control network.

Assigning Events to be Monitored

The Print in View One, Two, and Three fields allows an operator to select the events that should be displayed in each of the three monitor windows (see Figure 104). The default is for View One to display all events and for View Two and View Three to display no events.

Before assigning the events to be tracked by a monitor window, review the list of possible events and identify the events that should be tracked. In this example, view three will be configured for monitoring door access events. After reviewing the list of events, the following events will be selected for tracking in monitor window three.

- Access Denied
- Access Granted
- Door Closed
- Door Forced Open
- Door Locked
- Door Not Opened
- Door Opened
- Door Opened Too Long
- Door Unlocked

1. To access the assigning events to be monitored commands, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the Messages tab. The Messages window appears (see Figure 104).
3. Reviewing the above list, scan down the "Message Text" column and locate the "Access Denied" message text.
4. Scan across the access denied row to the "Print In View Three" column.
5. Click in the cell. It will change from a red OFF button to a green ON button.
6. Scan down the "Message Text" column and locate the "Access Granted" message text.
7. Scan across the access granted row to the "Print In View Three" column.
8. Click in the cell. It will change from a red OFF button to a green ON button.
9. The messages tab window should look similar to Figure 105.

10. Repeat this process for the seven other message text strings.
11. The resulting window will look similar to Figure 106.
12. To disable a print in view selection, locate the message text to be deleted. Scan across the text row to the print in view column to be disabled. Click in the cell. It will change from a green ON button to a red OFF button.

13. Click on the button. If the print in view change is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

14. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Save to File**

The save to file fields allow an operator to determine which events should be stored in the event file on the host computer’s hard disk when events are uploaded from the controllers to the host computer. Many events are normal day to day activities that an operator may not want to have take up space on the hard disk. The default is for all events to be saved to the event file on the hard disk.

In this example, the message text strings notifying when the controllers enable/disable Daylight Savings time will be disabled so they will not be recorded to the event file on the host computer’s hard disk.

1. To access the message text strings to not be saved to file, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the Messages tab. The Messages window appears (see Figure 107).
3. Use the scroll bar on the right side of the window and scroll down the list of message texts until the daylight savings message text strings appear (see Figure 108).

4. Locate the "Daylight Savings Off" message text.
5. Scan across the row to the "Save To File" column.
6. Click in the cell. It will change from a green ON button to a red OFF button.
7. Locate the "Daylight Savings On" message text.
8. Scan across the row to the "Save To File" column.
9. Click in the cell. It will change from a green ON button to a red OFF button.
10. The messages tab window should look similar to Figure 109.
11. Click on the \[button. If the save to file change is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

12. Now update the access control network with the new information. Click on the \[button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Controller Reports Events**

The controller reports events fields allow an operator to determine which events should be reported by the controller. Many events are normal day to day activities that an operator may not want to have take up controller processing time or event buffer space. The default is for all controller generated events to be stored and reported in the controller’s event buffer.

In this example, the message text strings (notifying when the controllers process the enabling/disabling of Daylight Savings time) will be disabled so they will not be stored and reported in the controller’s event buffer.

1. To access the message text strings to not be stored and reported in the controller’s event buffer, click on the Setup ⇒ Monitor and Events pull-down menu.
2. Click on the Messages tab. The Messages window appears (see Figure 110).
3. Use the scroll bar on the right side of the window and scroll down the list of message texts until the daylight savings message text strings appear (see Figure 111).

4. Locate the "Daylight Savings Off" message text.
5. Scan across the row to the "Controller Reports Event" column.
6. Click in the cell. It will change from a green ON button to a red OFF button.
7. Locate the "Daylight Savings On" message text.
8. Scan across the row to the "Controller Reports Event" column.
9. Click in the cell. It will change from a green ON button to a red OFF button.
10. The messages tab window should look like Figure 112.
11. Click on the button. If the controller reports event change is not saved before clicking any other button or exiting the setup monitor window, the data entered is lost and must be re-entered.

12. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).
Update the Network

Now that all of the instructions necessary to run the access control network have been created, they must be downloaded to the access control network. The Update Network command (also called Smart Update) uploads only the database changes from the host computer to the access control network.

1. Click on the icon on the tool bar. A series of windows similar to Figure 113 will appear as the program collects all the database changes to be sent to the access control network.

![Figure 113 – Collecting Information to Update the Network](image)

**NOTE:** Click on the **Cancel** button at any time to stop the update process.

2. Once all information has been collected, the host computer will connect to the access control network (if it isn’t already connected). The Net Communication window appears as the connection is being made (see Figure 114).

![Figure 114 – Connecting to the Access Control Network](image)

3. Once the connection is made a series of windows similar to Figure 115 appears indicating data is being transferred from the host computer to the access control network.

**NOTE:** Once the update process has begun, please be patient. The update process can take anywhere from several seconds to an extended period of time depending upon the amount of information to be updated and the number of controllers receiving information.
4. When these windows disappear, the access control network has received all updated information and has taken control of all doors/controllers.
System Operation

The system operation section explains how operators can manually and immediately perform the following tasks.

- lock and unlock doors
- perform a complete database update
- monitor and collect events from controllers
- create event reports
- identify an unknown card
- disconnect from the access control network
- window management
- retrieving the software revision and logged operator name

Locking, Unlocking, and Updating Doors

The locking and unlocking door commands allow an operator to manually override programmed door controls. The updating doors command allows an operator to rewrite database information from the host computer to doors on the access control network.

1. To enter the operate door commands window, click on the Operate ⇒ Doors pull-down menu option, or click on the icon on the tool bar. The Operate Doors window appears (see Figure 116).

![Operate Doors Window](image)

Figure 116 – Operate Doors Window

When working with the operate doors commands, the following buttons and fields apply to all commands (see Figure 116).
The **Select ALL** button selects all doors associated with the selected door class, allowing door operations to be performed on these doors.

The **Deselect ALL** button deselects all doors associated with the selected door class, not allowing door operations to be performed on these doors.

The **Cancel** button cancels any operation being performed.

The **STATUS** field lists each operation that has been performed and the status of that operation.

**Lock Doors**

The lock doors command can lock all doors in the access control system, all doors within a door class, or a single door. To lock doors, first select the doors to be locked and then perform the lock command.

**Lock All Doors**

To lock all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the **Select ALL** button, and then click on the **Lock** button. The resulting window should look similar to Figure 117.

![Figure 117 – Locking All Doors](image)

**Lock All Doors in a Door Class**

To lock all doors in a door class; for example, the Exterior Doors door class (refer to the **Assign a Door Class** section under **Setup Doors/Controllers** for information regarding door classes):
1. Click on the icon for the door class to be locked; under Door Classes, click on the **Exterior Doors** icon.

2. Click on the [Select ALL] button, and then click on the [Lock] button. In this example, the Exterior Doors door class was selected; the resulting window will look similar to Figure 118.

![Figure 118 – Locking All Doors in a Door Class](image)

**Lock a Single Door**

To lock a single door; for example, the Stockroom Door:

1. Locate the door to be locked. Either click on the **All Doors** icon or click on the door group icon the door is listed under. For this example, click on the **Interior Doors** door group icon.
2. Locate and click on the icon for the door to be locked. For this example, click on the **Stockroom Door** icon.
3. Click on the [Lock] button. The resulting window will look like Figure 119.
Unlock Doors

The unlock doors command can unlock all doors in the access control system, all doors within a door class, or a single door. To unlock doors, first select the doors to be unlocked and then perform the unlock command.

Unlock All Doors

To unlock all doors:

1. Click on the ALL DOORS icon under Door Classes.

2. Click on the Select ALL button, and then click on the Unlock button. The resulting window should look similar to Figure 120.

Figure 119 – Locking a Single Door
Unlock All Doors in a Door Class

To unlock all doors in a door class; for example, the Exterior Doors door class:

1. Click on the icon for the door class to be unlocked; under Door Classes, click on the Exterior Doors icon.

2. Click on the button, and then click on the button. In this example, the Exterior Doors door class was selected. The resulting window will look similar to Figure 121.
**Unlock a Single Door**

To unlock a single door; for example, the Stockroom Door:

1. Locate the door to be unlocked. Either click on the **All Doors** icon or click on the door group icon the door is listed under. For this example, click on the **Interior Doors** door group icon.
2. Locate and click on the icon for the door to be unlocked. For this example, click on the **Stockroom Door** icon.
3. Click on the **Unlock** button. The resulting window will look similar to Figure 122.

![Figure 122 – Unlocking a Single Door](image)

**Timed Unlock**

The timed unlock doors command unlocks doors until the door’s unlock time expires; then it re-locks the door. This command can timed unlock all doors in the access control system, all doors within a door class, or a single door. To timed unlock doors, first select the doors to be unlocked and then perform the timed unlock command (refer to the **Set A Door Unlock Time** section under **Setup Doors/Controllers** for information regarding door unlock times).

**Timed Unlock All Doors**

To timed unlock all doors:

1. Click on the **ALL DOORS** icon under Door Classes.
2. Click on the **Select ALL** button, and then click on the **Timed Unlock** button. The resulting window should look similar to Figure 123.
Timed Unlock All Doors in a Door Class

To timed unlock all doors in a door class; for example, the Exterior Doors door class:

1. Click on the icon for the door class to be timed unlocked; under Door Classes, click on the Exterior Doors icon.

2. Click on the Select ALL button, and then click on the Timed Unlock button. In this example, the Exterior Doors door class was selected. The resulting window will look similar to Figure 124.
Timed Unlock a Single Door

To timed unlock a single door; for example, the Stockroom Door:

1. Locate the door to be timed unlocked. Either click on the All Doors icon or click on the door group icon the door is listed under. For this example, click on the Interior Doors door group icon.
2. Locate and click on the icon for the door to be timed unlocked. For this example, click on the Stockroom Door icon.
3. Click on the button. The resulting window will look similar to Figure 125.

![Timed Unlocking a Single Door](image)

Figure 125 – Timed Unlocking a Single Door

Update Doors

Updating doors completely rewrites all database information stored on the selected controllers (as opposed to the update net command which only updates changes in databases). This command can update all doors in the access control system, all doors within a door class, or a single door. To update doors, first select the doors to be updated and then perform the update command.

**NOTE:** As an update doors command is a complete rewrite of databases, it takes longer to perform than an update net command. When an update doors command is performed, please be patient as data is transferred. Depending upon the number of controllers and the size of the databases, this operation can take several minutes to perform.

Update All Doors

To update all doors:

1. Click on the ALL DOORS icon under Door Classes.
2. Click on the button, and then click on the button. A series of status windows appear (see Figure 126), tracking the data being transferred to all the doors/controllers.
Figure 126 – Transferring Data Status Windows

3. Once the complete data transfer process is complete, the resulting window should look similar to Figure 127.

Figure 127 – Update All Doors

**Update All Doors in a Door Class**

To update all doors in a door class; for example, the Exterior Doors door class:

1. Click on the icon for the door class to be unlocked; under Door Classes, click on the Exterior Doors icon.

2. Click on the **Select All** button, and then click on the **Update Doors** button. A series of status windows appear (see Figure 126), tracking the data being transferred to all the doors/controllers. In this example, the Exterior Doors door class was selected. The resulting window will look similar to Figure 128.
Figure 128 – Updating All Doors in a Door Class

Update a Single Door in a Door Class
To update a single door; for example, the Stockroom Door:

1. Locate the door to be updated. Either click on the All Doors icon or click on the door group icon the door is listed under. For this example, click on the Interior Doors door group icon.
2. Locate and click on the icon for the door to be updated. For this example, click on the Stockroom Door icon.
3. Click on the Update Doors button. A series of status windows will appear (see Figure 126), tracking the data being transferred to all the doors/controllers. The resulting window will look similar to Figure 129.
Figure 129 – Updating a Single Door
Monitor and Collect Events from the Controllers

This section describes the use of the monitor windows and the process for collecting events from all controllers on the access control network for storage on the host computer’s hard disk.

1. To enter the operate system monitor window, click on the Operate ⇒ Start Monitor pull-down menu or click on the icon on the tool bar. The Operate Monitor window appears (see Figure 130).

![Figure 130 – Operate Monitors Window](image)

Verifying Communication Status

The Connection Status field displays the communication connection status between host computer and access control network. Within the connection status field are four panes with information (see Figure 130).

- Pane 1 (at the top) displays event collection status when event collection is underway – the number of events collected from each controller and the number of events processed by a monitor window.
- Pane 2 (second from the top) displays the type of connection between host computer and access control network – direct using a cable between master controller and host computer or remote using modems between master controller and host computer.
- Pane 3 (third from the top) displays the COM port used for communication.
- Pane 4 (at the bottom) displays if the network is ONLINE (actively connected and communicating with the host computer) or OFFLINE (disconnected from the host computer).

Starting Monitoring

The view window field is made up of three buttons: 1, 2, and 3; one for each monitoring window (see Figure 130).

1. To open a monitor window, click on the button corresponding to the desired monitor.
NOTE: Before opening a monitor, it must have been set up in the Setup ⇒ Monitors and Events section, defining what it monitors. Otherwise, the default is for monitor one to view all events, and for monitors two and three to view no events.

2. Once a monitor window is open, an operator can size it according to how the operator wants the monitor window positioned on the Doors window.

3. Any combination of the three monitor windows can be open at the same time. Each can be sized individually, but the default is for all three windows to be tiled horizontally across the Doors window (see Figure 131).

4. Once monitoring windows have been opened, monitoring can begin. Click on the Monitor button. If communication has not been established between the host computer and the access control network, Doors will make the connection.

5. As events occur on the access control network that meet the criteria of the monitoring window, they will be displayed in the monitoring window.

Collecting Events

Collecting events from all controllers clears the controller buffers and stores the events in an event file on the hard disk. Event data can then be processed into report formats.

1. To collect events, click on the Collect button. If communication has not been established between the host computer and the access control network, Doors will make the connection.

2. Pane 1 in the communication status field will display event collection status as each controller is contacted (see Figure 130). When complete, Pane 1 will go blank.

Stopping Monitoring

There are two ways to stop the monitoring process.

1. Click on the Stop button in the operate monitors window (see Figure 130). This ends the monitoring process but does not close the monitoring windows or the communication link between host computer and access control network.
2. To close all system monitor windows and disconnect the host computer from the access control network, click on the Operate % Stop Monitor pull-down menu or click on the icon on the tool bar.

Create Event Reports

There are two types of event reports: quick search reports and power search reports. In a quick search, the operator selects search parameters from a short list of commonly used search criteria. In a power search, the operator creates a search expression from lists of events, boolean operators, event values, and linking operators. Once created, power search expressions can be saved in a library for future use.

Quick Search Event Report

To create a quick search event report, click on the Reports ⇒ Events pull-down menu option. The Event Reports window appears (see Figure 132).

![Quick Search Event Reports](image1)

Figure 132 – Quick Search Event Reports

Clear all Fields

The clear button clears all data fields and returns all search selection parameters to default values (which shows all events). This is a destructive operation, removing all entered search parameters.

1. To clear all fields, click on the button. To verify the clear operation should be performed, a confirmation window appears (see Figure 133).

![Clear Search Fields Confirmation Window](image2)

Figure 133 – Clear Search Fields Confirmation Window
2. Click on the ✓ button.

Select Doors

The doors radio buttons allow an operator to select if event information should be reported for all doors or for just one selected door.

1. To select all doors, click on the All Doors radio button (the default value, see Figure 132).
2. To select one door, click on the Selected Door radio button. A list of all available doors appears in the window (see Figure 134).

![Figure 134 – Available Door List](image)

3. Scroll through the list and locate the door for which a report is desired. Click on that door name and it will be entered into the selected door field (see Figure 135).

![Figure 135 – Selected Door](image)

4. To select a different door, click on the box and the list of available doors will reappear.
NOTE: To accommodate the multiple sites feature, all door names are prefaced with their site name. If the sites feature has not been enabled, the door name is prefaced with "Default Site."

Select Cardholders
The cardholders radio buttons allow an operator to select if event information should be reported for all cardholders or for just one selected cardholder.

1. To select all cardholders, click on the **All Cardholders** radio button (the default value, see Figure 132).
2. To select one cardholder, click on the **Selected Cardholder** radio button. A list of all available cardholders appears in the window (see Figure 136).

![Figure 136 – Available Cardholder List](image)

3. Scroll through the list and locate the cardholder for which a report is desired. Click on that cardholder name and it will be entered into the selected cardholder field (see Figure 137).

![Figure 137 – Selected Cardholder](image)

4. To select a different cardholder, click on the box and the list of available cardholders will reappear.
Select Events

The events radio buttons allow an operator to select if event information should be reported for all events or for just events selected from the provided list.

1. To select all events, click on the All Events radio button (the default value, see Figure 132).
2. To select events from the provided list, click on the Selected Event radio button. Beneath the selected events radio button is a list of the five most commonly requested event report parameters.
3. To select any or all of these five events for event reporting, click on the checkbox beside the event. When a check-mark appears in the box, the event is selected. If the box is empty, the event is not selected (see Figure 138).

![Event Reports]

Figure 138 – Selected Events

Select Dates

The dates radio buttons allow an operator to select if event information should be reported for all dates or just between selected days and times.

1. To select all dates, click on the All Dates radio button (the default value, see Figure 132).
2. To select dates between selected days, click on the From . . . To radio button.
3. In the From field, enter the beginning date and time for reporting events. If the time field is left blank, the events from the beginning of the day (Midnight) are reported. For example, to report on events beginning on July 4, 1997 at 17:00 hours, double-click in the From date field and type **07/04/1997**. Double-click in the From time field and type **17:00** (see Figure 139).
4. In the To field, enter the ending date and time for reporting events. If the time field is left blank, the events from the entire day are reported. For example, to report on events ending on July 5, 1997 at 08:00 hours, double-click in the To date field and type **07/05/1997**. Double-click in the To time field and type **08:00** (see Figure 139).
Generate Report Output

Once a report search criteria has been set, there are three formats for generating the event report output.

- view the report on the computer
- print the report
- save the report to an ASCII text file

View Report on Screen

1. To view the event report on the computer, click on the button. All event data will be reviewed and sorted based on the criteria in the Quick Search window.
2. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 140). Click on the OK button and modify the search criteria in the Quick Search window.
3. If the search was successful, a success window appears (see Figure 141).
4. Click on the button and the report window appears (see Figure 142). Use the scroll bars to review the information within the report.

![Successful Report Window](image)

Figure 141 – Successful Report Window

![View Report Window](image)

Figure 142 – View Report Window

**Print Report**

1. To print the event report, click on the button. All event data will be reviewed and sorted based on the criteria in the Quick Search window.

2. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 140). Click on the OK button and modify the search criteria in the Quick Search window.

3. If the search was successful, a Windows Print Window appears. Enter any printer parameters as needed (print parameters vary based on the type of printer installed and on the Windows setup parameters).

4. Click on the OK button and the report is printed.

**Save Report to File**

1. To save the event report to an ASCII file on the computer, click on the button. All event data will be reviewed and sorted based on the criteria in the Quick Start window.
2. If there was no data that meets the search criteria, an empty report warning window appears (see Figure 140). Click on the OK button and modify the search criteria in the Quick Search window.

3. If the search was successful, a Windows File Save window appears.

4. In the File Name field, enter a descriptive file name. For example, for an event report of back door access:
   - in Windows 95 it could be named "Back Door Access.txt"
   - in Windows 3.11 it could be named "bkdracc.txt"

   NOTE: The Windows 3.11 operating system has a limitation of no more than 8 characters for the file name and 3 characters for the extension. The Windows 95 operating system maintains the 3 character limitation for the extension, but allows up to 255 characters for the file name.

5. In the Folders field, locate the folder where the report file should be saved (the default is to save it in "c:\kerisys\doors").
6. Click on the OK button and the report is saved.

**Power Search Event Reports**

Power search event reports allow an operator to create custom event reports by creating custom database search expressions. These expressions are created to filter out unwanted information so that the report contains just the desired information.

Power searches are performed on the event file stored on the host computer. The event file is a collection of all events received from all controllers on the access control network. Each event in the file is saved as a string of information. When generating a power search event report, the search expression is applied to each event string and those strings that meet the search expression criteria are added to the report.

   NOTE: To successfully create custom database search expressions, the operator must have a basic understanding of Boolean arithmetic. Boolean arithmetic is the tool used to create the custom search expressions. This Users Guide will describe the Boolean operators used in this program, but it cannot teach Boolean arithmetic.

To create a search expression, individual search criteria parameters are defined in the new criterion field (see Figure 143) and then are entered into the search expression field to create the complete search expression. There are five individual fields within the new criterion field. A search expression can consist of one Field Type, Operation, and Field Value for a simple data filter. Or it can include Link operators to combine simple expressions into complex expressions, and parenthetical operators to group certain expressions together to perform complex data filtering.

- Field Type – The type of data for which to search.
- Operation – The Boolean operator to use to determine how to include and exclude data.
- Field Value – The value of the Field Type data for which to search.
- Link – Combines Field Type, Operation, and Field Value expressions.
- Group – Parenthetical grouping operators to create complex expressions.
This section describes the individual fields and values used to create a power search expression, and then it provides an example of creating a complex power search.

**Field Type and Field Value**

The Field Type identifies the type of event data to be retrieved to generate a report. The items in the Field Type list correspond to information in each event file string. The Field Value is the specific value of the event data to be retrieved to generate a report.

There are five Field Types; each type having a specific set of Field Values.

- **Event (TYPE)** sets the search criteria to retrieve events (such as Access Denied, Door Forced, or Request to Exit). When Event (TYPE) is selected, a pull-down list of all 87 possible events appears for selection in the Value Field (see the Message Text String Definitions section, earlier in this users guide, for descriptions of all 87 possible events).

- **Time (MIN_MIDN)** sets the search criteria to retrieve all events that occurred at a specific time. When Time (MIN_MIDN) is selected, the specific time for which to search must be entered in the Value Field.

- **Date (TIMEDATE)** sets the search criteria to retrieve all events that occurred on a specific date. When Date (TIMEDATE) is selected, a specific date for which to search must be entered in the Value Field.

- **Door (DOOR)** sets the search criteria to retrieve all events that occurred at a specific door. When Door (DOOR) is selected, a pull-down list of all available doors in the access control network appears for selection in the Value Field.

- **Name (KEYNUM)** sets the search criteria to retrieve all events that occurred to a specific cardholder. When Door (DOOR) is selected, a pull-down list of all available cardholders in the access control network appears for selection in the Value Field.
Boolean Operators

Boolean operators determine how the data being searched will be filtered to locate the data specifically requested by the report. There are six Boolean operators.

- Equal To (=)
- Greater Than or Equal To (>=)
- Less Than or Equal To (<=)
- Greater Than (>)
- Less Than (<)
- Not Equal To (<>)

**Equal To (=)**
As a report is being generated, a search expression using the Equal To operator examines each data string in the event database, searching for data strings that meet the search expression’s Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is equal to the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date (TIMEDATE) and the Field Value is set to 07/04/1997, the report would only include events that occurred on July 4, 1997 (see Figure 144). Events that occurred on any other date would be excluded from the report.

![Figure 144 – Equal To Criterion Sample](image)

**Greater Than or Equal To (>=)**
As a report is being generated, a search expression using the Greater Than or Equal To operator examines each data string in the event database, searching for data strings that meet the search expression’s Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is greater than or equal to the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date (TIMEDATE) and the Field Value is set to 07/04/1997, the report would only include events that occurred on or after July 4, 1997 (see Figure 145). Events that occurred before July 4, 1997 would be excluded from the report.

![Figure 145 – Greater Than or Equal To Criterion Sample](image)
Less Than or Equal To (\(\leq\))
As a report is being generated, a search expression using the Less Than or Equal To operator examines each data string in the event database, searching for data strings that meet the search expression’s Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is less than or equal to the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date (TIMEDATE) and the Field Value is set to 07/04/1997, the report would only include events that occurred on or before July 4, 1997 (see Figure 146). Events that occurred after July 4, 1997 would be excluded from the report.

Figure 146 – Less Than or Equal To Criterion Sample

Greater Than Operator (>)
As a report is being generated, a search expression using the Greater Than operator examines each data string in the event database, searching for data strings that meet the search expression’s Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is greater than the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date (TIMEDATE) and the Field Value is set to 07/04/1997, the report would only include events that occurred after July 4, 1997 (see Figure 147). Events that occurred on or before July 4, 1997 would be excluded from the report.

Figure 147 – Greater Than Criterion Sample

Less Than Operator (<)
As a report is being generated, a search expression using the Less Than operator examines each data string in the event database, searching for data strings that meet the search expression’s Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is less than the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date (TIMEDATE) and the Field Value is set to 07/04/1997, the report would only include events that occurred before July 4, 1997. Events that occurred on or after July 4, 1997 would be excluded from the report (see Figure 148).
As a report is being generated, a search expression using the Not Equal To operator examines each data string in the event database, searching for data strings that meet the search expression’s Field Type.

If the Field Type is a match, the Field Value in the data string is then compared with the Field Value in the search expression. If the value in the data string is not equal to the value in the expression, the data string is included in the report; if not, it is excluded from the report.

For example, if the Field Type is set to Date (TIMEDATE) and the Field Value is set to 07/04/1997, the report would only include events that did not occurred on July 4, 1997. Events that occurred on July 4, 1997 would be excluded from the report (see Figure 149).

**Boolean Links**

Boolean links are used to link simple expressions together to create complex expressions where several conditions must be met before data should be included in a report. Since a link cannot be done until there are at least two expressions, the link field does not become active until at least one expression has been entered into the Search Expression field. There are three types of links.

- **AND**
- **OR**
- **NOT**

**AND**

An AND link allows operator to link two search expressions together so that as event data is being reviewed for a report the data must meet the criteria in both expressions to be included in the report.

For example, an AND link consisting of \texttt{TIMEDATE=07/04/1997 AND EVENT=Access Denied} would filter event data and create a report that displays only the Access Denied events that occurred on July 4, 1997.

**OR**

An OR link allows operator to link two search expressions together so that as event data is being reviewed for a report the data must meet the criteria in either expression to be included in the report.

For example, an OR link consisting of \texttt{TIMEDATE=12/24/1997 AND TIMEDATE=12/25/1997} would filter event data and create a report that displays all events that occurred on either December 24, 1997 or December 25, 1997.
NOT
A NOT link allows operator to link a search expression so that as event data is being reviewed for a report the data that meets the criteria is excluded from the report.

For example, a NOT link consisting of NOT Event=Access Granted would filter event data and exclude all Access Granted events from the report.

Grouping Operator
Grouping operators allow an operator to combine search expressions to create complex search expressions. Pairs are placed around expressions that need to be nested within larger expressions. The expressions with the pairs are evaluated as a group and the results will be applied to the larger expression outside the pairs.

For example, a complex expression consisting of (Event=Request To Exit AND DATE=07/04/1998) AND (Event=Door Opened AND DATE=07/04/1998) would filter event data and create a report that only consisted of Request to Exit and Door Opened events that occurred on July 4, 1998.

Search Expression Field
Once a search expression has been defined in the New Criterion field, it must be added to the Search Expression field. Searches are performed from the expressions in the Search Expression field.

1. To add a search expression to the Search Expression field, simply click on the button (see Figure 143). The expression in the New Criterion field is entered into the Search Expression field in the format used by the search/sort algorithm.

2. To delete a search expression from the Search Expression field, click on the button (see Figure 143). The last expression added to the search expression field will be removed.

Clear all Fields
Before creating a search expression, all data fields should be cleared to ensure no "left-over" search parameters affect the new entry. The clear button clears all data fields and returns all search selection parameters to default values (which shows all events).

1. To clear all fields, click on the button. To verify the clear operation should be performed, a confirmation window appears (see Figure 133).

2. Click on the button.

Power Search Example
An operator needs to create a search expression that generates a report that meets the following criteria.

- any Access Denied or Door Forced Open events
- occurring at either the Front Door or Back Door
- on July 5, 1997
- during 00:00 hours to 08:00 hours (Midnight to 8 A.M.)
Perform the following steps to set the search expression to search only for Access Denied or Door Forced Open events.

1. Click on the **CLEAR** button.
2. Click on the **Left Paren** button.
3. Set the Field Type to **Event(TYPE)**.
4. Set the Operation to **=**.
5. Set the Field Value to **Access Denied**.
6. Click on the **ADD** button.
7. Set the Link field to **OR**.
8. Set the Field Type to **Event(TYPE)**.
9. Set the Operation to **=**.
10. Set the Field Value to **Door Forced Open**.
11. Click on the **Right Paren**.
12. Click on the **ADD** button.

Figure 150 displays the search expression to this point.

Perform the following steps to add the Front Door and Back Door only requirement.

1. Set the Link field to **AND**.
2. Click on the **Left Paren** button.
3. Set the Field Type to **Door(DOOR)**.
4. Set the Operation to **=**.
5. Set the Field Value to **Default Site, Front Door**.
6. Click on the **ADD** button.
7. Set the Link field to **OR**.
8. Set the Field Type to **Door(DOOR)**.
9. Set the Operation to **=**.
10. Set the Field Value to **Default Site, Back Door**.
11. Click on the **Right Paren** button.
12. Click on the **ADD** button.

Figure 151 displays the search expression to this point.
Perform the following steps to add the July 5, 1997 requirement.

1. Set the Link field to **AND**.
2. Set the Field Type to **Date(TIMEDATE)**.
3. Set the Operation to **=**.
4. Set the Field Value to **07/05/1997**.
5. Click on the **ADD** button.

Figure 152 displays the search expression to this point.

Perform the following steps to add the 00:00 hours to 08:00 hours (Midnight to 8 A.M.) requirement.

1. Set the Link field to **AND**.
2. Click on the **Left Paren** button.
3. Set the Field Type to **Time(MIN_MIDN)**.
4. Set the Operation to **>=**.
5. Set the Field Value to **00:00**.
6. Click on the **ADD** button.
7. Set the Link field to **AND**.

Figure 152 – Limiting the Search to July 5, 1997
8. Set the Field Type to **Time(MIN_MIDN)**.
9. Set the Operation to **<=**.
10. Set the Field Value to **08:00**.
11. Click on the **Right Paren** button.
12. Click on the **ADD** button.

Figure 153 displays the complete search expression.

![Event Reports](image)

Figure 153 – Limiting the Search to the Hours of 00:00 to 08:00

This completes the creation of the power search example. Keri Systems strongly recommends saving power searches, as explained in the **Library Tab** section of the Event Reports window.

**Generate the Report**

The report generation process is identical between Quick Searches and Power Searches. Please refer to the **Generate the Report** section immediately following the **Quick Search Event Reports** section above.

**Library Tab**

As operators develop search expressions to generate specific event reports, these expressions can be saved into a library (see Figure 154). Once in the library, they can be retrieved and run at specific times, and they can be deleted.
Save a Search Expression

To save a search expression, a new search expression must have been created under the Power Search tab.

1. To save a search expression, click on the on the Library tab (see Figure 154). Verify that the expression to be saved is entered in the "Search Expression" field.
2. Click in the "Select Template" field and enter a descriptive name for the search expression. For example, using the search expression entered in the power search example above, type July 5 Door Check.
3. Click on the button.

Get a Search Expression

Search expressions that have been saved can be retrieved and run.

1. To retrieve a search expression, click on the Library tab (see Figure 150).
2. In the Select Template" field, click on the box and a list of available search expressions is displayed (see Figure 155).
3. Scroll up and down the list, locate the desired search expression, and click on it. For example, click on the **July 5 Door Check** template.

4. Click on the ![GET](image-url) button.

5. The search expression is then displayed in the "Search expression text" field. The operator can review the expression to verify it is the correct one (see Figure 154).

**Delete a Search Expression**

If a search expression is not needed, an operator can delete it.

1. To delete a search expression, get the search expression to be deleted as described in the **Get a Search Expression** section above.

2. Click on the ![DELETE](image-url) button (see Figure 154).

**NOTE:** Use the delete feature with caution. Once a search expression is deleted it cannot be recovered; it must be recreated.

**Options Tab**

There are two power search data sorting options available for an operator to choose.

- reverse order of sort
- use card ID numbers in report file

**Reverse Order of Sort**

An operator can choose to reverse the sort order of data in an event report. The default sort order for data is in ascending order, from A to Z or from lowest number to highest number. Reversing the sort order sorts in descending order, from Z to A or from highest number to lowest number.

1. To reverse the sort order, click on the **Options** tab. The Options window appears (see Figure 156).

2. To reverse the sort order, in the General Options field, click on the "Reverse order of sort" box. If the box has a checkmark, the report sorts in descending order, from Z to A or from highest number to lowest number.
3. If the box does not have a checkmark, the report sorts in ascending order, from A to Z or from lowest number to highest number.

Save Card ID Numbers in the Report File

An operator can choose to print card ID numbers instead of cardholder names in an event report. The default is to print cardholder names. Printing the card ID numbers replaces the cardholder name with the card number (the number etched into the body of the card) of the cardholder’s card.

1. Click on the Options tab. The Options window appears (see Figure 156).
2. To print the card ID number, in the Advanced Options field, click on the "Card ID numbers in report file" box; a checkmark appears. With a checkmark in the box, the report prints the card ID numbers.
3. To print the cardholder’s name, in the Advanced Options field, click on the "Card ID numbers in report file" box; the checkmark disappears. With no checkmark in the box, the report prints the cardholder’s name.
**Identify an Unknown Card**

The Doors program is able to read and identify a card’s holder in three different ways.

- reading the card at the enrollment reader
- entering the card’s internal number
- entering the card’s number – the number printed on the body of the card

1. To identify an unknown card, click on the Reports ⇒ ID Card pull-down menu. The ID Unknown Card window appears (see Figure 157).

![Figure 157 – Identify Unknown Card Window](image)

**ID by Reading the Card**

In this example, a card was found on the floor and the operator wants to identify whose card it is.

1. Click on the Read Card radio button (see Figure 157).
2. Click on the button.
3. Present the card to the enrollment reader.
4. The cardholder’s name and the card’s internal and external numbers are displayed in the "Instructions and Results" field (see Figure 158).

![Figure 158 – Card Identified by Reading](image)
ID by Entering the Internal Number

In this example, the operator has a card’s internal number and wants to identify whose card it is.

1. Click on the **By Internal Number** radio button (see Figure 157).
2. Click in the "Identify Unknown Card" field.
3. Type the card’s internal number. For this example, type **876091833**.
4. Click on the **button**.
5. The cardholder’s name is displayed in the "Instructions and Results" field (see Figure 159).

![Figure 159 – Card Identified by the Internal Number](image)

ID by Entering the Card Number

In this example, a card was found on the floor and the operator wants to identify whose card it is, but the enrollment reader is unavailable.

*NOTE: This method is only valid for K-series Keri Systems Proximity Cards (see Figure xxx).*

1. Click on the **By Card Number** radio button (see Figure 157).
2. Click in the "Identify Unknown Card" field.
3. Reading from the body of the card, type the card’s number (the last six digits etched on the card – see Figure 160). For this example, type **211774**.

![Figure 160 – Proximity Card Number](image)

4. Click on the **button**.
5. The cardholder’s name is displayed in the "Instructions and Results" field (see Figure 161).
Disconnect from the Access Control Network

In order to perform the following functions correctly, the host computer must be actively connected to the access control network. In the case of modem connections between a host computer and a remote site, Doors will automatically dial-up the remote site.

- Auto-Config
- Card Enrollment
- Set Time
- Update Net
- User Initiated Door Commands
- Monitor or Event Collection Modes

Doors does not automatically disconnect when these actions are completed. If the connection between host computer and access control network is made via modem over a distance that requires a toll call, the connection must be manually disconnected. Otherwise, the resulting phone bill can be needlessly high.

1. To disconnect from the access control network, click on the Operate ⇒ Net Disconnect pull-down menu. The access control network is immediately disconnected from the host computer.

Window Management

At times an operator might find it necessary or advantageous to have several database windows open at the same time. There are 5 tools to help in switching between open database windows.

- cascade windows
- tile windows
- tile windows horizontally
- arrange icons
- cycle windows

Cascading Windows

Cascading windows automatically takes all open windows and arranges them, one on top of another, with the title bars showing for each window.
1. To cascade all open windows, click on the Window ⇒ Cascade pull-down menu option. The individual database windows will be organized in the Doors window as shown in Figure 162.

Figure 162 – Cascading Database Windows

**Tiling Windows**

Tiling windows automatically takes all open windows and arranges them, side-by-side, from left-to-right, filling the Doors window.

1. To tile all open windows, click on the Window ⇒ Tile pull-down menu option. The individual database windows will be organized in the Doors window as shown in Figure 163.

Figure 163 – Tiled Database Windows

**Tiling Windows Horizontally**

Horizontally tiling windows automatically takes all open windows and arranges them, side-by-side, from top-to-bottom, filling the Doors window.
1. To horizontally tile all open windows, click on the Window ⇒ Tile Horizontally pull-down menu option. The individual database windows will be organized in the Doors window as shown in Figure 164.

![Horizontally Tiled Database Windows](image1)

Figure 164 – Horizontally Tiled Database Windows

### Arranging Icons

Database windows on the Doors window can be reduced to icons that sit on the bottom of the Doors window.

1. To reduce a database window to an icon, click on the box in the upper-right corner of the database window.
2. To horizontally tile all open windows, click on the Window ⇒ Tile Horizontally pull-down menu option. The individual database windows will be organized in the Doors window as shown in Figure 165.

![Windows Icons](image2)

Figure 165 – Window Icons
Cycling Windows

Cycling windows automatically takes all open windows and arranges them in a cascading fashion as explained above. And then, using the cycle windows icon, allows the operator to quickly switch between all cascaded windows.

1. To cycle between all open windows, click on the Window → Cycle pull-down menu option or click on the icon on the tool bar. The individual database windows will be organized as shown in Figure 166 and each click on the icon will switch to the next open window.

![Figure 166 - Cycling Database Windows](image)

Retrieving the Software Revision and Logged Operator

At times it is necessary to verify the revision of the Doors software and to verify which operator is logged on the program.

1. To determine which version of Doors software is installed on the host computer and which operator is logged into the Doors program, click on the Help → About pull-down menu. A window similar to Figure 167 will appear.

![Figure 167 - Retrieving the Software Revision and Logged Operator](image)

2. Displayed in this window is the software revision (2.10 for this example) and the current operator (Sys Supervisor).
3. Once this information has been retrieved, click on the button to close the window.
This page is intentionally left blank.
System Maintenance

To provide the best long-term operating conditions for the Doors software, there are three system maintenance steps that should be performed.

- secure storage of the Doors source disks
- periodic backup of the Doors software
- periodic event log archiving

Secure Storage of Source Disks

The original Doors installation disks should be stored in a safe, secure place away from environmental extremes and magnetic fields. Safe, secure storage is not just for the sake of software reinstallation should there be a host computer system crash, but to keep the software out of the hands of unauthorized personnel.

Using the installation disks, it is possible for an unauthorized person to reinstall the Doors software and use the default passwords to modify the system operator database. This can result in the creation of an operator or cardholder that will have unlimited access to the secured area, violating the integrity of the access control system.

Periodic Doors Software Backup

The Doors access control software and its databases should be backed-up periodically to a remote storage device (i.e. floppy disks or tape). The more often the system is backed-up, the less data reconstruction will need to be done in the event of a host computer system crash. The easiest method to backup data is to use the backup program provided in Windows 95 and Windows 3.11.

In Windows 95

Use the Microsoft Backup program (backup.exe) found in the Program Files\Accessories\ folder. Simply run the backup program, follow the instructions it provides, and select the "kerisys" folder when prompted. The program has on-line help to answer any questions regarding the operation of the backup program.

In Windows 3.11

Use the DOS backup program (msbackup.exe) found in the \dos subdirectory. Simply run the backup program, follow the instructions it provides, and select the "kerisys" subdirectory when prompted. The program has on-line help to answer any questions regarding the operation of the backup program.

NOTE: For a backup process, the size of the "kerisys" folder and the amount of storage space needed for backup is dependent upon the size of the event storage files; the longer a system has been in operation, the larger the size of the storage space needed to backup everything. By selecting the "kerisys" folder for backup, everything in that folder (and its sub-folders) will be stored.
Archiving the Event Logs

The event logs should be archived on a periodic basis. Archiving a event log, closes the original log and assigns it a descriptive name, allowing a new event log to be created. Periodic archiving prevents the event log from becoming too large for efficient data processing. Report generation can take a long time when the event log files are too large.

Event log storage is done by renaming the existing event logs. When the Doors program discovers the original logs are unavailable, it will automatically create a new set of event logs, using the default log names.

To ensure all current data is stored, collect all events per the instructions in the Monitor and Collect Events from the Controllers section of this Users Guide before storing the event logs.

NOTE: If the Doors software is backed-up periodically (i.e. monthly) as described in the previous section, the event logs are included in the backup and would not need to be archived. Locate and delete the EVT.DBF and EVT.MDX files in the "kerisys\doors\db\files" folder to clear the event logs.

In Windows 95

1. Run the Windows Explorer program.
2. Locate the EVT.DBF and EVT.MDX files in the "kerisys\doors\db\files" folder.
3. Rename these files using the following parameters.
   - The new names for the two files must be the same to track which event log files go together.
   - The new names must retain the .DBF and .MDX file extensions.
   - The new names may not have more than seven characters. Keri Systems recommends the following format: DDMMMYY.DBF and DDMMMYY.MDX.

   DD = day of archive
   MMM = month of archive
   YY = year of archive

4. Exit the Windows Explorer program.

Using this format for a set of event files archived on July 1, 1997, the EVT.DBF file would be renamed 01JUL97.DBF and the EVT.MDX file would be renamed 01JUL97.MDX.

In Windows 3.11

1. Open a DOS window.
2. Change directory to the "C:\kerisys\doors\db\files" subdirectory.
3. Rename the EVT.DBF and EVT.MDX files per the following instructions.
   - The new names for the two files must be the same to track which event log files go together.
   - The new names must retain the .DBF and .MDX file extensions.
   - The new names may not have more than seven characters. Keri Systems recommends the following format: DDMMMYY.DBF and DDMMMYY.MDX.

   DD = day of storage
   MMM = month of storage
   YY = year of storage
4. Using this format for a set of event files archived on July 1, 1997, the rename commands would be:

   REN EVT.DBF 01JUL97.DBF <ENTER>
   REN EVT.MDX 01JUL97.MDX <ENTER>

5. Type `exit<ENTER>` to return to Windows.

   The result would be the EVT.DBF file would be archived as 01JUL97.DBF and the EVT.MDX file would be archived as 01JUL97.MDX.

**Generating Reports from an Archived Event Log**

There are two ways to generate a report from an archived event log depending upon how the event log was archived.

If the event log was included as part of a periodic Doors software backup, the report generation process involves restoring the backed-up installation to a temporary folder, running the archived Doors program to access the report function, and then deleting the temporary folder.

If the event log was archived by itself, the report generation process involves several steps.

1. Rename the current event log files to temporary file names.

   REN EVT.DBF TEMP.DBF <ENTER>
   REN EVT.MDX TEMP.MDX <ENTER>

2. Copy the archived log files to the default event log file names.

   COPY 01JUL97.DBF EVT.DBF <ENTER>
   COPY 01JUL97.MDX EVT.MDX <ENTER>

3. Run the desired report in the Doors program.

4. Delete the default event log files.

   DEL EVT.DBF <ENTER>
   DEL EVT.MDX <ENTER>

5. Rename the temporary file names to the default event log file names. The program is now restored to its original configuration.

   REN TEMP.DBF EVT.DBF <ENTER>
   REN TEMP.MDX EVT.MDX <ENTER>

---

*Done incorrectly, either of these processes can damage the event logs or the Doors operating software. An operator must perform these steps carefully. Keri Systems recommends contacting your dealer for assistance in performing this operation.*
Advanced Features

The Doors program is capable of several advanced features that expand the program’s capabilities.

- multiple site control
- I/O control: linked and manual operation of inputs and outputs

Multiple Site Control

The multiple site feature allows a number of access control networks to be managed by the Doors program; all via modem. The host computer and each site must have a modem allowing communication between the host computer and each site.

When the sites feature is enabled, a number of windows throughout the Doors program are modified and the supporting databases are changed, adding the necessary hooks to support all sites.

![Warning]

*Once the sites feature is enabled, the changes made are permanent. They cannot be reversed.*

New sites can be added one-at-a-time; each independent from each other (no crossover of cardholders between sites), or any combination of interaction between sites can be made (cardholders can be assigned to a number of sites).

This section describes the following.

- The process for enabling the remote sites feature.
- The process for entering site related information.
- The process for adding a new site to the system.
- The differences in database entry and program operation.

Enable Sites

The Multiple Sites: Sites ON check box is used to enable the multiple sites feature (see Figure 168).

1. Click on the Setup ⇒ System pull-down menu or click on the button on the tool bar, then click on the System Configuration tab. The following window appears.
2. Click on the Multiple Sites: Sites ON box. Because the changes required to implement the sites feature make major changes to the Doors program and its supporting databases, a confirmation window appears (see Figure 169).

3. Click on the button to implement the multiple sites feature. Changes are made in the System Configuration tab, removing the configuration parameter fields for the remote modem. These have been moved to a new window tab and reformatted to allow for parameter entry for each site.

4. Click on the PC Phone Number field and re-enter the host computer’s phone number (see Figure 170).
5. Click on the button. If the change to multiple sites is not saved before clicking any other button or exiting the system setup window, the software conversion to sites is not complete.

6. Now update the access control network with the new information. Click on the button on the tool bar (for details on the update process refer to the Update the Network section found earlier in this users guide).

**Enter Site Configuration Information**

The Sites tab has now been added to the Setup System window. The Sites tab allows an operator to configure the communication parameters and provide identification information for the individual sites.

The following operations are performed in this section.

- assign a site name
- enter the site address
- enter the site PIN
- enter the site’s modem phone number
- enter the modem’s initialization string
- enter a global secure time
- enable the global unlock feature for a site
- enter a comment regarding a site

To enter the Sites tab:

1. Click on the Setup ⇒ System pull-down menu or click on the button on the tool bar. The following window will appear, including a new tab: Sites.
2. Click on the Sites tab. The Sites window appears (see Figure 171).
Assign a Site Name

The site name field allows an operator to assign a descriptive, identifying name to a site in the access control network. When monitoring system activity, or generating and reviewing event reports, it can be easier to follow a string of events if the site associated with the events has a descriptive name.

1. Click on the "Site Name" cell for the site to be named (see Figure 171).
2. Type a descriptive name for the site. For example, the first site is the Manufacturing and Sales office; type Mfg - Sales.

Enter the Site Address

The site address field allows an operator to store the address of a site in the access control network.

1. Click on the "Site Address" cell for the site (see Figure 171).
2. Type in the address for the site. For example, the Manufacturing and Sales office is located on 123 Elm Street; type 123 Elm Street.

Site Number

The site number is assigned by the Doors program. It helps the program track database information by site. It is not editable by the operator.

Site Personal Identification Number (PIN)

The site PIN field allows an operator to assign a "password" number to a site in the access control network. Once assigned to a site, an operator must know the PIN number to be able to access that site. The PIN is an extra security measure to ensure that an operator has authorization to access any given site.

1. Click on the "PIN" cell for the site (see Figure 171).
2. Type a four-digit number for the site. For example, the first site is assigned PIN 1111; type 1111.
Site Phone Number

The site phone number field allows an operator to assign the phone number for the modem at a site in the access control network. This is the phone number that the host computer will dial to contact the site.

1. Click on the "Phone Number" cell for the site (see Figure 171).
2. Type the phone number for the site. For example, the first site’s phone number is 555-4321; type 555-4321.

Site Modem Initialization String

The modem initialization field allows an operator to enter the initialization string for the modem at a site in the access control network. The modem initialization string provides the best operating parameters for the modem. As the modem initialization string differs per modem type and manufacturer, refer to the modem’s manual for the initialization string.

1. Click on the "Modem Init" cell for the site (see Figure 171).
2. Type the modem initialization string for the site’s modem.

Based on the parameters entered so far, the database for the Mfg - Sales site should look similar to Figure 172.

![Figure 172 – Default Site Information, Part 1](image_url)

Depending upon the size of the window displayed on the screen, you might need to use the scroll bar to bring the remaining columns into view (see Figure 173).
Site Global Secure Time

The global secure time field allows an operator to enter a time-of-day when all doors in the access control network should be locked. This ensures that regardless of the door status during the day, all doors in the access control network are locked at least once a day.

NOTE: All times are formatted to a 24-hour clock. For example, 5:30 P.M. is 17:30 under the 24-hour clock.

1. Click on the "Global Secure Time" cell for the site (see Figure 173).
2. Type the global secure time for the site. For example, the global secure time for this site should be 22:30 hours (10:30 P.M.); type **22:30**.

Site Global Unlock Enable

The global unlock enable button allows an operator to program general purpose input #1 on the master controller such that an active signal on the input immediately unlocks all doors on the access control network. General purpose input #1 is a normally-open input. To activate this input, the input terminals must be closed (shorted together).

1. To enable the global unlock input, click on the **OFF** button. The OFF button will toggle to ON and its color will change from red to green (see Figure 173).
2. To disable the global unlock input, click on the **ON** button. The ON button will toggle to OFF and its color will change from green to red (see Figure 173).

Site Comment

The site comment field allows an operator to enter a comment regarding the site.

1. Click on the "Comment" cell for the site (see Figure 173).
2. Type a brief comment about the site. For example, the Manufacturing and Sales site is the home office for the company; type **Home Office - Mfg and Sales**.

Based on the remaining parameters, the database for the Mfg - Sales site should look similar to Figure 174.
3. Once all information is entered, click on the **SAVE** button. If these changes are not saved before clicking any other button or exiting the system setup window, the data entered is lost and must be re-entered.

4. Now update the access control network with the new information. Click on the **UPDATE NET** button on the tool bar (for details on the update process refer to the Update the Network section found later in this users guide).

**Adding a New Site**

Perform the following to add a new site to the spreadsheet.

1. Click on the **NEW** site button. A new row appears on the Sites spreadsheet. Enter the site configuration information for the new site as per the instructions in the Enter Site Configuration Information section above. For example, a new site has been added for a Warehouse site and the configuration information has been entered. The resulting site spreadsheet information is displayed in Figures 175 and 176.
Changes in Database Entry and Program Operation

The following database and program operations have minor changes when the multiple sites feature is enabled.

- cardholder spreadsheet
- access group wizard
- net update button
- select a site button
- quick search reports

Cardholder Spreadsheet Changes

The cardholder spreadsheet adds a button that toggles the data displayed in the cards spreadsheet between displaying cardholder information for one site and displaying information for all sites.
1. To enter the setup cards spreadsheet click on the Setup ⇒ Cards pull-down menu option or click on the button on the tool bar.

2. Click on the button on the tool bar to enter spreadsheet mode.

3. When the Setup Cards spreadsheet window appears, a new button is displayed beside the original card management buttons.

4. If the button is displayed, the cardholder information in the spreadsheet is for the currently logged site only. To switch to displaying cardholder information for all sites, click on the button.

5. If the button is displayed, the cardholder information in the spreadsheet is for all sites. To switch to displaying cardholder information for the currently logged site only, click on the button.

6. Depending upon the size of the cardholder databases, switching between the one-site and all-sites modes can take up to several minutes. A verification window appears before the switch occurs to verify the switch should be performed (see Figure 177).

7. Click on the button to switch display modes.

**Access Group Changes**

The change within the access group wizard adds a select sites window, including site information as a part of the access group. This allows an operator to create new access groups or edit existing access groups to allow access to just one site or to any combination of sites in the access control network. When the select doors window in the access group wizard appears, only those doors associated with the selected sites are displayed.

**NOTE:** Selected sites can be differentiated from unselected sites by the appearance of the site icon. Selected sites stand out from the window and their site names are written in black text. Unselected sites appear to recede into the window and their names are written in grey text.

**For a New Access Group**

The Select Sites window appears between the Edit Access Group window and the Select Doors window (see Figure 178).
1. To select the sites to be used in an access group, follow the instructions in the Setup Access Groups section of this document, but include the following information.

2. After clicking on the **Next** button click on the **Next** button in the Edit Access Group window and the Select Sites window appears.

3. The Select Sites window displays an icon for every site recognized by the access control network.

4. Click on the icon for any site that should be included in the new access group. For example, click on the Mfg - Sales icon to include only the Mfg - Sales site in the access group (see Figure 178).

5. Click on the **Next** button and the Select Doors window appears. Complete the Create a New Access Group instructions.

---

**Figure 178 – Select Sites for Access Groups**

**For Editing an Access Group**

The Select Sites window appears between the Edit Access Group window and the Select Doors window (see Figure 178).

1. To select the sites to be used in an access group, follow the instructions in the Setup Access Groups section of this document, but include the following information.

2. After selecting an access group name and clicking on the **Next** button in the Edit Access Group window the Select Sites window appears.

3. The Select Sites window displays an icon for every site recognized by the access control network.

4. Click on the icon for any site that should be included in the new access group. For example, click on the Mfg - Sales icon to include only the Mfg - Sales site in the access group (see Figure 178).

5. Click on the **Next** button and the Select Doors window appears. Complete the Edit an Existing Access Group instructions.
Update Site

On the tool bar, the button changes to a button. The function is the same, uploading an access control system with all recent changes made to the database, but the upload only occurs on the currently logged site. To upload information to multiple sites, each site must be logged on and uploaded one-at-a-time.

1. Click on the button to upload information to the currently logged site.
2. Click on the Operate ⇒ Net Disconnect pull-down menu option to disconnect from the logged site.
3. Click on the button and select the next site to which information will be uploaded per the instructions in the Select a Site section below.
4. Click on the button. The Doors program will automatically connect with the new site and upload information.
5. Repeat this process for each site on the access control network.

Select a Site

A new button is added to the tool bar: . Clicking on this button displays a list of all available sites on the access control network, allowing an operator to select a specific site with which to work.

1. Click on the button. A window appears with a list of all available sites (see Figure 179).

![Figure 179 – Select Site List](image)

2. Scroll up and down the list and select the next site with which to work. Then click on the button.
3. The Doors software connects with the selected site and loads the program spreadsheets with the data from this site.
Quick Search Reports by Site

A new All Sites/Selected Site radio button is added to the quick reports feature allowing report data to be sorted by site. Follow the instructions in the Quick Search Event Report section of this document, but include the following information.

The sites radio buttons allow an operator to select if event information should be reported for all sites or for just one selected site.

1. To select all sites, click on the All Sites radio button (the default value, see Figure 180).

   ![Figure 180 – All Sites Radio Button](image)

2. To select one site, click on the Selected Site radio button. A list of all available sites appears in the window (see Figure 181).

   ![Figure 181 – Selected Site List](image)

3. Scroll up and down this list and locate the site for event reporting. Click on that site name and it will be entered into the selected site field (see Figure 182).
4. To change a selected site, click on the box and the list of available sites will reappear.

**Power Search Reports by Site**

A new Field Type/Field Value is added to the power search event reports feature allowing report data to be sorted by site.

The Site(SITE) Field Type sets the search criteria to retrieve all events that occurred at a specific site. When Site(SITE) is selected, a pull-down list of all available sites in the access control network appears for selection in the Value Field.
This page is intentionally left blank.
I/O Control

The I/O control feature allows an operator to have input events drive output responses. For example, an input connected to a vibration sensor or glass-break detector on a window can be linked to an alarm output so that a broken window will sound an alarm.

I/O control is managed through the I/O Config and Link Config tabs in the Setup System window. I/O Configuration defines the input and output points, and Link Configuration ties the inputs to the outputs.

Manual control for output points is also provided, allowing an operator to manually turn-on/enable or turn-off/disable an output point. This allows an operator to control an output point and to override a link event that is driving an output.

I/O Configuration

The I/O Config tab displays the input and output points that are available per controller (see Figure 183). An operator can assign a descriptive name to every available input and output point and can identify if an input is normally-open or normally-closed. Blank input and output point name fields indicate those inputs and outputs are reserved by the controller for door control and are not available for link assignment.

The following steps describe how to configure an input point and an output point for window monitoring as described in the example above. Controller 3 is a PXL-250 Tiger controller with an SB-293 Satellite board. This satellite board is configured to provide 6 inputs and two outputs that can be programmed into I/O links.

1. To configure input/output points, click on the Setup ⇒ System pull-down menu or click on the button on the tool bar. Then click on the I/O Config tab. A window similar to Figure 183 appears.

![Figure 183 – I/O Configuration Window](image-url)
2. To assign a name to an input point, click in the Input Point Name field for the desired input point and type the name to be assigned to the point. For example, for Input Point Name 3, type **Front Windows**.

3. The normal state for this input is normally-closed. If a window is broken the input will be opened. For the Mode of Input Point 3, click on the **N/C** radio button.

4. To assign a name to an output point, double click in the Output Point Name field for the desired output point and type the name to be assigned to the point. For Output Point Name 3, type **Window Alarm**.

5. The resulting window should appear similar to Figure 184.

![Figure 184 – Input/Output Point Definitions](image)

**Link Configuration**

The Link Config tab allows an operator to customize the controller’s output responses to events at the controller’s inputs (see Figure 185). Input points can be linked to output points, allowing a change of state at an input to activate an output relay. Blank input and output point name fields indicate those inputs and outputs are reserved by the controller for door control and are not available for link assignment. The following rules apply for link configuration:

- Up to 32 links can be defined per controller.
- Any input can be used by all 32 links.
- Inputs on a controller can only be linked to outputs on the same controller.
- Multiple inputs can be linked to multiple outputs using OR/AND functions allowing an operator to create complex input/output links.
- Outputs on one controller can be hard-wired to inputs on other controllers.
The following list is the parameters that need to be configured when defining an I/O link. Refer to Figure 185 to locate the parameter fields. Following this list is an example of an I/O Link.

**Controller**
The Controller field allows the operator to select the controller with I/O links to be configured.

1. Click on the arrow in the "Controller" field and a list of the controllers with available I/O points appears.
2. Scroll through this list and click on the controller which has the I/O points to be configured.

**Link Name**
To assign a descriptive name to a link:

1. Click in the "Link Name" field.
2. Type the name to be assigned to the point. For example, for the window alarm, type *Window Alarms*.

**Option Board**
The "Option Board" field displays the model number of the option board providing the input and output points. This is an information field and is not editable.

**Inputs**
The "Inputs" check boxes allow an operator to select the inputs that should be assigned to the I/O link. Inputs with grayed-out check boxes and without input point names are unavailable for assignment.

1. Click on the check box beside the input point name. A check mark appears indicating the input is selected. Every click in the check box toggles between selecting and deselecting.
2. To deselect an input, click on the check box. The check mark disappears indicating the input is deselected.

**Input Point Name**
The "Input Point Name" field displays the input point name assigned in the I/O Configuration section. In this window, this field is not editable. To change an input point name, refer to the I/O Configuration section of this users guide.

**Input Combinations**
The "Input Combinations" radio buttons allow an operator to define what the state of the selected inputs should be to generate an output. This is only valid if there are more than one input point being applied to the I/O link.

1. If the Or radio button is selected, an input signal on the first input point or the second input point or any of the input points will generate an output. Click on the Or radio button to select an Or input combination.
2. If the And radio button is selected, an input signal must be received on the first input point and the second input point and all of the input points at the same time to generate an output. Click on the And radio button to select an And input combination.

**Outputs**
The "Outputs" check boxes allow an operator to select the outputs that should be assigned to the I/O link. Outputs with grayed-out check boxes and no output point name are not available for assignment.

1. Click on the check box beside the output point name. A check mark appears indicating the output is selected. Every click in the check box toggles between selecting and deselecting.
2. To deselect an output, click on the check box. The check mark disappears indicating the output is deselected.

**Output Point Name**
The Output Point Name field displays the output point name assigned in the I/O Configuration section. In this window, this field is not editable. To change an output point name, refer to the I/O Configuration section of this Users Guide.

**Output Mode**
The "Output Mode" radio buttons allow an operator to define if the output relay should be driven to its active state or its normal state when an output is generated.

1. Driving to the active state opens the normally closed contact and closes the normally open contact. Typically, this is used to turn on an alarm or device. Click on the A radio button to select the active state.
2. Driving to the normal state closes the normally closed contact and opens the normally open contact (the normal or idle state of the relay). Driving an output to the normal state can be used to turn off an output that was driven to its active mode. Click on the N radio button to select the normal state.

**Enable Outputs**
The "Enable Outputs" and "Event Messages Only" radio buttons work in conjunction with each other. One or the other can be selected, not both.

1. Click on the Enable Outputs radio button to select if the input events in the I/O link should drive an output relay.
2. Click on the Event Messages Only radio button to select if the input events in the I/O link should just generate an event message.

**Event Messages Only**
See Enable Outputs.

**Output Alarm Type**
The "Output Alarm Type" radio buttons allow an operator to select how long an output is driven when activated. There are three output modes from which to choose.

- Click on the **Timed** radio button to make the output relay active for the period of time defined in the Seconds field. To set a time in the Seconds field, either double-click in the field and directly type in a value (255 seconds maximum) or use the arrows to scroll up and down and select a time.

- Click on the **Follow** radio button to make the output relay follow the state of the input. The output will stay active as long as the input is in its active state. When the input becomes inactive, the output becomes inactive. A Follow output uses two links internally which reduces the total number of available links.

- Click on the **Latched** radio button to have the output state triggered by the input state. When the input becomes active, the output becomes active and stays active until manually inactivated by an operator (using the manual output control commands given in the next section or by another link).

**Time Zone**
The Time Zone field allows an operator to assign a time zone to the I/O link. The entering or exiting of the time zone time period does not activate the link; the link will operate only during the time period defined by that time zone.

1. Click on the arrow. A list of all available time zones appears.
2. Scroll through this list and click on the desired time zone. If the link must be active all the time, click on the Always time zone.

**I/O Link Example**
The following steps describe how to link an input point to an output point for window monitoring using the example described in the I/O configuration section above. Controller 3 is a PXL-250 Tiger controller with an SB-293 Satellite option board. The satellite board provides 6 inputs and two outputs that can be programmed into I/O links.

1. To configure an input/output link, click on the Setup System pull-down menu or click on the button on the tool bar.

2. Click on the **Link Config** tab (see Figure 185).

3. Click on the Controller arrow and select controller C003 (see Figure 186).
Figure 186 – Select the I/O Link Controller

4. Click in the Link Name field and type **Window Alarms** (see Figure 187).

Figure 187 – Enter Link Name

5. Click on the **Input 3 check box** to select the Front Windows input point (see Figure 188).
   Since this is a single input point, the Input Combination radio buttons do not apply.
6. Click on the **Output 3 check box** to select the Window Alarm output point (see Figure 189).

7. Click on the **Active output mode radio button** to have the link drive the output relay to its active state, sounding an alarm (see Figure 190).
8. Click on the **Enable Outputs** radio button to activate the output relay (this is the default value for outputs – see Figure 190).

9. Click on the **Latched** output alarm type to have the alarm stay on until manually turned off (see Figure 191).

10. Click on the arrow and select **Activate Alarms** from the list of available time zones. A window similar to Figure 192 appears.
11. The completed I/O Link should appear similar to Figure 193.

Figure 193 – The Window Alarms I/O Link

12. Click on the \texttt{SAVE} button. If the new I/O Link is not saved before clicking any other button or exiting the setup system window the data entered is lost and must be re-entered.

13. Now update the access control network with the new information. Click on the \texttt{UPDATE NET} button on the tool bar (for details on the update process refer to the Update the Network section found earlier in this users guide).
Manual Output Control

Manual control for output points allows an operator to manually turn-on/enable or turn-off/disable an output point. This allows an operator to control an output point and to override a link event that is driving an output.

Following the window alarm example above, an operator can use the manual output control feature to manually test the window alarm periodically.

1. To manually control output points, click on the Operate ⇒ Output Control pull-down menu. A window similar to Figure 194 appears.

![Figure 194 – Output Control Window](image)

2. Under the Output Point Name list, locate the output point to manually control. For this example, locate output point 3 – the Window Alarm.
3. Under the Output Control Off/On buttons, click on the On button to turn-on/enable an output point.
4. Under the Output Control Off/On buttons, click on the Off button to turn-off/disable an output point.
5. The status field at the bottom of the window displays the results of the operations performed (see Figure 195).

![Figure 195 – Toggled Output Points](image)
Appendix

1. Database File Field Definitions
2. Glossary
This page is intentionally left blank.
Database File Field Definitions

Certain applications may wish to import the data within a quick search event report into a spreadsheet or database program (for example, time and attendance programs). The information in this section describes the format of the data written to a quick search event report file, identifying and defining the following:

- the total number of characters that make up a single event string in a quick search event report
- the information fields within an event string
- the number of characters in each information field
- the ASCII definition of the characters in the information field
- an example string
Data Format in Single Site Mode – Using the Cardholder’s Name

The following table defines the data within a quick search event report for a Doors application in Single Site mode, using the cardholders name to identify the cardholder associated with an event. One event string is made up of 85 ASCII characters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Date</th>
<th>Delimiter</th>
<th>Time</th>
<th>Delimiter</th>
<th>Door</th>
<th>Delimiter</th>
<th>Cardholder</th>
<th>Delimiter</th>
<th>Event</th>
<th>End of Record</th>
</tr>
</thead>
<tbody>
<tr>
<td># of characters</td>
<td>MM/DD/YYYY</td>
<td>0x20</td>
<td>0x20</td>
<td>HH:MM:SS</td>
<td>0x20</td>
<td>Door Name</td>
<td>0x20</td>
<td>Cardholder Name</td>
<td>0x20</td>
<td>0x20</td>
<td>0x0D 0x0A</td>
</tr>
<tr>
<td>Example</td>
<td>07/04/1997</td>
<td>&lt;space&gt;</td>
<td>&lt;space&gt;</td>
<td>19:30:17</td>
<td>&lt;space&gt;</td>
<td>Front Door</td>
<td>&lt;space&gt;</td>
<td>Adams, John Q</td>
<td>&lt;space&gt;</td>
<td>Access Granted &lt;5 spaces&gt;</td>
<td>&lt;CR&gt;&lt;LF&gt;</td>
</tr>
</tbody>
</table>
Data Format in Single Site Mode – Using the Cardholder’s Card Number

The following table defines the data within a quick search event report for a Doors application in Single Site mode, using the cardholders card number to identify the cardholder associated with an event. One event string is made up of 72 ASCII characters.

Table 2: Quick Search Event Report Data Format – Single Site Mode / Cardholder’s Card Number

<table>
<thead>
<tr>
<th>Field</th>
<th>Date</th>
<th>Delimiter</th>
<th>Time</th>
<th>Delimiter</th>
<th>Door</th>
<th>Delimiter</th>
<th>Card Number</th>
<th>Delimiter</th>
<th>Event</th>
<th>End of Record</th>
</tr>
</thead>
<tbody>
<tr>
<td># of characters</td>
<td>10</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>15</td>
<td>2</td>
<td>10</td>
<td>2</td>
<td>19</td>
<td>2</td>
</tr>
<tr>
<td>Description</td>
<td>MM/DD/</td>
<td>0x20</td>
<td>HH:MM:</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>Cardholder</td>
<td>0x20</td>
<td>Event</td>
<td>Event Text String padded with 0x20</td>
</tr>
<tr>
<td></td>
<td>YYYY</td>
<td>0x20</td>
<td>SS</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>Cardholder’s Card Number</td>
<td>0x20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>front-padded with 0x20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>07/04/</td>
<td>&lt;space&gt;</td>
<td>19:30:</td>
<td>&lt;space&gt;</td>
<td>Front</td>
<td>&lt;space&gt;</td>
<td>&lt;space&gt;</td>
<td>&lt;space&gt;</td>
<td>Access</td>
<td>Access Granted &lt;5 spaces&gt;</td>
</tr>
<tr>
<td></td>
<td>1997</td>
<td>17</td>
<td>17</td>
<td></td>
<td>Door</td>
<td></td>
<td>187491</td>
<td></td>
<td>Granted</td>
<td>&lt;5 spaces&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;5 spaces&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example:

07/04/1997 <space> <space> 19:30:17 <space> <space> Front <space> Door <5 spaces> <space> <space> <4 spaces> 187491 <space> <space> Access <space> Granted <5 spaces> <CR><LF>
Data Format in Multiple Site Mode – Using the Cardholder’s Name

The following table defines the data within a quick search event report for a Doors application in Multiple Site mode, using the cardholder’s name to identify the cardholder associated with an event. One event string is made up of 102 ASCII characters.

Table 3: Quick Search Event Report Data Format – Multiple Site Mode / Cardholder’s Name

<table>
<thead>
<tr>
<th>Field</th>
<th># of characters</th>
<th>Date</th>
<th>Delimiter</th>
<th>Time</th>
<th>Delimiter</th>
<th>Site</th>
<th>Delimiter</th>
<th>Door</th>
<th>Delimiter</th>
<th>Card Number</th>
<th>Delimiter</th>
<th>Event</th>
<th>End of Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>10</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>15</td>
<td>2</td>
<td>15</td>
<td>2</td>
<td>10</td>
<td>2</td>
<td>19</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Description</td>
<td>MM/DD/YYYY</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>0x0D 0x0A</td>
</tr>
<tr>
<td>Example</td>
<td>07/04/1997</td>
<td>&lt;space&gt;</td>
<td>&lt;space&gt;</td>
<td>19:30:17</td>
<td>&lt;space&gt;</td>
<td>Home</td>
<td>&lt;space&gt;</td>
<td>Front</td>
<td>&lt;space&gt;</td>
<td>&lt;space&gt;</td>
<td>187491</td>
<td>&lt;space&gt;</td>
<td>&lt;CR&gt;&lt;LF&gt;</td>
</tr>
</tbody>
</table>

Example:

07/04/1997 <space> 19:30:17 <space> Home <space> Office <4 spaces> <space> Front <space> Door <5 spaces> <space> Cardholder’s Card Number front-padded with 0x20 <space> Event Text String padded with 0x20 <0x0D 0x0A>
Data Format in Multiple Site Mode – Using the Cardholder’s Card Number

The following table defines the data within a quick search event report for a Doors application in Multiple Site mode, using the cardholder’s card number to identify the cardholder associated with an event. One event string is made up of 102 ASCII characters.

Table 4: Quick Search Event Report Data Format – Multiple Site Mode / Cardholder’s Card Number

<table>
<thead>
<tr>
<th>Field</th>
<th>Date</th>
<th>Delimiter</th>
<th>Time</th>
<th>Delimiter</th>
<th>Time</th>
<th>Delimiter</th>
<th>Site</th>
<th>Delimiter</th>
<th>Site</th>
<th>Delimiter</th>
<th>Door</th>
<th>Delimiter</th>
<th>Door</th>
<th>Delimiter</th>
<th>Cardholder</th>
<th>Delimiter</th>
<th>Event</th>
<th>End of Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>#of characters</td>
<td>10</td>
<td>2</td>
<td>8</td>
<td>2</td>
<td>15</td>
<td>2</td>
<td>15</td>
<td>2</td>
<td>23</td>
<td>2</td>
<td>19</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>MM/DD/YY</td>
<td>0x20</td>
<td>HH:MM:SS</td>
<td>0x20</td>
<td>0x20</td>
<td>0x20</td>
<td>Site Name padded with 0x20</td>
<td>0x20</td>
<td>Door Name padded with 0x20</td>
<td>0x20</td>
<td>Cardholder Name padded with 0x20</td>
<td>0x20</td>
<td>Event Text String padded with 0x20</td>
<td>0x0D 0x0A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>07/04/1997</td>
<td>&lt;space&gt;</td>
<td>19:30:17</td>
<td>&lt;space&gt;</td>
<td>Home</td>
<td>&lt;space&gt;</td>
<td>Office</td>
<td>&lt;space&gt;</td>
<td>Front</td>
<td>&lt;space&gt;</td>
<td>Door</td>
<td>&lt;space&gt;</td>
<td>Adams, John Q</td>
<td>&lt;space&gt;</td>
<td>Access</td>
<td>&lt;CR&gt;&lt;LF&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example: 07/04/1997 19:30:17 Adams, John Q Access Granted
Glossary

access control – Access control is a general term describing the management of the ingress and egress of people through secure areas.

access control network – An access control network is an interconnected set of controllers, managing the ingress and egress of people through secure areas.

access group – An access group combines time zones and doors into a superset of information that is applied to cardholders. Basically an access group defines at what times and through which doors cardholders are granted access. To be granted access to a secure door, a cardholder must meet the criteria of the access group assigned to the cardholder: be at a door that is a member of the access group during a time period within the time zone assigned to the access group.

address, controller – Each controller must be assigned a unique address, identifying that controller in the network. A controller address is similar to a home address. By addressing an envelope, mail is sent to a specific individual at a specific home. By assigning unique controller addresses, operating information can be sent directly to specific controllers.

auto-configuration – Auto-configuration is a process within the Doors software where the software polls the access control network to determine which controllers on the access control network are responding and then receive configuration information from these controllers.

card – A card is an access control identification device assigned to an individual to give that individual access rights to an access control network. It is the size of a credit card. Each card has a unique identification code. That identification code is then associated with an access group to determine through which doors and at what times cardholders are granted access.

cardholder – A cardholder is an individual who has been assigned an access control card or tag.

COM port – A COM port is a serial data communications device on a computer. Communication between the host computer and the access control network is done through this device.

controller – A controller is a microprocessor based circuit board that manages access to a secure area. The controller receives information that it uses to determine through which doors and at what times cardholders are granted access to that secure area. Based on that information, the controller can lock/unlock doors, sound alarms, and communicate status to a host computer.

database – A database is an organized set of information.

department group – A department group is an operator assigned field in the cardholder database. It is not actively used by the Doors software, but is provided to allow an operator to sort the cardholders within the database based on the department for which they work.

dialog box – A dialog box is a text window that the Doors software displays on screen when the software needs information from an operator. The operator enters the information by reading the instructions in the window and then filling-in-the-blanks in designated fields in the window.

download – Downloading is the process by which the host computer receives information from the access control network; information is downloaded to the host computer. (See upload.)

egress – Egress is a term for exiting a secured area. (See ingress.)
enroll – Enrolling is the process of activating a card for use by a cardholder in the access control network. A card must be entered into the access control network and then assigned to a cardholder.

event – An event is an occurrence at a controller (such as unlocking a door, requesting to exit, forcing a door open) that generates a message stored by the controller.

firmware – Firmware is a set of operating instructions for a controller, stored on a ROM on the controller.

host computer – The host computer is the computer running the Doors software and communicating with the access control network.

ingress – Ingress is a term for entering a secured area. (See egress.)

input – An input is a set of points on a controller that is able to receive a signal indicating when an external device changes state. For example, the door switch input on the controller is attached to a switch on the door. Using the switch, the input is able to keep track of when the door is opened or closed; when the switch is open, the door is open and when the switch is closed, the door is closed.

loopback plug – A loopback plug is a small, serial port connector used by the COMTEST program to verify basic operation of the host computer’s COM port. It is used to route signals sent out via the COM port transmit line back to the COM port receive line. Before running the COMTEST, the loopback plug is connected to the COM port designated for use by the Doors software. When the test is complete, the loopback plug is removed and the communication line is connected.

menu bar – A menu bar is a horizontal field near the top of a program window of a program operating in a Windows operating system that allows a program operator to select program commands and options.

modem – A modem is a communication device that converts computer serial data to a format that can be transmitted and received via telephone.

monitor – A monitor is a window within the Doors software that tracks events that are occurring on the access control system as they happen.

offline – The access control network is offline when it is not actively communicating with the host computer.

online – The access control network is online when it is actively communicating with the host computer.

on-line help – On-line help is a mini-program within the Doors software that provides basic descriptions and instructions for the Doors software. On-line help can be run at the same time as the Doors program, side-by-side, making it easier for an operator to receive basic information regarding a program command or operation.

operator – An operator is an individual who has been granted the authority to perform certain Doors program managerial operations.

output – An output is a relay on a controller that is toggled, to open or close an external circuit based on either commands programmed into the controller or based on the state of an input. For example, if a door is forced open, an output relay is programmed to sound an alarm.
personal identification number – A personal identification number is an optional site identification number that may be assigned to a site by an operator. When using PINs, an operator must know a site’s PIN to be allowed access to that site. This can provide an extra level of site security, allowing some operators to access a remote site, but not all.

PIN – An acronym for personal identification number (see personal identification number).

pull-down menu – When an operator clicks on an option on the menu bar, a pull-down menu appears listing all the available options for that menu selection. An operator then selects the desired operation.

radio button – Radio buttons are used whenever a program command has a set of options that require the selection of one and only one option. As an operator clicks on the radio buttons within an option set, the old selection is disabled and the new selection is enabled.

reader – A reader is a device that “reads” an identification number from a card or tag presented to the reader by a cardholder. It then sends that identification number to the controller for processing.

report – A report is a summary of event information generated from the event log collected from all controllers on the access control network. A report may be displayed on the computer system screen, printed at a local printer, or saved to an ASCII text file for processing by another program.

ROM – A ROM is a memory device on the controller that permanently stores instructions and information. ROM stands for Read Only Memory, referring to the fact that information can only be read from the device. Information cannot be changed unless the device itself is replaced.

site – A site is another term for an access control network. Site is generally used when there are more than one access control networks all being managed from one host computer. The Doors software within the host computer keeps track of the different access control networks by assigning each one a site number.

spreadsheet – A spreadsheet is an organized collection of information managed in a matrix format.

tag – A tag is an access control identification device assigned to an individual to give that individual access rights to an access control network. It is designed to be attached to a keyring. Each tag has a unique identification code. That identification code is then associated with an access group to determine through which doors and at what times cardholders are granted access.

time zone – A time zone is a definition of the time-of-day and the days-of-the-week when a cardholder may be granted access to a secure area.

tool bar – The tool bar is a set of buttons in a horizontal field beneath the menu bar, made up of shortcuts to the commonly used Doors program features.

upload – Uploading is the process by which the access control network receives information from the host computer; information is uploaded to the access control network. (See download).
This page is intentionally left blank.
Index

A

Access Groups, 75
   Adding/Removing Doors, 81
   Changing Time Zones, 82
   Creating New, 75
   Deleting, 84
   Editing, 80
Alarm Output, 72
Archiving Event Logs, 176
Auto-Collecting Events - Enable/Disable, 117
Auto-Config, 39
   Failed, 41

B

Backing Up an Existing Installation, 17
Backing Up an Installation to Remote Storage, 175

C

Cards, 87
   Assigning a Department Group, 97
   Block Copying Data, 111
   Card Number Function - Enable/Disable, 98
   Deleting a Card, 96, 109
   Department Group Function - Enable/Disable, 98
   Editing Cardholder Data, 94, 114
   Enrollment
      Dialog Box Method, 87
      Presenting to a Reader, 90, 103
      Spreadsheet Method, 103
   Entering Cardholder Data, 92, 104
   Identifying Unknown Cards, 167
   Personal Data Categories
      Creating, 99
      Entering Data, 101, 113
      Printing Cardholder Data, 116
      Sorting Cardholder Data, 110
   Voiding a Card, 94, 107
COM Port, 37
   Communication Speed, 38
   Setting, 37
Communication Parameters, 37
   Communication Speed, 38
   Modem Parameters, 39
   Saving, 39
Computer - See Host Computer
COMTEST, 12
   Failing COMTEST, 14
   Running COMTEST, 12
   Starting, 12
Controllers
   Assigning Events to be Reported, 130
   Collecting Events, 148
   Dial-Out Parameters, 63
   Get Status, 45
       All Controllers, 45
       One Controller, 47
   Set Date, 42
   Set Time, 42

D

Database File Format, 205
   Multiple Site - Cardholder’s Card Number, 209
   Multiple Site - Cardholder’s Name, 208
   Single Site - Cardholder’s Card Number, 207
   Single Site - Cardholder’s Name, 206

Database Programming
   Access Groups, 75
   Cards, 87
   Doors/Controllers, 63
   Operators, 49
   Order of Operation, 25
   Setup Monitor and Events, 117
   Time Zones, 53

Date
   Setting Controller, 42
   Setting Host Computer, 15

Desktop, 33
Dial-Out Parameters - See Door/Controller Configuration
Door Class, 66
Door Name, 65
Door/Controller Configuration, 63
   Alarm Output, 72
   Class Assignment, 66
   Dial-Out Parameters, 63
       Disable Dial-Out, 64
       Enable Dial-Out, 63
       Threshold Percentage, 64
   Disable Reader, 67
   Enable Reader, 67
   First Person In, 71
   Name Assignment, 65
   Open Time, 69
   Unlock Time, 68
   Unlock/Lock Time Zone, 70

Doors Program
   Capabilities, 9
   Desktop, 33
   Exiting a Window, 35
   Logging On, 30
   Revision, 172
   Starting Doors, 29
   Tool Bar, 34
E

Events
Archiving Event Logs, 176
Assigning Events to be Reported by the Controllers, 130
Assigning Events to Monitors, 126
Auto-Collection - Enable/Disable, 117
Collecting From Controllers, 148
Configure Monitor Windows, 118
Create Reports - See Reports
Message Text String Definitions, 121
Message Text Strings, 119
Naming Monitor Windows, 118
Selecting Events to Save to File, 128
Setup Monitor Windows, 117
Exiting a Doors Window, 35

F

First Person In, 71

H

Holiday Schedules - See Time Zones
Host Computer
Set Date, 15
Set Time, 15
System Requirements, 11

I

I/O Control, 193
Configuring Links, 194
Link Example, 197
Manual Output Control, 202
Input Control - See I/O Control
Installing - See Installing Software
Installing Software, 17
Back Up an Existing Installation, 17
Deleting an Original Installation, 21
New, 17
Recovering an Original Installation, 20
Troubleshooting, 19
Upgrade, 17

K

Key Tag, 88

L

Links - See I/O Control
Locking Doors, 136
All Doors in a Door Class, 136
All Doors, 136
Single Door, 137
Logging On, 30
Loop-Back Plug, 12
M

Maintenance, 175
Archiving Event Logs, 176
Generating a Report From an Archived Event Log, 177
Software Backup to Remote Storage, 175
Storing Source Disks, 175
Message Text Strings, 119
Definitions, 121
Modem Parameters, 39
Monitors
Assigning Events, 126
Collecting Events, 148
Configuring Windows, 118
Create Reports - See Reports
Naming Windows, 118
Operating, 147
Setup, 117
Starting, 147
Stopping, 148
Verifying Communication Status, 147
Multiple Site Control - See Sites

N

Network
Disconnecting, 169
Update Screen, 31
Updating, 133

O

On-Line Help, 25, 34
Open Time, 69
Operators, 49
Creating a New Operator, 50
Editing the Default Operator, 49
Logged Operator, 172
Output Control - See I/O Control
Outputs
Manual Control, 202

P

Program Revision, 172
Proximity Card, 88
Proximity Key Tag, 88

R

Reader
Disable Reader, 67
Enable Reader, 67
Recovering an Original Installation, 20
Reports
  Creating, 149
  Generating Output, 153
Power Search, 155
  Boolean Links, 159
  Boolean Operators, 157
  Example, 160
  Fields, 156
  Generating From an Archived Log, 177
  Library, 163
  Sort Order - Reverse, 165
  Use Card Numbers, 166
  Use Cardholder Names, 166
Quick Search, 149

S
  Save to File - Selecting Events, 128
Serial Port Test - See COMTEST
Sites, 179
  Adding New, 185
  Configuration Information, 181
  Database Changes, 186
  Enable Multiple Sites, 179
  Program Operation Changes, 186
Smart Update - See Updating the Network
Software Installation, 17
  Backing Up an Original Installation, 17
  Deleting an Original Installation, 21
  New, 17
  Recovering an Original Installation, 20
  Troubleshooting, 19
  Upgrading, 17
Spreadsheet
  Printing Cardholder Data, 116
  Resizing a Column, 116
  Resizing a Row, 116
Starting Doors, 29
System Maintenance - See Maintenance
System Operation, 135
  Lock Doors, 136
  Timed Unlock, 140
  Unlock Doors, 138
  Update Doors, 142

T
Time
  Setting Controller, 42
  Setting Host Computer, 15
Time Zones, 53
   Crossing Midnight, 57
   Day Shift Example, 53
   Deleting, 61
   Displaying, 60
   Editing, 60
   Grave Shift Example, 57
   Holiday Schedules, 58
   Janitorial Shift Example, 56
   Unlock/Lock, 70
Timed Unlock, 140
   All Doors in a Door Class, 141
   All Doors, 140
   Single Door, 142
Tool Bar, 34

U
Unlock Time, 68
Unlock/Lock Time Zone, 70
Unlocking Doors, 138
   All Doors in a Door Class, 139
   All Doors, 138
   Single Door, 140
Update Doors, 142
   All Doors in a Door Class, 143
   All Doors, 142
   Single Door, 144
Upgrading Existing Software, 17

W
Window Management, 169