



**Millenium<sup>®</sup>**  
expert



# User Guide

First Edition

A publication of Kaba Ilco, Inc.  
7301 Decarie Blvd.  
Montreal, Quebec  
Canada H4P 2G7

Printed in Canada, 2003  
Copyright by Kaba Ilco, Inc., 2003  
All rights reserved.

No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without prior written permission from the Publisher.

The information contained in this publication is accurate to the best of Kaba Ilco's knowledge.

Specifications are subject to change without notice.

PK 2934 09/03





# Table of Contents

<b>CHAPTER 1: OVERVIEW.....</b>	<b>1</b>
The Millenium Expert Family of Devices.....	2
<b>CHAPTER 2: LOGGING ON/OFF THE SOFTWARE.....</b>	<b>6</b>
<b>CHAPTER 3: SETUP .....</b>	<b>9</b>
Default Settings .....	9
Configuring Millenium Expert Setup .....	9
Set up PORTS.....	10
LEGEND: ABA Data Format .....	13
How do I set up ABA for Use with System 800 Encoder? .....	13
Wiegand Data Format.....	16
How do I set up a Wiegand Reader?.....	17
Setup OPTIONS.....	19
Set up Custom User-Defined Data Fields.....	20
Setup Screen Colors.....	21
Millenium Expert Options Setup - Definitions.....	22
<b>CHAPTER 4: SITES.....</b>	<b>23</b>
How do I add a Site? .....	23
How do I configure a Dial-up Site? .....	25
Windows-installed modem (DIAL-UP communications) .....	27
Antipassback .....	27
Updating a Site.....	27
Disable All Sites.....	28
Network Communications .....	28
Dialup Communication History .....	29
Site: Buffer at 80% full .....	30
<b>CHAPTER 5: TIMEZONES.....</b>	<b>31</b>
VACATIONS:.....	32
HOLIDAYS: .....	32
How do I set up a Timezone? .....	32
How do I set up holidays? .....	33
How do I set up vacations? .....	34
<b>CHAPTER 6: ACCESS POINTS .....</b>	<b>36</b>
How do I add an Access Point? .....	37
How do I set up door alarms? .....	40
How do I set up DCD Relays?.....	43
How do I configure the Door Ajar feature?.....	44
Forgive Antipassback .....	47
Execute button .....	47

Override Strike .....	48
Remote Unlock.....	49
How do I execute remote unlock? .....	49
Updating.....	50
STATUS of a Device (Door).....	50
<b>CHAPTER 7: ACCESS GROUPS .....</b>	<b>51</b>
How do I create an Access Group?.....	51
How do I assign a Timezone?.....	54
<b>CHAPTER 8: USERS.....</b>	<b>55</b>
How do I add a user?.....	56
How do I give a user access to the doors? .....	56
How do I label a lost keycard? .....	59
How do I create custom user fields, notes and badge tabs? .....	60
<b>CHAPTER 9: OPERATORS.....</b>	<b>63</b>
How do I add an operator?.....	64
How do I change a password? .....	66
How do I create custom operator levels? .....	69
<b>CHAPTER 10: ELEVATORS.....</b>	<b>71</b>
How do I add elevator control units? .....	72
How do I set up Elevator Readers?.....	76
How do I set up elevator alarms.....	77
How do I set up elevator events? .....	79
How do I set up Elevator Floor Relays? .....	80
How do I execute an elevator remote unlock? .....	83
<b>CHAPTER 11: RELAY CONTROL DEVICES.....</b>	<b>85</b>
How do I add a Relay Control Device?.....	90
<b>CHAPTER 12: ALARM EDITOR .....</b>	<b>93</b>
How do I log on to Alarm Editor?.....	93
How do I set up Alarm Editor?.....	102
<b>CHAPTER 13: ALARM MONITOR.....</b>	<b>107</b>
<b>CHAPTER 14: TOURS.....</b>	<b>119</b>
How do I set up a tour?.....	128
How do I run and assign a Global Tour? .....	130
How do I assign a user to a Tour?.....	130
How do I assign a user to a Global Tour?.....	131
How to handle tours that cross midnight .....	132
<b>CHAPTER 15: MUSTER TRAC.....</b>	<b>135</b>
How do I create default settings for the Muster Trac hot button? .....	137
How do I set up Total Time parameters?.....	139

How do I create Device Groups? ..... 143

**CHAPTER 16: SCHEDULER ..... 155**

How can I duplicate an existing schedule? ..... 175

Alarm Shunting ..... 178

How do I shunt alarms on access points for scheduled events?..... 178

**CHAPTER 17: REPORTS ..... 181**

How do I archive Alarm or History Reports? ..... 189

How do I create a Dossier Report? ..... 190

**CHAPTER 18: FILTERS ..... 195**

How do I create a Device Group ..... 203

**CHAPTER 19: MAPS ..... 206**

How do I Select the Date Format ..... 208

**CHAPTER 20: DATABASE UTILITIES ..... 211**

How do I Import user data with the Millenium Database Utility? ..... 212

How do I import User ACCESS CODE, ACCESS GROUP, and/or User PIN data with the  
Millenium Database Utility? ..... 217

Step-by-Step: Deleting Users by means of Import Utility..... 227

How do I Export User data from the Millenium database? ..... 230

How do I archive history data using Millenium Database Utility?..... 232

How do I perform database repair? ..... 240



# Chapter 1: Overview

## Minimum System Requirements

- Pentium class PC
- 64 MB RAM (Standard)
- 128 MB RAM (with Windows NT 2000 or XP Pro)

## 5 GB Hard Drive

- CD ROM drive 16X
- 800 X 600 16 bit color VGA card
- Two Serial Ports
- Accurate Clock (1 to 5 minutes per year)
- Windows® 98 SE,NT (SP6), Me, 2000 (SP 2) or XP Pro

## System Requirements for Millenium Networks

### Millenium Application Server

- Pentium class PC
- 128 MB RAM
- 5 GB Hard Drive
- CD ROM drive 16X
- 800 X 600 16 bit color VGA card
- Two Serial Ports
- Accurate Clock (1 to 5 minutes per year)
- Windows® NT (SP6), or 2000 (SP 2)
- Network card
- TCP/IP with static addresses

### Workstation

- Pentium class PC64 MB RAM (Standard)
- 128 MB RAM (with Windows NT 2000 or XP Pro)

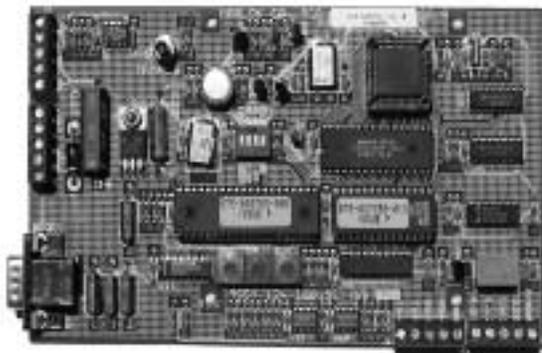
- 2 GB Hard Drive
- CD ROM drive 16X
- 800 X 600 16 bit color VGA card
- Accurate Clock (1 to 5 minutes per year)
- Windows®, 98, SE,NT (SP6), Me, 2000 (SP 2), or XP Pro
- Network card
- TCP/IP static IP addresses

For special requirements for the Millenium Badging, please refer to the ***Millenium Badge User Guide, PK 2909.***

### ***The Millenium Expert Family of Devices***

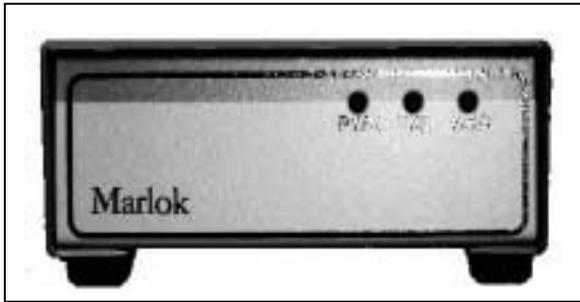
- Site Control Unit (SCU)
- Door Control Device (DCD)
- Relay Control Device (RCD)
- Elevator Control Unit (ECU)
- Elevator Control Device (ECD)
- Site Ethernet Interface (SEI)
- Trunk Interface Unit (TIU)
- Power Supply w/Line Conditioner (PS1)

#### **Site Control Unit**



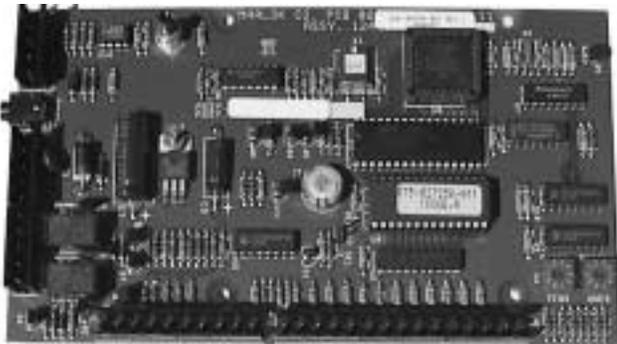
The SCU is the Millenium communications traffic COP. It takes inbound RS232 or RS485 communications protocols and routes them to the necessary pieces of equipment on the system.

### Trunk Interface Unit



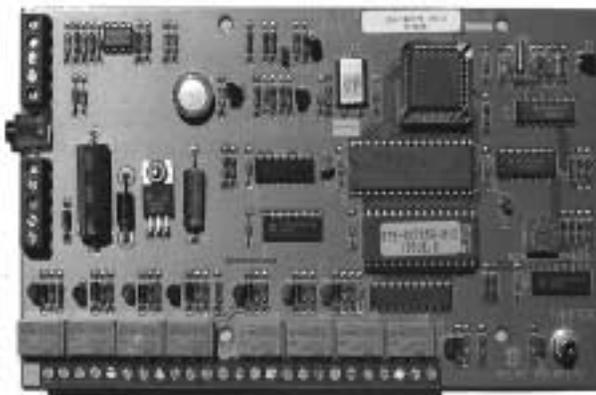
The TIU is an RS232 to RS485 converter box. Use the TIU when the SCU is more than 50ft away from the main PC or when using more than 1 SCU.

### Door Control Devices (DCDs)



The DCD is the heart of the Millenium System. This is the device that connects each of the door peripherals devices to the system like the electronic lock, the reader, request to exit device (REX), and the door position switch.

### Relay Control Devices (RCDs)



The RCD is an optional (8) relay output board that is employed within the system if additional relays are required to operate external devices.

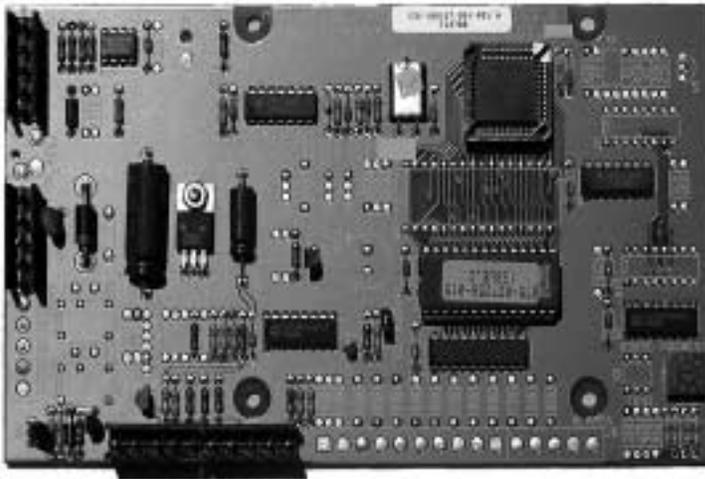
Each RCD board (Relay Controller Board) has eight programmable relays, with a maximum of 10 boards per Site Controller Unit (SCU) or total 80,000 additional relays, if needed.

## Elevator Control Unit (ECU)



The ECU is used to interface the Millenium access control system directly to an elevator controller. This board has 16 output relays.

## Elevator Control Device



The ECD is a stripped down version of the DCD. It resides on the elevator car and it is used as an interface liaison between the reader and the ECU.

## The Millenium Family of Software add-ons

- Millenium Badging
- Millenium Server
- Millenium Workstation

## Millenium Expert Systems Toolbar

- Icons across the top of the window take you into each programming function within Millenium software. Each toolbar icon corresponds to a topic in the help file.



- Some topics contain one dialog where you create and program a part of your Millenium access control network.
- Some topics contain multiple TABS that display additional dialogs you can jump between to create and program a part of your Millenium access control network.
- For example, the TIMEZONE icon displays a dialog with two additional TABS: Vacations and Holidays.

### TABS

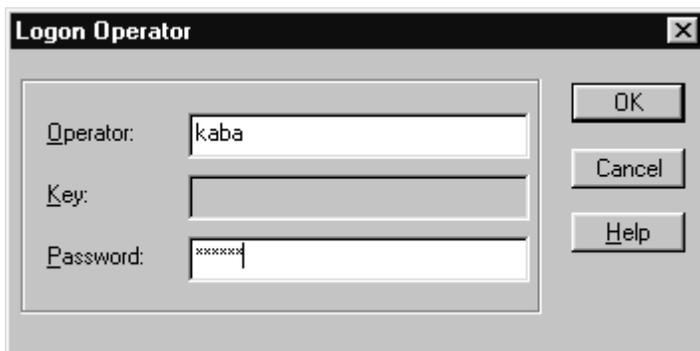
Millenium Expert Systems also has a Menubar with access to each main function within the software. The menubar includes some additional functions.

## Chapter 2: Logging on/off the Software

When you first open the Millenium Expert Systems software, a **Log on Operator** dialog box automatically appears. The system requires a valid logon before it will permit exiting the software. It is important that you follow the proper exiting procedure to avoid damage to your Millenium database.

**To log on to the software**, type your operator Log on ID, as established in the Operator dialog.

If you haven't created an operator yet, remember to use **kaba** as the login and **expert** as the password.



**NOTE:** Once you open Millenium Expert Systems, a logon is required before logoff software can be exited.



Once an operator is logged on, the log on button is disabled (dims.)



If a Level One operator sets up the Automatic logoff feature, a logged on operator is automatically logged off the system after a set amount of time. The log on button becomes enabled and all other Millenium toolbar buttons disabled. History displays in the application workspace (for DIRECT communication configurations.) The system now requires a valid operator log on.

**To log off the software**, click the LOG ON menu item. Then select the **Logoff Operator** option.



- Millenium Expert Systems remains ONLINE (in DIRECT communication applications) with system history displaying, “as-it-happens,” in the application window.
- Except for the Log on toolbar button, all Millenium software toolbars remain disabled until another valid operator logs on (described above.)

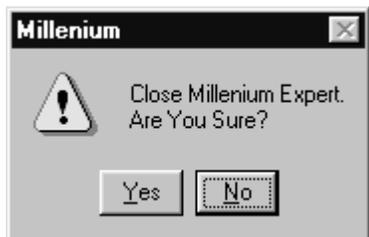
## Login ID

- Login ID is a brief name the operator can use to log on to Millenium Expert Systems. The ID should be brief to cut down on the number or keystrokes required to log on to the software. Each Login ID must be unique.
- This Login ID will identify the operator in Millenium history, as well as in the Alarm Monitor.
- A Level 1 operator establishes the Login ID in the OPERATORS dialog.

**NOTE:** Limit Login ID name to letters and numbers. Avoid using symbols. For example, if an operator named Mike O'Dell wants his Login ID to be his last name, it should be odell—without an apostrophe.

## Exiting Millenium Expert Systems Software

When you exit the Millenium Expert Systems software, the following confirmation prompt appears:



- Closing the software is the same as taking the software off-line from the Millenium Expert Systems access control devices (DCDs, SCUs, RCDs, ECUs, and ECDs.) Devices continue to retain history of access control activity.
- DIRECT communication systems will download accumulated history at the next initial log on.
- DIAL-UP communication configurations will download accumulated history when an operator selects the *Download History from Site* command on the Dialup Connections dialog or the next time the scheduled automatic dial-up connection occurs.



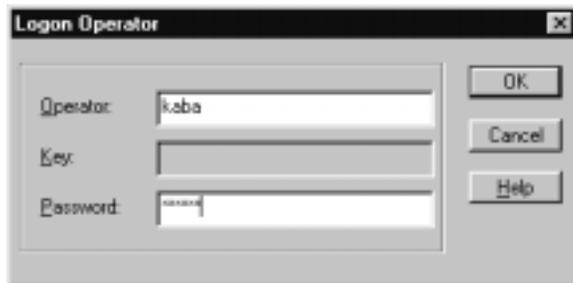
# Chapter 3: Setup

The SETUP program controls the settings in the software. The program, limited to use by Level One operators, is also referred to as **setupmpw**.

## Log in to Millenium Setup

The Millenium Setup requires a separate login.

1. Click on the Setup button  on the main Toolbar button and the following dialog box appears.



2. If you have not yet created an Administrator in your Millenium Expert application, use kaba as the Operator and expert as the password – both in lower case.
3. If you have an operator, use his/her name and password, as in the example above.
4. The Setup Module can be closed without logging off.

## *Default Settings*

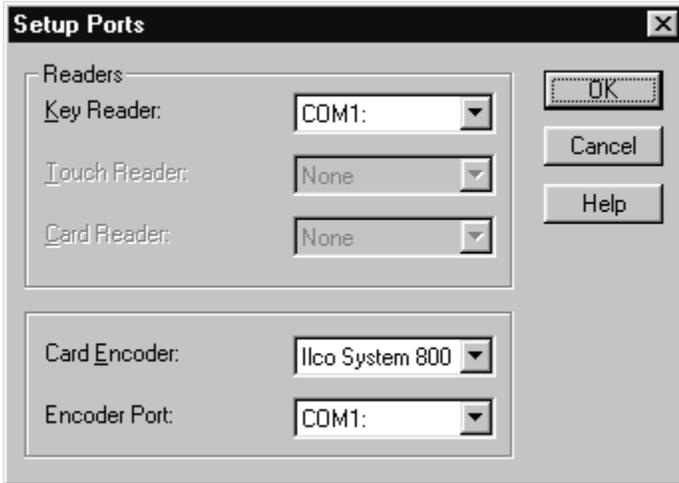
Millenium Expert Systems is configured with default settings that should be checked after installation and following upgrades to software or control devices. Some of these defaults **MUST** be modified depending on your individual access control installation.

## *Configuring Millenium Expert Setup*

**SETUP** affects the following portions of Millenium Expert Systems:

## Set up PORTS

1. Click on Icon  and the following Dialog box appears, enabling you to configure two things:



2. **Serial port assignment for Millenium console keyreader**, if applicable.
  - Identify the PC serial COM port into which the wedge-shaped key reader is plugged. This console Key Reader reads Marlok key codes into the PC. Default in PORTS dialog is **None**.
3. **Com port assignment for making ABA cards on an ILCO System 800 encoder**, if applicable.
4. Click on Ports menu and the following dropdown menu appears, enabling you to configure two things:



- Serial port assignment for Millenium console key reader, if applicable. – same dialog box as above
- TCP/IP to sites IP Addresses  
If you use Site Ethernet Interface (SEI) units, select SEI IP Address under the Ports menu to record the appropriate TCP/IP addresses for each SEI in use.

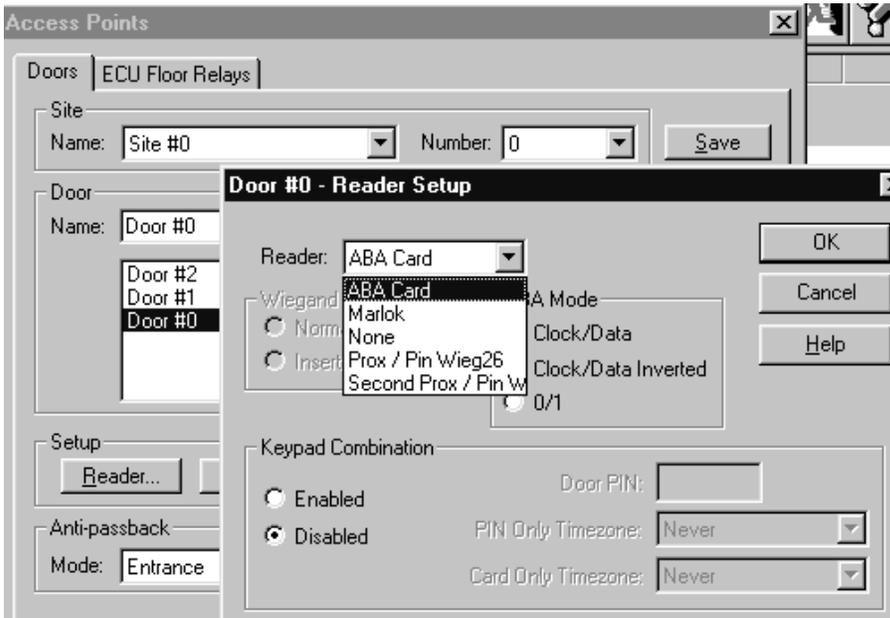
## READERS

### Setup Readers

The following dialog box shows important settings you must make depending on the types of access control CARD READERS installed in your facility's Millenium network.

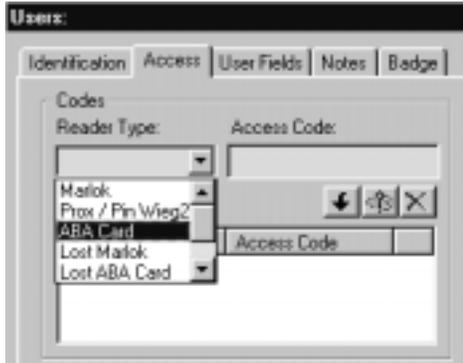


The READER NAME you type in here in Millenium Setup will be the option that appears in the door's READER field in the Access Point Dialog in the Millenium Expert main application.



### Access Point Dialog

1. In the dialog, click on the **Reader...** button. The Reader Setup dialog pops up.
2. The Reader identifications you have named will also appear as options in the READER field on the USERS' ACCESS tab, as shown below.



### ABA Setup Tab



- All ABA data formats are custom. Record one custom ABA data pattern for your facility. Group the display format the way you want it to appear throughout the software.
- READER NAME field shows the exact description of the reader as it will appear in the dialog.
- DISPLAY FORMAT reflects the result of the DATA FORMAT you create. The display format

controls how the data digits on the card will display in the Millenium software. The above example shows 6 decimals (DDDDDD.) You may include hyphens or spaces in the display format.

- DATA FORMAT reflects the symbols you record as the **exact** data format generated by the cards used at your facility.

### ***LEGEND: ABA Data Format***

Use the following symbols when creating a custom **DATA FORMAT** for ABA cards:

<b>SYMBOL</b>	<b>SYMBOL REPRESENTS</b>	<b>SYMBOL Means</b>
#	Data digit	This exact position in the DATA FORMAT will be a data digit.
–	Separator character	This exact position in the DATA FORMAT will be a separator character.
.	Ignore digit	This exact position in the DATA FORMAT will be an ignore digit.

### ***How do I set up ABA for Use with System 800 Encoder?***

Millenium Expert Systems can make ABA cards by using the Ilco System 800 encoder. Millenium can read any 14 of the 37 possible characters generated by a standard ABA card. A System 800 encoder generates a 14-character card. You can set up the DATA and DISPLAY formats to use selected characters.

1. First, select the COM port where the System 800 Encoder is plugged. (PORTS dialog in this setuppw.)
2. Then setup the reader as described in the following example:



With a Kaba Ilco System 800 encoder, the DATA FORMAT must be 14 characters long.  
The 14 characters can be any combination of data, or separator, or ignore characters.

**DATA FORMAT examples:**

- (1.) #####
- (2.) .....##### (includes *ignore* [.] for total of 14 characters)

The number of Ds in the DISPLAY FORMAT must match the number of #s in the DATA FORMAT.

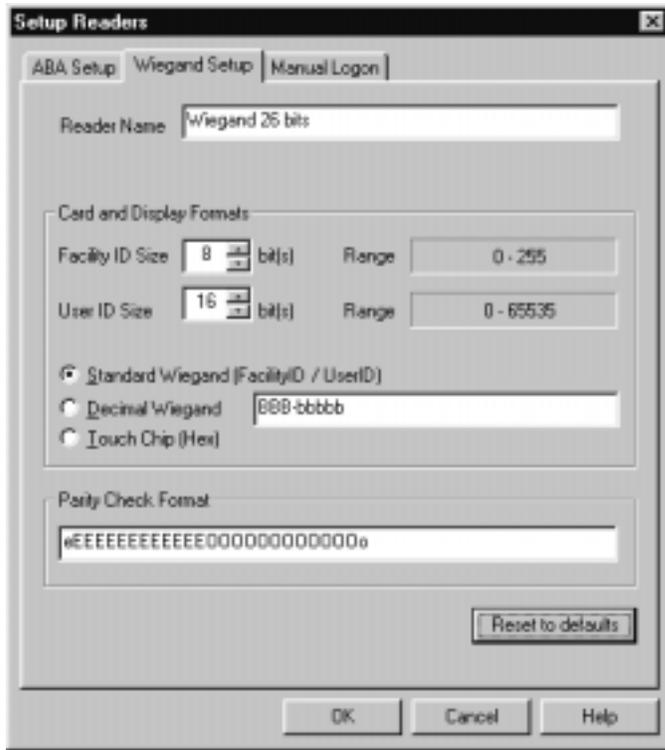
**DISPLAY FORMAT examples:**

- (1.) DDDDDDDDDDDDDDD
- (2.) DDDDDDD (or you could include separators: DD-DDDDDD)

Once you have completed the steps in setupmpw, you are ready to make cards through the main Millenium Expert Systems software (USER dialog, ACCESS tab.)

## Wiegand Setup Tab

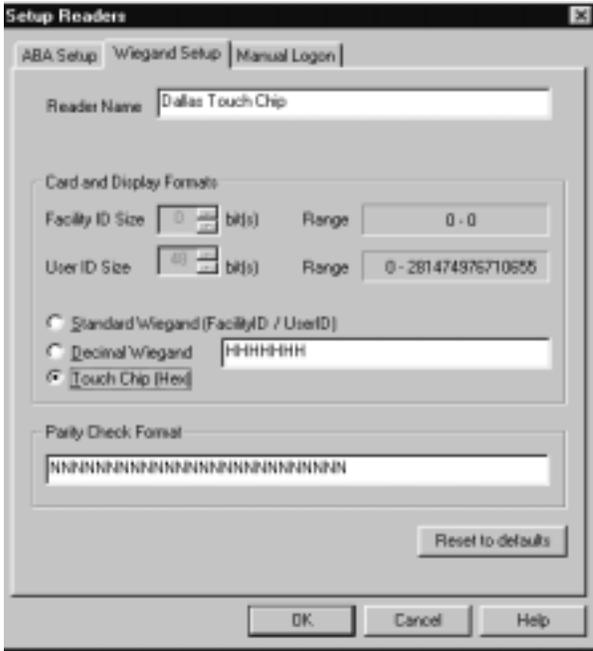
- The default card reader format is 26-bit Wiegand. You can record one Wiegand data bit pattern—standard or custom—for your entire facility. Group the display format the way you want it to appear throughout the software.
- (Any other Wiegand data bit output–Data Format–either 37-bit or custom, must be recorded, exactly.



- Three possible display options (DISPLAY FORMATS) exist for the **default** 26-bit Wiegand output shown in the second illustration below:
- **3-5 BBB-bbbbb** (designed for a facility code followed by User ID for access codes. The capital "B" is used for access code and the small for the User ID number.

### Less often used display formats:

- Six hex characters HHHHHH
- Dallas Touch/chip keys use hex Display Format. The number of characters can vary from 6 to 8 or 10, meaning you may need to modify the number of H's in the display format.



### Wiegand Data Format

Use the following symbols when creating a custom **DATA FORMAT** for Wiegand cards:

<b>SYMBOL</b>	<b>REPRESENTS</b>	<b>SYMBOL MEANS</b>
o	ODD parity bit	This exact position in the DATA FORMAT will be an <i>odd</i> parity bit character.
e	EVEN parity bit	This exact position in the DATA FORMAT will be an <i>even</i> parity bit character.
O	Data-making ODD parity bit	This exact position in the DATA FORMAT will be an <i>odd</i> parity bit character that will result in access code data.
E	Data-making EVEN parity bit	This exact position in the DATA FORMAT will be an <i>even</i> parity bit character that will result in access code data.
N	Data, but NO PARITY	This exact position in the DATA FORMAT will be a non-parity data bit.
.	Ignore bit and NO PARITY	This exact position in the DATA FORMAT will be a non-parity-ignored bit.

The 26-bit Wiegand default DATA FORMAT is:



### ***Important!***

- Data formats for each type of card (other than ILCO supplied) are proprietary and are not the responsibility of KABA ILCO. Please contact the vendor/manufacturer of the cards for exact specifications to ensure that you are using the correct format.

**NOTE:** Remember, if you use Hexadecimal Display format required by Dallas Touch/chip keys, you will not be able to read the number on the User card. Be sure that you have entered the number correctly and that you maintain an accurate list of all the numbers elsewhere.

- Eight decimal digits DDDDDDDD
- Record the one display you prefer in the DISPLAY FORMAT field. Use as many hyphens and spaces as you wish. Again, you may prefer to copy (Ctrl-C) and paste (<Shift><Insert>) the above formats into the DISPLAY FORMAT field.

### ***How do I set up a Wiegand Reader?***

1. Select Setup from the Start menu
2. Log in, using your Millenium Expert System password.
3. Click on the Setup Readers button on the main toolbar.
4. Select the Wiegand Setup tab.



- READER NAME field shows the exact description of the reader as it will appear in the dialog.
- DISPLAY FORMAT reflects the result of the DATA FORMAT you create. The display format controls how the data bits on the card will display in the Millenium software. The example shows the standard 3-5-digit display format with a 3-digit facility code followed by a 5-digit access code.
- DATA FORMAT reflects the symbols you set as the exact data format for the cards used at your facility.

## Manual Logon tab

**MANUAL LOGON** is the way to enable users who operate Millenium Expert Systems software to logon to the PC by manually typing their **Logon ID** and **Password**.

Also, when assigning cards to a USER (on Access tab in USERS dialog in the software,) the operator types in the Access Code. The access code either comes from printing on the card, or from placing the card in a reader and noting the access code as it displays in the software.

**NOTE:** Card-based access control systems must keep this field enabled. If operators receive Marlok KEYS instead of cards, change MANUAL LOGON to disabled so operators are required to insert their key in the special RS-232 wedge Key Reader that should be located beside the computer.

### ***Important!***

**Never** disable manual log on in a card-based system. If you do this, you will not be able to log back onto the system, so you will not be able to re-enable it.



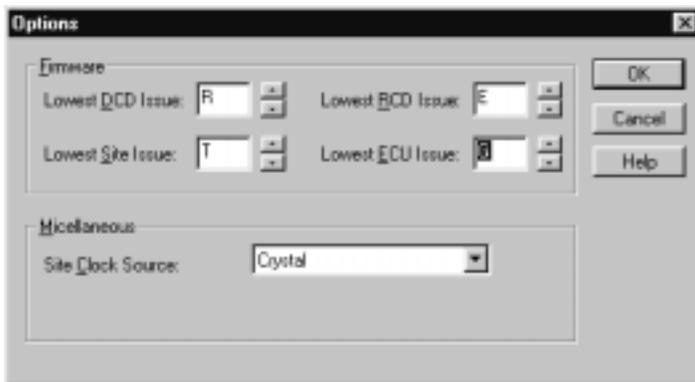
## Setup *OPTIONS*



Click on this icon and the following dialog box appears:

### Firmware issue levels (EPROM)

- EPROM stands for Erasable Programmable Memory. An EPROM is a memory chip on the circuit board that contains the programming about how the circuit board functions. You could think of it as the brain of the device.
- EPROM chips in Millenium devices (DCD, SCU, RCD and ECU) come with a label that identifies the issue level of the memory. This identification tracks whether or not a device contains the new programming that comes as device and software features expand.



The lowest EPROM issue levels for circuit board devices in the Millenium Expert System network appear in the second column below.

Device EPROM Issue Level	Lowest
DCD	R
SCU	T
RCD	E
ECU	G

All access control DEVICES in the Millenium network must be at least the issue level listed as lowest for Millenium Expert Systems software to operate. The current EPROM issue level is subject to change as new features are added to the software.

**Miscellaneous (Site Clock Source:)** The default (Crystal) means the on-board clock on the Site Controller Unit is used to set time. Keep this default clock in all but very unique circumstances. The 50 or 60 Hz option changes the clock source from the circuit board device's on-board clock to an AC power source."

### Options Menu

Click on Options in the menubar and the following appears:



Setup system Options will bring up the same dialog box as above.

### Set up Custom User-Defined Data Fields

Click on the icon  shown at left and the following dialog box appears:

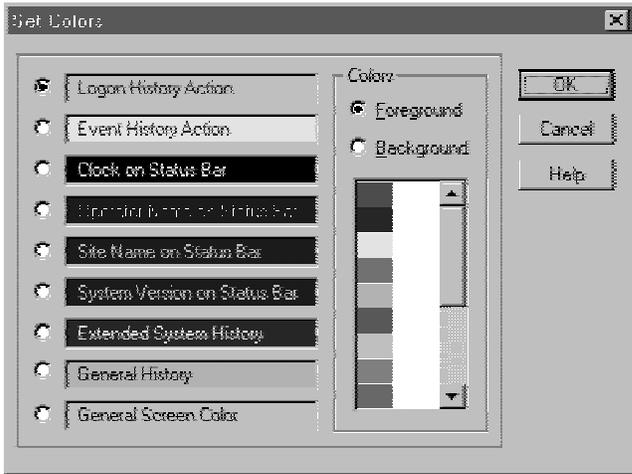


Name up to ten custom fields in the User Fields dialog. The field names you create will appear in the **Users** dialog on the **User Fields** tab. You can choose to have these fields display in the

history portion of the Millenium workspace each time a user UNLOCK occurs.

## Setup Screen Colors

To control the color in which certain types of Millenium software data show up on your monitor, use the Colors dialog . 



The screen shows the COLORS setup function in Millenium Expert Systems.

## Setup in Millenium Expert



The setup dialog under the Options file on the Millenium Expert Systems menubar differs from the complete Setup (setupmpw) in the Millenium Expert Systems program group . Use this menubar Options setup to fine-tune selected settings. Most of these options deal with communications.



## Millenium Expert Options Setup - Definitions

<b>Site Polling Retry Count</b>	<p>Sets the number of times the PC tries (unsuccessfully) to poll each site before labeling the site as offline.</p> <p>Example: If count = 5, you tell the PC to complete five polling cycles over the Millenium network before considering the site offline. Recommended setting is 2.</p> <p><b>Important!</b> When Site Polling is enabled, polling is never discontinued. After the retry count designates a site is offline, the PC goes ten (10) times around the polling cycle before trying to poll the non-responding site again. After ten (10) times with no response, the PC tries the site every 100 times around the polling cycle.</p>
<b>Modem Delay in milliseconds</b>  <i>For DIAL-UP</i>	<p>Shows the maximum amount of time the modem should take between transmissions of individual blocks of data. Increase this delay setting to efficiently send <b>large amounts of data over long distances to other sites</b>. (Most often, <b>500 ms</b> is the recommended setting in leased-line modem communications. Other types of communication configurations can use settings between <b>0-50 Ms.</b>)</p>
<b>Global Send Count</b>	<p>Shows the number of times a global message is repeated. Global messages are those that affect the entire Millenium device network. Increase this count where communication lines (usually leased lines) experience frequent "noise" or interference. Higher global send counts avoid missing global message information.</p>
<b>Cold Reset Update</b>	<p><b>Cold Reset:</b> A cold reset occurs when all data in memory of the circuit board device is gone due to: (a) deliberate action of resetting the board's memory, (b) the board being offline for more than the 24-hour memory capacity, or (c) anything that corrupts the data. A Cold Reset occurrence generates a <i>Cold Reset</i> history message.</p> <p><b>Enabled:</b> Update automatically takes place when the <i>Cold Reset</i> history message occurs.</p> <p><b>Disabled:</b> Update action does not automatically occur following a cold reset. Operator must manually perform .</p>
<b>Online Update</b>	<p><b>Enabled:</b> Whenever a device (DCD, SCU, RCD, ECU) goes off-line, any system programming changes made during the off-line period automatically update when the device comes back online.</p> <p><b>Disabled:</b> Whenever a device goes off-line, operator must manually perform an update to send any system programming changes.</p>
<b>PC Modem Number (Base)</b> <i>For DIAL-UP</i>	<p>Record the base modem number at the main Millenium PC. Leave Area Code and any dialing prefixes off the number you record here. Use the Site dialog's CALLBACK PREFIX field to record such site-specific digits.</p>

# Chapter 4: Sites

Set up Site Control Units (SCUs) to communicate (in a Dial-up modem or Direct configuration) between Millenium software and the electronic access control devices installed in your facility.

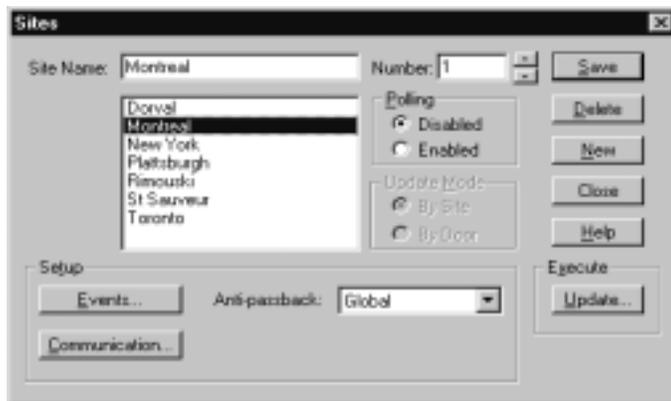
The picture below shows the SITES dialog in Millenium Expert Systems. Sites are also known as Site Control Units (SCUs) in the Millenium network of devices. First add the installed Site to the software, then determine which options to configure in this dialog for the features required by your facility. Software settings will *program* each site according to how you want the Millenium Expert system to operate.

## How do I add a Site?

After preparing user data and planning access groups, and Timezones; and after adding a user and making the user a Level One operator;, the next programming step would be to add a site.

Make sure a Level One operator has made any special communication settings in setup (setupmpw.) Special settings would include IP addresses or installation of a modem through Windows Control Panel. If you use Marlok keys, the port where the console key reader is plugged should be recorded in the PORTS dialog of the setup program.

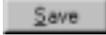
1. Click the SITES  toolbar button.



2. If this is the first site being added, type a SITE NAME that will identify this site (SCU device) throughout the system. Otherwise, if sites already exist in the software, press the  button to clear the data fields in preparation for adding a new site.

**NOTE:** Avoid using symbols such as apostrophes. If you have a large number of sites, you will be able to sort sites in ascending or descending order by name as an aid in selecting a particular site.

3. Select the NUMBER that corresponds to the Address Select setting on the rotary dial of the SCU circuit board. This **unique** number identifies the site to the entire system.
4. POLLING: During setup, polling should remain disabled until the software is programmed and all programmed access control devices (SCUs, DCDs) are installed and ready to communicate with the software.

5. In DIRECT communication configurations, once you enable the site, each time you load the software, history will identify the site as "On Line." After each on-line SCU gets status from all devices under its control, the history displays "Site Status Received."
6. DIAL-UP communication configurations require that the modem be installed and ready to select from the  dialog.
7. Once you enable the site, click the  button to choose a modem communication site and execute a dial-up command from the Dialup Connections dialog.
8. Click this action button  to set up the COM Port being used for DIRECT communication to the given site.
9. A Site Communications dialog displays. For DIAL-UP communication sites, see information on Setting up a Dial-up modem site on page **Error! Bookmark not defined..**
10. Click this action button  to select those DCD Alarms and site-specific actions to be tagged as Site Events for this site.
11. ANTI PASSBACK If this site uses the Antipassback protection feature, select the type of Antipassback in use.
12. Press the  button to add the new site to the database.
  - Once a DIRECT site is ready to go ONLINE, and polling is ENABLED, this action immediately communicates to the SCU.
  - Once a DIAL-UP site is ready to go ONLINE and polling is ENABLED, this action must be followed by sending the new site data to the remote site through the Dialup Connections dialog.

## How do I configure a direct communication site?

1. After a Site Control Unit (SCU) is installed and connections to Doors (DCDs) are complete, the next phase is to program the communications.
2. For DIRECT communication configurations, once you select the **Enabled** polling setting, the data from the computer goes to the Door Control Device each time you press the  button.



**Polling Disabled** - Disabled polling means the system does not attempt to connect or communicate with the site (SCU.) You should disable a Direct site when a site controller (SCU) is being replaced.

3. Update - To perform a site update, an operator clicks the **Execute...** button and selects **Update...** command on the main site dialog.

**Setup Events** - Site events are those pre-defined actions that trigger a relay in the Millenium Expert Systems, AND that will be reported to the ALARM MONITOR for action by an operator. Click on the **Events...** button to bring up a dialog box to select events that this Site will report.

**NOTE:** You should set up DCD alarms and DCD Events for doors (ACCESS POINTS dialog) before selecting Site Events.

**Setup Communications** - Click on the **Communication...** button to set up direct or dialup communication.

4. The button pops up a Site Communications dialog where you select the communications port used by the given site. Port selection may be a: **Windows COM port** (DIRECT communications)
5. Operator selects a COM port from those ports recognized though Windows and displayed in the COM PORT listbox on the Site Communications dialog.

### ***How do I configure a Dial-up Site?***

1. First, set up the dial-up site the same way you set up any site. Follow the steps in the main Site dialog.
2. Press the **Communication...** button on the main SITE dialog to display the Site Communications dialog.
3. Then, select a Windows-installed modem from the COM PORT field. The following steps describe fields that become enabled after you select a modem from the COM PORT field on the Site Communications dialog.



4. TIME DIFFERENCE: If this site is enabled for Daylight Savings Time, record the time difference between this site and the timezone where the Millenium PC is located.
5. CONNECT MODE: Select whether the dial-up modem connection will be through Manual operation by the operator, or whether you set up an **Automatic** time when the modem will dial up the Site.

**NOTE:** Automatic means that all of the following will be done automatically: Connect, Disconnect, Refresh, History Download

6. If you select the automatic option, the time fields become enabled. Fill in the hour and minute in military time when the call should take place. If you have multiple dial-up sites, the automatic connections will take place one site at-a-time.
7. SITE MODEM #: Record the modem number the Millenium PC modem must dial to reach the Site Control Unit's (SCU's) modem.

**NOTE:** To adjust the modem delay, go to the Options menubar. (The Setup dialog from the options menubar also holds the modem number of the Millenium PC.)

8. Press the  button to add the new DIAL-UP site to the database.
9. Once a DIAL-UP site is ENABLED and the modem is operational, this site is ready for the modem-specific actions.

### ***Important!***

If you change a site from DIAL-UP modem communication to DIRECT by changing the selection in the COMM PORT field, **remove the Site Modem #**. The software considers a site to be dial-up if a number appears in the Site Modem # field.

## *Windows-installed modem (DIAL-UP communications)*

Operator selects the Windows-installed modem and completes additional modem information.

Once you install a Windows-compatible modem, complete the software programming, and select the Enabled polling setting, you must connect to the dial-up site through the Dialup Connections dialog. Then you perform an **Update** through the Update Site dialog.

## *Antipassback*

(Optional - If a site uses the Antipassback feature, select the type of Antipassback in effect at the given site (Paired or Global.) Otherwise, leave the setting at the default "Not Used." For information on all the types of Antipassback and how to set it up, see page 45.

## *Updating a Site*

The  action button on the SITE dialog sends all programming data out to Millenium access control devices for one or more specified sites.

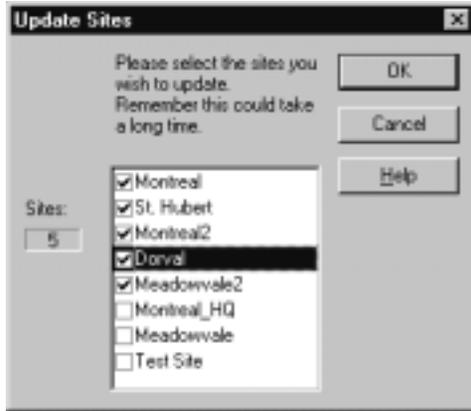
Sites must have Polling Enabled on the main SITE dialog.

**Sites in DIRECT communication** automatically send data to devices each time an operator press the button. Therefore, site updates are only called for in special situations.

*Examples:*

- After a newly installed site has been programmed and polling has been enabled.
- After a site has been off-line or without power for an extended period of time (usually more than 24 hours.)
- As a trouble-shooting technique to replace all data with the current software data.
- After performing a *Millenium Database Utility* import of Users with Access Group assignments.
- After changing card readers and/or card reader data formats.

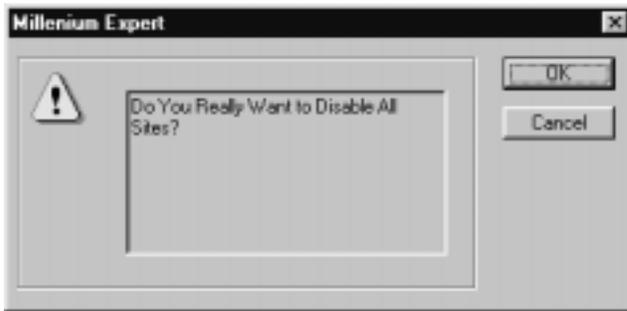
**Sites** appear disabled unless the site is currently connected to and online through the Dial-up Connections dialog. Once a dial-up site is online, that site appears enabled in this update dialog. Then, an operator can perform the update process.



Select the sites and then click OK.

## ***Disable All Sites***

Under the Site menu bar, the following warning appears if an operator selects **Disable All Sites**;



- This disables communication to all sites in the Millenium Expert Systems network.
- Only operators with EXECUTE rights can perform this operation.

### ***Important!***

The **Disable All Sites** function is only intended for specific troubleshooting purposes, such as to stop polling all Millenium devices to troubleshoot overall network problems. This function is rarely used.

## ***Network Communications***

**Network communications** set up occurs through Millenium Expert Systems Setup program (setupmpw.)

- Requires optional Server and Workstation software.
- TCP/IP protocol network must already be installed and set up by a network administrator
- Requires IP Addresses provided by your network administrator.

## Dialup Communication History

1. Configure the Dialup communication History by clicking on the Dial-up toolbar button . The following dialog box appears.



2. Press this radio button  **Connect with Continuous History Polling** on the Dialup Connections dialog to dial up and connect to the site to get site history from the devices (SCU, DCDs, RCDs, & ECUs.)
3. History displays in the application workspace and automatically saves in the history database, as part of the Millenium Expert Systems system. The system automatically **disconnects** as part of the process after the download slows to intermittent.

### **Important!**

There are three options to get history from a dial-up site:

1. Execute the  **Download History from Site** command described above to download all site history.
2. Set up the automatic update option through the Connect Mode field under the **Options** menubar. When the automatic connection occurs, all history downloads as part of the process.
3. Execute the  **Connect with Continuous History Polling** command.

## ***Site: Buffer at 80% full***

- Site Control Units (SCUs) hold history until the history is downloaded to the Millenium Expert Systems software.
- After a Site Control Unit reaches its full capacity to store history, the oldest records begin to be **deleted** from the storage.

**NOTE:** A Site option called Buffer at 80% full can be set up to report when the SCU reaches 80 percent of its capacity to hold history. This condition is designed for sites with dial-up communications. This option is displayed when you click on the  button in the main dialog for Sites.

If the following conditions exist, the operator gets special notice when the Site's buffer is near capacity:

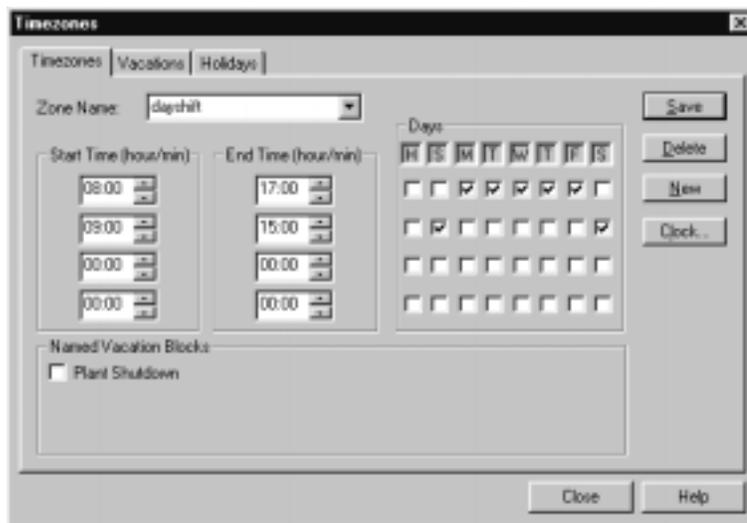
- Alarm Editor is set up, (with *Buffer at 80% full* site event selected)
- Alarm Monitor is running.

# Chapter 5: Timezones

## Timezone - Definition

Timezones are blocks of time established in Millenium software to limit or control:

1. when user Access Groups can have access to doors within the Millenium network.
  2. when time-related relay functions start and stop.
- Timezones are at the heart of controlling access to your facility. For any given Access Group, one Timezone links to each access point in the facility. Then you assign each user to an Access Group. As a result, users can only have access to points in your facility during pre-determined times.
  - Timezones can also automatically control access points, automatically activate devices, and automatically determine when a pre-defined action is handled as an event in your facility.
  - The picture below shows the TIMEZONE dialog in Millenium Expert Systems. Notice this dialog has three tabs of time-related information.



- A Timezone can include up to four intervals. Each interval includes a starting and ending time, in military time. In the above sample, the second interval shows that on Saturday, the *Day Shift* Timezone has a START TIME of 9:00 and an END TIME of 15:00. The weekdays, however, end at 17:00.
- Two system Timezones exist: **Never** (default) and **Always**.
- One Timezone interval can cross midnight. For example, the START TIME for a *Cleaning* Timezone could be 22:00 and the END TIME could be 02:00.

## VACATIONS:

- NAMED VACATION BLOCKS show those time periods you've established on the Vacation tab.
- A check in a vacation block means the vacation period applies to the Timezone—the TIMEZONE becomes **invalid** during the selected vacation block.

**NOTE:** One Vacation cannot cross a year. To handle a situation such as a Christmas break requires two Vacations period—one at the end of the year and a second in the new year.

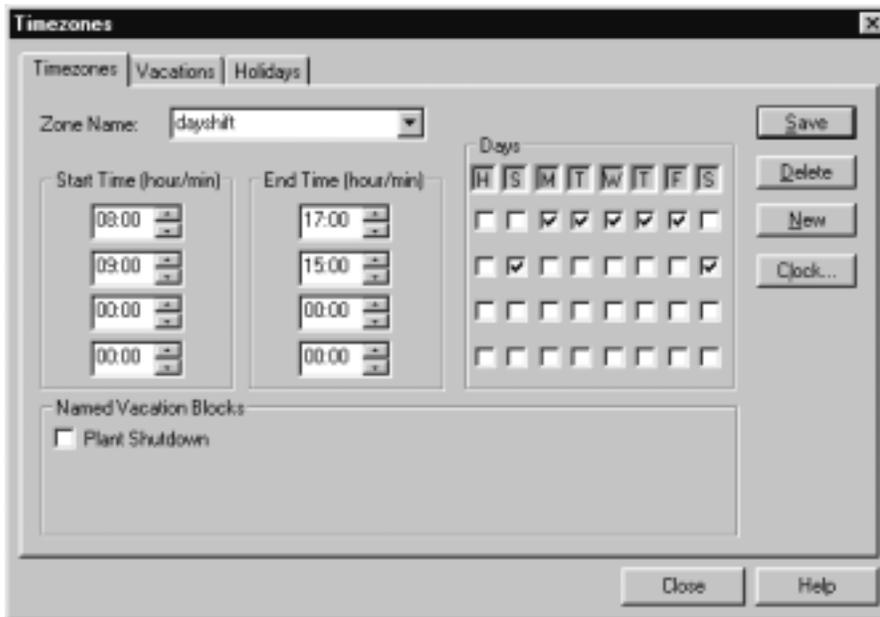
## HOLIDAYS:

A check in the column (DAYS section) of the main Timezone tab means **all holidays** established on the Holidays tab are included as part of the given TIMEZONE. The TIMEZONE remains **valid** for all holidays if a check appears in the H column for a given Timezone interval.

### How do I set up a Timezone?



1. Click the  icon on the Millenium Expert Systems toolbar.
2. The Timezone dialog appears with three tabs that hold time-related data:



3. Press the button to clear any field data on the main Timezones tab. Then name the Timezone you want to create. Zone Name:
4. Give Timezone a name that will have meaning to an operator when it's time to assign a Timezone somewhere else in the Millenium software.

5. Move to the **Start Time** section of the first interval, and click the  button.
6. Select or type the time of day (in military hours and minutes) the timezone begins.
7. Press the <tab> key to move to and establish the **End Time** for that interval.
8. If needed, use addition intervals for this Timezone. Each Timezone can have up to four intervals. For example, if a Timezone has a different End Time on Saturday, put the Saturday settings on a different interval.
9. Move to the DAYS section. If you have Holidays established, set the column as follows:
  - Timezone becomes invalid during **all** system holidays.
  - Timezone is valid during **all** system holidays.
10. Click on the days of the week that apply to the Start and End times you have established. (Click, again, to de-select a day.)
11. Move to the NAMED VACATION BLOCK section. All vacation periods established on the Vacations tab appear for your selection. Select the vacation blocks, as follows:
  - Timezone is valid during the selected vacation period.
  - Timezone becomes invalid during the selected vacation period.
12. Press the  button.

### *How do I set up holidays?*

Holidays are those time periods, usually statutory holidays observed by the entire Millenium Expert Systems network.

1. Click on the Holidays Tab:



2. Enter a name for the holiday. Name as many as 20 holidays observed at your facility.
3. Select the date of the holiday from the dropdown calendar by clicking the arrow to the right of the Date field.



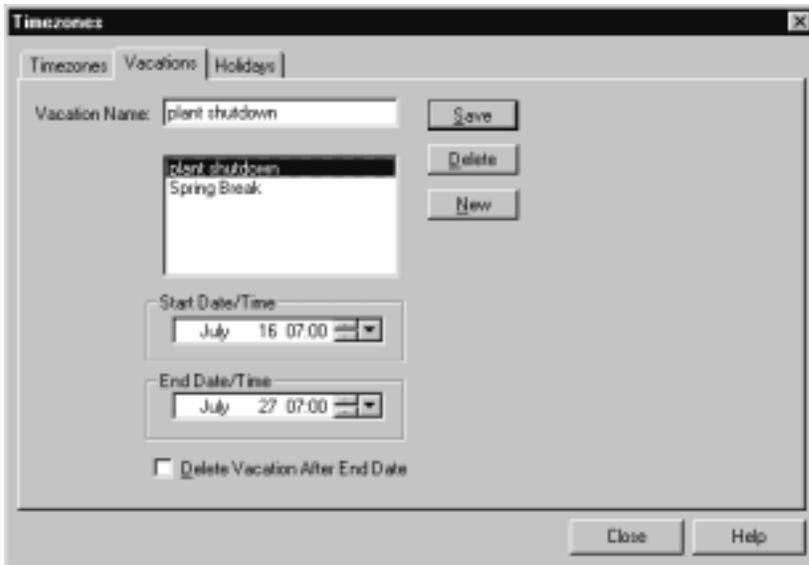
**Important!**

- Operators must establish a procedure for updating the actual date of those holidays that change from one year to the next. Since holidays may be part of the TIMEZONES created for your system, it is important that holidays, which fall on different dates every year (such as Thanksgiving), are accurate for each ensuing year.
- The  **Delete Holiday After Date** checkbox lets you make sure such holidays are deleted from the system. Once you click the delete option, the Date box displays day-of-the week and the current year data. After the holiday is past, the software deletes the expired holiday from the database. A history message ("Holiday expired") helps the operator know to re-program this type of holiday for the following year.

**How do I set up vacations?**

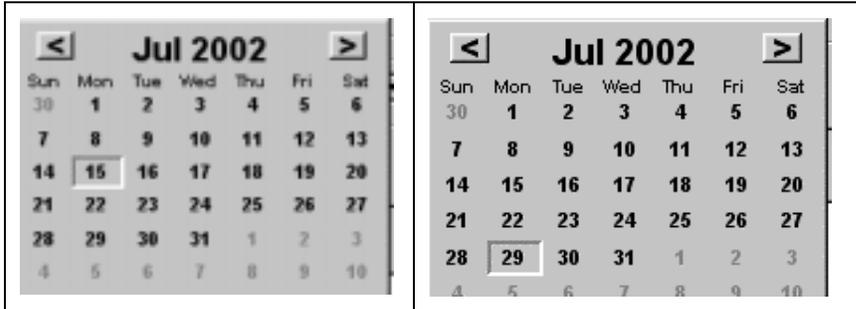
Named vacations appear on the main TIMEZONE tab. The operator selects those vacation periods that apply to the given TIMEZONE.

A check in a named vacation block of the TIMEZONE tab means the TIMEZONE will be **invalid** during that vacation period.



1. Enter a name for the vacation period.

2. Set up as many as eight (8) vacation periods.
3. Click the  button.
4. Use the calendar to help you select the MONTH and DAY for start and end of the vacation period.



You can also use the spin control buttons  to move forward and backward through highlighted segments of the date and time field, or you may choose to type the data.

### ***Important!***

One Vacation cannot cross a year—two Vacations are required.

For example, if a Winter break runs from December 18TH through January 8TH, a *Winter2000* vacation from 12/18 through 12/31 and a *Winter2001* vacation from 1/1 through 1/8 must be established.

The   checkbox lets you set up a vacation for automatic deletion from the system after it occurs. Once you click the delete option, the Date box displays day-of-the-week and the current year data. After the vacation is past, the software removes the expired vacation from the database. A history message ("Vacation expired") helps the operator know to re-program this type of vacation for the following year.

## Chapter 6: Access Points

- Access points are those locations in your facility where a user requires valid identification by key or card before being granted access. Some examples include doors, parking gates, or elevator floors, etc. where a key or card-reading device is installed to electronically read a user's identification.
- A Millenium Door Control Device (DCD) or Elevator car Control Device (ECD) electronically reads the key or card. DCDs retain history of all activity at the access point and Elevator Control Units (ECUs) retain history of all activity at the elevator floor access point. In some cases, the access point may take advantage of alarm inputs and relays on the DCD or ECU. Alarms can trigger events. Events can cause relays to operate electric strikes, or respond to devices such as motion detectors or trigger an external device such as a bell, buzzer, or camera.
- Use the Doors tab to program those doors in your facility that have Door Control Units (DCDs) installed.
- For facilities with elevators and Elevator Control Units (ECUs) installed, the dialog box includes an ECU Floor Relays tab where you name and assign elevator floors—each of 16 ECU Floor relays—as access points. Then you select Elevator car Control Device (ECD) readers that will activate the given floor, and program how and when the elevator reader will control access to the floor.
- Once you communicate software data to the DCDs, the doors (or other devices) will be controlled electronically based on your Millenium Expert Systems settings.

**Doors - The picture below is the ACCESS POINTS dialog in Millenium Expert Systems. Once you learn which options to use to configure features required by your facility, customize each access point according to how you want your Millenium Access Control system to operate.**

**Doors Tab:** Doors or devices controlled by Door Control Devices (DCDs)



- First four fields allow you to select the name and number of the site, then select a door or enter a new door name and number.
- Clicking the buttons below will pop up dialog boxes that allow you to do the following:

**Reader...** identify type of reader device installed at a given door.

set up keypad combos.

set up Card Readers in Wiegand or ABA modes.

**Relays...** set up DCD Relays for a Millenium access point

**Alarms...** set up alarms inputs used on this door

**Events...** identify events to which this door will respond

**Execute...** perform or update door events from the PC (includes the **Update** and **Status** actions along with **Remote Unlock**, **Override Strike** and **Forgive Antipassback**.)

### ***How do I add an Access Point?***

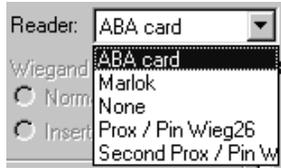


1. Select the ACCESS POINT icon to pop up Access Point (Door) dialog.
2. Highlight a SITE NAME for which you want to create Access Points.
3. Type a DOOR NAME that identifies this door (DCD device.) Avoid using symbols such as apostrophes.
4. Type in the NUMBER that corresponds to the Address Select setting on the rotary dial on the

DCD circuit board. This unique number identifies the door (DCD) to the entire system.

5. Use the **Setup** section of action buttons:

6. To set up the Reader installed on this door, click the **Reader...** button.



7. If the DCD is not connected to a reader, select *None*. For card readers, set up the Wiegand or ABA mode for the particular reader. If a keypad is in combination with another type of reader, click the ENABLED button, and set up the Keypad combo options.

8. To set up either of the two on the DCD, click the **Relays...** button.

9. If door operates by electric strike, use the *First DCD* relay to set up the strike operation. If the door is **not** strike-operated, you can use the First DCD or Second DCD relay output to trigger a supplemental device for the individual door, such as a camera or buzzer.

10. If you want door to respond to ALARMS, use the *Second DCD* relay to respond to alarm inputs (Alarm-related DCD relay modes,)

**NOTE:** An RCD relay can also respond to a Door EVENT that may or may not be caused by an ALARM.

11. To trigger a secondary device based on system **Events...**, set up the ALARMS (and select the EVENTS.) Then set up the DCD relays.

**NOTE:** You can always add programming for these optional relay features later.

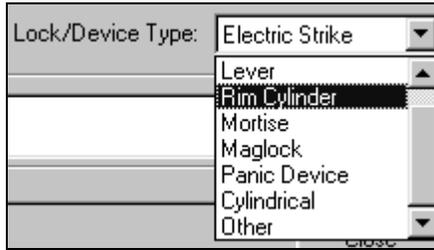
12. To set up any of the seven possible alarm inputs that might be wired on the DCD, click the Alarms button (**Alarms...**.)

13. To select those events to which this DCD will respond, click the **Events...** button.



14. Select all or check individual events.

15. Select the LOCK TYPE that describes the type of hardware installed on this door. If the DCD only uses its relay contacts and is not connected to locking hardware, select *Other*.

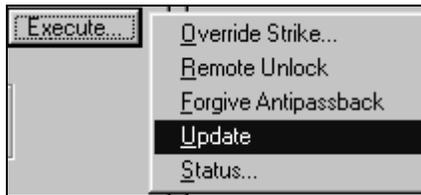


16. Use the NOTES box to describe the access point, as needed. You may summarize the Setup for this door to save an operator from having to check the individual setup dialog windows.

17. Press the  button to add the door to the Millenium database.

**Important:** Be sure to save before selecting or creating another access point. If you select a different access point without saving the one you just created, you lose your work.

18. Updating door data to the DCD device:



Online systems (with polling Enabled) in DIRECT communication configurations will automatically add this door to the DCD as soon as you save the door. (A Level One operator would only use the deliberate Update action to send all data to a newly installed door.)

## Door events

- In Millenium Expert Systems, an event is a pre-defined action that triggers a relay.
- Once you have set up door alarms ( button,) to show one or more of the seven possible DCD alarms wired for the given door, the name you give to each alarm appears in the DCD Events setup dialog. Click to select those alarms (and usually the corresponding reset) that you want to be treated as “events” for the given door.



- Each event goes out to the Millenium network as data output from the DCD. In the above sample dialog, the given DCD uses one of its seven possible alarms (Dock Camera.) The Alarm and its reset (Dock Camera Reset) are designated as EVENTS. When the door opens, the Dock Camera alarm triggers the camera to record. When the door closes, the reset stops the camera.

## Door alarms

- Millenium Door Control Devices (DCDs) come with seven alarm inputs. Alarm input number 7 offers a special Door Ajar feature where the door can be set to respond if left propped for more than a designated amount of time.
- Alarm inputs from the DCD can cause an output to occur through two possible relays in the Millenium Expert Systems system:
  - the 2ND DCD relay
  - an optional RCD relay (when the input is also defined as a DCD event.)

### *How do I set up door alarms?*

The screenshot shows a configuration window titled "Dock door - Device Alarms". It includes the following fields and controls:

- Alarm Name:** Text input field containing "dock door camera".
- Number:** Spin box containing the value "1".
- Shunt Delay:** Spin box labeled "(seconds)" containing the value "0".
- IGNORE Timezone:** Dropdown menu with "Never" selected.
- Mode:** Dropdown menu with "Normal" selected.
- Door Ajar Time:** Spin box labeled "(minutes)" containing the value "0".
- Priority:** A slider control ranging from "High" to "Low", with the value "10" displayed in a text box above it.
- Notes:** A text area containing the text: "Second DCD relay triggers a camera to run for one minute each time the dock door is opened."

On the right side of the window, there are five buttons: "Save", "New", "Delete", "Close", and "Help".

1. Give the alarm a NAME.
2. Select the NUMBER (1-7) that corresponds to the alarm input used on the DCD for the given alarm. (Only Alarm 7 offers the Door Ajar feature.)
3. Select one Timezone during which the alarm will be ignored. If you never want the alarm ignored, select the **Never** Timezone. Otherwise, select the user-defined Timezone that applies to the given alarm.
4. SHUNT DELAY: Establish a grace period before the alarm triggers. Options are between 1-255 seconds.
5. Prioritize the alarm in a scale from 1-100. The Alarm Monitor will use this information for display options.
6. Use the NOTES section to record any free-form text for operators about the alarm setup.
7. Press the button.

## Table of DCD Relay Modes

Setting up (programming) DCD Relays Both relays on a DCD can operate in any of the following modes:

<b>Auto Activate</b>	Relay contact activates during a selected TIMEZONE. Relay automatically deactivates when the TIMEZONE ends. Valid users can enter outside of the ACTIVE TIMEZONE, for the designated number of seconds set in SECONDS ACTIVATED field.
<b>First User Auto Activate</b>	Relay contact activates for first valid user during the selected TIMEZONE. Contact remains active until the TIMEZONE ends. Valid users can enter outside of the ACTIVE TIMEZONE, for the designated number of seconds set in SECONDS ACTIVATED field.
<b>Valid User</b>	Relay contact activates for a valid user, for the designated number of seconds—only during the selected TIMEZONE.
<b>Invalid User</b>	Relay contact activates for a rejected user, for the designated number of seconds—only during the selected TIMEZONE.
<b>Any User</b>	Relay contact activates for any user (valid or invalid,) for the designated number of seconds—only during the selected TIMEZONE.

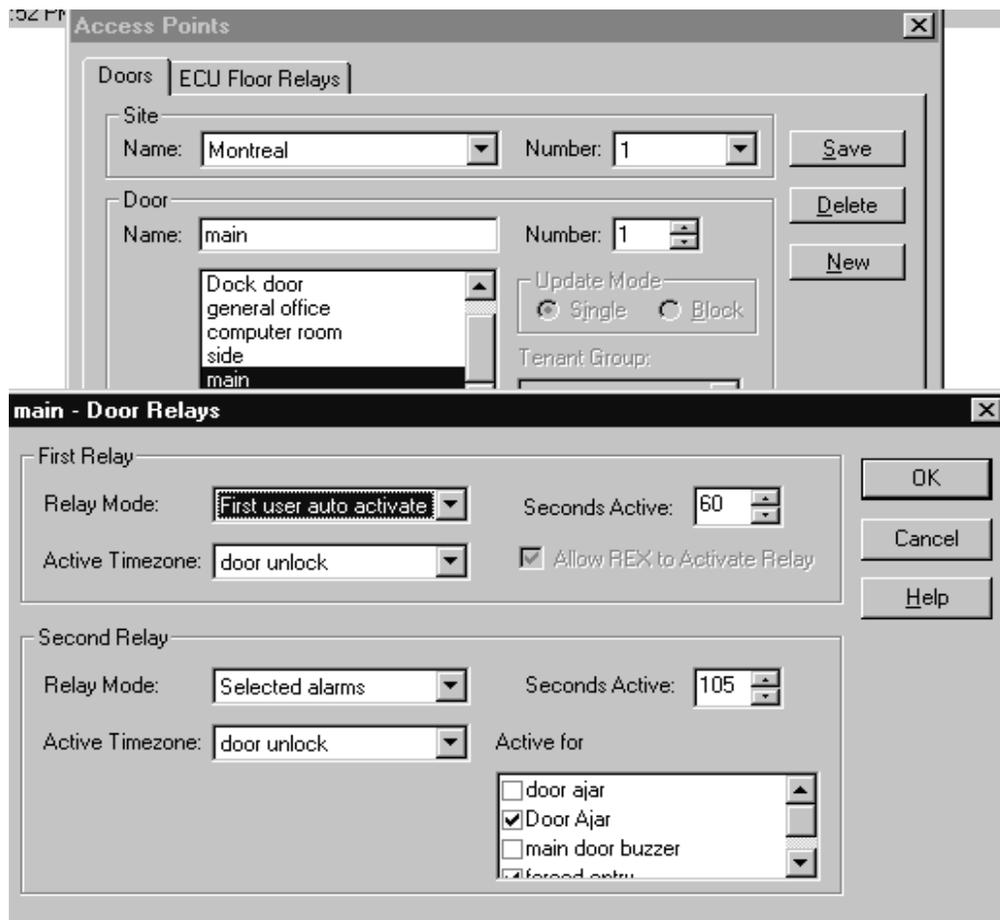
The 2ND DCD Relay includes two *additional* mode options:

<b>Selected Alarms</b>	<p>2ND Relay contact activates for the designated number of seconds, during the selected TIMEZONE when one or more of the seven possible alarm inputs from the DCD are activated.</p> <p>The Active for Alarm(s) listbox becomes enabled, and displays only those alarms setup up for the given door.</p> <p>Example: Assuming ACTIVE TIMEZONE = Always, and SECONDS ACTIVATED = 120:</p> <p>If a dock door has a magnetic switch contact input, and Alarm 1 on the DCD triggers a camera, when the door opens, the following occurs:</p> <p>(1) Magnetic switch creates an alarm input which, in turn, (2) sends output to run the camera for a period of two minutes (120 seconds.)</p>
<b>Mirror Selected Alarms</b>	<p>2ND Relay contact activates when the selected alarm is activated. With multiple alarms, the 2ND DCD relay is active while those selected alarms are active. The Mirror Selected Alarms mode lets you further limit the relay to be active not only while the selected alarm is active, but also only during relay's ACTIVE TIMEZONE.</p> <p>Example: Assuming ACTIVE TIMEZONE = Always:</p> <p>If a door relay is set to run a camera based on a motion detector alarm, the camera would Always run when motion is detected and stop running when no motion is detected.</p>

## How do I set up DCD Relays?



1. Select the ACCESS POINT icon.
2. Highlight a SITE where you want to set up a DCD relay.
3. Highlight the DOOR where you want to set up a DCD relay.
4. Click the **Relays...** button. The following window pops up:

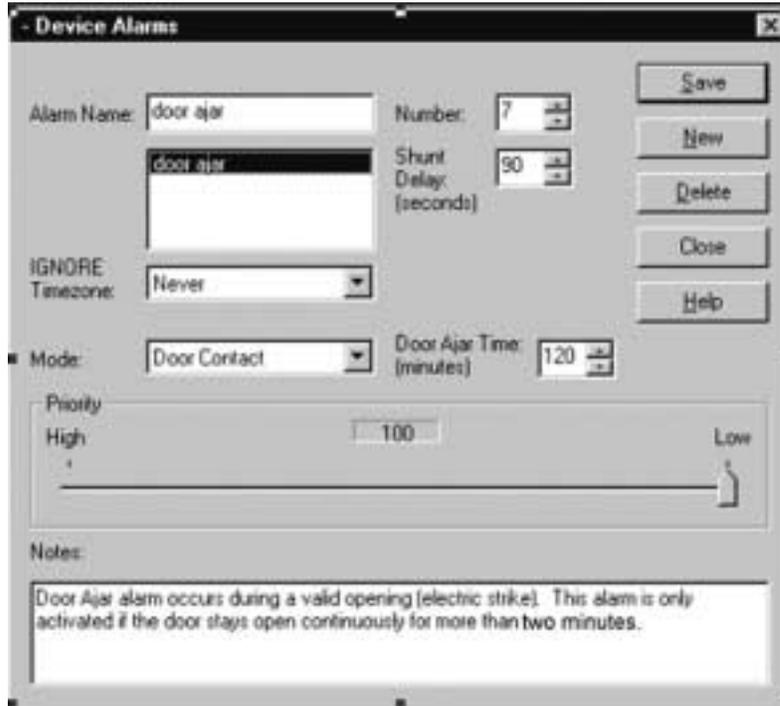


5. Set up the 1ST or 2ND DCD Relay depending on which relay on the DCD is in use.
6. First, select the RELAY MODE.
7. Then highlight the ACTIVE TIMEZONE during which this relay is in effect.
8. SECONDS ACTIVATED: Set the amount of time in seconds the relay will remain activated as part of a valid opening.
9. For 2ND Relay, only: Select the alarm or alarms for **Selected alarms** or **Mirror selected alarms** modes.

## Door Ajar feature

Alarm # 7 on a Door Control Device offers a special Door Ajar feature. The feature lets you set up an alarm to activate if a door is propped open, following a valid entry, for more than a pre-set amount of time.

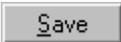
### *How do I configure the Door Ajar feature?*



1. Give the new alarm a NAME.
2. Select NUMBER 7. (Only Alarm 7 offers the Door Ajar feature. Notice a special **Mode** field becomes enabled.)
3. Select one Timezone during which the Door Ajar alarm will be ignored. If you never want the Door Ajar ignored, select the **Never** Timezone.
4. SHUNT DELAY: Establish a grace period before the alarm triggers. Options are between 1-255 seconds. (Shunt Delay must always be less than Door Ajar Time.)
5. MODE: (with Alarm # 7, only) Two modes control whether the seventh alarm operates like all other alarms, or whether the seventh alarm operates in response to a door contact.

**Normal** Alarm responds to an input on the DCD (like Alarms 1-6.)

**Door Contact** Alarm responds to Alarm # 7 input on the DCD, following a door contact. With this mode, the **Door Ajar Time** field enables.

6. DOOR AJAR TIME: Set the amount of time (in minutes) you want to allow before the door contact alarm goes off following a valid entry. Beyond the Shunt Delay, this Door Ajar Time lets you set how long the door can be propped open or left ajar following a valid opening, before the alarm triggers. Options are 1-255 minutes.
7. The door ajar alarm activates following a valid access, after the pre-set Door Ajar Time period has passed. History displays: "<Alarm name>: **Door Ajar**"
8. With invalid access, the system does not wait for the Door Ajar Time period to pass before issuing an alarm. History displays: "<Alarm name>: **Forced Entry**"
9. Prioritize the alarm in a scale from 1-100. The Alarm Monitor will use this information when deciding which active alarm requires attention first.
10. Use the NOTES section to record any free-form text for operators about the alarm setup.
11. Press the  button.

## Antipassback: Definitions

If you select one of the two Antipassback options in the Site dialog, the site is ready to set up to use the Antipassback feature for its doors. Antipassback is designed to prevent users from passing their key/card back to someone else to gain access to your facility. Operator may forgive Antipassback from the PC.

Two types of Antipassback exist:

**PAIRED** A user must exit the facility by an EXIT DOOR other than the one used as an ENTRANCE before his/her key/card is valid to work again in the system.

**GLOBAL** A user must exit the facility by any door designated as a GLOBAL exit.

When Antipassback is enabled in the SITE dialog, the ACCESS POINTS dialog Antipassback fields are automatically enabled. The system will require any necessary Antipassback field selections before allowing you to save the data.

**PAIRED** The following options appear in the ACCESS POINTS dialog with Paired Antipassback:



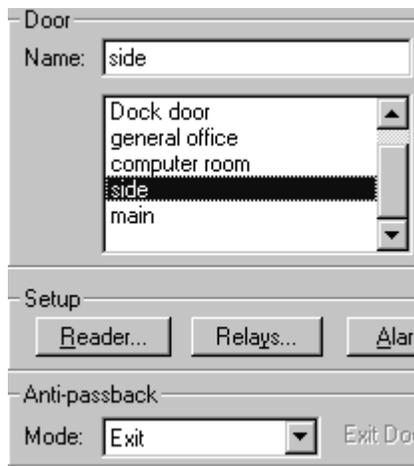
The screenshot shows a dialog box titled "Anti-passback". It contains two dropdown menus. The first is labeled "Mode:" and is currently open, displaying a list of options: "None", "Entrance", "Exit", and "Timed Entrance". The second dropdown menu is labeled "Exit Door:" and is currently closed.

**None** Door does not use the Antipassback feature.

**Entrance** Door is designated as an entrance. The EXIT DOOR field automatically enables, and a selection is required.

**IMPORTANT:**

**In order to have a list of EXIT DOORS on the dropdown list, you must have designated them first.** To do this, select Exit under Mode (shown above) and designate some doors as exits. Then you can choose Entrance and have a list of exit doors to use in Paired Antipassback mode. In the example below, the west side and side doors were selected, exit mode was chosen and both doors were saved. The next move was to choose another door in Entrance mode and choose one of those two previously created exits, side or west side to pair with the entrance.



**Exit** Door is "paired" with the entrance door and is designated for exiting the facility. Once a user comes through the entrance door, that user must exit through the door selected in this field before their key will again permit entrance.

**NOTE:** The exit door requires a DCD on the inside and the user must use their key/card to exit.

**Timed Entrance** Door is designated for entrance based on a user's key/card and Access Group TIMEZONE. User cannot re-enter the building within the designated Timezone. In other words, user's key/card remains temporarily "invalid" until the **beginning** of the Timezone assigned to their Access Group. The system requires an EXIT DOOR designation before allowing you to save the data.

**GLOBAL** Global Antipassback offers different options:



**Global Entrance** Door is designated for entrance. Users enter any global entrance door.

**Global Exit** Door is designated as a global exit. Users must exit any global exit door before their key/card will again be valid at an entrance.

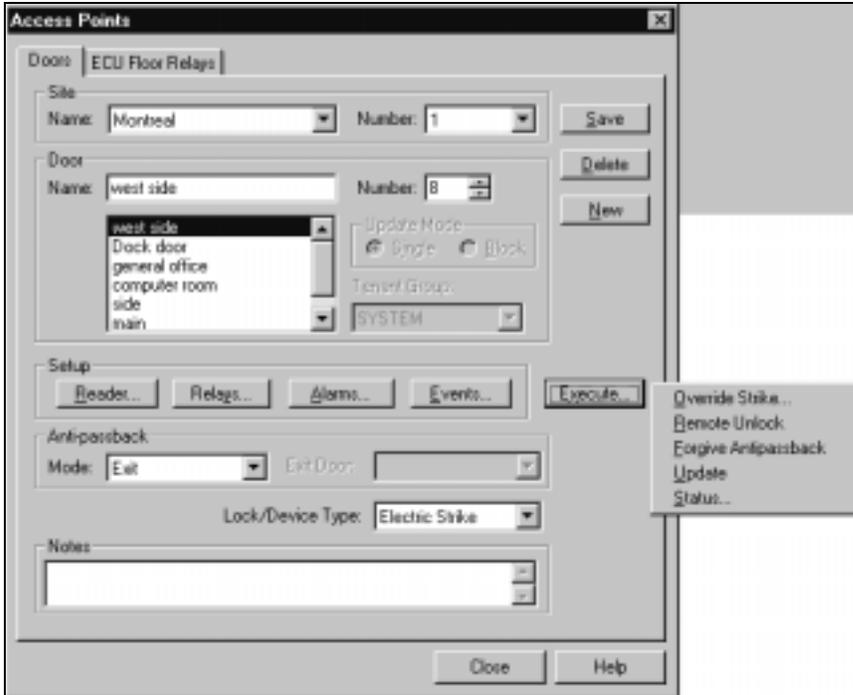
## ***Forgive Antipassback***

Sites that use the Antipassback function can have Millenium operators use the **Execute...** button (ACCESS POINTS dialog) to forgive anti- passback at a given door.

## ***Execute button***

The ACCESS POINTS window (**Doors** tab) includes a special **Execute...** button with options to control the following door functions from the PC:

- Override Strike;
- Remote Unlock
- Forgive Antipassback
- Update Door Control Device (DCD)
- Status



## Override Strike

Doors set up to operate by electric or magnetic strikes are subject to a temporary operator override of the LOCK or UNLOCK condition for a specific number of hours. The option appears under the **Execute...** button in the ACCESS POINTS dialog.



<b>Override Mode</b>	<b>None</b>	This door is not in a temporary override mode.
	<b>Unlocked</b>	This door is set to temporarily unlock for the OVERRIDE TIME indicated.
	<b>Locked</b>	This door is set to temporarily lock for the OVERRIDE TIME indicated.
<b>Override Time (hours)</b>	Set the number of HOURS (maximum 24) this temporary override of the magnetic or electric strike relay is to remain in effect. The relay mode and the Timezone you override continue in the background. Both the relay mode and the Timezone return to normal operation at the end of this Override Time.	

For DIAL-UP sites, operator must already have executed one of the following commands from the Dialup Connections dialog: **Connect without History Polling** or **Connect with Continuous History Polling**.

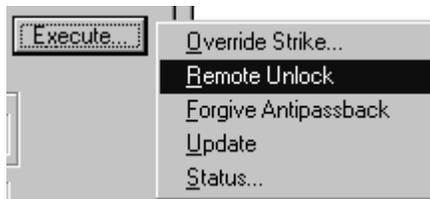
## Remote Unlock

Doors operated by electric strike can be remotely unlocked from the PC by any Millenium operator with EXECUTE rights to the Door dialog (Access Points, Millenium tab.) Pre-defined operator levels 1 and 2 have EXECUTE rights. A Level One operator may create additional custom Operator Levels with rights to perform this function.

Custom operator levels can only perform a remote unlock if the user-defined level is set up with EXECUTE rights to this feature.

### How do I execute remote unlock?

1. Open the ACCESS POINTS dialog, and select the SITE and DOOR to be unlocked
2. Click the button from the Access Points dialog.



3. Click the REMOTE UNLOCK action from the pop-up selection box.
4. (For doors with a Marlok Keylok, observe the note below.)

**NOTE:** If the door has Marlok Keylok reader, two people must be involved in the remote unlock process. A user must insert and turn a key in the lock cylinder while the operator performs the function at the computer.

5. History reflects "*Operator Unlock*," and identifies the door and site. After the remote lock actually opens, history reflects "*Remote Unlock*," and identifies the door and site. The operator ordering the action displays earlier in history as the most recent operator to log on.

	11/9/1998 7:56:27 a	Operator Unlock	Elgin	Second Door
	11/9/1998 7:56:27 a	Remote Unlock	Elgin	Second Door

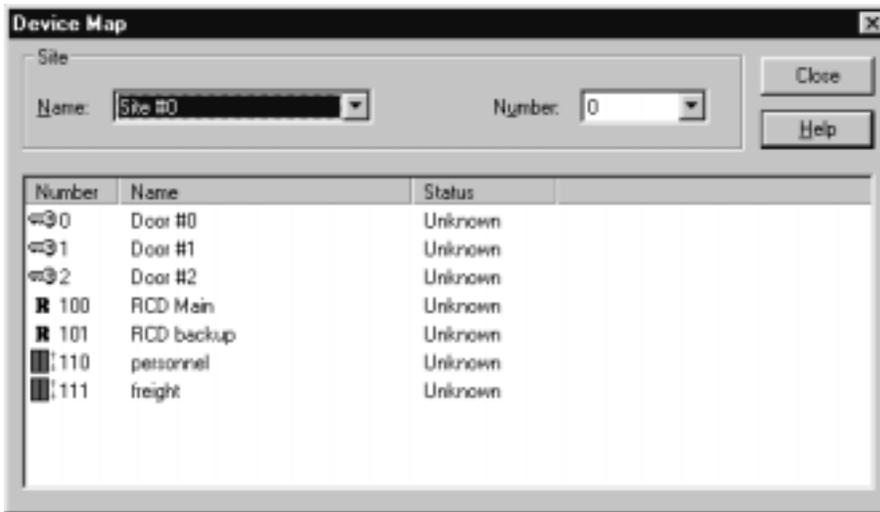
6. For DIAL-UP sites, operator must already have executed one of the following commands from the Dialup Connections dialog:  Connect without History Polling or  Connect with Continuous History Polling.

## Updating

- Click **Execute...**, then **Update** option in the ACCESS POINT dialog (or through the Update button located on the main RCD dialog.) This update action is for **individual updates to a door** (Door tab on the ACCESS POINTS dialog) **or to an RCD** (RELAY CONTROL DEVICE dialog box.)
- For example, a door update would send users for the specific door along with any associated Timezone data.

## STATUS of a Device (Door)

The **Execute...** button on the Access Point dialog performs an on-the-spot status check for the current device. The following example shows the Status of a door on the Device Map.



Device information includes a description of whether or not the device is online.

### **Important!**

This status feature requires SCU Issue **U** and DCD Issue **Y**.

# Chapter 7: Access Groups

## Access Group: Definition

- Access Groups, along with Timezones, are the basis around which the Millenium system controls access to the designated access points in your facility.
- Operator assigns users to an Access Group.
- Access Group has permission to use specific points (doors) in your facility.
- Access is limited to a specific TIMEZONE.
- System will only unlock a door when the user's valid key or card is used in a reader device on a door to which the user's Access Group has permission. Also, the system will only unlock a door during the TIMEZONE specified for that door, for the given Access Group.

## How do I create an Access Group?

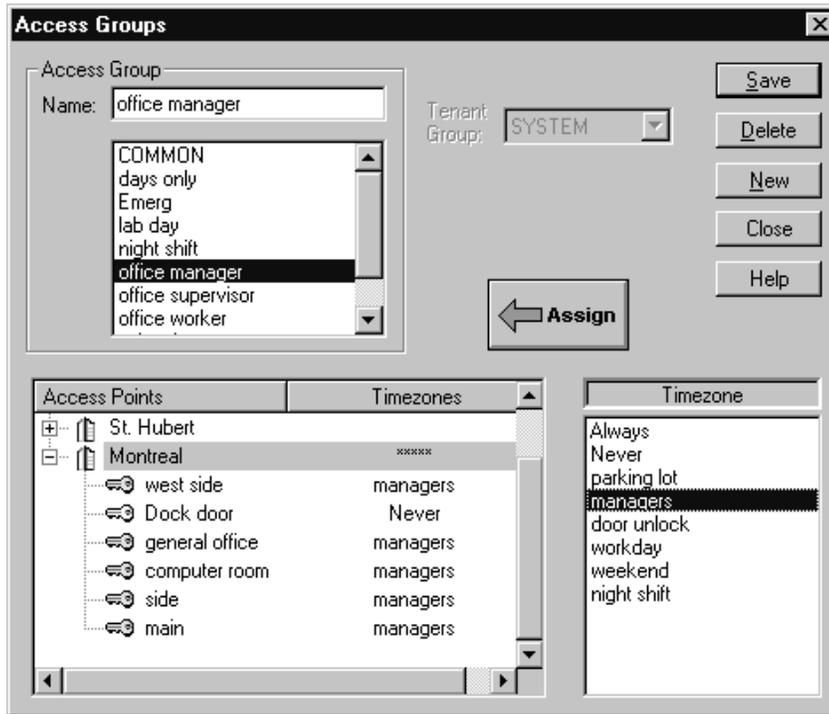
The picture below is the ACCESS GROUPS dialog in Millenium Expert Systems. Access groups are assigned admission rights to specific points in your facility during specific time periods.



- Establish Access Groups based on which ACCESS POINTS the group requires and during which TIMEZONES the group has permission to use the access points. Then assign each user to an Access Group (USERS dialog, Access tab.)
- ACCESS GROUPS link to specific TIMEZONES during which they may gain admission to specific ACCESS POINTS in your facility.
- Before creating Access Groups, you must first have programmed SITES, ACCESS POINTS, and TIMEZONES in the software.



1. Select the Access Group icon .
2. In the NAME field, type a name you can recognize when it comes time to assign an Access Group to a user. Create access group names that cover categories of people who use your facility. Make the groups universal in nature so users can change but the Access Groups remain the same. Examples: First Shift, Cleaning, Sales, Supervisor —or Freshmen, Resident Assistants (RAs,) Maintenance. Avoid using symbols such as apostrophes in-group names.
3. Move to the Access Points / Timezone listbox. Notice all Sites set up in your facility appear down the left-hand column. A "+" symbol appears at the left of each Site.



Under the Access Points column, each site expands into a "tree" when you click on the "+" symbol beside it.

The "tree" lists all access points created under that site in Millenium software.

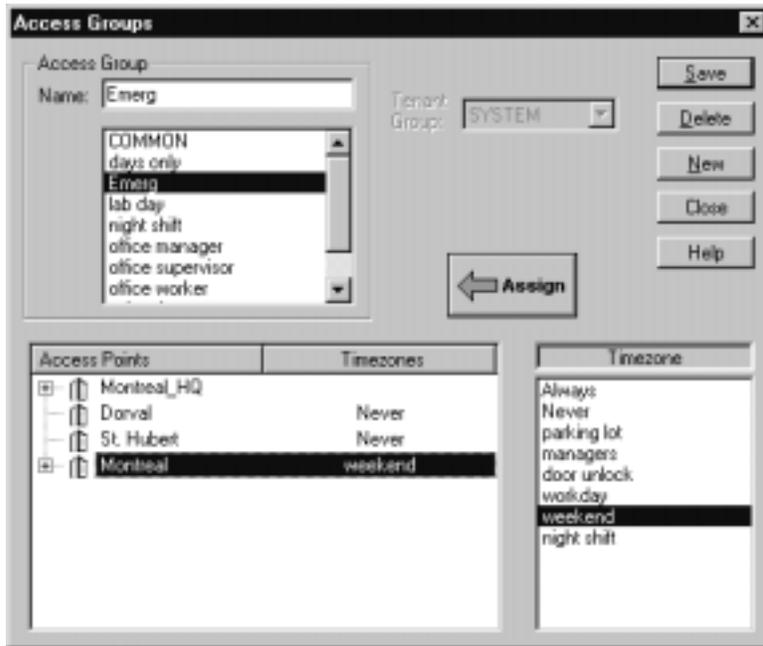
The second column is where you **assign** one established Timezone to each ACCESS POINT.

4. First highlight a Site's Access Point by clicking on the name. Make sure the one Timezone to be assigned to that access point is highlighted. (**NOTE:** To pick multiple access points, hold down the <Ctrl> key to highlight more than one individual access point. To select a group of access points, hold down the <shift> key to highlight the first and the last access point in the group.)



5. Then click the  button to replace the default Timezone assignment in the listbox on the left (**Never**) with the highlighted Timezone from the listbox on the right. Repeat the Timezone assignment process for the other access points under the expanded sites

6. When you finish assigning Timezones to the entire site click the "-" symbol beside the Site Name to close the .expanded tree list. One of two things happen:
7. \*\*\*\*\* appears to show you have already expanded a site during the current session. A variety of Timezones have been assigned to access points for the given Site.
8. Timezone name appears to show you have already expanded a site during the current session and the same Timezone is assigned to all access points in that Site.
9. Montreal site has been opened and access points have a variety of Timezone assignments.
10. St Hubert site has not been expanded during this session.



For the Emerg Access Group (shown above) Montreal has been opened but the timezone applies to ALL the Timezones at the site

Now you are ready to add users to the system.

## How do I assign a Timezone?

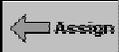
Every Access Group in Millenium Expert Systems can have one TIMEZONE assigned to each ACCESS POINT in the system. Two system Timezones are: Always and Never. Never is the default. For each Access Group in the system, assign the TIMEZONE during which the group has access to each door in a site. Make the assignment by changing the Never Timezone to one of the user-defined Timezones established in the system, as outlined below:

1. Select the Access Group icon .
2. Highlight an Access Group already established in the system.
3. Move to the Access Points/Timezone assignment window in the lower left hand side of the window.



4. Highlight one of the TIMEZONES in the listbox on the right.
5. Highlight one of the ACCESS POINTS in the listbox on the left.

**NOTE:** To highlight a block of Access Points, select the first row (either at the beginning or at the end of the block.) Then press the <Shift> key, and hold it down while you click on the end of the block you want to select.

6. Now press the  button to replace the Timezone on the left with your selected Timezone. When you assign this ACCESS GROUP to USERS, the user's valid key/card will gain them admittance to the selected DOOR during the specified TIMEZONE.
7. Press the button to save the ACCESS GROUP assignments you just created. Be sure to save before creating or selecting another access point.

Now, to give users access to a door, open the USER dialog (Access tab.) Select one ACCESS GROUP for each individual user.

# Chapter 8: Users

The picture below is the USERS dialog in Millenium Expert Systems. Users are people who are assigned keys or cards. They use these to gain admission to access points in your facility. The USERS dialog has multiple tabs that let you switch between multiple windows of information on users. The name of the user in focus appears across the title bar of the dialog.

## Identification Tab:

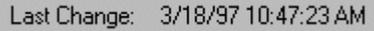
- Click the ACCESS tab to assign keys/cards and Access Group to the user.
- Click the USER FIELDS tab to create operator-defined custom fields to hold user data.
- Click the NOTES tab to record any free-form text information for use by Millenium operators.
- Click the BADGE tab to display the optional Millenium Badge software module for the given user, if you have purchased the optional module.

**NOTE:** Four types of user data (address, phone, birth date, and Social Security number) can be blanked out from appearing on this identification tab by creating a custom operator level.

The BIRTHDATE field above, and the EXPIRATION date field on the ACCESS tab feature a pop-up calendar for ease in entering dates.

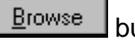
To find a particular user:

- Click the **Find User...** button and type the name of the user you want to locate. The system will look up users based on the first few letters you type.
- To move forward and backward to a specific user, click the **≥>** and **≤<** buttons from any user tab.

- To find a user from an alphabetical list, click the  button and scroll to the user's LAST name. Then use the FIRST NAME and MIDDLE INITIAL to pinpoint your selection.
- To do an incremental search in any of the **blue-shaded fields**, press the  button. Then go to the field for which you want to match data, and type the first letter(s)/number(s) of the data you want to find. Click the  button. The first record matching the data you typed displays in the dialog. On the ACCESS tab, the search works a bit differently. Press the  button and type complete **Reader Type** and **Access Code** data to locate the user by their access code.
-  Date only changes when user **Access code**, **Access Group**, or **PIN#** changes.

### *How do I add a user?*

Before creating Users, you must first have programmed SITES, ACCESS POINTS, TIMEZONES, and ACCESS GROUPS in the software. You will use the ACCESS GROUP component to define (1) those Access Points to which the user has permissions and (2)

1. Select the User icon .
2. Press the  button.
3. Identification tab: Click to pop up main user dialog.
4. Complete the field information that will identify this user.  
The blue-highlighted fields are indexed so you can search users by typing matching data in these fields. In other words, if you want to find all the Vice Presidents in your database, always begin the TITLE fields entry with "Vice President." Then you can find the first VP in your database— "Vice President-Advertising." Example— by: (a) pressing the  button, (b) focusing the cursor in the TITLE field, (c) pressing the  button, (d) typing the first few letters matching the data you want to find such as "Vice President."  
(To see more information about the , , or  buttons:)
5. Fill in all the information you want to record on the user.
6. Click on .

### *How do I give a user access to the doors?*

The Access tab is also where you can assign a User PIN number. The PIN is an integral part of the optional Keypad combination reader function.

**EXPIRATION DATE:** To have a user's key or cards automatically expire at the beginning of the designated date (00:01,) type the date or use the  button to select the expiration date from the drop-down calendar.

Users: Miller, Steve

Identification | Access | User Fields | Notes | Badge

Codes

Reader Type: Access Code

Reader Type: Access Code

Reader Type	Access Code
Wiegand	000000000-000...

Expiration Date: 11/10/04

User PIN #: 0403  Display Image

Access Group: sales

Buttons: << >> Save New Delete Browse Find User... Search Make Card Close Help

1. Click on ACCESS tab.  
Assign the user a key or card, an optional expiration date and personal identification number (PIN,) and an Access Group.
2. Select the **Reader Type** and record the **Access Code**.

The READER TYPE field displays three options: the Marlok Key (Keylok or Keyreader), and up to two card reader options (one Wiegand and one ABA.) You can add or delete a key or card, or designate key or card as "LOST" on this dialog. If a user loses their key or card, you can tag that key/card as and assign another key or card.

#### For keys—

Insert the key in the wedge keyreader unit attached to the PC.

#### For cards—

Depending on the type of card, do **ONE** of the following:

- Swipe or insert the card in an installed reader, and record the access code that comes up in the history portion of the Millenium Expert Systems display screen
- Record the code printed on the card. Record both the site identification number and the access code.

**NOTE:** If you try to add a duplicate Access Code, the system gives you the following message:



1. Assign a key or card to the user

#### For keypads—

Type the keypad code into the last five digits of the default 26-bit Wiegand access code 000-00000. The number you type will be the keypad access code for the given user.

For keypad combinations—

Record the Reader Type and Access Code for the type of reader being used in combination with the keypad. Record the user's PIN to be used on the keypad. (Door must have **Keypad Enabled** in the Reader Setup dialog.)

3. Record an ABA code to be encoded on a card using an optional System 800 encoder.

You also have the option to display the user's image if you have the Millenium Badge module and have captured images for your users.

: Press the arrow  or the  button to make assignment appear in the listbox

To designate a lost key or card as lost, use the  button.

To delete a key or card, or use the  button.

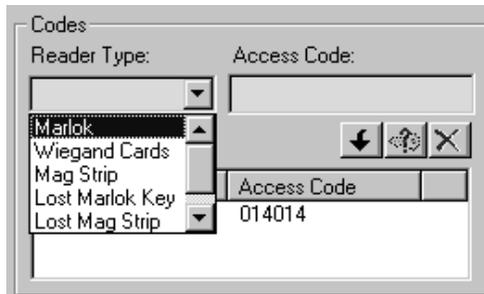
#### ***Important!***

Users may be assigned ONE key and ONE Wiegand card and ONE ABA card.

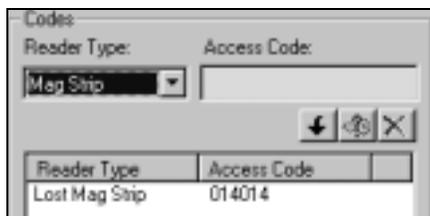
Blue-shaded fields mean you can use the button to search for a user by **Reader Type** and **Access Code**.

## How do I label a lost keycard?

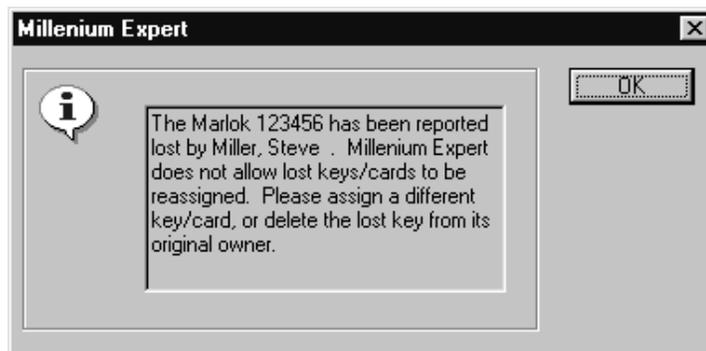
1. Go to the Users dialog, Access tab.



2. Highlight the lost key or card in the **Reader Type** column of the listbox.
3. Click the lost key button (  ).
4. The tag "Lost" appears in front of the **Reader Type** column of the listbox.



5. Click the  button.
6. Tagging a lost key/card results in the following:
  - The key/card is tagged in history as lost for the given user.  
(Example: *Lost Key/Card;*<user's name> *Lost* <ABA card #####>.)
  - If the key/card is ever used to attempt entry, the system will not only refuse entry, but history will identify Invalid User along with the lost key/card (Example: *Invalid User;...;Lost* <ABA card #####>.)



NOTES: To re-use a key/card tagged as LOST, you must first delete it from the original user. If you accidentally DELETE a key/card rather than tag it as LOST, you can add the key/card back in for the user. Highlight the appropriate LOST key/card option (Marlok, Wiegand or ABA) from the Reader Type field, and record the appropriate Access Code (as recorded from history)

## *How do I create custom user fields, notes and badge tabs?*

Millenium Badge is a complete badging system available as an option in the full Millenium Expert Systems access control software. Once the Badge option is installed, the BADGE tab appears enabled in the USERS dialog.

- Click on custom user fields tab
- Record custom, user-defined information such as License Plate No.
- Custom fields appear on this tab if they have been user-defined in setupmpw. To see more, refer to page 20.
- Notes tab: Type any additional information that could be useful to Millenium Operators
- Badge tab: For use with the optional Millenium Badge software.
- **BADGE STYLE** field will contain one or more custom badge layouts you have created throughout the Layout function.
- Five Millenium Badge action buttons (Capture, Preview, Print, Layout, and Setup) are the heart of the badge-producing system. An operator captures photo images of users. The system stores the images in the mpw\itc1000\Portrait folder.
- The Contents page in the online help introduces each of the button functions.
- Descriptions of the remaining fields on this main BADGE tab appear below:
- Each layout you prepare will contain images, photos and database information placed on the badge according to your design.
- **BADGE STATUS** states whether the badge is active, inactive, etc.
- **CARD CODE 1** and **CARD CODE 2** fields are where the operator can record the following types of additional special information:
  - Displaying a User Photo
  - When based on *Events*, the following selections will only display a user photo if the actions are selected as Site or Door .
  - When based on *History*, the following selections will display a user photo whenever the actions occur as part of normal history.

**NOTE:** Elevator events must be based on *History* since unlocks and invalid attempts do not record as events for elevators.

- **Door Unlock** displays user photo (based on Events or History) when a valid user unlocks a door. Door Unlock includes First Key Unlock action (First user auto activate) from DCD Relay Setup. **NOTE:** You can display a user's image by double-clicking a row in the Millenium history that displays the **Unlock** action.
- **Invalid User** displays user photo (based on Events or History) when an invalid user attempts to unlock a door.
- **Invalid Time** displays user photo (based on Events or History) when a valid user attempts to unlock a door during an invalid Timezone.
- If you remove an expiration date, notice the user's Access Group automatically reverts to **No Access**. To reinstate a user, you must, therefore, re-assign the user to the appropriate Access Group.
- To remove an Expiration Date, highlight any part of the date and press the Delete key on the keyboard.
- If you have the optional Millenium Badge module, and you have captured user images, click DISPLAY IMAGE option to show the user's image on this dialog.



# Chapter 9: Operators

## Operators: Definition of Levels

Operators are those users who operate the Millenium Expert Systems software.

A **Level 1** administrative operator assigns each operator an OPERATOR LEVEL in the OPERATORS dialog

- A Level 1 operator can change any operator's password.

Valid operators can change their own passwords through the Change Password dialog (**Log on** menu.)

- .A Level 1 operator can also create custom operator levels with selective rights.

Two **pre-defined** operator levels come with the software: **Level 1** and **Level 2**.

Unauthorized functions either do not appear, or a message informs the operator of insufficient rights to perform the function when attempted.

### Level 1

- Operator has rights to all Program Features in Millenium Expert Systems PLUS the following SPECIAL FUNCTIONS:

- Rights to Setup Millenium Expert Systems (setupmpw ) 
- Rights to add an operator or to change operator settings. (Actions from the lower half of the Log on menu)



- Rights to the OPERATORS. Dialog to add/delete operators.
- Rights to create a custom operator (Operator Levels option under the Log on menubar.)
- Rights to Set Autologoff.

## Level 2

Rights to all Program Features in Millenium Expert Systems **EXCEPT SPECIAL FUNCTIONS** of Level 1 operators (listed above.)

Notes: The first operator created in the software after installation is always a Level 1. A default operator exists after installation and disappears as soon as you create the first operator. At least ONE Level 1 operator must exist in the software at all times. The system will not allow you to delete the last Level 1 operator in the system. The recommendation is that you always have at least two people trained as Level 1 operators. Valid operators can change their own passwords, and a Level 1 operator can change any operator's password.

## Automatic logoff

Millenium Expert Systems comes with an optional automatic logoff feature that lets a Level One operator establish a pre-set amount of time (in minutes) any logged-in operator's keyboard can remain inactive before the system reverts to a secure mode.



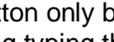
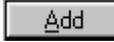
In the **Auto Logoff Timeout** field, record the number of minutes the system will allow the keyboard to remain inactive before reverting to a log on-required condition. Millenium Expert software goes into a "safe mode," during which the history continues to display in the background (for DIRECT communication configurations,) but no software functions can be performed. To use the software, a valid operator must, again, log on.

If the operator leaves the PC with an open dialog box (**not recommended!**), the autologoff function takes over at the pre-established time.

### **Important:**

Autologoff does NOT save any data programming that might have been in progress.

### ***How do I add an operator?***

1. When you first open the Operator dialog, the first button appears as a *disabled* CHANGE button ().
2. The button only becomes enabled () after you go through each field in the dialog, including typing the password and re-typing the password confirmation.
3. If you click the  button, the first button switches to an  button **after you complete all the fields in the dialog.**

4. Make sure the person already exists as a User in the USERS dialog.



5. Click the button to pop up OPERATOR dialog.

The screenshot shows the 'Operators' dialog box with the following fields and controls:

- User Name:** A text input field.
- Operator Level:** A list box with a scroll bar, currently displaying a list of names: Baker, Bernice; Blake, Simon; Burke, Peter; Chang, Holly; Chavez, Carlos; Cooper, Carl.
- Login ID:** A text input field.
- Password:** A text input field.
- Confirm:** A text input field.
- Current Operators:** A list box showing 'Ani' and 'carl'.
- Buttons:** Add, Delete, New, Close, and Help.

- Scroll to the Name of the user you want to add as a system operator.
6. Select the **Operator Level** to be assigned to this new operator.
  7. Type in a unique operator **Login ID** for the user.

**NOTE:** Limit Login ID name to letters and numbers. Avoid using symbols. For example, if an operator named Mike O'Dell wants his Login ID to be his last name, it should be odell—without an apostrophe.

8. Type a **Password**.
9. Re-type the password to confirm the first entry.
10. Press the button.

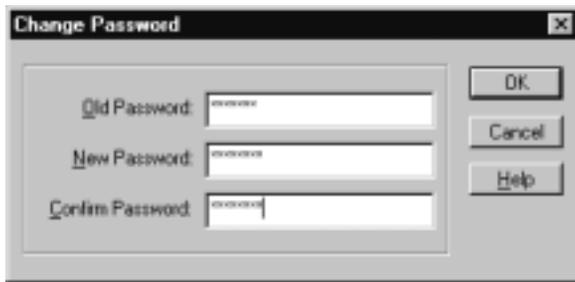
**NOTE:** The button switches to an ADD button after you type in all operator data.) Only a Level 1 operator has authority to change operator settings or add an operator to the system. This includes changing an operator's password. Valid operators can change their own passwords, but a Level 1 operator can also change operator passwords through this OPERATORS dialog.

## *How do I change a password?*

1. Select Change Password from the **Log on** menu.



2. Type your current password in the OLD PASSWORD field.

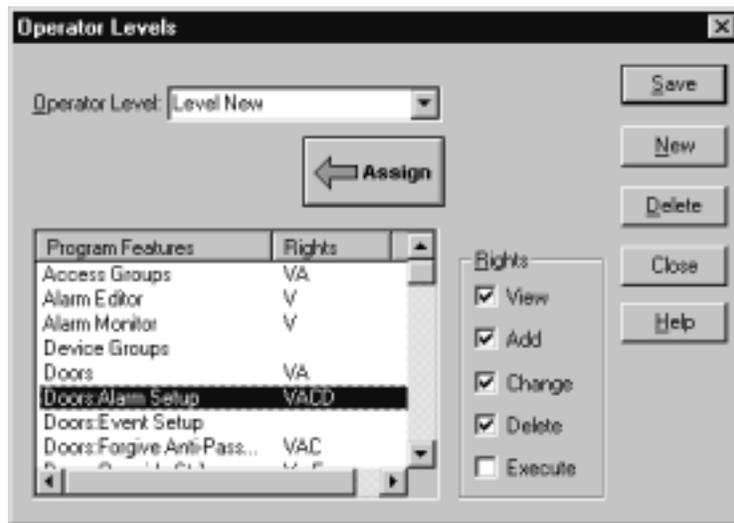


3. Press the <Tab> key (or down arrow, or <N> key) to move to the NEW PASSWORD field.
4. Type the new password.
5. Press the <Tab> key (or down arrow, or <C> key) to move to the CONFIRM PASSWORD field.
6. Re-type your new password.
7. Click the  button to save the new password for your log on.

## Custom Operator Levels: Definitions

Level 1 operators have the option to create custom operator levels tailored to exactly those Millenium Expert Systems menu functions they want to include. For operators logged in at their assigned level, the software only displays or enables those dialogs or menu actions to which that operator has access. Unauthorized functions either appear disabled or inform the operator of insufficient rights to perform the function.

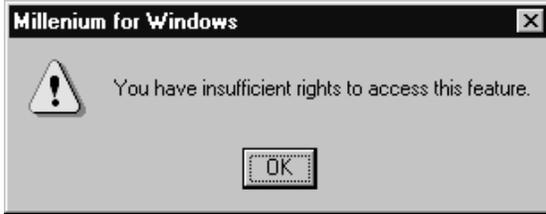
NOTES: Without the VIEW rights, a dialog such as Doors does not even display to the operator. Four fields on the USER Identification tab can be removed from view by creating an operator level without rights to view and/or change USER: *Address, Phone, Birth date, or Social Security Number* fields. See more information under View, below.



- The above example shows four “rights” (**V**iew, **A**dd, **C**hange and **D**elete) assigned to the **Program Feature-Doors** (Access Points dialog, Millenium Expert System tab) for the custom **Operator Level, Level New**. This example means *Level New* custom operator level can View, Add, Change, Delete and (**E**xecute...) door data—all features on the Access Points dialog (Millenium Expert System tab.) Without the rights to Execute, this operator cannot perform any actions that affect the entire Millenium Expert System network.
- Single letters under the **Rights** column correspond to the first letters of the five “rights” available to software operators.

### View

Controls whether or not the dialog box displays. If the right to View is not selected, the following prompt informs the operator when they try to open the dialog or select the menu option:



A special option exists for the USER Identification dialog. Four fields appear under the Program Features listbox, and may be removed from **View** and **Change** rights for a custom, user-defined operator level.

**Add**

Controls whether or not the  button lets you add a new item to the Millenium database. If the right to Add (create a NEW database item) is not selected, an operator cannot save a newly created door, timezone, access group, user, etc.

**Change**

Controls whether or not the  button is enabled. If the right to Change is not selected, an operator cannot save changes made to an existing item in the Millenium database.  
For DIRECT communication configurations, this means the operator cannot affect/update access control devices online.

**Delete**

Controls whether or not an operator can use the key to remove an item from the Millenium database.

**Execute**

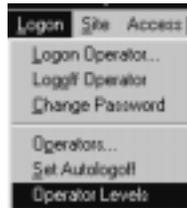
Controls whether or not an operator can perform actions using any of the following special action buttons that affect the entire Millenium network:

SITE:  and

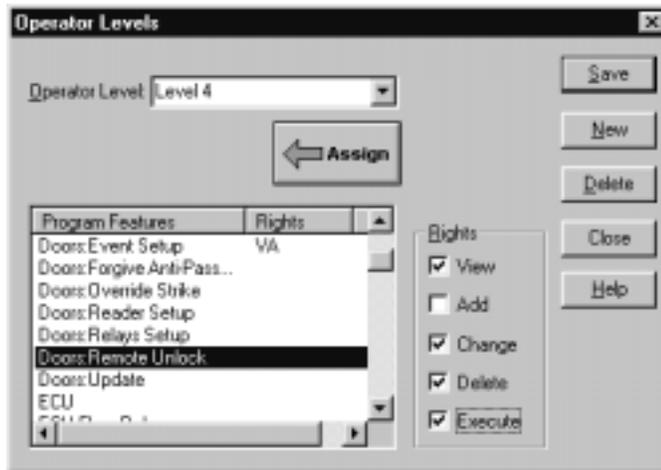
DOOR:  **Remote unlock, Update, Override Strike, Forgive Antipassback**

RELAYS: 

## How do I create custom operator levels?



1. Click the **Logon** menubar item to display the submenu.
2. Then select the **Operator Levels** option to display a dialog similar to the following



3. Click the **New** button to set up a new operator level. Operator levels appear in the OPERATORS dialog so the Level 1 administrator can assign the level to all operators created to run Millenium Expert Systems.
4. OPERATOR LEVEL: Type a name as you want it to appear in the OPERATOR LEVEL listbox on the OPERATORS dialog.
5. Click to select the **Rights** that apply to the highlighted PROGRAM Features) for the given OPERATOR LEVEL. Then press the **Assign** button to assign selected **Rights** to the highlighted PROGRAM Features.) The initials representing the rights appear beside the selected features.

**NOTE:** You can use the <shift> key to highlight a block of features— Highlight one feature, hold down the <shift> key, and click on the last feature in the block you wish to select. –OR– Use the <ctrl> key to highlight several features— Highlight one feature, hold down the <ctrl> key to highlight an additional feature.

- Then click the button to save the custom operator level you just created.



# Chapter 10: Elevators

## Elevator Toolbar Button

Elevator access control is offered as part of Millenium Expert Systems. The option requires that you install at least one Elevator Control Unit (ECU.) Most configurations include an Elevator car Control Device (ECD) for each elevator car with a reader device either inside or outside the car.

Press the  toolbar button to program Elevator Control Units (ECUs.) Once you have programmed ECUs and up to 16 relays per ECU, you press the ACCESS POINTS  button to begin assigning access to ELEVATOR FLOORS (much the same as you assign access to DOORS.)

## Elevators: Definitions

### Elevator Control Unit

- The main **Elevator Control (ECU)** tab is where you set up or program the Elevator Control Unit. Each Site Control Unit can support up to four Elevator Control Units (ECUs,) and each ECU has 16 relays to handle as many as 16 floors. The Elevator tab includes set up for elevator alarms and events.
- The **Elevator Car** tab is where you name elevator cars and select site floors for which the ECD reader is active. One Site Control (SCU) can handle up to 10 elevator cars (ECDs.)



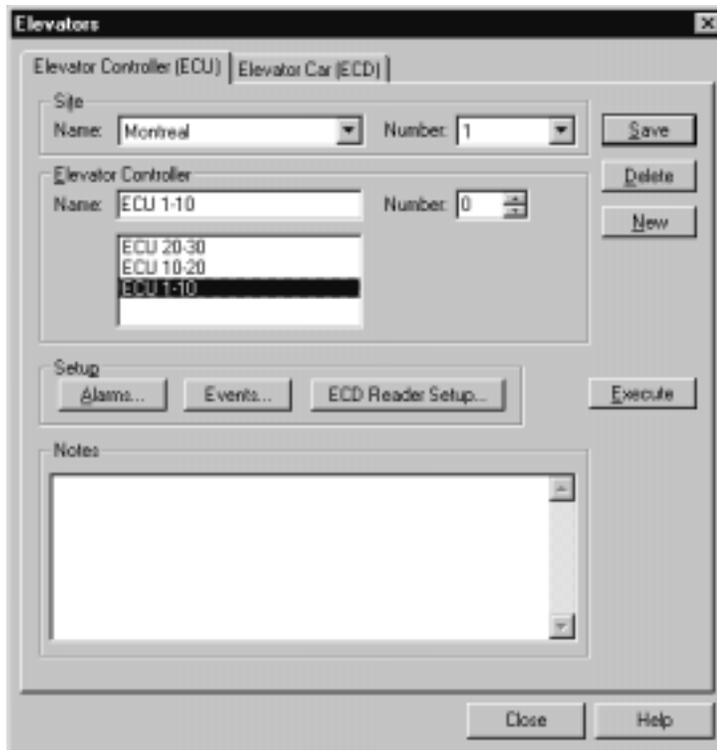
- The ACCESS POINTS dialog has an ECU Floor Relays tab where you set up or program up to 16 relays on an ECU.
- Each relay represents a "button on the elevator passenger control panel" — a floor access point where the elevator stops.

- The **Setup** section on the main Elevator tab is where you program elevator functions.
-  button opens a dialog where you set up elevator alarms.
-  button opens a dialog where you select alarms or actions to be treated as EVENTS for the given Elevator Control Unit (ECU.)
-  button only appears enabled for the FIRST ECU per site. This is where you select the **one** reader type to be used with all elevators under the given Site Control.
- The  button is where you can perform an update of programming data to the ECU or a status check on an ECU.

## How do I add elevator control units?

### Part 1

1. Select the ELEVATOR icon. 



2. On the main Elevator tab, highlight a SITE NAME where you want to add (program) an Elevator Control Unit (ECU.)
3. Type a NAME for the Elevator Control. The first ECU at a given site must have ECU number zero. ECU 0 serves as the **master** elevator controller .
4. Since all elevator cars under a given site must use the same type of reader device, this

ECD Reader Setup; button becomes enabled for ECU .

5. Select the type of reader to be used at all elevators under this Site Control. Wiegand and ABA readers require additional settings based on the type of reader being used.
6. At this point, you can type in any notes describing the given ECU. You can also set up  and  for an ECU.

### Part 2.

1. In the ELEVATOR dialog, click to select the Elevator Car tab.  
The next step is to name elevators (Elevator Control Devices—ECDs) and select the floors that will be served by a given elevator car's reader.
2. The currently selected SITE NAME appears highlighted if you already selected the site on the main Elevator tab. If no site has been selected, highlight a SITE NAME where you want to define and name the elevator floor relays.
  - In the ECD section, type a Name for the elevator car (ECD) that operates under the given Site Control. You can have as many as ten (10) elevator cars for one site. The name can be up to 19 characters long.

### Site Floors:

The Site Floors listbox appears empty now.

As shown in the following example, once you complete steps under **C.** (Access Points dialog,) this list box will show all ECU floors programmed under the given Site Control.



- Notice the ECU that controls each floor relay will appear in parentheses after the floor name.
- Selected floors will be served by the given elevator car reader. That is, when a valid passenger uses their key or card in the elevator reader, corresponding button(s) on the elevator control panel will light according to that passenger's access group rights. Passenger then chooses the desired floor.



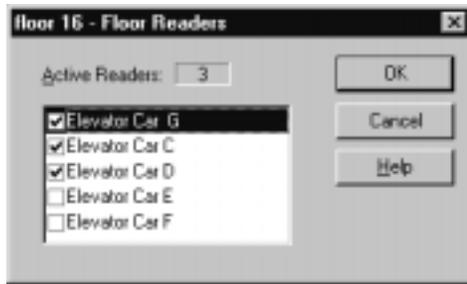
3. In the ACCESS POINTS dialog (ECU Floor Relays tab—covered in steps under **C.** below) you will **select elevator car reader that will be active for the given floor.**
4. The Floor Readers dialog and the Site Floors listbox both show identical data in two different ways.
5. Type in any notes to provide more description of the given Elevator car Control Device (ECD), if desired.
6. Press the  button. Repeat the process to name additional ECDs and select the floors they serve.
7. The next step is to program **ECU Floor Relays** (ACCESS POINTS dialog);

**Part 3**

1. Click the ACCESS POINTS toolbar button , and select the ECU Floor Relays tab.
2. Select the ECU for which you want to name and define up to 16 relays (floors.)
3. Press the  button or move to the blank ECU Name field.
4. Type a NAME to identify/describe the **floor** for a given relay. The name you type will appear in the ELEVATOR dialog's Elevator Car tab (Site Floors listbox.) From the Site Floors listbox, you will select those floors an elevator car will serve.

**NOTE:** Elevator floors correspond to the 16 possible relays on an ECU. Floor NUMBERS for the 16 relays range from zero (0) to 15. The ECU Relay Number must accurately reflect the relay wiring. Relay 1 on the ECU must be wired to activate the button for the floor in the elevator car's passenger control panel.

5. Click the  button to select the Elevator car Control Device (ECD) reader(s) that will control access to the given floor.



6. The reader device attached to a selected ECD will receive a user's key or card and grant or deny elevator floor access based on the user's Access Group. You can also select readers in the **Site Floors** listbox (ELEVATOR dialog's **Elevator Car tab**, covered under step 7 above)
7. Program the floor reader to control access to the given floor:
  - **Relay Mode** - Select the mode that will control how the reader controls access to the elevator floor.
  - **Active Timezone** - If appropriate, select the TIMEZONE during which the given floor relay will be available to valid users. The Active Timezone is commonly used with the Auto activate and First User Auto Activate relay modes.
  - **Seconds Active** - Time-related relay modes let you set the number of seconds you want the elevator control relay to remain active (de-energized.) Maximum is 255 seconds with 5 seconds being an average setting.
8. Click **Execute...** to perform special Elevator floor functions:



- Temporarily **override** a floor relay for a set number of hours. The relay returns to normal mode following the number of hours designated in the override dialog.
  - **Unlock** of elevator floor relay from the PC.
  - **Update** Send current programming data to the ECUs. This occurs naturally when you press the Save button, See Updating devices in the Millenium network on page 50 for more about the update function.
9. Press the **Save** button. Repeat the process for additional elevator floor relays, as required.

**NOTE:** It is possible to have more than one Elevator Control Device (ECD) per car. For example, with elevator cars that have doors on the front and back, you may have two ECDs to allow independent operation of the two access points.

ECD	Controls
Floor 1 - Car 1	Front door
Floor 1 - Car 1	Back door
Floor 2 - Car 1	Front door
Floor 2 - Car 1	Back door

- It is possible (but NOT recommended) to have floor relays common across all elevator cars (sometimes referred to as "wired in parallel.")
- This situation might arise when you have only one Elevator Control Unit (ECU) controlling 16 floors along with the multiple elevator cars (10 maximum per Site Control.)
- This type of configuration compromises security— a floor can be activated from multiple elevator cars (ECDs.) Passenger puts key/card in ECD reader and corresponding floor buttons light up in all elevator cars.
- A separate ECU for each bank of elevators is preferable.

### *How do I set up Elevator Readers?*

1. Elevators under any one Site Control Unit (SCU) must all use the same type of reader. Therefore, when you select the first Elevator Control Unit (ECU) for a given site, the **ECD Reader Setup...** button becomes enabled.
2. Click the **ECD Reader Setup...** button.



Select the Reader from those options established in Millenium Expert Systems Setup (setupmpw.)

If you choose a **Marlok** (for Keylok or Keyreader,) click the **OK** button to save the setup.

If you choose a Wiegand device, the Wiegand Mode section enables. Select whether the ECD reader is of the normal or insert type.

If you choose an ABA device, the ABA Mode section enables. Select whether the ECD reader

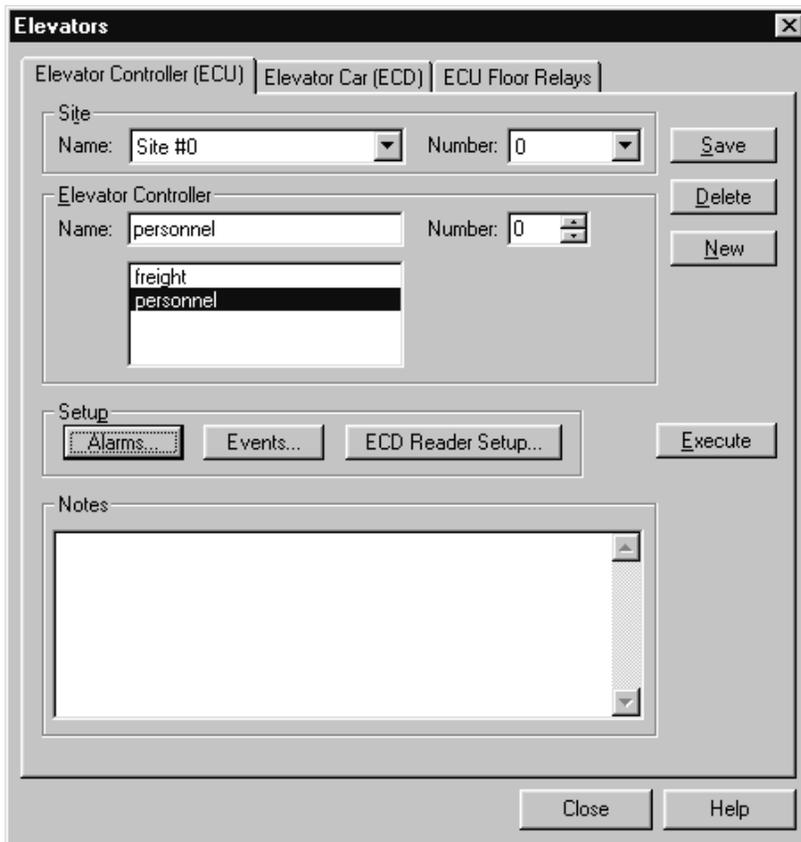
operates as Clock/Data, Clock/Data Inverted, or 0/1.

Click the  button on the main Elevator dialog.

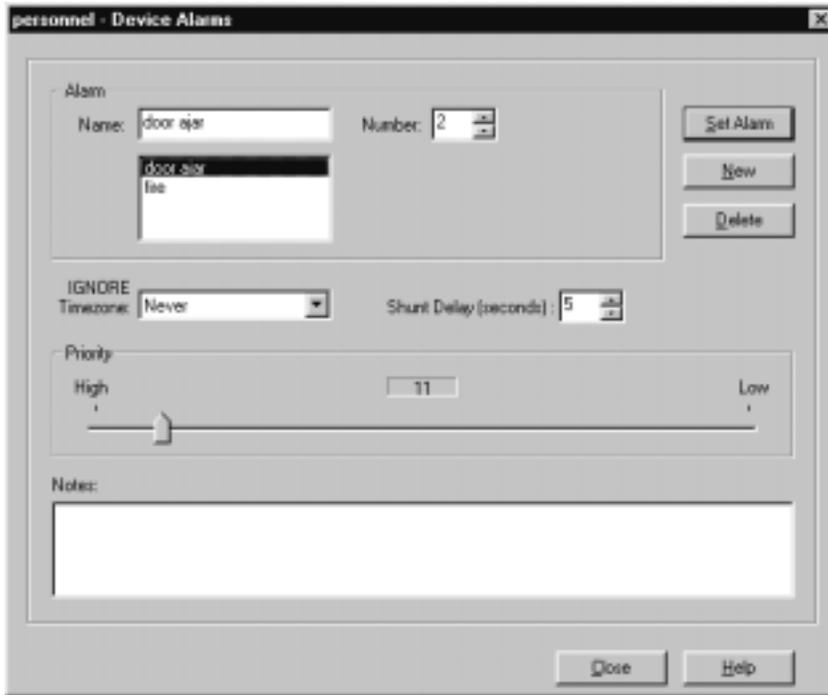
## *How do I set up elevator alarms*

Millenium Elevator Control Units (ECUs) come with a tamper alarm and an optional external manual bypass alarm. In addition, four unsupervised alarm inputs may be programmed through the software as follows:

1. Select the ELEVATOR icon. 
2. On the main **Elevator tab**, highlight a SITE NAME where you want to add (program) an Elevator Control Unit (ECU.)



3. Select the Elevator Control (ECU) for which you want to set up an alarm.
4. Click the  Setup button.

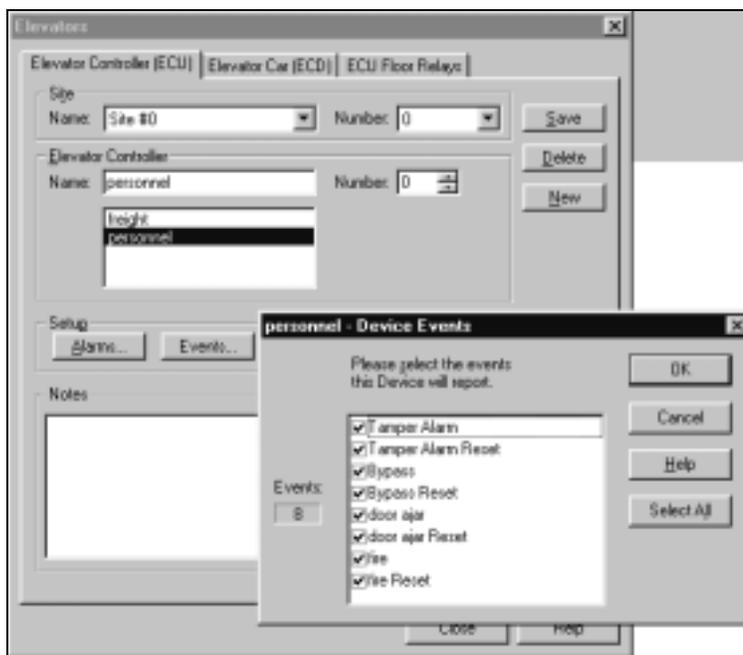


- The popup screen shown above appears.
5. Give the alarm a descriptive name that will clearly identify the alarm in other parts of the Millenium Expert Systems such as in the Alarm Monitor, in the ECU **Events...** dialog, and in history.
  6. Select the NUMBER (1-4) that corresponds to the alarm input used on the ECU for the given alarm.
  7. IGNORE TIMEZONE: If applicable, select the TIMEZONE during which the alarm is to be ignored. If you never want the alarm ignored, select the **Never** Timezone. Otherwise, select the user-defined Timezone that applies to the given alarm.
  8. SHUNT DELAY: Establish a grace period before the alarm triggers. Options are between 1 and 255 seconds.
  9. Prioritize the alarm in a scale from 1-100. In the Alarm Monitor, an operator must respond first to those alarms with the highest priority.
  10. Use the NOTES section to further describe the alarm you are setting up.
  11. Press the **Save** button.

## How do I set up elevator events?

1. Once you have set up elevator alarms (  button,) to use one or more of the four possible ECU alarms wired for the given elevator controller, the name you give to each alarm appears in the Device Events setup dialog.

2. Click on the Elevator Toolbar button .
3. Click on the  button in the main ECU dialog.
4. A popup Events screen appears as shown below.



5. Click to select all or select only those alarms (and usually the corresponding reset) you want to be treated as “events” for the given elevator controller. A check mark appears beside selected events.
6. Click the OK button to save your selections.
7. Each event goes out to the Millenium network as data output from the ECU.
8. The ALARM MONITOR module displays alarm events only. If you use optional RCDs, the ECU event can cause an action by its respective relay on an RCD circuit board.

## Elevator Relay Modes: Definitions

The 16 relays on an Elevator Control Unit (ECU) can operate in any of the following modes:

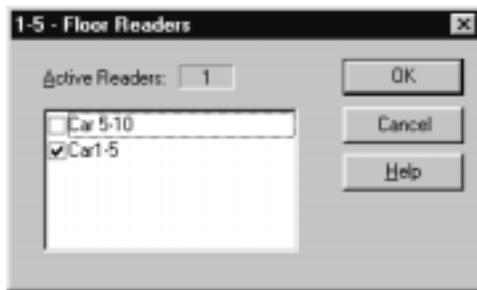
<b>No action</b>	Elevator relay does not activate for the given floor.
<b>Auto Activate</b>	Elevator relay activates (de-energizes) for valid key/card during a certain period of time based on the Active Timezone. Relay automatically deactivates when the Timezone ends. Valid users can enter outside of the Active Timezone, for the designated number of seconds set in Seconds Active field.
<b>First User Auto Activate</b>	Elevator relay activates for first valid user during the Active Timezone. Contact remains active until the Timezone ends. Valid users can enter outside of the Active Timezone, for the designated number of seconds set in Seconds Active field.
<b>Valid User</b>	Elevator relay activates for a valid user, for the designated number of Seconds Active—only during the Active Timezone.
<b>Rejected User</b>	Elevator relay activates for a rejected user, for the designated number of Seconds Active—only during the Active Timezone.
<b>Any User</b>	Elevator relay activates for any user (valid or invalid,) for the designated number of Seconds Active—but only during the Active Timezone.

### *How do I set up Elevator Floor Relays?*

1. Before programming elevator floor relays, you must have previously;
  - Added the Elevator Control Unit (ECU ) to the software through the ELEVATOR dialog, and
  - Selected the one reader type to be used for all elevator cars at the given site.
2. On the Elevator Car tab, name the Elevator car Control Device (ECD) commonly known as the elevator car, and
3. Select Elevator floor relays that will become activated when a passenger uses their key or card in the elevator card reader. Options in the Site Floors list box come from your entries in the ACCESS POINTS dialog — ECU Floor Relays tab or in the Elevators dialog box shown below, in the ECU Floor Relays tab.



4. In the Elevators dialog box, the ECU name appears after the name of the **Site Floor** for your reference, and floors for **all** ECUs under a given Site Control also appear. You may select additional floors under the same Site Control that can be activated by the highlighted elevator's reader.



5. Click to select the elevator car **reader** that will activate for the highlighted floor.
6. In the example, the reader selected in the pop-up dialog (—the reader wired to the ECD for Elevator Car 1-5) will activate for the highlighted floor (Floor 1-Car 1.)

## Overriding Floor Relay

Like doors, elevator floors set up to operate by relays are subject to a temporary operator override of the LOCK or UNLOCK condition for a specific number of hours. The option appears under the button in the ACCESS POINTS dialog (ECU Floor Relays tab. as well as in the Floor Relays tab in the main dialog.



**Override Mode**

**None** This elevator floor is not in a temporary override mode.

**Unlocked** This elevator floor is set to temporarily unlock for the OVERRIDE TIME indicated.

**Locked** This elevator floor is set to temporarily lock for the OVERRIDE TIME indicated.

**Override Time (hours)** Set the number of HOURS (maximum 24) this temporary override of the ECU Floor relay is to remain in effect. The relay mode and the Timezone you override continue in the background. Both the relay mode and the Timezone return to normal operation at the end of this Override Time.

For auto-activated relay modes:

- To ensure that the override reverts back to the background relay mode and Timezone after the temporary condition, set OVERRIDE TIME to end at the same time or later than the end of the auto-activate Timezone.
- To override auto-activated mode for just a portion of the Timezone, set OVERRIDE TIME to end before the end of the auto-activate Timezone.

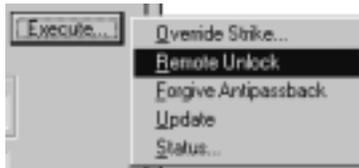
For DIAL-UP sites, operator must already have executed one of the following commands from the Dialup Connections dialog:  Connect with Continuous History Polling or  Connect without History Polling.

## How do I execute an elevator remote unlock?

Elevator floors can be remotely unlocked from the PC by any Millenium operator with EXECUTE rights in the ACCESS POINTS dialog (ECU Floor Relays tab.) or Elevator dialog ECU Floor Relays tab.) Pre-defined operator levels 1 and 2 have EXECUTE rights. A Level One operator may create additional custom Operator Levels with rights to perform this function.

Custom operator levels can only perform a remote unlock if the user-defined level is set up with EXECUTE rights to this feature.

1. Open the ACCESS POINTS or ELEVATOR dialog.
2. Click the ECU Floor Relays tab.
3. Select the SITE and ECU to be unlocked
4. Click the button.



5. Click the REMOTE UNLOCK action from the pop-up selection box.
6. (For elevator cars (ECDs) with a Marlok Keylok, observe the note below.)

**NOTE:** If the Elevator has a Marlok Keylok reader, two people must be involved in the remote unlock process. A user must insert and turn a key in the lock cylinder while the operator performs the function at the computer.

7. History reflects "*Operator Unlock*," and identifies the elevator floor, site, and operator ordering the action. After the remote lock actually opens, history reflects "*Remote Unlock*," and identifies the floor and site.
8. For DIAL-UP sites, operator must already have executed one of the following commands from the Dialup Connections dialog:  Connect with Continuous History Polling or  Connect without History Polling.



# Chapter 11: Relay Control Devices

- Door Control Devices have two (2) relay contacts that work with a specific door to trigger electric strikes and/or to activate a supplemental device.
  - DCD relays can be TIMEZONE activated or activated by input from a reader device.
  - The 2ND DCD relay can respond to an alarm input.
  - To set up DCD relays, click the  button on the Door tab in the ACCESS POINTS window.
- To check the status of DCD relays, click the  button on the Door tab, and select ;
- Relay Control Devices have eight (8) relays to respond to events. When an event occurs that has an RCD relay assigned, the Site Control Unit (SCU) polls for events and can report them across the full Millenium network.
- RCD relays can also respond to more than one device (door or another RCD) under a given site.
- The first relay on the first RCD takes over polling for events if a Site Control Unit (SCU) goes offline.
- The first RCD relay can also be used to activate an auto-dialer to alert an operator of a communication failure.
- To set up an RCD relay, click the  button on the main Millenium toolbar.
- To check the status of an RCD, click the  button on the RCD tab, and select **Status**

Elevator Control Units have 16 relays to control elevator floors.

To set up ECU relays, click the ECU Floor Relays tab on the ACCESS POINTS or Elevator dialog.

To check the status of an ECU, click the  button on the main ECU tab and select **Status**;

## Relay Control Devices

Relay Control Devices are optional circuit boards with **eight** relays that you can program:

- To respond to EVENTS for more than one door or device,
- To respond within specified Timezone,
- To control optional devices such as a sprinkler system or heating/air-conditioning in the Millenium Expert Systems network,
- And you can take advantage of a special System Supervisor function reserved for the first RCD relay.



### DCD Relays

The button in the ACCESS POINTS window (Doors tab) displays a second window where you set up one or both of the two relay contacts on a Door Control Device (DCD) circuit board.



## RCD Relay Modes

Use optional Relay Control Devices (RCDs) to respond to events and alarms within TIMEZONES, or to respond to more than one device under a Site Control. The Site Control polls for event occurrences and can report the events across the entire Millenium network. RCDs can also trigger other devices and be set to activate an auto-dialer.

Up to eight relays on each optional Relay Control Device (RCD) can operate in any of the following modes:

<p><b>System Supervisor</b></p>	<p>(Only applies to Relay #0 on the first RCD (RCD #0) per Site Control )                  Relay activates when PC is polling other devices on the system. If the PC and SCU go offline, RCD #0 takes over polling for EVENTS.                  If RCD #0 detects device failure during the polling, Relay #0 de-activates until the PC comes back online. This de-activated state can be set to activate an alarm and alert the system operator to the problem through—for example—an auto-dialer.</p>
<p><b>Alarm Latch</b></p>	<p>Relay changes state (activates or de-activates) until the specified EVENT resets, at which time the relay returns to normal state. You must specify only one event from one device. Event choices are:                  Tamper Alarm -or-                  Alarms 1 through 7 -or-                  Tamper Alarm Reset -or-                  Alarms 1-7 Resets</p>
<p><b>First Event Activation</b></p>	<p>Relay activates at some time during the TIMEZONE after receiving the specified EVENT or EVENTS. Relay de-activates at the end of the TIMEZONE. You must specify Timezone, Event(s) and Device(s.)                  Do not use the system Timezones— Never or Always.</p>
<p><b>First Event Release</b></p>	<p>Relay de-activates at some time during the TIMEZONE after receiving the specified EVENT or EVENTS. Relay activates at the end of the TIMEZONE. You must specify Timezone, Event(s) and Device(s.)                  Do not use the system Timezones— Never or Always.</p>
<p><b>Timed Release</b></p>	<p>Relay de-activates for specified length of time after receiving the specified EVENT or EVENTS. Release cannot last more than 255 seconds. Relay activates after 255 seconds. Time field replaces Timezone field. You must specify Event(s) and Device(s.)</p>
<p><b>Timed Activation</b></p>	<p>Relay activates for specified amount of time after receiving the specified EVENT or EVENTS. Activation cannot last more than 255 seconds. Relay de-activates after 255 seconds. Time field replaces Timezone field.</p>
<p><b>Timezone Activation</b></p>	<p>Relay activates at the start of a specified TIMEZONE and de-activates at the end of that Timezone.                  Do not use the system Timezones— Never or Always.</p>

## System Supervisor Relay (RCD)

- The first relay on the first Relay Control Device (RCD) for a Site Control Unit (SCU) has a special function within Millenium Expert Systems. Relay 0 on the first RCD (RCD 0) added to a site is reserved for this special purpose—meaning an operator cannot change the function of this first RCD relay.
- The System Supervisor Relay **activates** when PC is polling other devices under the given SCU to look for event occurrences. If the PC (or Server) and SCU go offline, RCD #0 takes over polling for EVENTS.
- If RCD #0 detects *device failure* during the polling, Relay #0 **de-activates** until the PC (or Server) comes back online. This de-activated state can be set to activate an alarm and alert the system operator to the problem through—for example—an auto-dialer.
- **Device failure** in Millenium Expert Systems occurs when: The PC or server polls a device **twice** and gets No Response both times. After the second full cycle of polling with no response, the system labels the device as Off Line.

## Alarm Latch Mode

- One possible RCD relay mode that sets the relay to respond to ONE EVENT for ONE DEVICE in the Millenium Expert Systems network. Alarm Latch relays do not involve a TIMEZONE because the time is recorded as part of the ALARM setup (IGNORE TIMEZONE field.)
- Device information includes a description of whether or not the device is online. In addition, the status for each relay and the status of the tamper alarm input on the RCD displays.
- **RCD Issue** tells you the EPROM (Erasable Programmable Memory) Issue level for the given RCD.
- Similar Device Status dialogs appear for DCDs and ECUs.

### ***Important!***

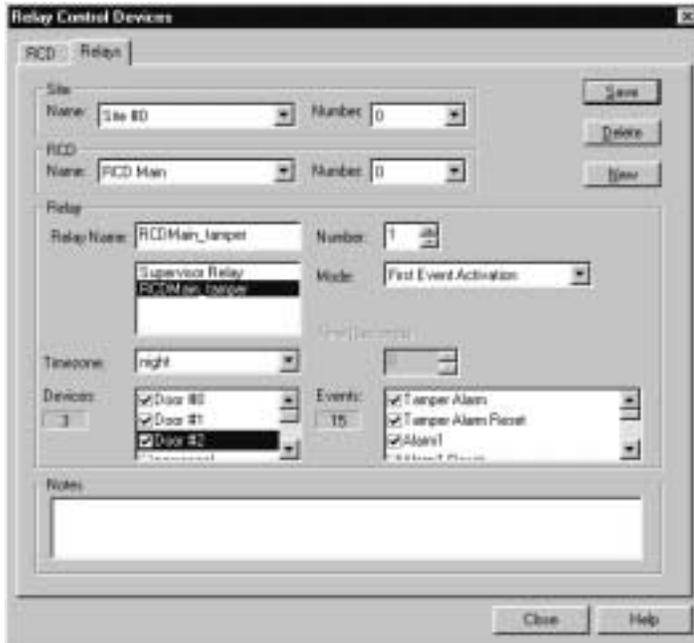
This status feature requires SCU Issue **U**

## How do I add a Relay Control Device?

1. Select the RCD icon 



2. If you have not yet added the Relay Control Device to the software, do so before setting up any of the eight RCD relays. If you have already programmed the RCD circuit board device into the system, click the Relays tab.

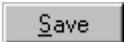


3. Select the SITE NAME where the Relay Control Device (RCD) circuit board is installed.
4. Highlight the NAME of the RCD on which you want to program a relay.
5. Give the RELAY a NAME that will identify it throughout the system. Notice the **first relay** on the **first RCD per Site Control Unit** is reserved as the “supervisor” relay. The first usable relay on the first RCD is Relay Number 1. Millenium handles up to 10 RCDs per Site Control. After the first RCD per site, all ten relays are available for use.
6. Select the Relay MODE by which this relay will operate.
7. Depending on which mode you select, one or more of the following fields become enabled:
  - TIMEZONE: This window only appears enabled when the selected Relay MODE is time-related.
  - TIME (Seconds): This window only appears enabled when the selected Relay MODE requires a specific amount of time in seconds.
  - DEVICES: For all but the Alarm Latch mode, select one or more devices in the

Millenium network for which the relay will respond. (Alarm Latch mode uses **one** device and **one** event.)

- **EVENTS:** If this relay is being set up to respond to **EVENTS**, select the event(s) for which this relay is to respond.
- Only **EVENTS** set up for the selected device(s) appear enabled. RCD modes that involve events must have **EVENTS** set up for **DEVICES** before RCDs can be fully programmed.

The software lets you save RCD Relay setups that **require** **DEVICE** and **EVENT** selection even when you have not made **EVENT** selections for the selected device(s). In other words, you can save a partially set up relay in cases where you need to go back and set up **ALARMS** or select **EVENTS** for a device.

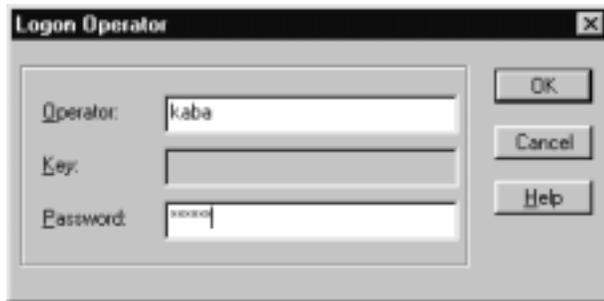
- Time-related modes do not involve **EVENT** selection.
  - Alarm Latch mode only responds to one event for one device.
  - Use the **NOTES** box to enter free-form descriptions of the particular relay function being set up.
8. Click the  button to finish the RCD relay setup process.



# Chapter 12: Alarm Editor

## *How do I log on to Alarm Editor?*

- The Alarm Editor requires a separate login.
- Click on the Alarm Editor button on the main Toolbar button and the following dialog box will appear.



- If you have not yet created an Administrator in your Millenium for Windows application, use kaba as the Operator and expert as the password.
- If you have an operator, use his/her name and password, as in the example above.
- The Alarm Editor Module can be closed without logging off.

## Alarm Editor

The Alarm Editor lets you prepare a visual display of alarms wired in your Millenium network and programmed in Millenium Expert Systems. The Alarm Editor differs from the Alarm Monitor, which is the module that displays active alarms history to an attending operator. The operator can then refer to images and alarm properties established in this editor. When you first click the Alarm Editor button, nothing but the toolbar appears. The following graphic sample shows a fully programmed ALARM EDITOR complete with an image of the facility and icons representing programmed alarms.



- By using the Alarm Editor, you can set up a graphic illustration of alarm points in your facility. You provide the graphic “blueprint” of your facility and use **Alarm Palette** icons to lay out the alarm scheme, as installed. Then, the *Alarm Monitor* tracks and reports an audit trail of alarm activity, including operator action in running or shutting down the monitor function.
- The Alarm Editor automatically displays a network tree of devices installed in your Millenium Expert Systems—one site at a time. Each Door Control Device (DCD) shows the seven potential alarm inputs.
- The Alarm Editor offers four potential layouts for each alarm point. Each layout is called a Floor Map. You may provide one or up to four different mapped views of the area where the fire alarm is installed.

NOTES: Alarms you have wired to the DCD and programmed in Millenium Expert Systems appear with the name you established in the software. The graphic floor plan you set up can appear to the operator through the Alarm Monitor (Inspect Alarm dialog,  View tab.)

## Toolbar Contents

The Alarm Editor toolbar contains tools to help you search for a particular site as well as the usual Print and Help buttons.



	Searches for a particular site by NUMBER or NAME. Notice the "tree" of site alarm information covers one site at a time.	
	Saves currently displayed alarm layout to the Millenium Expert Systems database.	
	Displays alarm icon palette. Drag-and-drop the icon to the location on your layout that most nearly represents your alarm.	
	Moves to the FIRST site programmed in Millenium Expert Systems' database. Sites display in the order they were created in the software. This is not alphabetical order.	 Moves to the LAST site programmed in Millenium Expert Systems' database.
	Moves to previous site.	 Moves to next site.
	Prints the currently displayed floor map.	
	Displays the on-line help for the Alarm Editor. To see on-line help for an individual dialog, click the button in that dialog.	

## Search for Site

Millenium Alarm Editor offers two ways to display one site's alarm information based on alarms setup for sites in your Millenium Expert Systems software. Toolbar buttons provide the easiest way.

1. Click the magnifier button . The following search dialog displays:



2. Type the Name or Number of a site you want to display.  
(You can also click **Search** from the **Site** option under the **File** menu.)
3. Toolbar button or Menu scroll through programmed sites
4. Click the large arrow buttons to scroll forward or backward through programmed sites as described below. (You can also use the Site options shown below.)

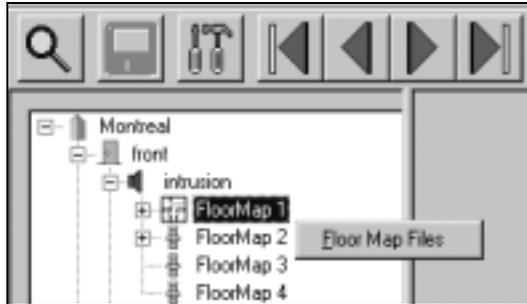


5. After you select a site, the Alarm Editor displays alarm information in a "tree" format—one site-at-a-time.

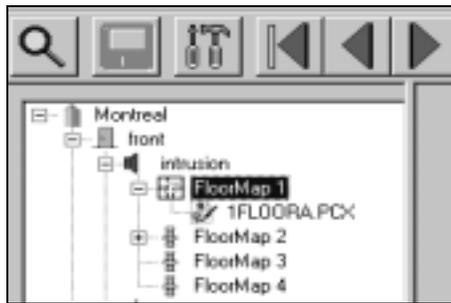
## Floor Maps

- Floor Maps are graphic views of your facility that you provide. Formats can include: .pcx, .bmp, .wmf, .tif, .jpg, .pct, .tga. Each of the seven (7) possible door alarms can have up to FOUR floor maps.
- When setting up the Alarm Editor, you have the option to include alarm icons showing location of installed alarms. The Floor Map can then aid a guard or security operator in locating a triggered alarm by displaying a graphic view of the active alarm as part of the operator's investigation.
- If you choose to use the palette of icons to help describe the type of alarm in picture form:
- When an alarm is triggered, the Alarm Monitor (View tab of the operator response dialog) offers the operator a graphic image of the alarm's location along with a pallet icon that indicates the type of alarm. Palette icons even appear animated, in the Alarm Monitor, to further highlight an active alarm.

1. When you right-click on one of the four Floor Maps that may be set up for each alarm, a Floor Map Files option appears.



2. Double-click the Floor Map Files option to display a selection dialog. Then choose the graphic file to be used as one of four possible floor maps for a given alarm.
3. Graphic file selection for Floor Map 1 (above) appears in the following sample dialog:



4. Available Files appear from the **ImpwMaps** folder where you must place any graphic layout files to be used in the Alarm Editor.
5. Alarm Editor can use any of the following image formats: .pcx, .bmp, .wmf, .tif, .jpg, .pct, .tga.

## Alarm Editor Palette



The ALARM Palette offers a choice of graphic images to use as you lay out your Alarm Editor Floor Maps. The alarm icon you select helps the responding operator identify and pinpoint a triggered alarm in the Alarm Monitor.

- To see a word explanation of each graphic, hold the mouse pointer over the image until its "title" appears.
- To select an alarm icon, just click the desired alarm image.
  - To place the icon, click the appropriate location on your Floor map where you want the image to go.
  - To move and re-size the image, either use the mouse or right-click the icon within the floor map.
  - The same icon will automatically appear on each Floor map under a given alarm.
  - To **delete** an icon, press the <Delete> key on your keyboard.
  - To replace an icon with a different pallet selection, you must delete all icons for each floor map under the given alarm.

## Alarm Palette (titles)

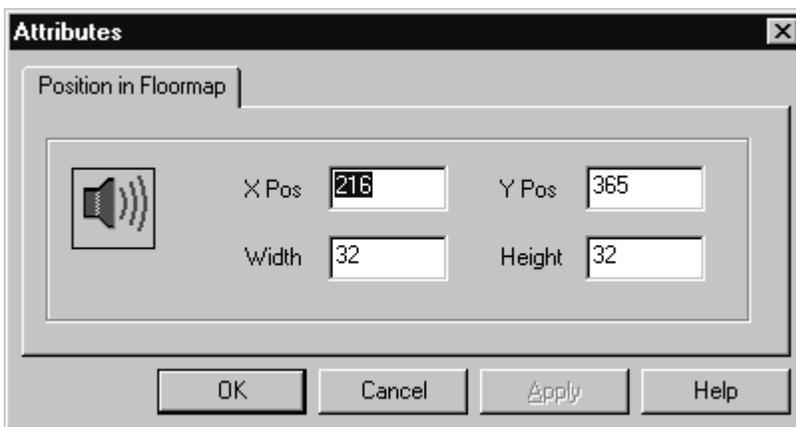
The following graphic shows the word title for the individual icons you can use to show the location of alarm devices installed in your Millenium network:



<b>Fire Alarm</b>	<b>General Alarm #1</b>	<b>Temperature Alarm</b>	<b>Lost AC Power to Site</b>
<b>Smoke Detector</b>	<b>Door Ajar</b>	<b>Invalid User</b>	<b>Water Detector</b>
<b>General Alarm #2</b>	<b>Forced Entry</b>	<b>Noise Detector</b>	<b>Motion Detector</b>
<b>Glass Breakage</b>	<b>Tamper Alarm</b>	<b>Camera</b>	<b>SELECT</b>

## Palette Icon Position

When you right-click on an alarm palette icon, the following positioning dialog appears:



You may either adjust the **position** and **size** of the graphic using exact coordinates through this dialog, or you may use the mouse.

## Require Comment on Action Taken

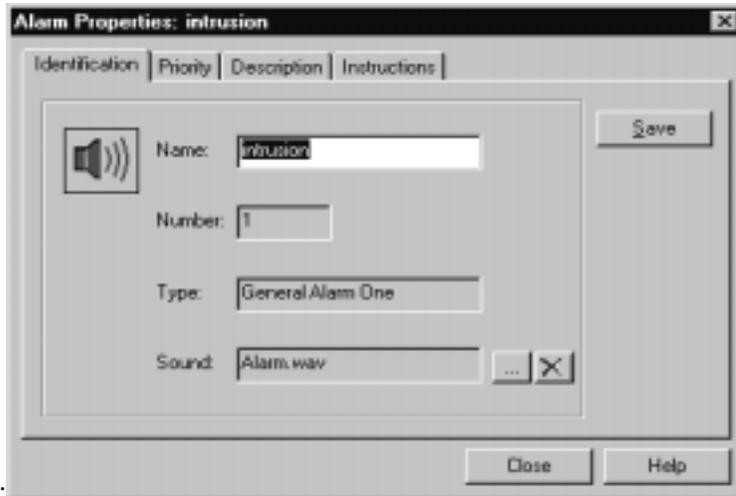
This checkbox is in the Alarm Properties dialog—Instructions tab (in ALARM EDITOR.)

If checked, this option controls the following:

- Operator **MUST** type a response in the ALARM MONITOR's *Inspect Alarm* dialog.
- Inspect Alarm dialog will not allow the operator to close the dialog by pressing the **OK** or **Cancel** buttons without a response in the Enter Action Taken box.
- RESET alarms will not automatically disappear from the main ALARM MONITOR until operator records a response in the Enter Action Taken box.  
("Automatic removal of reset alarms" is an option in the Alarm Monitor's *Setup* dialog.)
- Operator will not be able to right-click and REMOVE an active alarm in the main ALARM MONITOR unless the Enter Action Taken box contains a response.  
("Removal of active alarms" is an option in the Alarm Monitor's *Setup* dialog.)

## Alarm Properties

When you right-click on one of the seven possible door ALARMS in the Alarm Editor, the following properties dialog appears:



### Identification tab:

- Displays general information about the alarm at a given door.
- The NAME appears as established in the ACCESS POINTS' setup dialog.  
Re-naming can be done through this dialog.
- If you used an icon from the **Alarm Palette**, the selected icon appears on the left side of the dialog, and the type of icon appears in the TYPE field.

- **Sound:** Click the ellipse button ( ) to select a sound file (.wav) that will associate with the given alarm. At the time the alarm triggers, the sound also plays at the PC (as long as the workstation has the .wav file in the \mpw\Sounds directory.)
- To remove a selected .wav sound, click the button.
- **Priority tab:** Lets you change the priority of an alarm. This setting affects which alarms must be responded to **FIRST** in the Alarm Monitor. If more than one alarm triggers, the system uses your priority rating to display the highest priority alarm in RED so an operator will have no doubt as to what alarm has priority.
- **Description tab:** Lets you record any special information about the alarm that might be helpful to the security/guard operator who might be responding to the triggered-alarm situation. Information typed in the Description dialog also appears as NOTES in the door's alarm setup dialog.
- **Instructions tab:** Lets you require an operator to log a response describing actions taken when responding to the alarm situation. Also has room for instructions to the operator who would be responding to the triggered alarm.

**NOTE:** Alarm Properties information comes from data you record in Millenium 's ACCESS POINTS. Any changes you make in the Alarm Properties dialog will also affect the information in the ACCESS POINTS dialogs.

## Sound Files

When operator clicks the ellipse button from the Alarm Properties: IDENTIFICATION tab, the following dialog appears:



1. Select the sound file (.wav) you want associated with the alarm you are setting up.
2. Click the PLAY button to hear a sample of the sound. Millenium Expert Systems comes with Alarm.wav sound file. You may place special .wav files in the \mpw\Sounds directory, if desired.

3. For sounds to work in the Alarm Monitor, you must click the "Reminder sound" option on Alarm Monitor's Setup dialog.
4. In configurations with a server and workstations, the .wav file must exist on the workstation machine or the default sounds instead of a selected .wav file.

## Description

### Description tab:

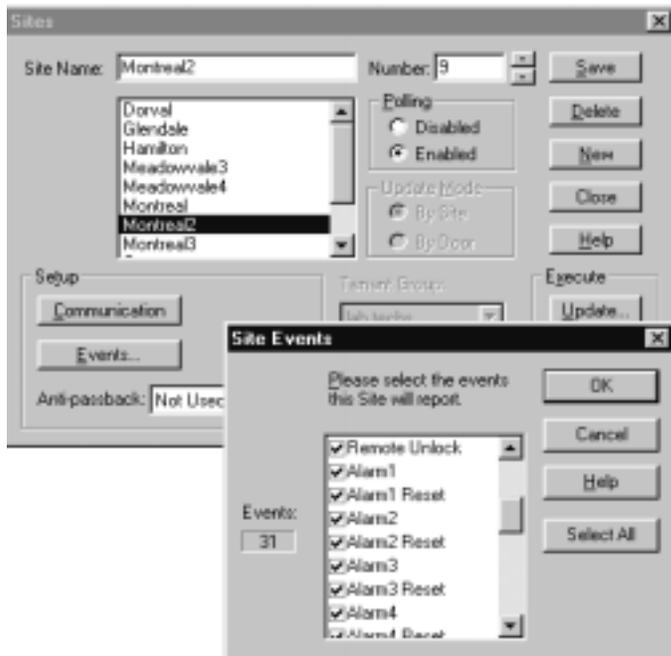
- Lets you describe, in more detail, the alarm wired and programmed at this location.
- This is the same as the **NOTES** information that appears in the ACCESS POINTS' (Door) dialog.
- You might add details about the alarm setup to help the operator who would be monitoring the alarm system.

### How do I set up Alarm Editor?

In Millenium Expert main program: Set up door Alarm: Click the button (ACCESS POINTS dialog–Door tab, Setup section.) Example shows "Main01," Alarm 1. Assign the Timezone during which the alarm is to be ignored, and set the Shunt Time during which the alarm is to delay before triggering.



- **Select what alarms will be treated as Events for the given door:** Under the button (ACCESS POINTS dialog,) select the alarm. (Example: Alarm 1 for "Main01.")
- **Select what alarms will be treated as Events for the given SITE:** Select Alarm 1 (under the button (SITE dialog.) This makes Alarm 1 a site event for the site named "Kaba."



- Create a graphic layout of your facility. This might be one floor plan or up to four different floor plans. Keep the image as simple as possible so the Alarm Monitor display is clear of distractions.
- Place your graphic image in Millenium Expert. Store graphical maps of the area where the alarm is installed in the \mpw\Maps folder. Alarm Editor can use any of the following image formats: .pcx, .bmp, .wmf, .tif, .jpg, .pct, .tga.



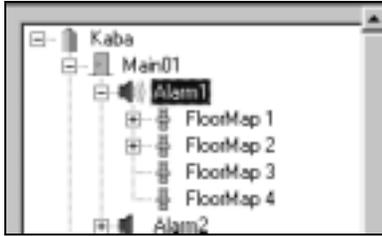
1. Click the Alarm Editor button and log on to the Alarm Editor. A Toolbar displays. In Alarm Editor:
2. Select the Site and Door. Example shows "Kaba" and "Main01."



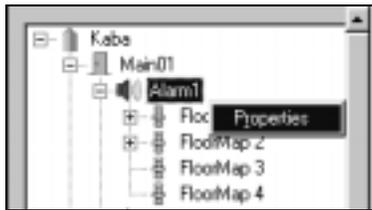
3. If you need help locating a particular site, use the Alarm Editor Toolbar to search. The fastest way to find a particular site among a large number of sites is to use the magnifying glass icon. Another way is to use the large arrow buttons on the toolbar to scroll forward or backward between programmed sites.

4. **Then double-click on the alarm you want to set up:**

The example shows "Alarm 1 on "Main01" DCD. After you double-click, the four possible floor maps appear.

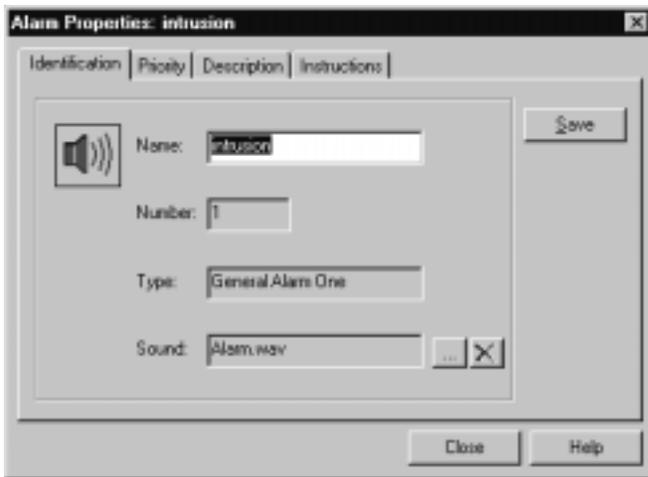


5. **If desired, take a look at the PROPERTIES set up for the given alarm:** Highlight the alarm name, and right-click. A **Properties** option appears. Highlight and click to pop up an Alarm Properties dialog. The Alarm Properties dialog includes four "tabs" of information:



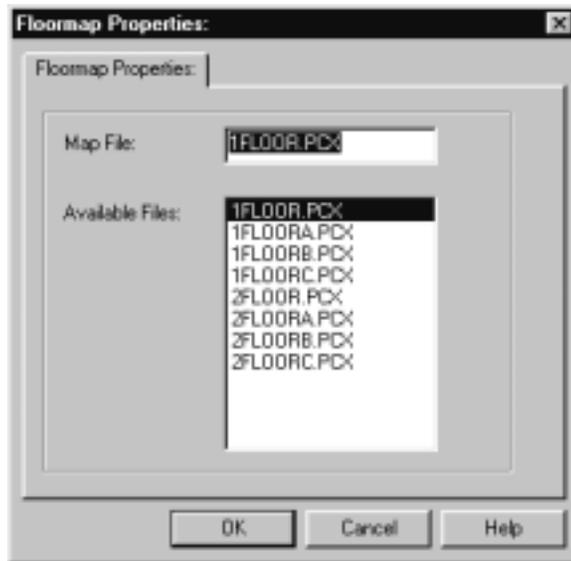
6. Setup the four tabs of Information

- Identification
- Priority
- Description
- Instructions



7. **If desired, select the graphic layout to illustrate this alarm:**

Highlight the floor map for which you want to select a graphic file. Then right-click to highlight the Floor Map Files option. A list of graphics file names pops up.



- - The graphic file you select will become the Floor map for the given alarm. (Graphic files come from those you created in STEP 2 and placed in the **ImpwMaps** folder in STEP 3.)
  - You may then **choose to place an alarm icon** from a palette of choices at the location on your graphic layout where the fire alarm exists.
  - **Example:** Fire icon appears in help file sample. The fire icon will flash to aid the security guard in pinpointing the problem. Depending on the Alarm PROPERTIES setting (right-click on the individual alarm in the "tree,") you can require an operator response to an active alarm situation.
8. To select an alarm icon, just click the desired alarm image.
  9. To place the icon, click the appropriate location on your Floor map where you want the image to go.
  10. To move and re-size the image, either use the mouse or right-click the icon within the floor map.
  11. The same icon will automatically appear on each Floor map under a given alarm.
  12. To **delete** an icon, press the <Delete> key on your keyboard.
  13. To replace an icon with a different pallet selection, you must delete all icons for each floor map under the given alarm.



# Chapter 13: Alarm Monitor

The Alarm Monitor oversees all alarm event activity in the Millenium network. Alarm Monitor is designed for use in a security or guard station.

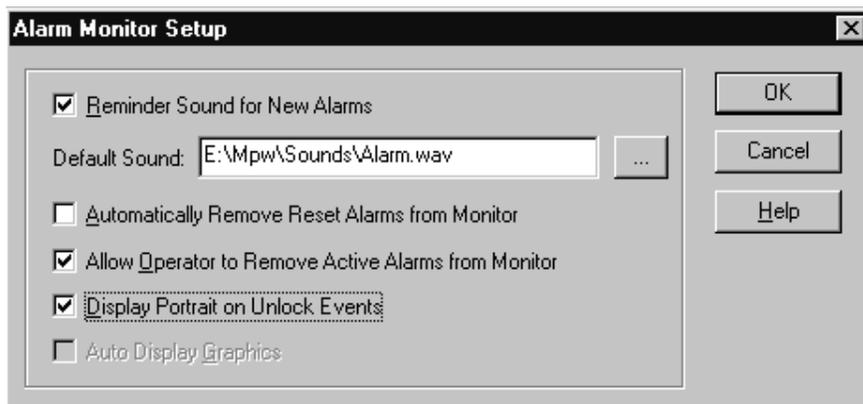
## Log on and Log off



- The Alarm Monitor requires a separate logon.
- Notice the ALARM MONITOR requires a logoff as well as a logon. Since the Alarm Monitor is often run continuously on a dedicated PC, a logoff should not be a common occurrence.
- To end the alarm monitor function, an operator MUST identify himself or herself for the audit trail. If an operator decides to turn off the monitoring function, that operator is responsible for the decision.
- Even if the Alarm Monitor is not running, Millenium Access Management Systems continues to log alarm activity as part regular history.

## Alarm Monitor Setup

The following setup options let you control how the Alarm Monitor works:



If you want to layout a graphical display of alarms, the graphical setup takes place through the Alarm Editor.

## Reminder Sound for New Alarms

- Operator will get an auditory sound when a new alarm triggers.
- If you leave the **Default Sound** field blank, the reminder is a beep (Windows NT) or tone (Windows95.)
- To set special .wav files to sound for specific alarms, use the Alarm Editor.
- To select the **Default Sound**, use the ellipse button .
- Select any audio .wav file. (Shorter sounds are most efficient.)
- Select the sound (**alarm.wav.**) that comes with Millenium Security Management Systems
- Default Sound is unique per workstation.
- **Interval:** Reminder sound comes approx. every 15 seconds for any alarm or Event that has NOT been Reset, or formally ACKNOWLEDGED or IGNORED by an operator.
- After checking the alarm status, the system looks for the active alarm/event with highest priority (1 appears at the beginning of the Alarm Monitor row.) System then plays the sound for this alarm.
- Specific sound (if a specific .wav file was selected for given alarm in the Alarm Editor.)
- Default Sound (if no specific sound is selected in Alarm Editor.) Beep or Tone sound (if no Default Sound.)

## Alarm Monitor

The illustration below shows the ALARM MONITOR function in Millenium . The Alarm Monitor oversees all alarm event activity in the Millenium network. Alarm Monitor is designed for use in a security or guard station.

1 Notice the highest priority alarm is in red so that it stands out. An operator must first respond to highest priority alarms among all ACTIVE alarms. You set priority levels as part of setting up alarms in Millenium and can modify priorities in the Alarm Editor.

### **Important!**

- Alarm Monitor requires that Millenium Security Management Systems be running before active alarms display. If Millenium Security Management Systems is not running, active alarms stored in the Site Control's memory will display in Alarm Monitor as soon as you logon to Millenium software.
- Alarm EVENTS must be checked (selected) in both the DCD and the SITE dialogs in Millenium® Security Management Systems software.
- Regardless of whether or not you use this Alarm Monitor, Millenium® Security Management Systems still records all history of alarm activity. The Alarm Monitor tracks and displays an audit trail of alarm activity, including operator action in running or shutting down the monitor function. The REPORTS dialog in Millenium® Security Management

Systems includes an Alarm-Incident Report on Alarm Monitor information.

- Alarm Monitor Setup includes an option to display user photo with door unlock actions.
- The Alarm Monitor can work together with the Alarm Editor to produce a graphic illustration of the alarm points in your facility. Through the Alarm Editor, you provide a graphic "blueprint" of your facility. You can use Alarm Palette icons to layout visual alarm schemes, as installed.
- Then, Alarm Monitor offers an Inspect Alarm dialog that can include the following information from the Alarm Editor:

**NOTE:** To open the Inspect Alarm dialog, double-click on the individual alarm row in the monitor, or click the inspection magnifying glass icon from the toolbar.

- Expanded description of the particular alarm.
- Includes anything recorded in (1) NOTES section from Door setup, and (2) DESCRIPTION tab in Alarm Editor's Alarm Properties dialog.
- Special directions to the operator on how to respond to a particular alarm event. (INSTRUCTIONS tab in Alarm Editor's Alarm Properties dialog.)
- A required operator response to individual alarm occurrences. (Required response comes from a setting in the alarm's PROPERTIES dialog, in the Alarm Editor.)
- A View tab with the optional graphic illustration of your facility featuring the active alarm.
- If permitted in Setup, an operator can remove an alarm from the monitor by right clicking and selecting the Remove option.

## Alarm Monitor Data

The Alarm Monitor produces an on-screen report that tracks the following alarm activity data:

Priority	Site Name	Access Point	Alarm Name	Operator Response	Timestamp	Alarm Status
----------	-----------	--------------	------------	-------------------	-----------	--------------

- Priority** Comes from your numerical rating in the DCD setup (Access Points dialog-Door tab) or from your setting under Alarm Editor (Alarm Properties–Priority tab.)  
The active alarm with the highest priority must be handled first.
- Site Name** Identifies the site where the alarm activity is taking place.
- Access Point** Identifies the door (DCD) where the Alarm has been triggered as a result of a change of state (Normally Open contact is closed, or Normally Closed contact is opened.)
- Alarm Name** Identifies the alarm as it was named in the DCD  setup.
- Operator Response** Records operator response based on whether operator presses the  or  button in the Operator Response dialog. (Dialog displays when operator double-clicks on the alarm row to display details.) A new alarm shows operator response of **NONE**. If operator is required to record a response ( *Alarm Editor* setting,) an alarm cannot be removed from the monitor without the response step.
- Timestamp** Records the time the alarm activity occurred.
- Alarm Status** Triggered alarms display as **ACTIVE**.  
Logs when the triggered alarms **RESET**.

You can generate a text printout of alarm data in the monitor window. Millenium® Security Management Systems History Report can produce an Alarm report according to several operator selection options.

## Alarm Monitor Toolbar Button

Alarm Monitor is an aid for identifying, tracking the status, and reporting on triggered alarms in the Millenium network.

Activate this optional function to monitor all alarm events set up through Millenium Access Management Systems software. The monitor is designed to run continuously on a dedicated PC; however, the monitor can operate in the background of Millenium Access Management Systems software. Regardless of whether or not you use this option, Millenium Access Management Systems always records history of alarm activity.

The advantage of the Alarm Monitor is that it displays alarm activity only. The history portion of Millenium workspace displays alarm activity interspersed with all access control activity. Alarm Monitor also tracks the status of alarm activity such as when the alarm relay resets and when an operator acknowledges and responds to the alarm.

### **IMPORTANT!**

If you set up the optional Alarm Editor, the Alarm Monitor can include a graphic image of your

facility to help locate a triggered alarm within your facility. (You provide the graphic layout of your facility.)

## Toolbar Contents



<b>Setup</b>	Dialog with some basic options on how you want Alarm Monitor to work.
<b>Logon &amp; Logoff</b>	Alarm Monitor requires a formal logon as well as a formal logoff. Alarm Monitor is designed to run continuously on a dedicated PC, and also requires that Millenium Access Management System be running.
<b>What the monitor reports</b>	Under the columns shown above, Alarm Monitor reports all alarms set up as events through Millenium Access Management System software. Alarms must be set up for DCDs and EVENT must also be selected for both the DCD and the SITE. The Alarm Monitor then reports when the setup alarm triggers. Monitor ranks triggered alarms according to their PRIORITY, and require the operator respond to highest priority alarm event before any others.
<b>Operator's Investigation of Triggered Alarm</b>	<ul style="list-style-type: none"> <li>• Dialog where operator responds to a particular triggered alarm. Operator can either ACKNOWLEDGE or IGNORE the alarm. Investigation dialog can include three types of information:           <ul style="list-style-type: none"> <li>expanded information about the alarm (from Alarm Editor's Alarm Properties dialog —Description tab.)</li> <li>instructions on how to respond to a particular alarm (from Alarm Editor's Properties dialog —Instructions tab.)</li> <li>operator's response to the triggered alarm (Enter Action Taken free-form entry box)</li> </ul> </li> <li>• This response can be required through a selection in the Alarm Editor's Properties dialog— <i>Instructions tab</i>. Depending on the settings in the Alarm Monitor <b>Setup</b> dialog, (1) alarm can automatically disappear upon reset, or (2) operator can or cannot remove an active alarm from the Alarm Monitor display. If operator response is set as <b>required</b>, the program will not allow an operator to remove alarms from the Alarm Monitor display without recording a response.</li> </ul>
<b>Operator's Incident Report</b>	Dialog where operator can report incidents that do NOT come from triggered alarms. The Incident Report is an option through the History Report (REPORTS dialog.)
<b>Print</b>	Prints a text file of information on a particular alarm in the monitor. The responding guard or operator can then carry along the information while responding to the alarm.
<b>Help</b>	Displays the on-line help file. A button in individual Alarm Monitor dialogs displays help on the specific topic.

- Once the Alarm Monitor is set up to operate the way you prefer, the operator just observes the monitor as outlined in the following example: (Set up can include: Alarm Monitor Setup dialog and/or *Alarm Editor*.)
- **Color-Coded Display:** Notice the five colors used in the Alarm Monitor display. The colors visually classify the alarm activity as follows:

<b>Red</b>	<b>Active Alarm</b> Notice the alarm is prioritized. Priority 1 must be handled before any other alarm row. Prioritizing comes from data you enter in Alarm Setup (ACCESS POINTS dialog) or in Alarm Editor's Properties dialog tabs.
<b>Gray</b>	<b>RESET Alarm</b> Triggered alarm's relay has reset to resting state—either normally open or normally closed. If you have the sound option, established in Setup, the audio for an active alarm will continue to sound until an operator responds to the triggered alarm. Setup also has an option to automatically remove reset alarms (as long as an operator response is not required.)
<b>Aqua</b>	<b>RESET Alarm (requires an operator response)</b> Triggered alarm's relay has reset to resting state, but you have selected Alarm Setup's option to require an operator response to all triggered alarms. This aqua color shows those alarms that still require an OPERATOR RESPONSE.
<b>Yellow</b>	<b>Active Alarm</b> Although important, this alarm's Priority setting is NOT highest of all active alarms in the current display.
<b>Green</b>	<b>Incident Report</b> Operator has logged a report that is NOT ALARM RELATED. Report could describe, for the record, any suspicious activity. Acknowledged alarms can also take on this color if no reset is involved.

Before any operator action, only the Active Alarms (prioritized and unprioritized) would appear, as they are triggered. Depending on the setup, an operator may hear an accompanying "beep," "tone," or specified .wav file sound when an alarm displays and while it is active.

**Operator Response:** The operator responds to the alarm as follows:

Looks at the row to determine the site, device, and specific alarm triggered. Also notice the priority setting.

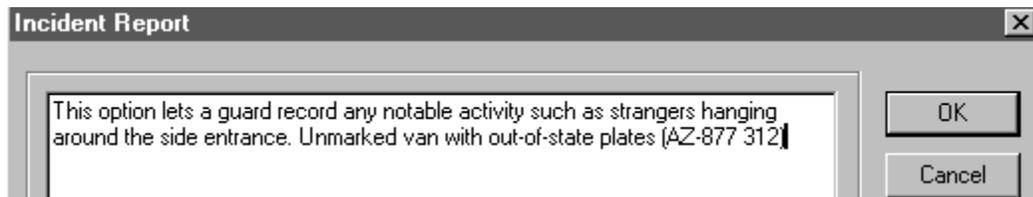
## Reading the Alarm Monitor

- When the alarm relay resets, the row in the Alarm Monitor changes from red to gray or aqua, and the ALARM STATUS column changes from Active to RESET.
- A reset alarm may be set up to automatically disappear from the ALARM MONITOR based on a setup option.
- If operator is required to record a response to a triggered alarm, the ALARM MONITOR display will not automatically clear once the alarm resets.

- If sound is set to give an auditory indication of an active alarm, the sound continues until you respond to all active alarms in the Alarm Monitor.
- Select the row with which you want to work. Click the inspection icon ( ) or double-click the selected row, or right-click the selected row and choose *Inspect*. Depending on the information recorded in other parts of the Millenium Security Management Systems software, you may see the following additional information on the triggered alarm:
- Click the icon to open an incident report dialog. Then type in as much as needed to describe the incident.
- Click to save the report.
- Notice the incident report displays as a green row on the ALARM MONITOR display.
- Removing rows from the monitor: Depending on the setup, reset alarms will either automatically clear from the ALARM MONITOR or the operator can remove them by right-clicking on a row, and choosing the *Remove* option. If an operator response is required, the alarm row cannot be cleared until the operator logs a response in the Inspection dialog.

## Incident Report

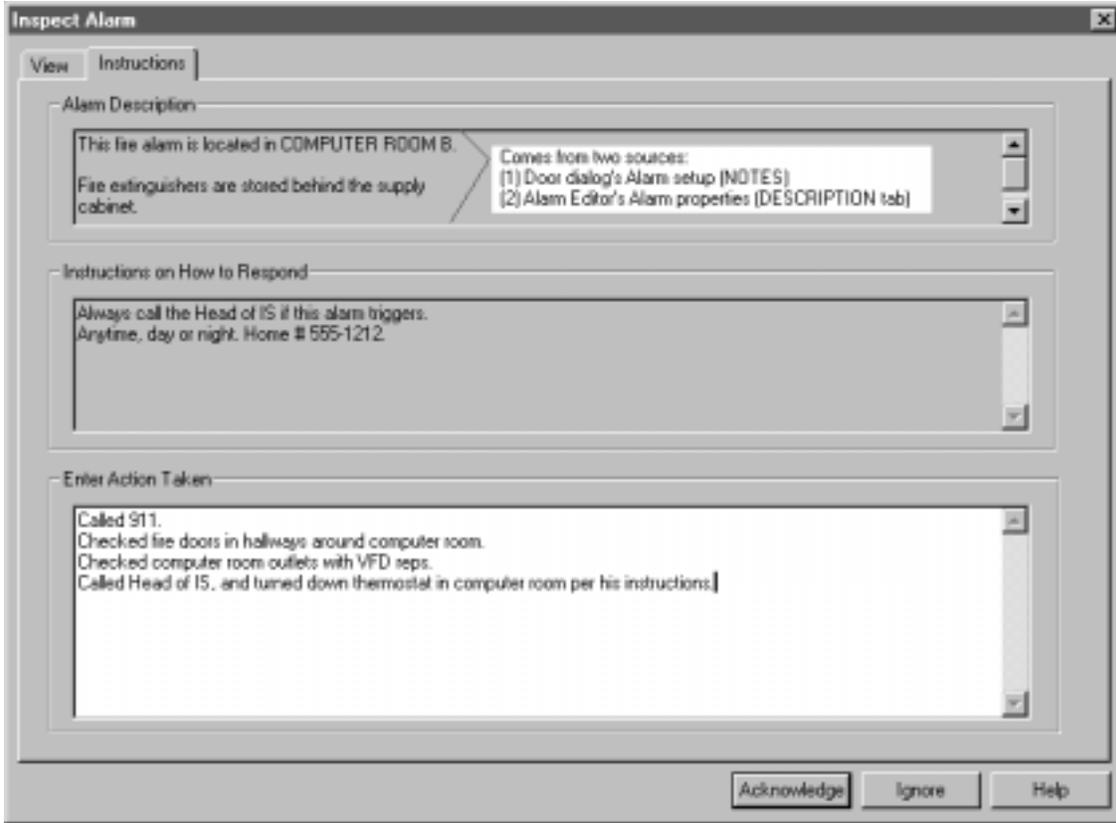
The following incident report dialog lets the operator log a report on **activity other than triggered alarm events**:



- Operator records response to triggered alarms in the Enter Action Taken box of the Inspect Alarm dialog. To get to Inspect Alarm dialog, either click the Alarm Monitor's inspection icon  or double-click on the specific alarm row in the Alarm Monitor display.

## Inspect Alarm

When an operator clicks the icon or double-clicks on a particular alarm in the Alarm Monitor, the following inspections report dialog appears:



- Two tabs of inspection information are available:
- Instructions tab, View tab
- Two buttons give the operator a choice of responses:
- An operator can be required to Enter Action Taken based on setting in Alarm Editor Properties.

## Automatically Remove Reset Alarms from Monitor

Monitor display automatically removes a row when the triggered alarm RESETS. If operator response is required (through Alarm Editor's Properties dialog, Instructions tab,) reset alarm will not disappear until operator logs a response (Inspect Alarm dialog.)

- Allow Operator to Remove Active Alarms from Monitor
- Operator can right-click on an alarm row in the Monitor and remove the alarm display.

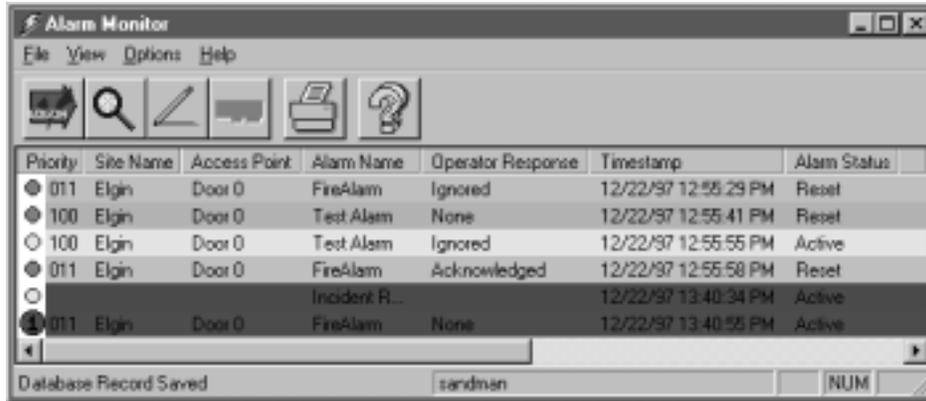
## Auto Display Graphics and Display Portrait on Unlock Events

If user images exist through the optional Millenium Badge module, the user's photo can pop up when **UNLOCK** events occur. Unlock events include:

- Invalid User
- Invalid Time(zone)
- Unlock door
- First user unlock (DCD relay mode of First user auto activate)

## Ignore Button

When operator clicks this button, it means he knows the alarm was triggered, but ignores the alarm in a pre-determined situation. The alarm row in the monitor shows OPERATOR RESPONSE— "Ignored."



- For example, operator might use this type of response for: (a) special, pre-approved door ajar situations or (b) when electronic "noise" causes an alarm to trigger repeatedly.
- If required, operator records actions taken in response to the situation (Enter Action Taken box).
- If operator tries to Ignore or Acknowledge an active alarm without completing the Enter Action Taken box, the Alarm Monitor Message appears.
- Depending on response in the Alarm Monitor **Setup** dialog, an operator may not be allowed to remove active alarms from Monitor without recording a response about the alarm situation.

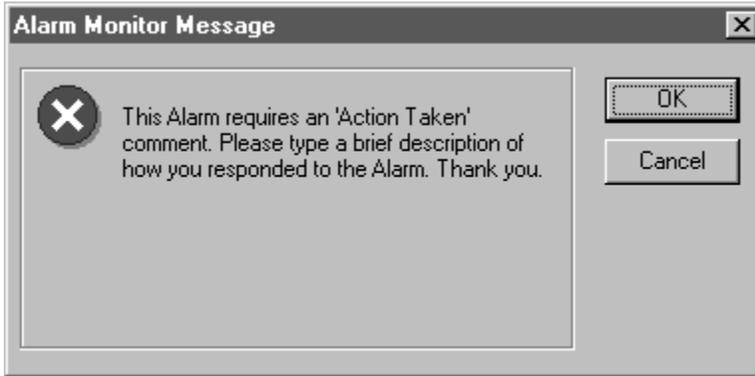
## Instructions Tab

Shows any **Description** or **Instructions** from Alarm Editor's *Properties* dialog.

<b>Alarm Description</b>	Expanded description of the particular alarm as established in the Alarm Editor's Properties dialog ( <i>Description tab</i> .)
<b>Instructions on How to Respond</b>	Special instructions to the responding operator as established in the Alarm Editor's Properties dialog ( <i>Instructions tab</i> .) These instructions appear in the Alarm Monitor's <b>Inspect Alarm</b> dialog when the alarm triggers.

Includes free-form text entry box where operator records his or her response to the particular triggered alarm:

### Enter Action Taken



This is where the responding operator records what was done in response to the triggered alarm. If an entry is **required** in this box:

- the dialog will not close until an entry is made.
- the particular alarm row cannot be removed from the main Alarm Monitor display until an entry is made.
- the particular alarm will not automatically clear from the main Alarm Monitor display when the RESET occurs until operator makes an entry.
- **Required** entry comes from a checkbox entry on the Alarm Editor's Properties dialog—*Instructions tab*.

## Acknowledge Button

Operator clicks this button when he has inspected the alarm by opening The Alarm Monitor's Inspect Alarm dialog. The alarm row in the monitor shows OPERATOR RESPONSE—"Acknowledged."

The Inspect Alarm dialog includes an expanded **description** of the alarm and any special **instructions** to follow for the given alarm. Special instructions come from the Alarm Editor's Properties dialog.

- If required, operator records actions taken in response to the situation (Enter Action Taken box).
- If operator tries to Ignore or Acknowledge an active alarm without completing the Enter Action Taken box, the Alarm Monitor Message appears.

Depending on your response in the Alarm Monitor Setup dialog, an operator may not be allowed to remove active alarms from the Monitor without recording a response about the alarm situation.

## View Tab

Displays optional graphic image of where the triggered alarm exists.

**NOTE:** You provide the graphic image and set up Millenium Access Management System' alarms on the image through *Alarm Editor*.



The graphic is designed to help a responding operator visually pinpoint the location of a triggered alarm. Icons appear in motion to help visually pinpoint and describe the type of active alarm that has been activated. The following buttons appear if you have set up more than one graphic file:



jumps to **next** Floor map file for the given alarm.



jumps to **previous** Floor map for the given alarm.

# Chapter 14: Tours

## Tour Toolbar Button

Tour is a module of Millenium Expert Systems. Press the  button to display a Logon dialog that launches the application.

- Millenium Tour lets an operator set up a series of access points where a designated user (usually a security guard) must check in as part of touring the facility.
- Tour handles up to 100 named tours.
- Tours include as many as 96 intervals that consist of an arrival time, a DELTA time (leeway,) and a specified station (SITE and ACCESS POINT.)
- The access point may or may not grant the assigned touring personnel access—Tour only requires that a reader and DCD be installed at the checkpoint station.

A tour person must

- arrive at a specified station within a window of time (DELTA) established for each interval, and
- check into stations in order.

If tour personnel misses a station or arrives out-of-sequence, Tour history records the activity, accordingly.

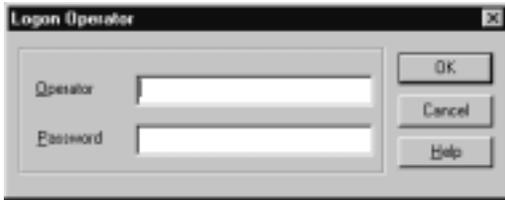
- Reports for Millenium Tour module appear in the Report Selection dialog that displays when you click the REPORTS () button.

## Logging On to the Tour Module

1. First, log onto Millenium Access Management System

2. Click the Tour icon  on the main Millenium Expert Systems toolbar.

The following dialog appears where you Log on to the Tour application:



3. Type the Login ID assigned through Millenium Expert Systems OPERATOR dialog.
4. Type password, as recorded in Millenium .
5. Press the <Enter> key. The Tour toolbar appears.

## Tour : Definitions

Millenium Tour is an add-on application that works with Sites and Doors established in Millenium Expert Systems software. A tour is a sequence of doors at which assigned personnel must arrive within a specified time (delta.) The sequence is linear, meaning the personnel must follow a predetermined order. Tour personnel must first exist in the software as "users."

### ***Important!***

Millenium Expert Systems must be running, and only one workstation should run Tour to prevent duplicate history. Millenium Expert Systems continues to record access control history at the same time the single workstation records Tour activity.

Millenium Expert Systems toolbar



Millenium Expert Tour toolbar



**Preliminary programming required before you set up a tour:**

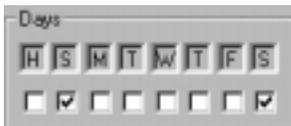
Ensure that:

- People you want to assign to tours already exist as USERS in Millenium Expert Systems
- There are SITES (Site Control Unit circuit boards) installed and created in Millenium Expert Systems software.
- There are DOORS (DCD circuit boards) installed at checkpoint stations and created in Millenium Expert Systems software.
- Holidays are programmed under TIMEZONES in Millenium Access Management System
- A reader device is installed at each checkpoint station. The Reader either can be installed as a tour checkpoint only, or can double as an access control device. That is, the reader can serve merely to record (log) the touring person's arrival at a station, or the reader can also grant or deny access to a door or elevator floor based on user's Access Group and Timezone.
- Have users assigned a key or card for the readers installed at checkpoint stations.

To view or print reports on tour programming and on tour history, click the REPORTS icon (.)

**Day**

Tour days are defined as starting anytime between **00:00** and **23:59**. You assign days to a tour by clicking the  checkbox below the day-of-the-week letter on the main tour setup dialog.



The **H** box represents all Holidays established in the Millenium Expert Systems Timezone dialog (Holiday tab.)

**Delta**

Delta refers to the period of time or "leeway" a person has to reach a door on his or her tour.

If the delta is 5 (minutes,) the person may arrive at the interval station 5 minutes before or 5 minutes after the established Arrival Time and still be considered on time. Depending on when the user arrives at a station, one of the following history messages appears:

**Arrival at Station** If the person arrives at the assigned station, in sequence, within the DELTA period, the Tour history records the arrival.

**Missed Station** If the person arrives at a reader checkpoint after the delta period, the door is tagged as missed.

**Arrival Out of Sequence** If the person arrives at an assigned station any time outside of the DELTA (early or late,) the arrival records as out-of-sequence.

- Establish the delta time in the main Tour dialog.
- To view or print a report of tour history, select **History of Reports** from Millenium Expert Systems ' REPORTS dialog.

**Global Tour**

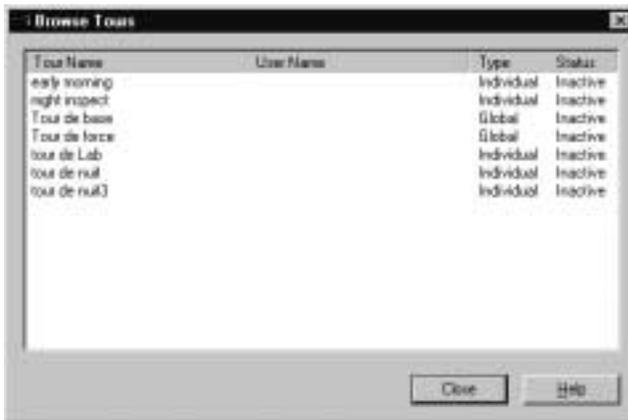
- A Global tour has no specific user assigned to it.
- The software operator "runs" a (global) tour by clicking the  button
- and selecting a user to perform a particular global tour.
- After a global tour ends, the user is no longer assigned to that tour.

**Individual Tour**

- An INDIVIDUAL tour has one specific user assigned to it.
- The operator clicks the  button to assign an individual to a tour.

**Browsing All Tours**

All named tours display along with the assigned user, the tour type and status.



The Browse Tours dialog identifies Global tours as well as Individual tours.

**NOTE:** A person gets assigned to a Global tour at the time an operator" runs" the tour (.)

Tour STATUS shows the following:

**Inactive** No Tour history is being generated. Inactive status means one of the following:

- Tour interval **Arrival Times** have all come and gone.
- Tour is named but with no intervals set up, or
- Tour (individual type) has no user assigned to it.

**Active** The Tour program evaluates all tours every 15 seconds. As the Arrival Time of the first interval takes effect, Tour history registers whether a user has:

- Arrival at station, or
- Missed the Arrival Time delta ("Missed Station,") or
- Arrived out-of-sequence (arrived late or early.)
- Tour history generates one of the above messages.

**To override current status;** Right-click on the tour's STATUS. The Tour program will then re-evaluate the tour. If no activity occurs, the tour returns to Inactive status until the Tour application is run the following day.

### Tour Interval

An interval represents one station or checkpoint in a tour. The interval is a combination of a SITE and ACCESS POINT along with a target arrival time and a Delta window within which the station should be checked.

- One tour can have up to 96 intervals.
- Intervals display in sequence based on ARRIVAL TIME.
- Intervals must be within the same day (00:00 through 23:59.) **To span midnight, you must create a separate tour.**
- The same access point can only appear **once** during a tour. (To repeat-check an access point, create a separate tour.)
- Delta window time period is in MINUTES.



— Add an interval



— Edit/change a selected interval



— Remove the selected interval

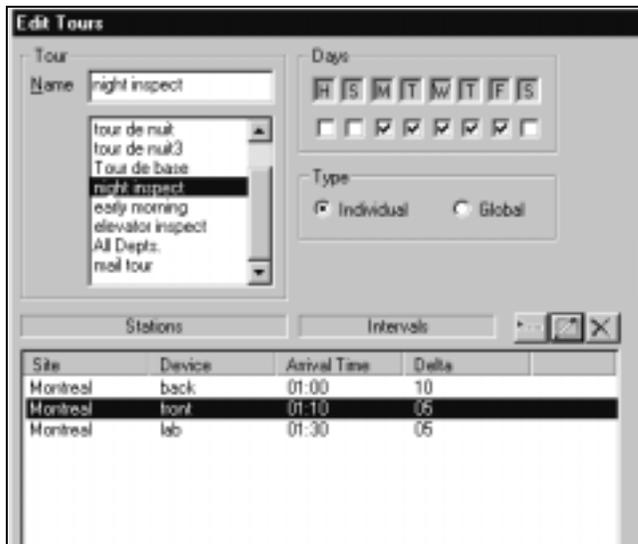
### Changing an Interval

Highlight the interval you want to modify, and click the edit  button. Make changes to the station or time intervals and press the  button.



### Deleting an Interval

Highlight the interval you want to remove, and press the delete  button.



### Canceling a Tour

Canceling a tour removes it from Active to Inactive status. The tour still exists in the programming, and will be Active the next time an operator opens the Tour application.



### Tour History

The Tour module displays its own history.

Time	Tour Name	Check-in	Delta	Status	Site	Dr.	Name	Key/Card Code
08:07	Main			Logon Operator			Mateo	
10:42	All Depths			Run Global Tour			Mateo, Site	Dallas 2543544
10:42	night inspect			Assign To Tour			Mateo, Site	Dallas 2543544
10:43	night inspect	01:00	10	Moved Station	Monreal		Joan	
10:43	night inspect	01:11	05	Moved Station	Monreal		Joan	
10:43	night inspect	01:31	05	Moved Station	Monreal		Joan	
10:43	tour de nuit			Cancel Tour			Mateo	



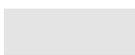
Aqua - indicates: Operator activity



Red - indicates: "Missed station" or "Arrival out-of-sequence."



Green - indicates: "Arrival at station"



Yellow - indicates: Cancelled tour



To print a report of TOUR history, open the Reports  dialog in the main Millenium Expert Systems software.

## Reports on Tours

Millenium TOUR offers reports on the tours programmed through the Tour Setup dialog as well as a report on the history of tour activity.



Tour reports appear under the Standard section of Millenium Expert Systems REPORTS dialog.

### Millenium TOUR List

Lists all data on intervals, days, users assigned to run INDIVIDUAL tours, type of readers installed on access point reader for each interval.

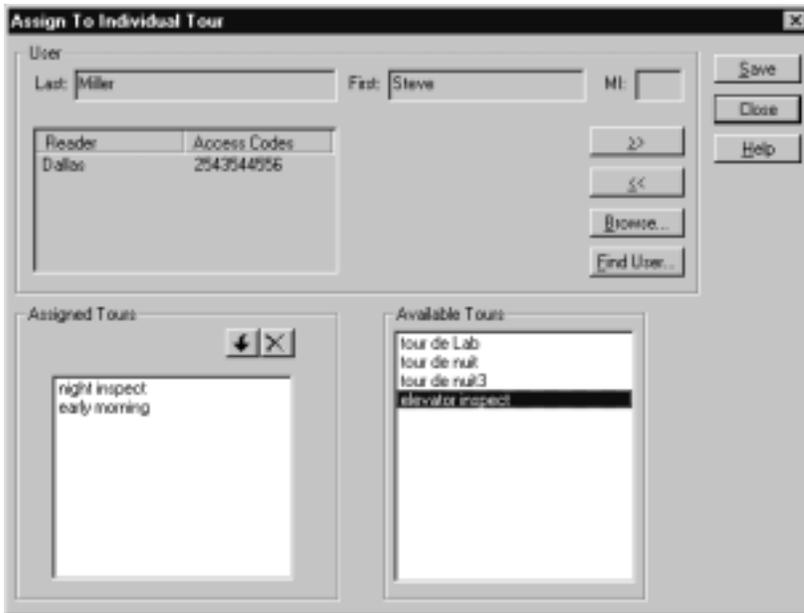
### Millenium TOUR History (Tours only)

Presents a selection dialog from which you choose one or more tours and choose whether you want history on tour programming performed by an operator and/or tour checkpoint history. Checkpoint history covers whether assigned tour personnel

- arrived at interval stations on time,
- arrived at station out-of-sequence, or
- missed the station entirely.

## Tour Assignments (Individual)

Use the following dialog to assign a specific user to an individual tour:

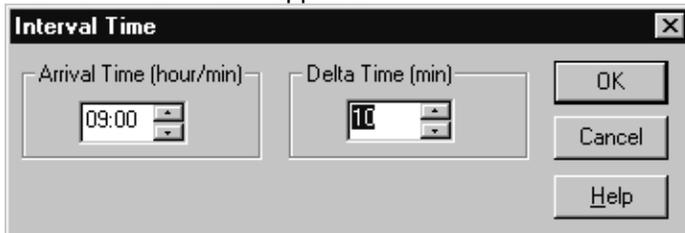


Select the tour personnel from all USERS set up in Millenium Expert Systems (USERS dialog.) Notice you can move forward and backward between users in the database, or you can browse a pop-up window of all users in the system. Notice, also, that each user's access key or card appears for your information. The first key or card assigned will display in Tour history.

## Adding an INTERVAL to a Tour

1. To add an interval, click the add/edit tour button (  ) and highlight a tour.

2. Click the **Add Interval** button  in the middle of the Tour Edit/Setup dialog. The following **Interval Time** window appears:



Set the **Arrival Time** (in hours and minutes) at which the tour personnel should arrive at the station.

3. Establish the Delta Time in minutes (The Delta is the leeway the user has to arrive at the checkpoint station after the Arrival Time.)

4. Click  or press <Enter> key.

5. The interval will display in sequential order within the given tour, based on **Arrival Time**. If you change the Arrival Time, the interval (row) will move to the appropriate location within the sequence.

 To Change an interval  To Delete an interval



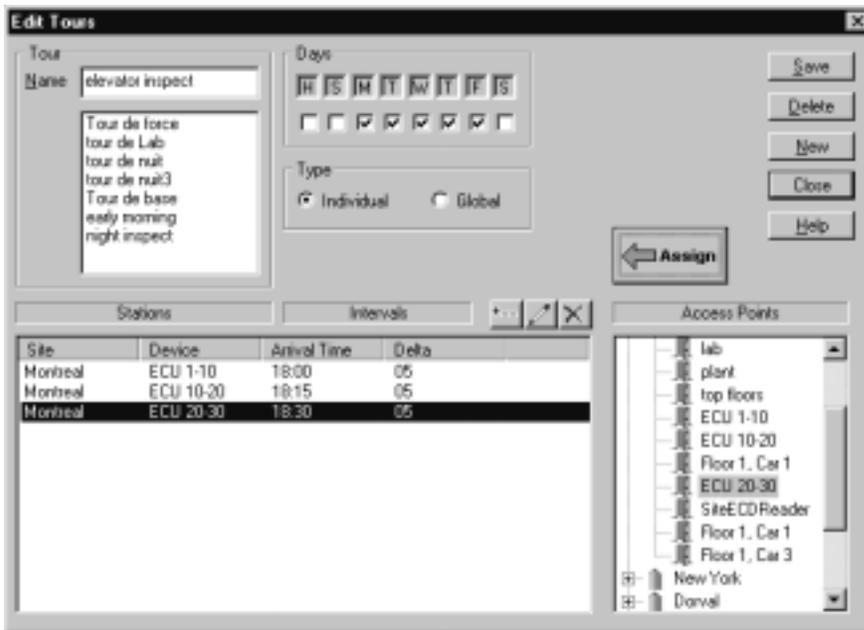
## Assigning a station to an interval

As part of creating a tour interval, first you set up the interval **arrival time** and **delta** (leeway.) Then you assign the Site and Access Point station to the interval, as follows:

1. Select the SITE and Access Point for this particular station interval. Together the site and access point will become a "station" in this tour.
2. First, click the "-" beside the SITE name. A "tree" of access points for the given site expands below.
3. Then, highlight the access point to be assigned to the given interval.



4. Click the Assign button (or double-click the Access Point in the previous step.) Notice the interval row now shows both the station and interval times.



## How do I set up a tour?

1. Log on to Millenium Expert Systems software .

2. Select the Tour icon  button.

3. Log on to the Tour application .

4. Click the Tour setup/edit button .

5. Name the tour.

6. Select the **DAYS** of the week during which the tour is to run.



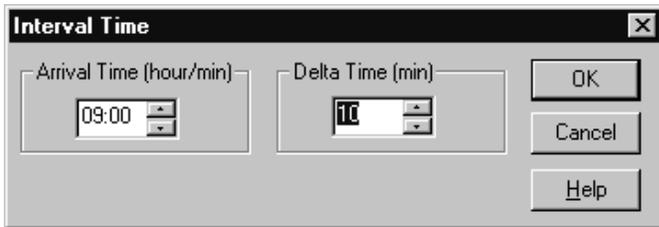
7. A day is defined as **00:00 am** through **23:59pm**. Days do NOT span midnight.

8. In the DAYS section,  stands for all holidays established in Millenium ' TIMEZONE dialog (Holidays tab.) A check in the "H" box means the tour remains **valid** for all holidays established in the system.

9. Designate whether the tour is individual or global.

10. The tour is now named in the software, but nothing happens if you **SAVE** the tour at this point. The next part of the dialog is where you set up a sequence of intervals for designated stations or checkpoints (Sites and Access Points defined in Millenium Access Management System)

11. Click the **Add Interval** button  (first of three small buttons in the middle of the dialog.) A **Interval Time** window appears:



12. Set the **Arrival Time** (in hours and minutes) at which the tour personnel should arrive at the station.

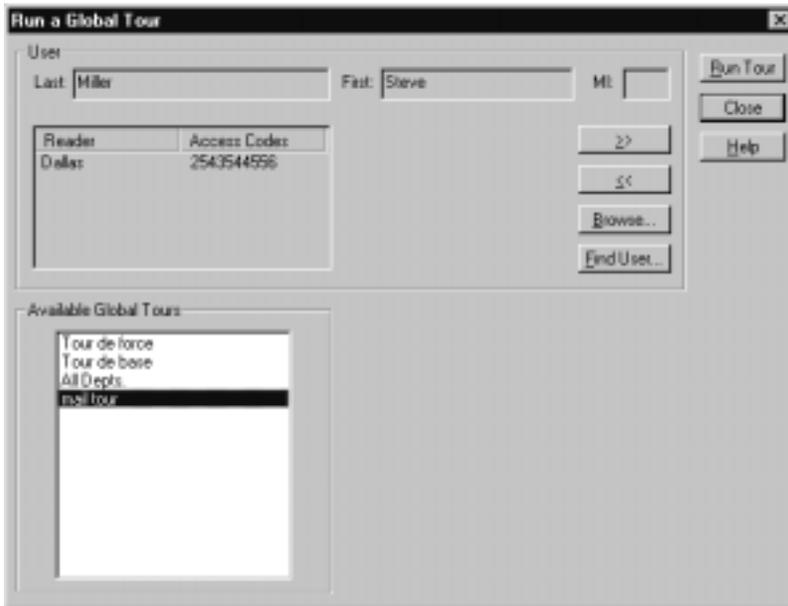
13. Establish the Delta Time in minutes (The Delta is the leeway the user has to arrive at the checkpoint station after the Arrival Time.)

14. Click  or press <Enter> key.  
The interval will display in sequential order based on **Arrival Time**. If you change the Arrival Time, the interval (row) will move to the appropriate location within the sequence.

 To Change an interval  To Delete an interval

## How do I run and assign a Global Tour?

1. To run a global tour:
2. Select a person who will be performing the tour from all users in Millenium Access Management System
3. Then highlight a global tour, and press the  button to assign the highlighted tour to the selected person.
4. Notice each user's assigned reader access appears, as assigned in the USERS dialog of Millenium Expert Systems (ACCESS tab.)



## How do I assign a user to a Tour?

Both Individual and Global tours require a Tour operator to assign a user to a tour.

Assign a user to an **individual** tour at any time. When the tour's first Arrival Time comes, the assigned user is expected to make the rounds.

1. Select the person who will be assigned to do the tour from all users in the Millenium Expert Systems database.
2. Use the forward  and backward  buttons to scroll through individual users, one-at-a-time.
3. Use the browse button  to select from a pop-up window list of all users in Millenium Access Management System

4. Use the find  to search for a particular user.
5. Type the first few letters of the users name in the pop-up dialog. The software will search for the first user that matches what you type.
6. Click the SAVE button .
7. When operator logs on and starts the Tour application, all individual tours for the day automatically load into memory and become active until their arrival times have passed.

### *How do I assign a user to a Global Tour?*

1. Click the "Run a Global Tour" button. 
2. Follow the procedure described above, to select a person from all users in Millenium Access Management System
3. Double-click to select one of the **Available Global Tours**.
4. Click the "run" button.   
This global tour now becomes Active.

## Tours that cross MIDNIGHT

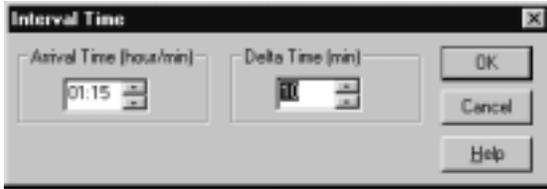
### ***Important!***

A tour cannot cross midnight. Tour days are defined as anytime between 00:00 and 23:59, and tour intervals are not designed to go past MIDNIGHT.

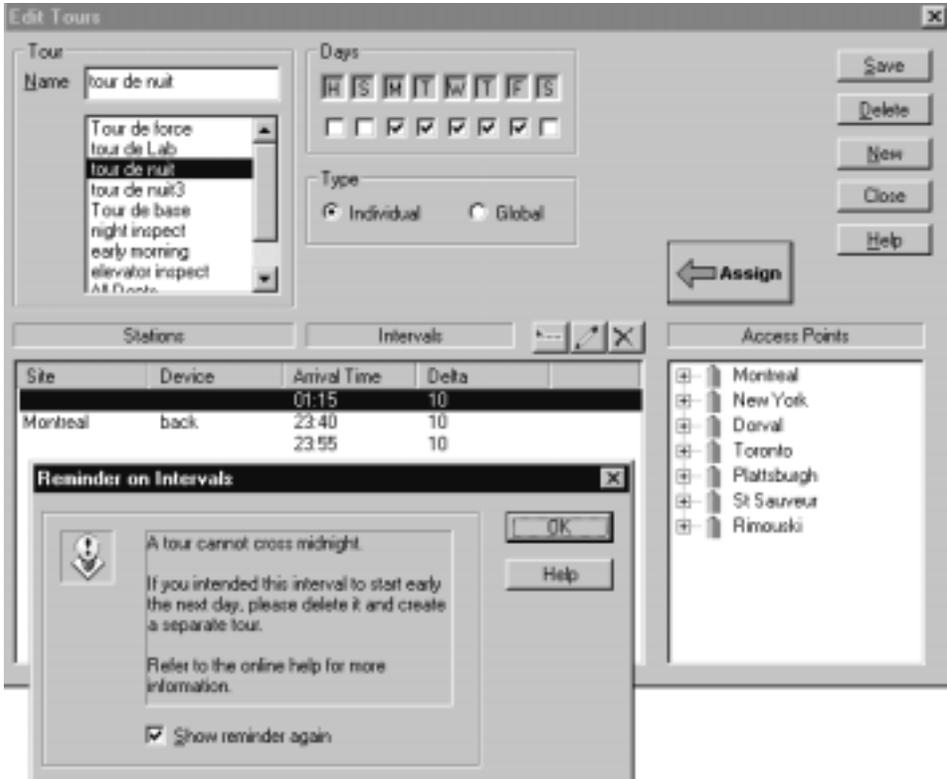
If you need to make a tour that begins in the evening and extends into the early morning hours, you must create **two separate tours**. Then assign the same user to both tours. The combination of both tours will sequence through midnight. (Steps are outlined below.)

If you are creating a pattern of intervals intended to span midnight into the following day, the software will treat your time entry as follows:

- Assumes interval is earlier in the same day according to the interval pattern you have created so far.
- Places new interval before all existing late evening intervals.
- Gives you an information message box to alert you to the situation.
- Example: You have created intervals beginning at 11:40 p.m. (23:40), 11:50 p.m. (23:50), and 11:55 p.m. (23:55.) Then you add an interval with an Arrival Time at 1:15 am (01:15.)



After you press OK in the Interval time dialog, the software displays the following **Reminder on Intervals** prompt and throws the newest interval to the *beginning* of the list of intervals in sequence for the given day.



**NOTE:** The software considers the new interval as fifteen minutes after one o'clock—the afternoon of the same day, rather than fifteen minutes after 1:00 in the morning of the following day.

### *How to handle tours that cross midnight*

**Summary— to span midnight in the example:**

1. Delete proposed interval from the original tour.
2. Create a **separate tour** for the same user, with the first interval beginning at 01:15 (fifteen minutes after one o'clock.)
3. Proceed to create intervals, as needed, through the early hours of the given day.

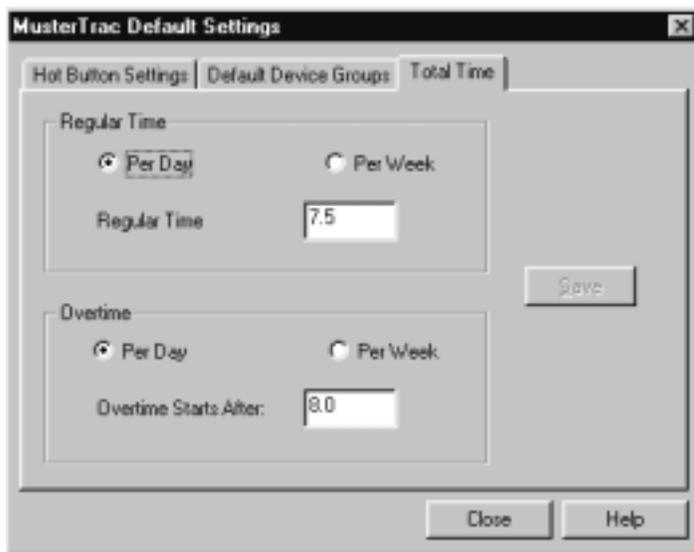
4. Assign the second tour to the same person.
5.  Show reminder again
6. To turn off reminder for next five instances, click to remove check.



# Chapter 15: Muster Trac

## Muster Trac

- Muster Trac provides basic data for security, administration or payroll purposes. The Millenium Expert System exploits existing features to provide the **Muster Trac** data.
- **Muster Trac** reports may be produced in two different ways, using two different kinds of inputs.
- **Method 1: Time and Attendance Report Selection Window** - the operator adjusts parameters for the required report by selecting from and/or filling in data fields in the selected window. This method is perfect for detailed monitoring. You can check total time spent in the building per day or week, total time absent and total overtime.



In the example above, Attendance, Total Time has been selected.

### Method 2: MusterTrac Hot Button

By clicking on this button on the main menubar of Millenium System, the operator can print a report but the content of the report is determined by the Default Settings which have been previously selected and saved in the dialog in **Menu Options > Muster Trac Default Settings**.

This method is good for obtaining immediate feedback, such as total number of employees present in the building in case of fire, for example. The Button, when clicked, immediately prints out a report to a designated printer - for example a printer in the Security Guard's station or Human Resources.

The list could then be used as an attendance sheet to ensure that all employees have evacuated the building.

Reports produced by using the **Hot Button** are the following:

**Employees Absent**

Lists employees **NOT** in the facility for a specified time period (up to five days)

**Employees Present**

Lists all employees present in the building/s for a specified time period (up to five days).

**Employees Present (Total Hours)**

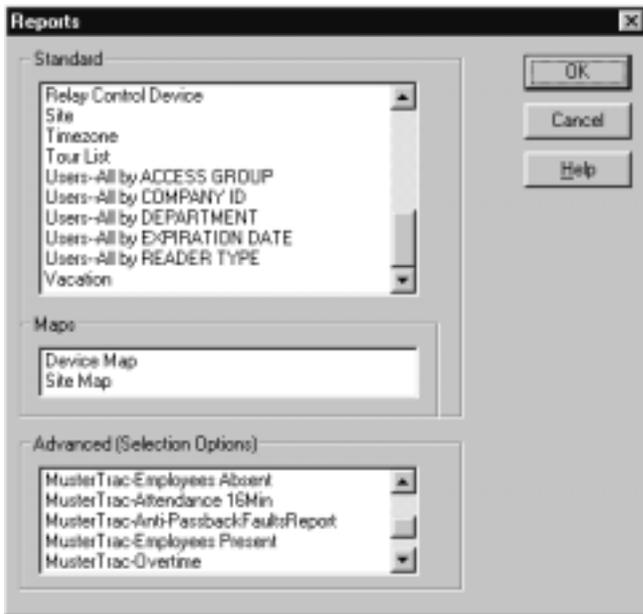
Lists the total length of time spent in the facility by each employee during the specified time period(up to five days).

## MusterTrac Report Samples: Employees Present

**Employees Present**

This report can have the content you select, using the dialog box below, or it can be generated by using the Hot button . If you use the Hot Button, the content will be determined by the default settings you chose. See *MusterTrac: Create Default Settings*.

Select type of report as shown below, selecting: Employees Present.



## MusterTrac: Create Default Settings

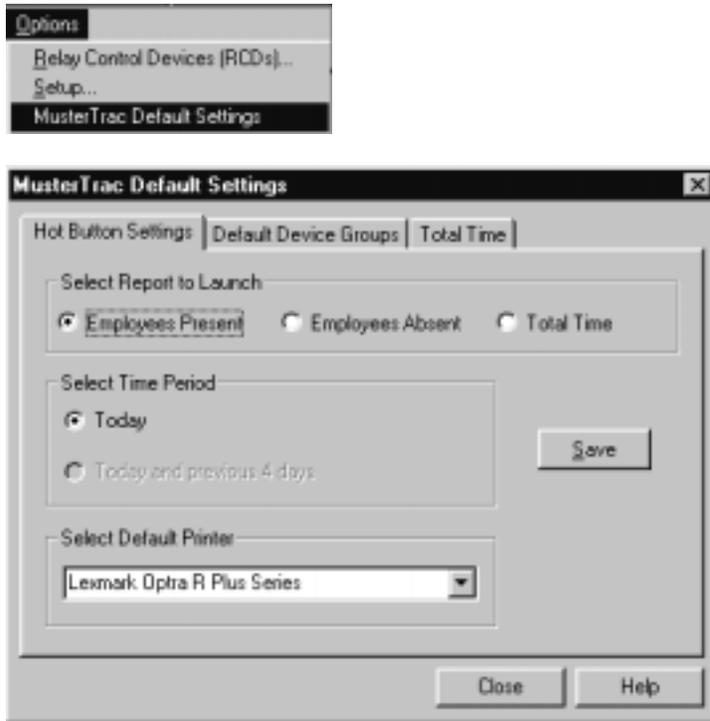
**Requirements:**

You must be a Level 1 or Level 2 operator to create these defaults

You must have previously created Device Groups for Entrance and Exit access points.

### ***How do I create default settings for the Muster Trac hot button?***

Click on the menu **Options**>MusterTrac Default Settings to start the dialog.



The " Hot Button" tab (shown above) allows you to define the content of the report you will receive when you click on the Hot Button .

**NOTE:** Remember that clicking on the Hot Button will send the report to the printer immediately; you cannot preview the report. If the report is very long, be sure that you want to print it out.

- Select the type of report - Employees Present, Employees Absent, Employees Present (Total Time).
- Select the time period to be covered in the printed report: Today or Today and the Previous 4 Days, inclusive.

**NOTE:** If you select the option for Today and the Previous 4 Days, you would usually want this report on a Friday. If you select this option on a Wednesday, for example, you receive a report of Saturday, Sunday, Monday, Tuesday and Wednesday (today). This is fine if you specifically want to check employees present on Saturday and Sunday but you would probably prefer to run the report on Friday to get a picture of Attendance during the normal workweek.

- Select the default printer. Since this information is confidential and should not be seen by just anyone, ensure that you choose a printer in a private location, a single-user printer in Security or Human Resources for example.

## ***How do I Create Default Settings for Default Device Groups?***

1. Click on the menu Options> MusterTrac. Default Settings to start the dialog.

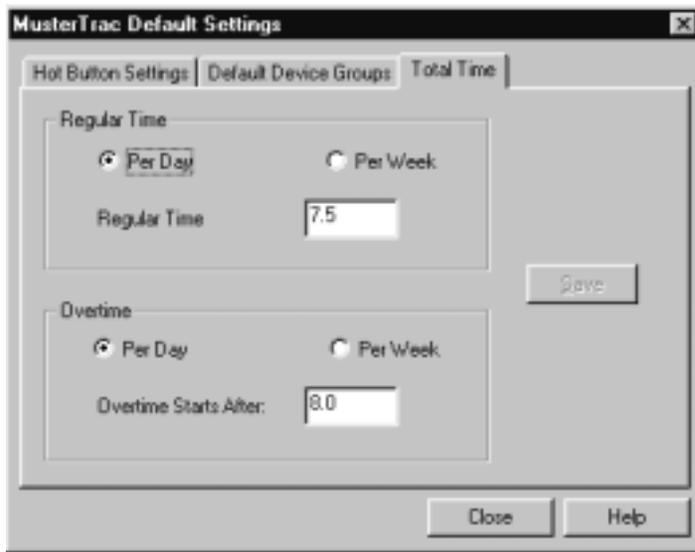


- 2.
3. The Default Device Groups tab allows you to define the device groups that will be used to generate the reports you request. Select the device groups from the dropdown menus here.



4. Remember you must have one entrance and one exit device group defined.
5. Click on Save and your default device groups are saved.

## How do I set up Total Time parameters?



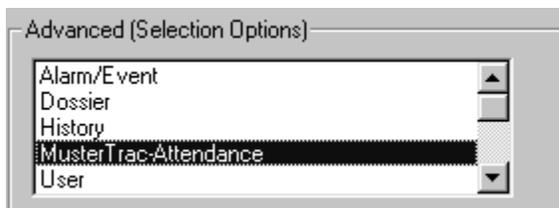
1. The **Employees Present (Total Time)** tab allows you to define the time periods that will be used to generate the reports on **Employees Present (Total Time)** and **Employees Present (Overtime)**
2. Enter your definitions of regular time and overtime here. In the above example, Regular Time is defined as 7.5 hours per day and Overtime is defined as work performed after 8 hours per day.
3. Click on Save and your default time settings are saved.
4. To see examples of reports, go to MasterTrac Total Time sample Report.

## MasterTrac - Exporting Files

MasterTrac reports can be exported to other departments or individuals that need the data for statistics, or insurance purposes, for example. Each of these departments or even other companies may want to put the files in their own particular format.

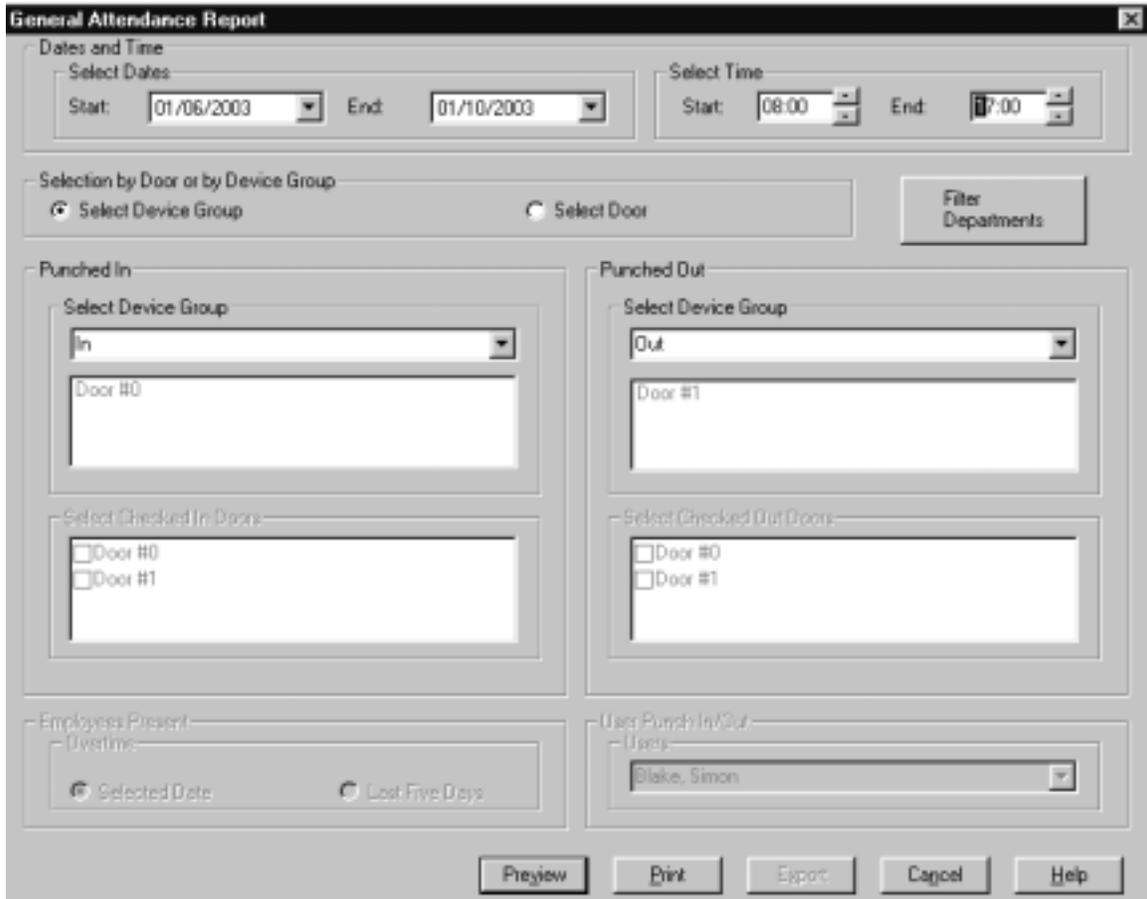
The data most commonly required is employee attendance, so that is the example we will use here.

1. First, select the report type:



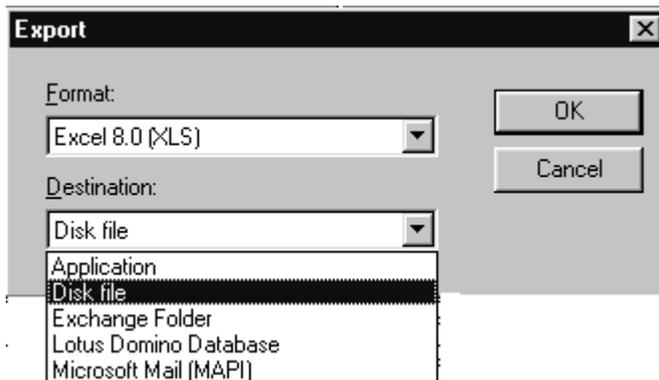
2. Next, when the report parameters dialog box appears, select your criteria and then click on the Preview button at the bottom of the box.

3. The following dialog box appears:

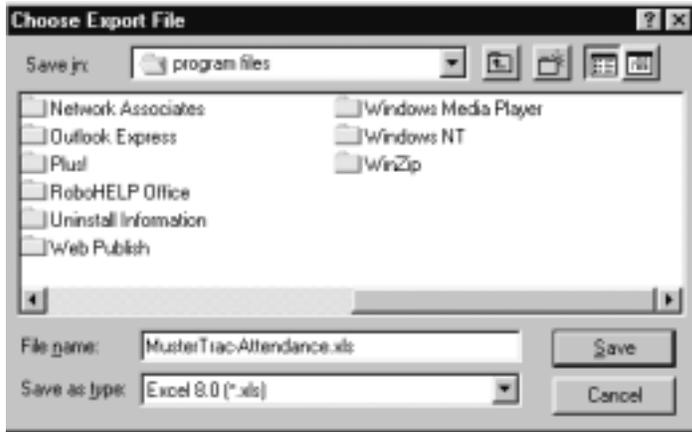


4. Click on the envelope icon.

5. Browse to select the type of format you want the data to be exported as.



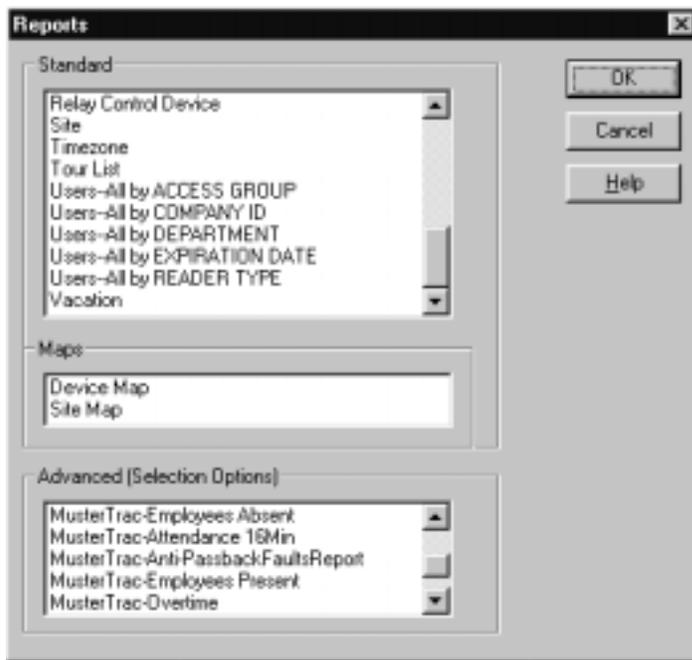
6. Select the directory and the file name for your report.



## MusterTrac - General and Specific Reports

- MusterTrac can offer reports on all the employees in a building or a detailed look at one employee's entries and exits throughout the facility.
- In the Employees Absent and Employees Present reports, you can see who was in or out of the facility and for how long.
- On the other hand, from the Punch In/Punch Out report, you can see which user or users entered and exited specific access points during a given time period.
- In other words, you can map the traffic pattern of a particular employee or of access groups. This is very useful for example, if you want to change the access points, perhaps to put certain points in Passage Mode to ease congestion.

When you select the type of report



The following type of screen appears:

## MusterTrac: Create Device Groups

The Device Groups option lets you select individual Millenium devices (doors, elevator floors, site controllers and relay controllers) and group them together into two groups: Entrances and Exits. Create device groups for entrance and exit access points in each area where you want to Monitor the following for a specific time period.

- Employees Present
- Employees Present (Total Time)
- Employees Present (Overtime)
- Employees Absent
- In the MusterTrac dialog, you can then assign a report to automatically print on designated printers.

## How do I create Device Groups?

1. The Device Groups option appears under History in the main Millenium menubar.



2. When you select the option, the following dialog displays:



3. Type a name for the device group you are forming ("IN" in the above example).
4. Click to select the devices to be included in the named device group.
5. If you click the **Site** name, a check automatically appears beside all devices under that Site Control Unit (SCU.)  
If you remove the check for a site, all checks disappear from devices under that site.
6. Click the  button.



7. Now you have two groups, "IN" entrances and "OUT" exits.
8. Be careful not to assign the same door to both groups. Each access point can only be assigned to **either Entrances or Exits**. Compare the entrances and exits in the two screens above. and note that they are different doors in each group.

**Reminder:** Icons beside the devices identify the type of device:

-  Site Control Unit (SCU)
-  Door Control Device (DCD)
-  Relay Control Device (RCD)
-  Elevator Control Unit (ECU)
-  Elevator car Control Device (ECD)

## MusterTrac - Anti-Passback

### What is anti-passback?

Anti-passback is a Millenium feature that control user access on specific doors. Anti-passback is designed to prevent users from passing their keycard back to someone else to gain access to your facility. With this feature, users are forced to use specific doors to enter or exit the facility. For example, you would set up a pair of doors (In and Out) and apply anti-passback to them. Users who present their cards to the "in" door will have to present their cards to the "out" door in order to have access to the "in" door again.

### Do I have to use anti-passback?

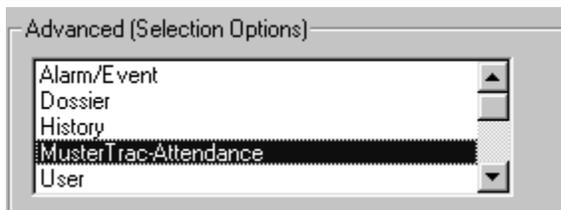
No. The Millenium MusterTrac module is flexible enough for you to dynamically choose the doors or group of doors you want the reports to be based on.

What happens for users that work through midnight?

The time and attendance module will base all its reports on the start and end time you choose, thus the time and attendance module is NOT midnight sensitive; it takes into account the midnight crossover.

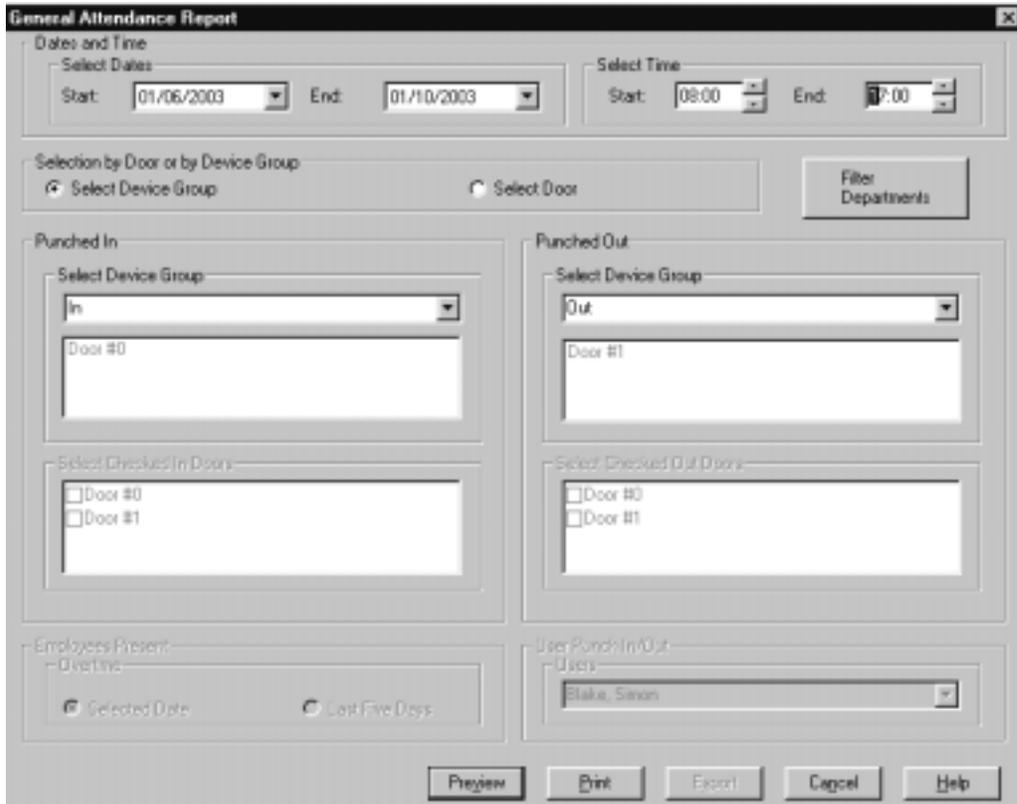
## MusterTrac: General Attendance

Select type of report, as shown below, selecting MusterTrac-Attendance.



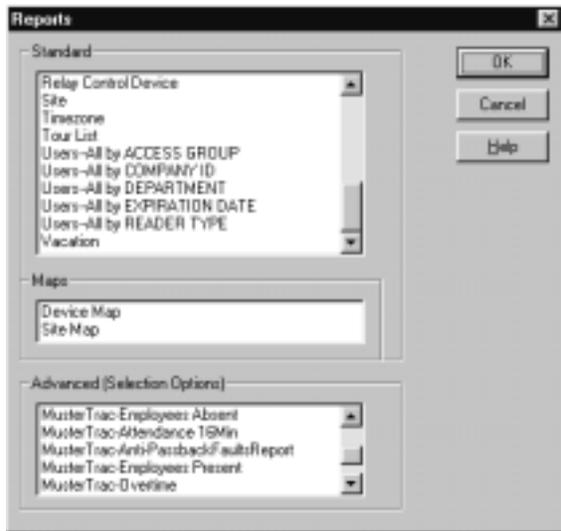
Select date and time.

Preview and/or Print the report.



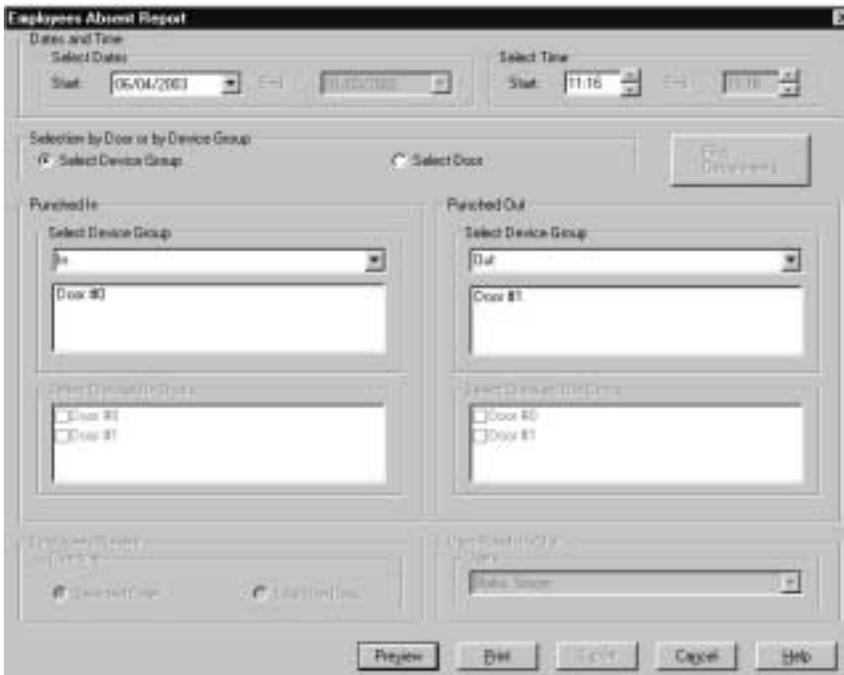
## MusterTrac Report Samples: Employees Absent

Select type of report, as shown below, selecting MusterTrac -Employees Absent.



Select date and time.

Preview and/or Print the report.



If everyone is in, you will receive the following message:



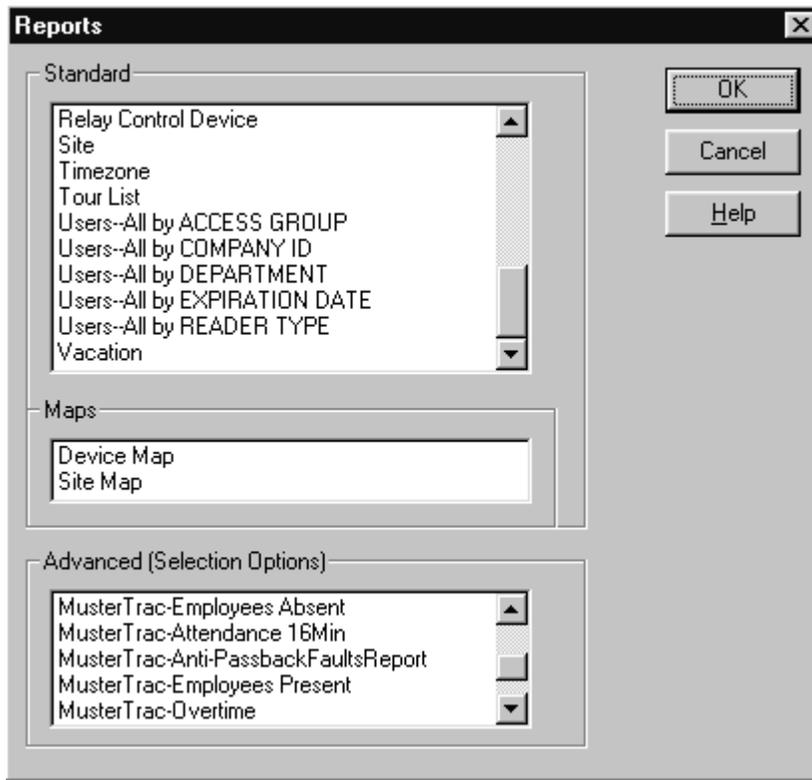
If there are employees out of the building, you'll receive a report like the one shown below. This particular report shows a lot of absences because of the time chosen - a time when many are out to lunch. To get a more accurate picture of who may be out of the building for the day, choose a time such 10:30 or 3:30 in the afternoon.

## MusterTrac Report Samples: Overtime

### Overtime Report

For the Overtime report, select the date (or time period) for the report . Notice that the fields you cannot change are grayed out. For example, you cannot select a user, because this report only shows the amount of overtime spent by all employees. Of course, you can then find a particular employee or group of employees within the report.

1. Select type of report as in the example below, selecting Attendance: Overtime.



2. In all report selection windows, select the dates by clicking on the down arrow beside the date field and using the pull down calendar, as shown below.
3. Select Device Group or Door. In the selection dialog box below, Device Group is selected. This means that you only see when the user entered and exited the building - specific doors are not mentioned.
4. Select the time period - either overtime for a specific day or for the last five days from the date you have entered.

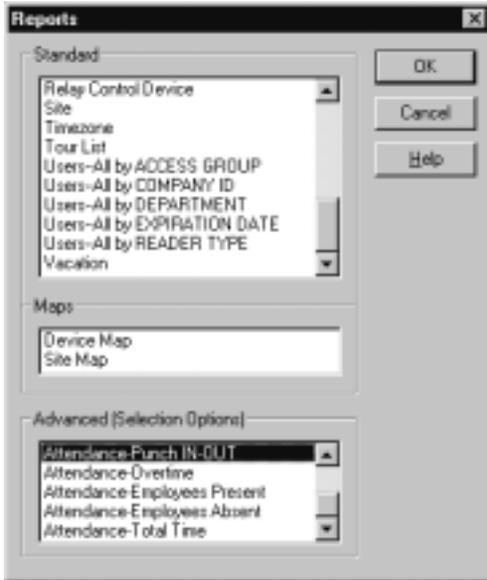
5. Click on the Preview button to view the report before printing it, or print immediately. The report, in the example below shows that Advertising must have had a pressing deadline that week.
6. Notice that, as in all printed reports, the date at the top shows the date that the report was generated and printed.

		<b>Overtime Report</b>	
Printed 03/01/2002 - 11:09:22AM			
Date Period:		01/03/2002 00:00:01 AM	To 01/03/2002 11:59:59 PM
Department	User	Hours	Minutes
	Blake, Simon	10	47
	Burke, Peter	10	56
	Chang, Holly	10	56

## MusterTrac Report Samples: Punch In/Out

### Punch In/Out Report

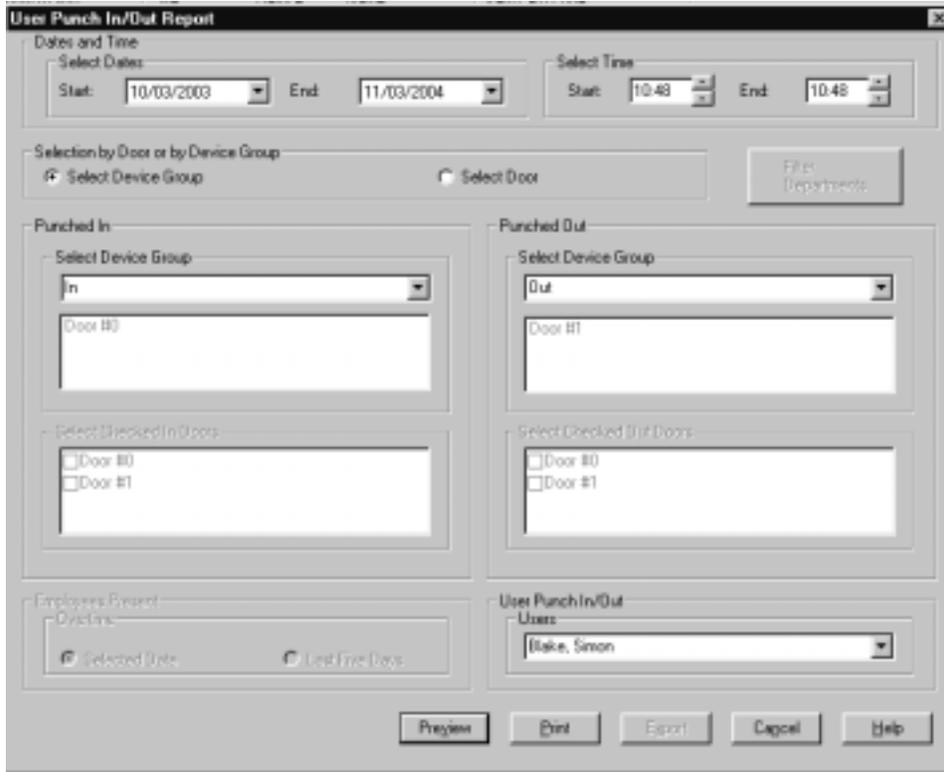
1. For the Punch In/Punch Out report, select the date (or time period) for the report and then select a user.
2. Select type of report as shown below, selecting MusterTrac-Punch IN-OUT.



3. In all report selection windows, select the dates by clicking on the down arrow beside the date field and using the pull down calendar, as shown below.



4. Select Device Group or Door. In the selection dialog box below, Device Group is selected.
5. This means that we only see when the user entered and exited the building; specific doors are not mentioned.



If we select a specific door, as shown in the dialog box below, a similar report will be produced.

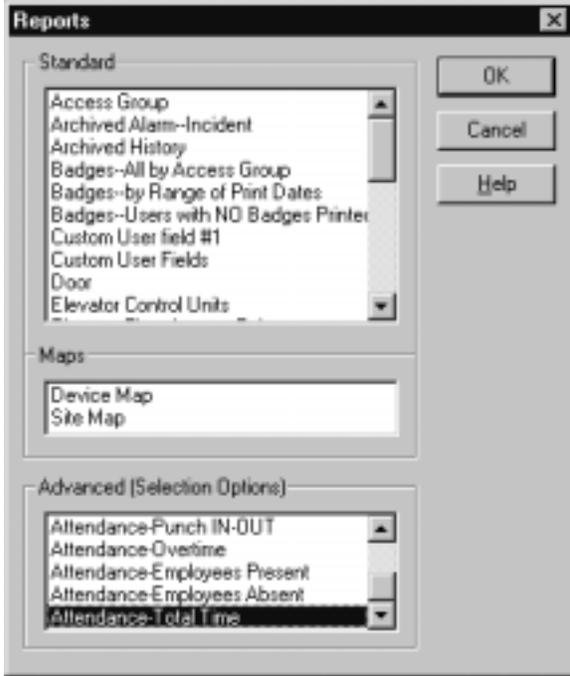
## MusterTrac Report Samples: Total Time Present

### Employees Present - Total Time

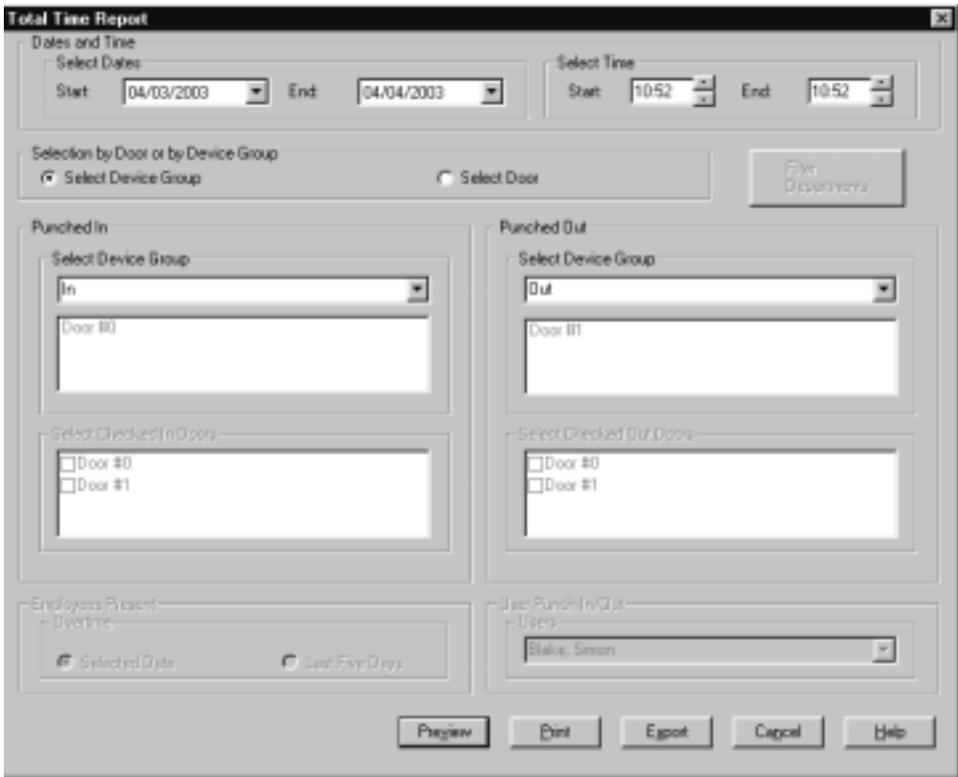
The total time report will display all the users, by department (in the date and time range you've selected in the report selection menu) for specific doors or device groups. Millenium will calculate the total time within the date and time range you've selected.



1. Click on the Report button in the main menu of Millenium and select from the Advanced Reports Section.



2. MusterTrac - Total Time has been selected. So, you receive a report on the total number of hours each employee spent in the facility during your specified time.
3. Produce the report by selecting the type, as above and then filling in the data fields in the window appearing below:



4. You can preview the report before printing by clicking on the Preview button.
5. You should see a report like the one below:

		<b>Total Time Report</b>	
Printed 03/01/2002 - 10:54:18AM			
Date Period:		01/03/2002 08:54:01 AM	To 01/03/2002 10:54:59 AM
<u>Department</u>	<u>User</u>	<u>Hours</u>	<u>Minutes</u>
	Blake, Simon	1	59
	Burke, Peter	2	0
	Chang, Holly	2	0

**Anti-Passback Fault report**

This report will give you the list of all employees within the date / time range you've selected that are at anti-passback fault. This means you have a list of those who tried to circumvent the anti-passback feature by passing their card to another employee or using the wrong doors.

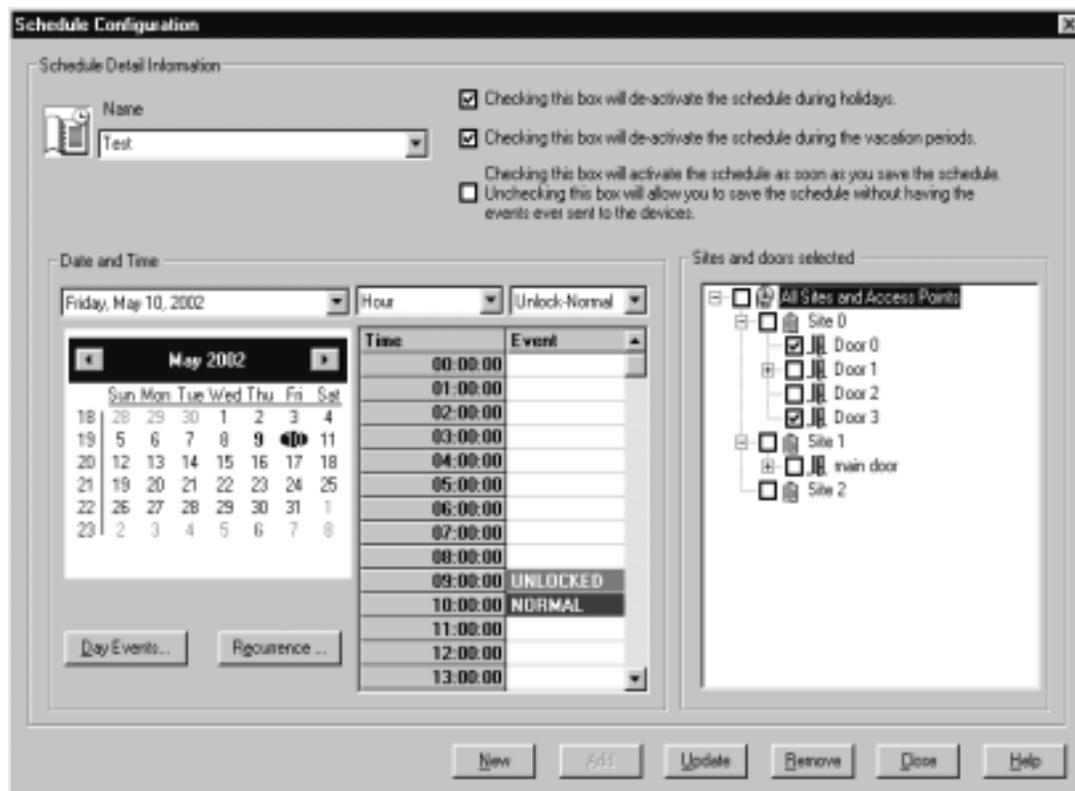
<b>Anti-Passback Faults Report</b>				
Printed 14/02/2001 - 9:36:30AM				
Date Period:		2/14/01 09:34:01 AM	To 2/14/01 09:34:59 AM	
<u>Department</u>	<u>User</u>	<u>IN/OUT</u>	<u>First punch</u>	<u>Second punch</u>

# Chapter 16: Scheduler

## Millenium Scheduler

- Millenium Scheduler is a convenient feature that is especially useful in large facilities. Doors may be set to remotely unlock for certain periods of time. Millenium Scheduler allows you to select entire facilities, entire sites or large blocks of access points at once. You then assign unlocking times to all these access points.
- Millenium Scheduler also permits you to set recurring time periods when you want to open or close these Access points.
- The main window of this module contains the two elements which are all you need to schedule access to however many access points you select - a calendar and a list of all your access points. Days where events are scheduled appear in **bold**.
- See the procedure in Scheduler-- Create a Schedule to use this window.

**Note:** Millenium Scheduler is not a Module that can work on its own, like Alarm \$Editor for example. The full Millenium Expert application must be up and running in order to use Scheduler.



## How Scheduling Works in the Millenium System

You can create many custom schedules for locking/unlocking Access Points and keep all the schedules in one easily accessible database.

**Definition** - A schedule is a collection of dates during which specified access point/s will be unlocked for a specified time period and then returned to their normal state at the end of that period.

**Operation** - Each time the Millenium application software is loaded/started up, the event schedules are started. Events that are theoretically already in progress are discarded. For example, if a meeting is scheduled to take place from 7:30 to 8:30 and you turn on the system at 7:45, that event will not be loaded. However, the next event scheduled to begin at 8:30 will be loaded into the locks in the system.

At midnight, Millenium Schedule automatically updates to the next day's scheduled events.

**History Display** - Unlock events caused by the Millenium Schedule automatically opening and closing doors are displayed in the main Millenium History Screen

Unlock events caused by a user's unlocking the door are shown with the symbol , while unlock events caused by a Millenium Scheduler schedule taking effect are shown with the clock symbol .

Millenium Expert						
File Logon Site Access Points Time Access User History Options Map View Schedules Help						
						
Time	History Action	Site	Device	Name	Key/Card Code	
05/27/2002 8:59:14 AM	Comm Port not avail...	Site #0				
 05/27/2002 8:59:24 AM	Logon			ani		
 05/27/2002 9:11:31 AM	Schedule added			Finance Meetings		
 05/27/2002 9:12:42 AM	Schedule updated			Finance Meetings		
 05/27/2002 9:15:56 AM	Schedule updated			Finance Meetings		
 05/27/2002 9:18:59 AM	Schedule added			HR Conf		
 05/27/2002 9:20:18 AM	Schedule added			Sales reps		
 05/27/2002 9:26:37 AM	Schedule added			marketing		
 05/27/2002 9:27:00 AM	Schedule updated			marketing		
 05/27/2002 9:40:40 AM	Schedule added			Customer Support		
 05/27/2002 9:41:05 AM	Schedule updated			Customer Support		

## Access Points Normal/Unlocked

For each schedule that you create in your system you must decide whether you will change your selected access points from Normal to Unlocked or the other way around.

### Definitions:

**Normal** -means that the lock is in the normal state for that the access point. This could mean that the user has to swipe a card, use a key, or just turn the handle if the access point is usually open to all.

**Unlocked** -means that the lock is in an unlocked state, programmed by Millenium Schedule to be unlocked.

**Reserved or Booked** - means that an event is scheduled at that access point so it cannot be booked on another schedule for that time.

You can schedule an event to go

- from a Normal to an unlocked state at the beginning of the time period and from unlocked back to Normal at the end of the time period.
- or
- from an unlocked to a Normal state at the beginning of the time period and from Normal to unlocked at the end of the period.

For example, if you are booking a meeting in a room, you would want the door to be unlocked at the beginning, stay unlocked during the meeting and then revert to Normal when the meeting is over.

On the other hand, you might want a certain area to be inaccessible because it is being renovated, for example, so the doors would switch from unlocked to Normal (needing some kind of programmed access) and remain Normal for the duration of the period.

Here are examples of the two choices:

Hour	Unlock-Normal
03:00:00	
04:00:00	
05:00:00	
06:00:00	
07:00:00	
08:00:00	
09:00:00	
10:00:00	UNLOCKED
11:00:00	BOOKED
12:00:00	BOOKED
13:00:00	BOOKED
14:00:00	BOOKED
15:00:00	NORMAL
16:00:00	

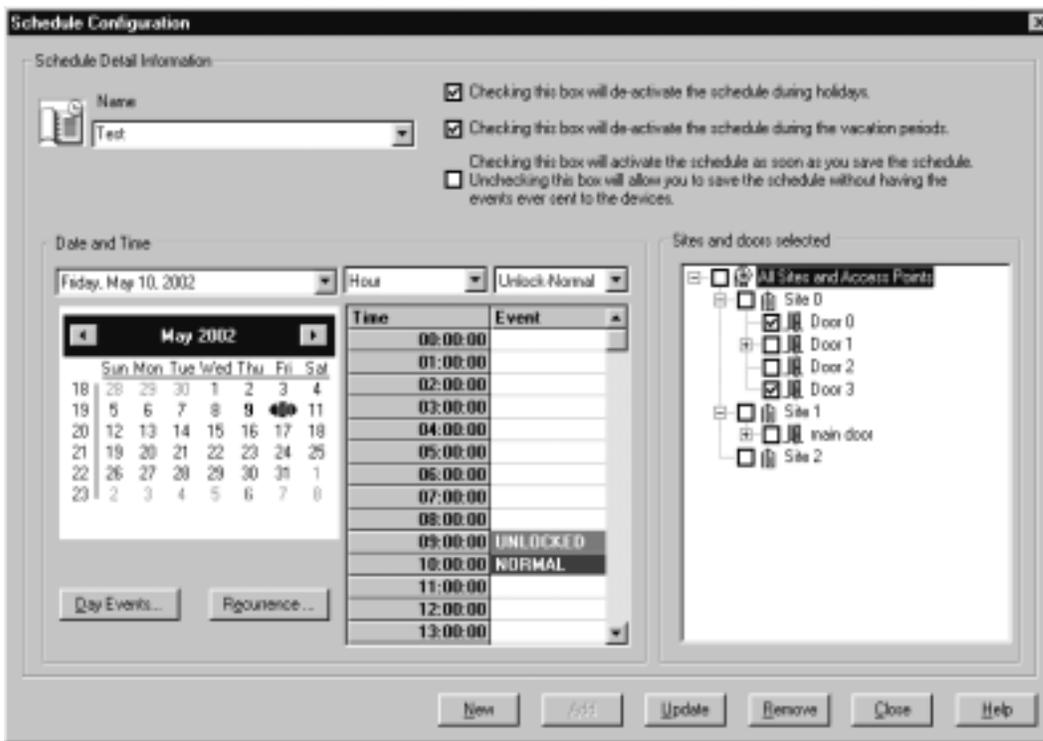
Hour	Normal-Unlock
05:00:00	
06:00:00	
07:00:00	
08:00:00	
09:00:00	
10:00:00	NORMAL
11:00:00	BOOKED
12:00:00	BOOKED
13:00:00	BOOKED
14:00:00	BOOKED
15:00:00	UNLOCKED
16:00:00	
17:00:00	
18:00:00	

**NOTE:** If there is a block of time reserved, for example from 10:00 to 15:00 as in the schedule above and you change the mode from Unlocked-Normal to Normal-Unlocked, the planned event schedule will reverse itself, as shown in the two examples above. If you choose different times, the scheduled planned event will disappear. What if you do one of these two actions and then change your mind? If you haven't already clicked on the  button, you can close the dialog box, re-open it and the old schedule will re-appear.

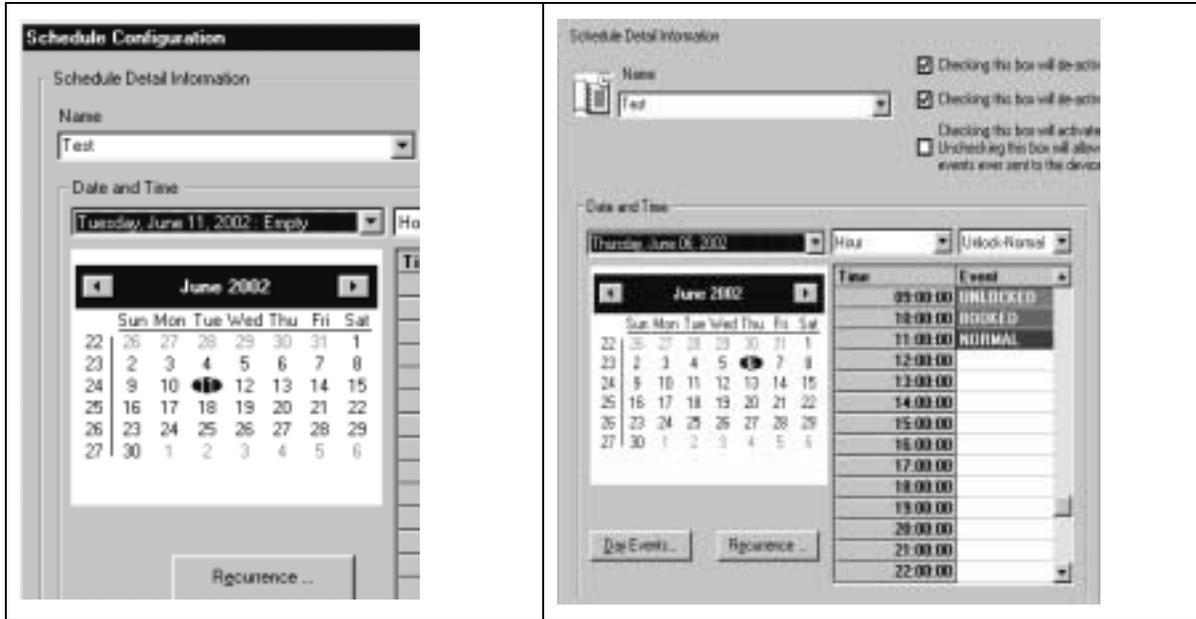
### How can I create a new schedule?



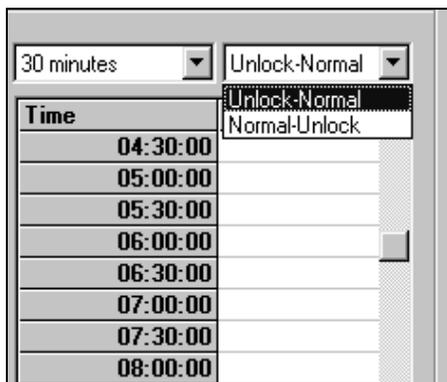
1. Click on the Schedule button on the Millenium toolbar
2. The main window appears, showing the current date highlighted.



The date will show as Empty if there is no schedule for that day. - picture at below left). If there is already a schedule applicable to that day (**Test** on the example below) the times booked on the schedule will be displayed, along with the normal/unlocked start/end for the access point See the example below at the right.

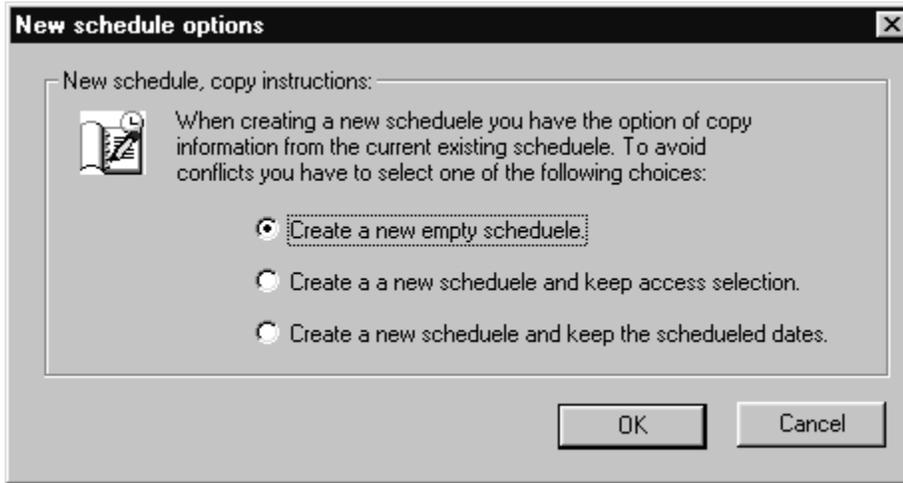


3. Select the unit of time that you want to use for the access areas to be open/closed. Since **Hour** is the most often used, it is the default.
4. If you change the unit the blocks of time shown on the schedule change, as shown below, and any selections you have already made will be cleared and you have to re-book the times in half-hour periods.



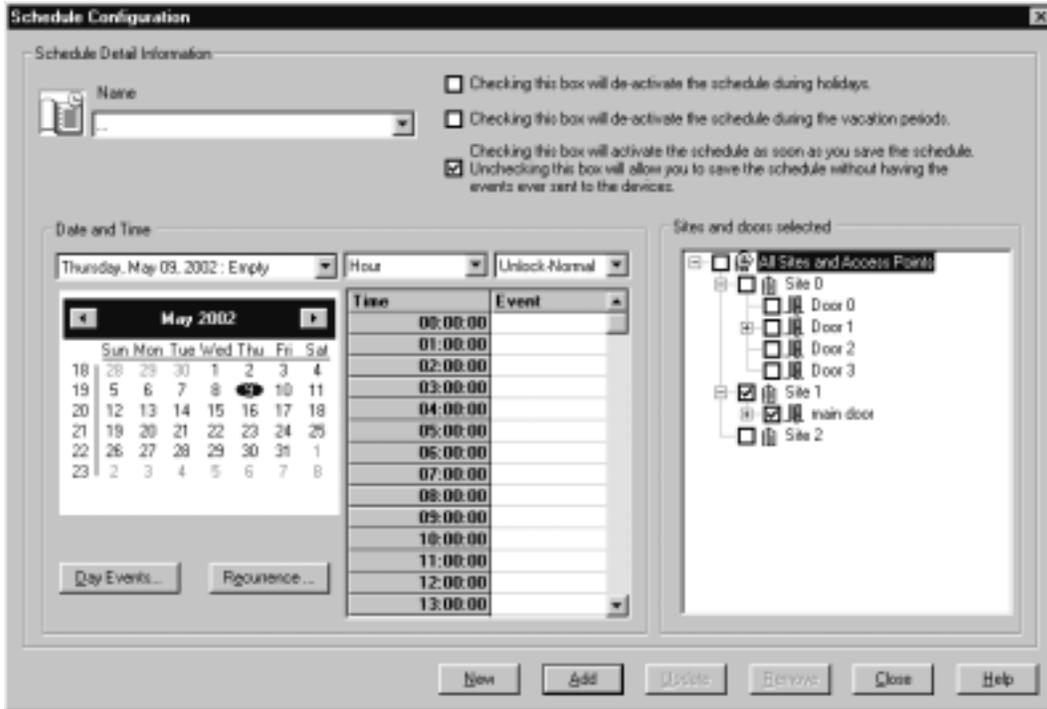
5. Select whether you will change the time period from **Normal** (whatever the normal state of the door is, for example, needing a keycard to enter ) to **Unlocked** (meaning the door can be entered by just turning the handle, pushing the elevator button, etc.) or the other way around.
6. Click on **New**. This will clear all the fields for the schedule you were looking at and give you a chance to enter the name of the New schedule.

7. Because you can create a brand new schedule or copy an existing schedule for either the times or the locations, you will see the following prompt:



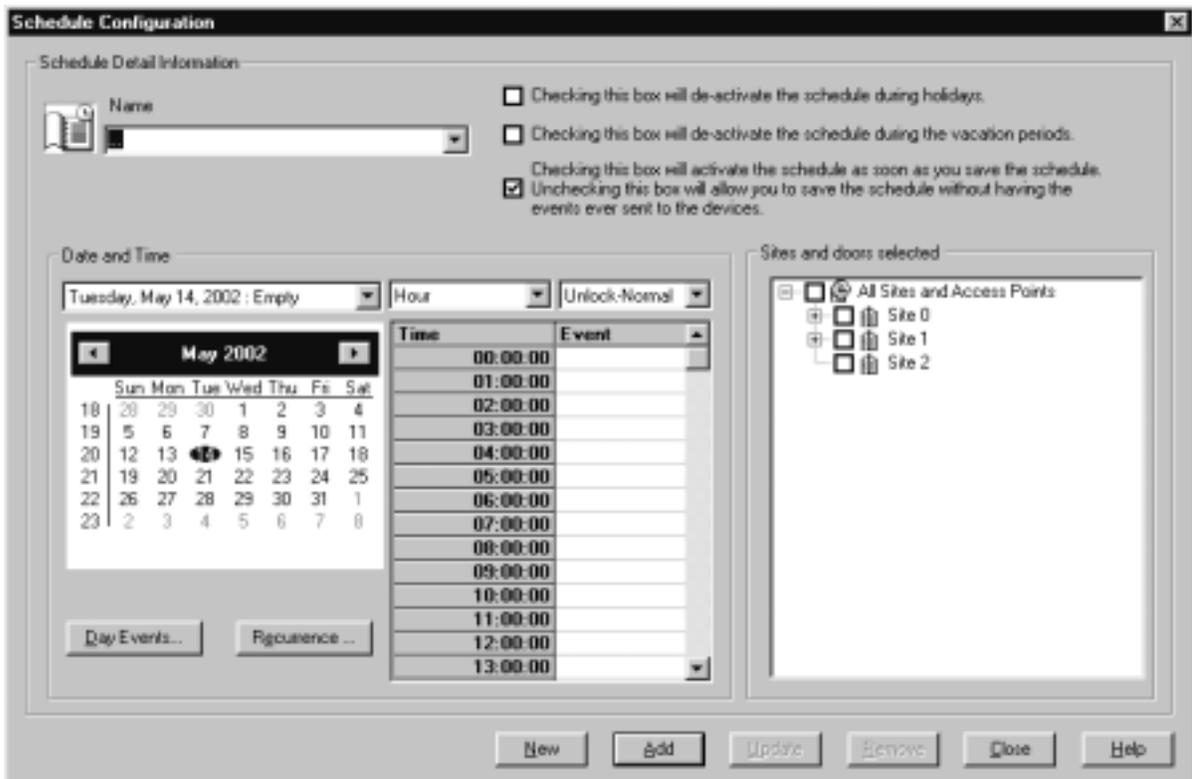
- If you want to copy an existing schedule that is recurring, the dialog box will appear in Recurring mode.
- If you want to copy a schedule selected by choosing calendar dates, the dialog box will appear in calendar mode. See Scheduler- Copy an Existing Schedule.
- If you select the first option, the name field becomes blank and the dialog box is in Calendar mode, as shown below.

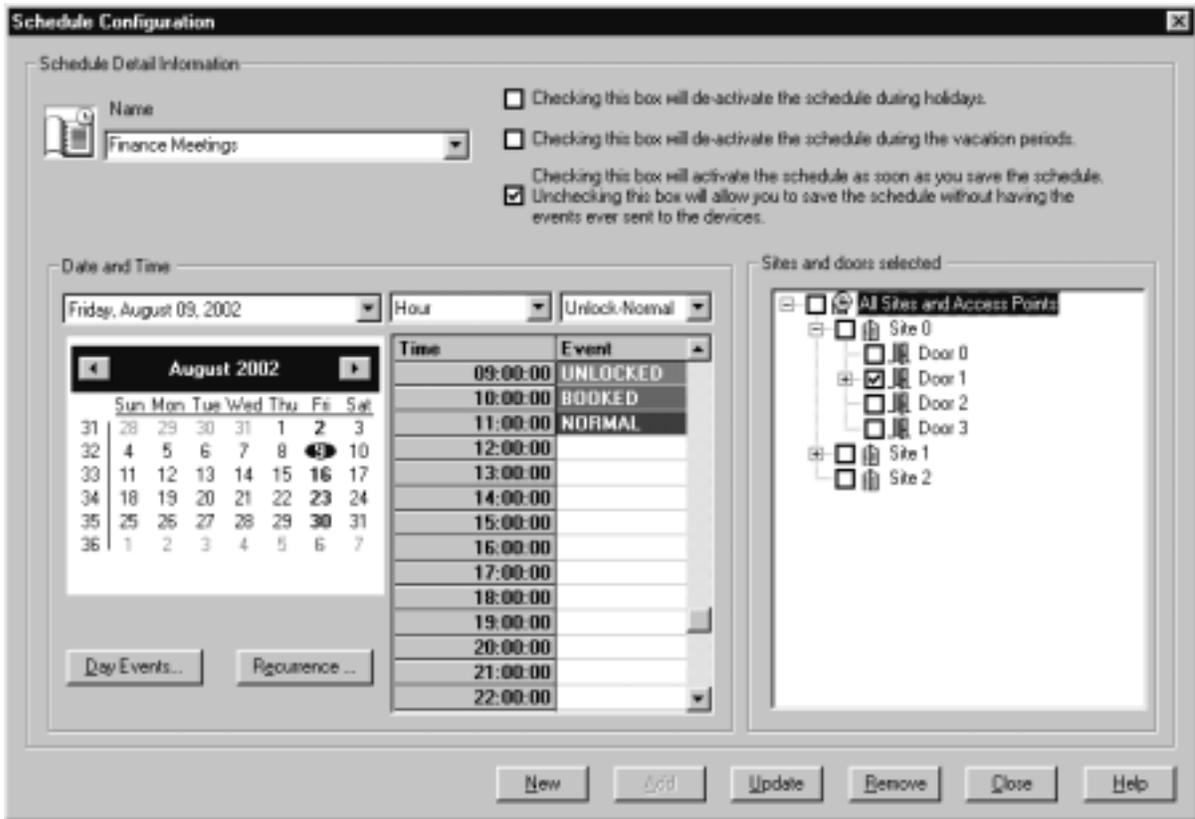
Notice that the **Update** button is grayed out and the **Add** button goes from grayed-out to active.



8. Enter the name of the schedule, for example, Finance Meetings.

9. When you have named the schedule, click on .





10. Select dates from the calendar to add to this schedule, using the forward and backward arrows to move through the months of the calendar. If you pass December, the calendar will continue to the next year.
11. If you make a mistake in the date or time period you want to add, just double-click again on the beginning and end of the time period of the relevant date and that time period will become empty again.

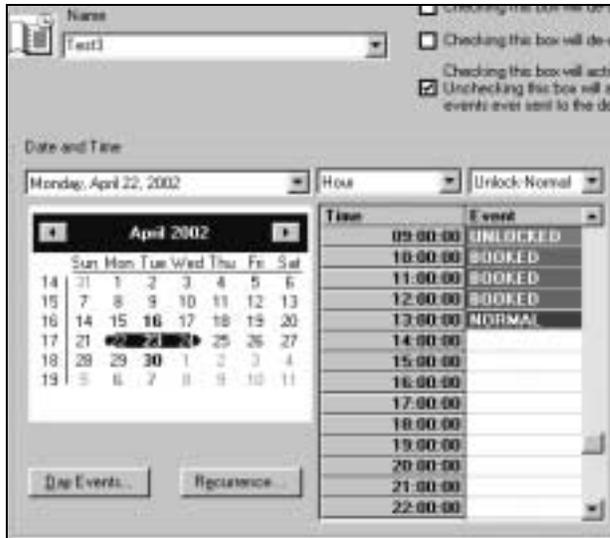
Warning: Do not use the **Remove** button; if you do, it will delete the entire schedule.

12. Dates that now have events on this schedule **appear in bold on the calendar.**
13. You can select multiple dates by clicking on the first date and dragging over to the end date of where you want the schedule to apply. **You can only drag the cursor for up to seven days, including weekends.**

***Important***

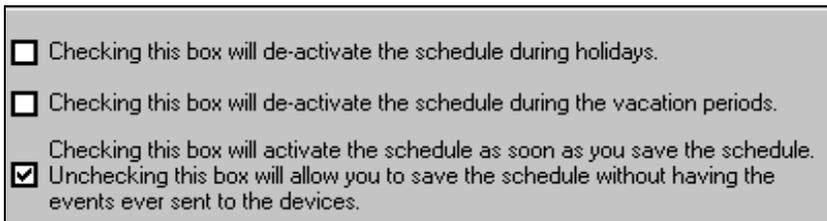
If you drag the cursor over Saturday and /or Sunday the doors will be unlocked for those times. **Be sure you do not do this by mistake.**

The example below shows that you have booked the same times for April 22, 23 and 24 by dragging the cursor across. Go to April 24th to check and you should see the same period of 9:00 to 13:00 booked on the Test3 schedule.



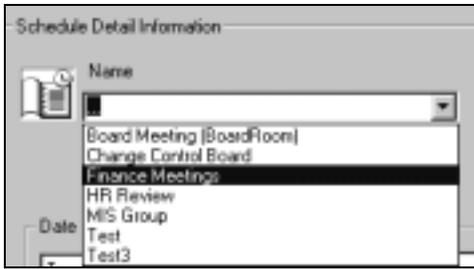
14. **BEFORE SAVING THE SCHEDULE**, read the three options at the top right of the dialog box. Decide whether you want to

- **de-activate** the schedule during Holidays and/or company-wide vacations. (This is a good idea because it prevents the doors from automatically unlocking when there is nobody in the building).
- **activate** the schedule immediately by sending the data to the doors now or
- **save** the schedule in the Millenium Scheduler memory but activate it later. (this would be done by selecting the schedule name, checking in the "activate" box and then clicking  )

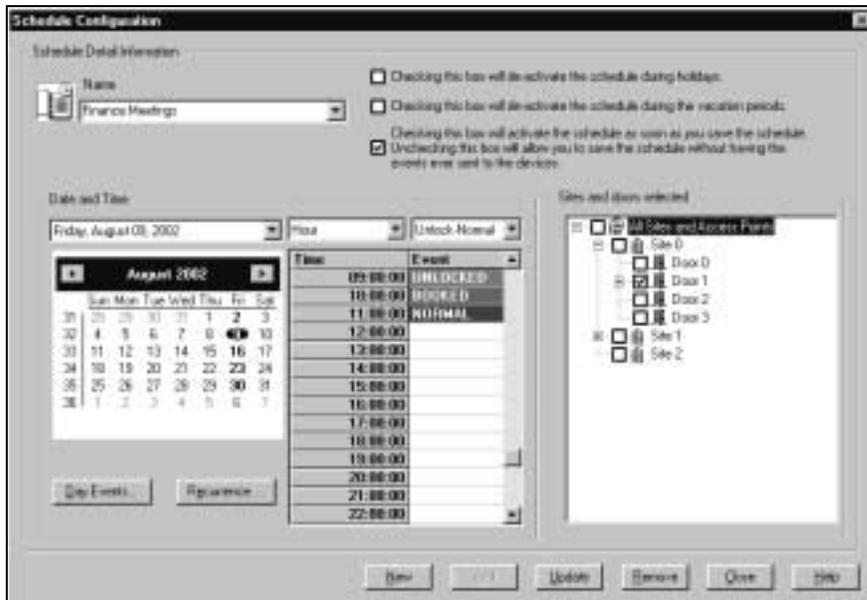
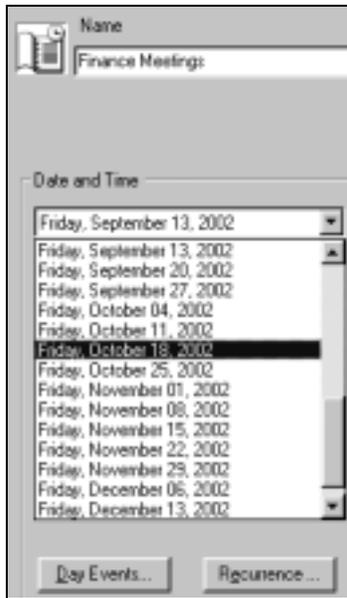


15. When the schedule is completed, click on  .  
All the dates you selected will be saved under the name of that schedule.

16. The next time you open the schedule window, check that the schedule you created, Finance Meetings, in the example, is one of the Schedules in the dropdown listbox, as shown below.



17. Check that all the dates and times you have booked for the schedule called Finance Meetings are present in the dropdown Date and Time listbox.

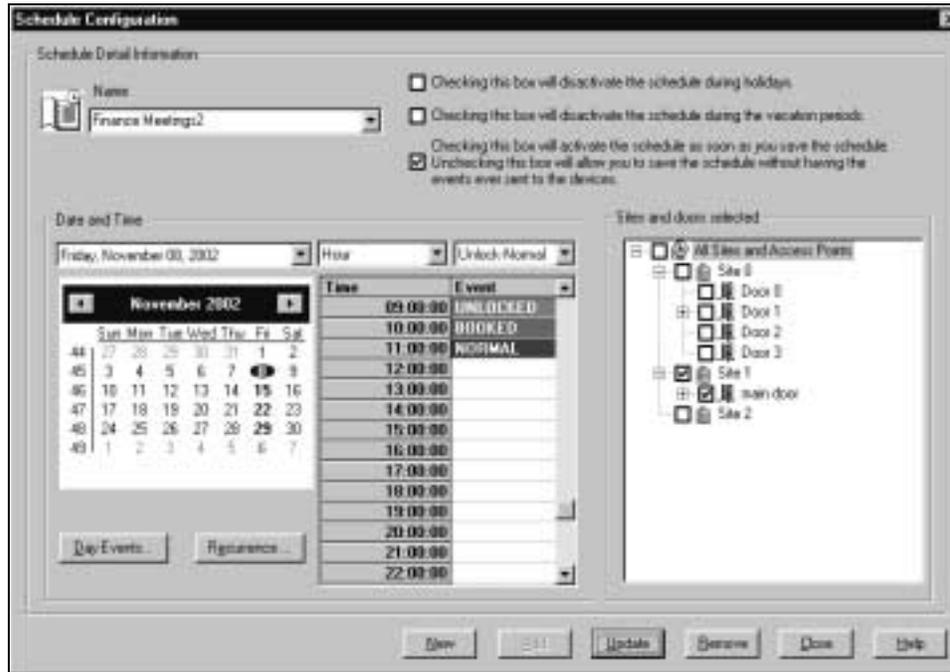


In a schedule, the system keeps the **same access point/s** ( in the example, Site 0, Door 1) throughout all the configured dates.

## How can I schedule the same event but in a different location?

1. You must create a different schedule for a different set of access points.

For example, if you know that in November and December of 2002 the Finance Meeting must take place at Site 1 because Site 0 is being used for something else, create a Schedule called Finance Meetings2 or Finance Meetings Nov/Dec and assign the same schedule (9:00 to 11:00) but in Site 1, Main Door as shown below.

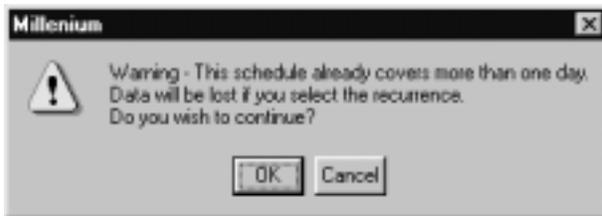


2. Continue adding dates to Finance Meetings2 as long as you need for the access point at Site 1, main door.
3. If the access points for the schedule Finance Meetings become available again, return to Finance Meetings and add more dates if you wish.
4. See **Copy an Existing Schedule** if you need to create an identical schedule in terms of dates but using another location for the events.

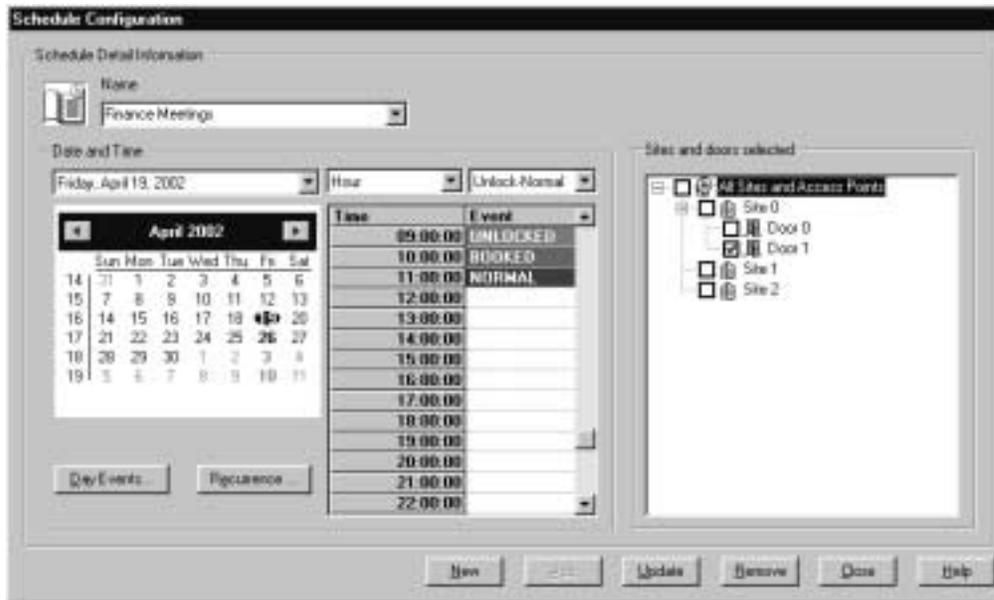
You may want to open certain access points for an event that occurs on a regular basis, such as a meeting. If you have a Finance meeting in a certain room every week you can arrange for that room to unlock at the start of the meeting time. Recurrences can be daily, weekly, monthly or even yearly. You can end the recurring unlock/lock event after a certain number of occurrences, a certain period of time, or leave it open to recur indefinitely.

## How can I schedule a recurring event?

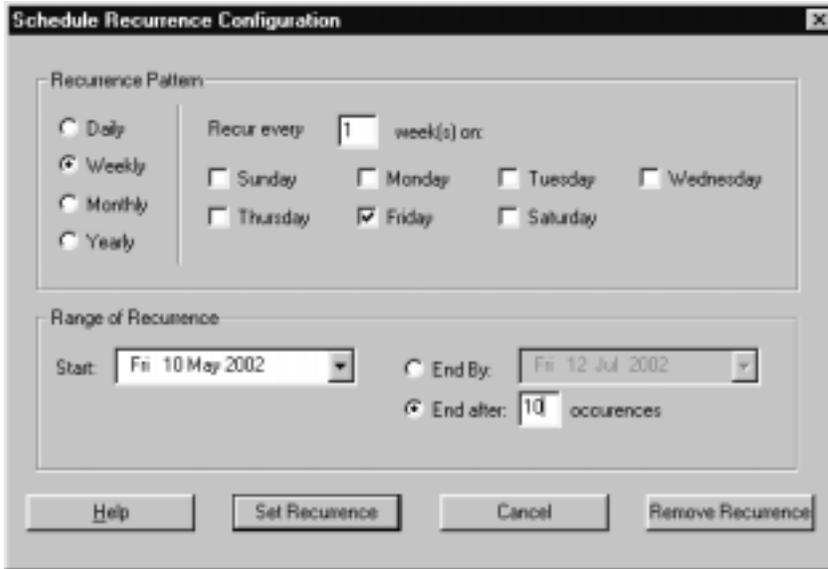
1. Click on the schedule button  to open the main window.
2. Select or create the schedule you want to change to recurring (Finance Meetings in the example below)
3. Click on Update to save it if it is a new schedule.
4. Click on the  button.
5. If you have already entered more than one date for this schedule and then decide to make it recurring, you will see this message



If you switch to Recurring mode, only the first date you entered will be kept and used as the recurring date. A schedule is either selected manually on the calendar or set as recurring from one particular date and time, not multiple dates. This prevents such possible errors as, for example, having selected two days and then trying to make a recurrence everyday.

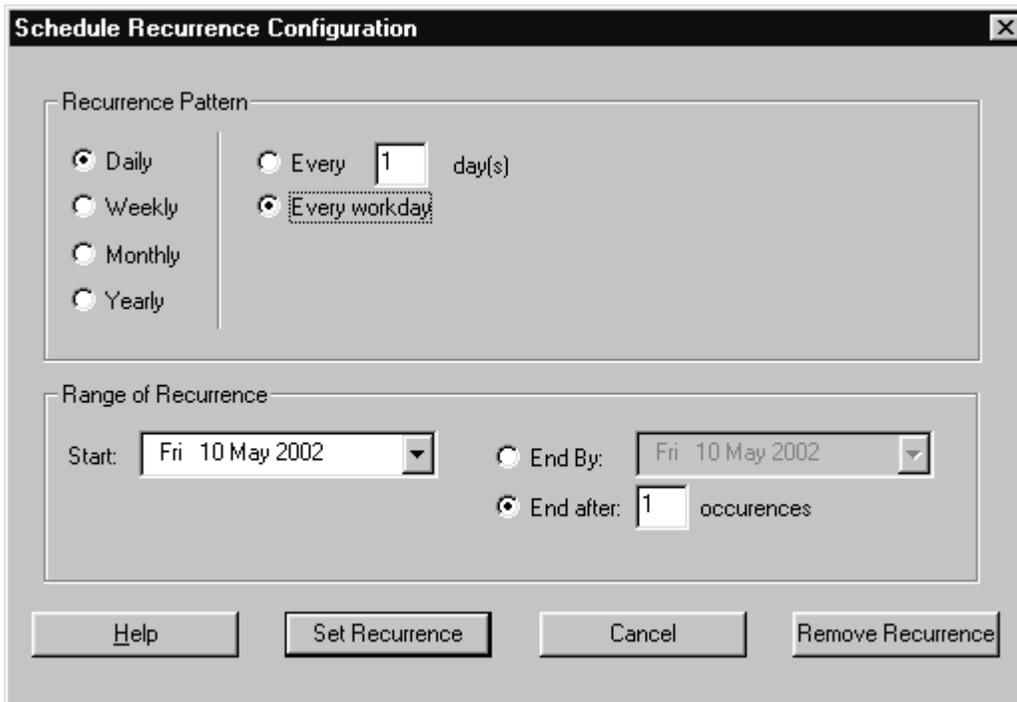


The following dialog box appears.



6. Select the recurrence pattern in the top part of the dialog box.

**NOTE:** If you select Daily, Remember the difference between selecting Every day and Every workday - if you select Every workday, the events will not occur on weekends, only Monday to Friday.



The selections you can make will change depending on which Recurrence Pattern you choose, as in the examples below.

**Schedule Recurrence Configuration** [X]

Recurrence Pattern

Daily      Recur every  week(s) on:
   
 Weekly       Sunday       Monday       Tuesday       Wednesday
   
 Monthly       Thursday       Friday       Saturday
   
 Yearly

Range of Recurrence

Start: 
    
  End By: 
    
  End after:  occurrences

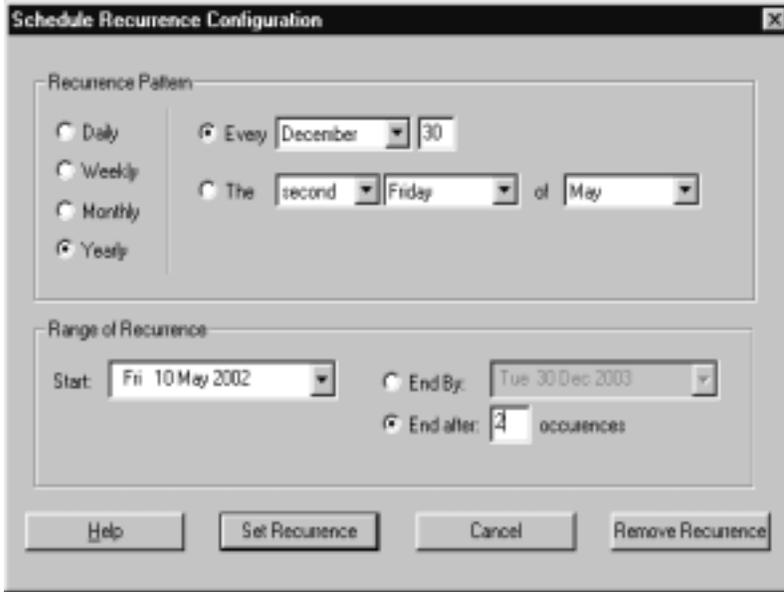
**Schedule Recurrence Configuration** [X]

Recurrence Pattern

Daily       Day  of every  month(s)
   
 Weekly       The   of every  month(s)
   
 Monthly
   
 Yearly

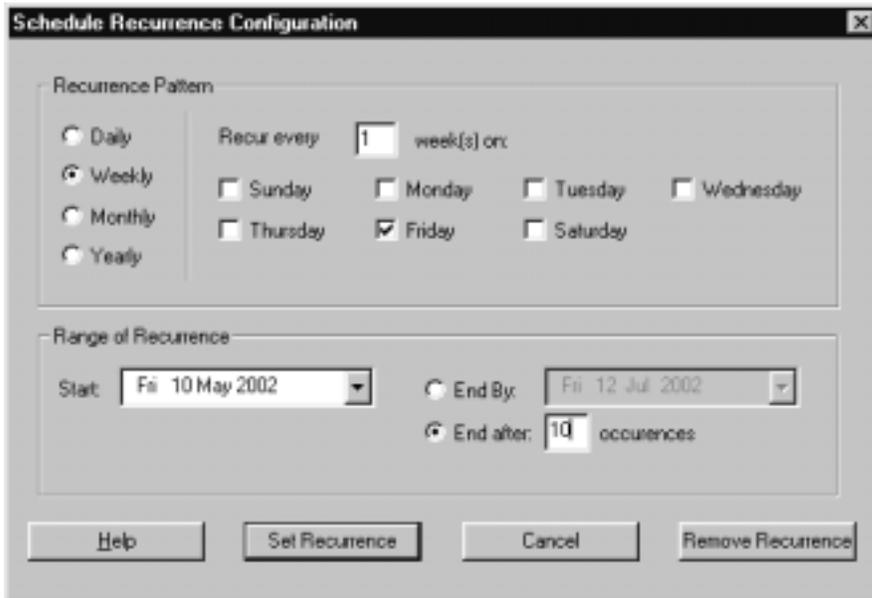
Range of Recurrence

Start: 
    
  End By: 
    
  End after:  occurrences

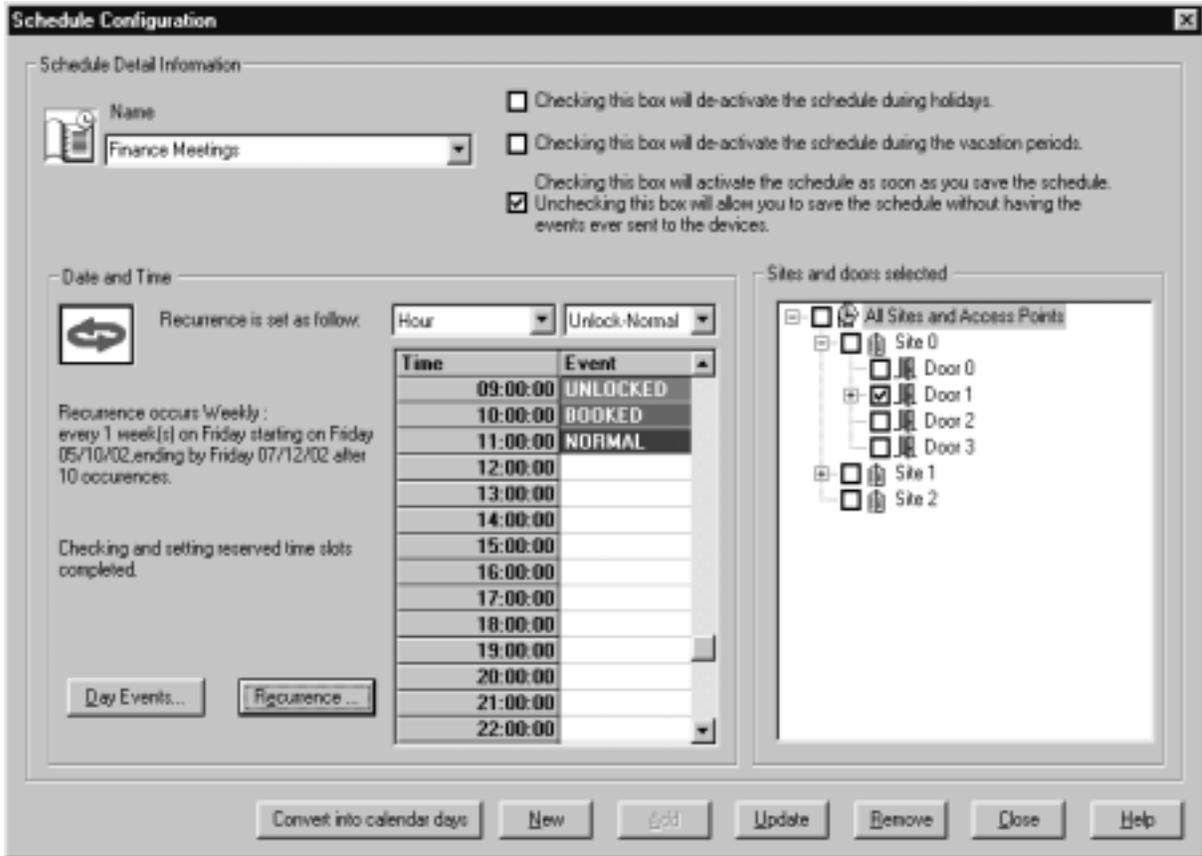


In the example with Finance Meetings shown below, we have selected Weekly, with the day of Friday and a start date of May 10/2002 and an ending after 10 occurrences.

If you select start and end dates, the number of occurrences will fill in automatically.



7. Click on Set Recurrence, and the following screen will appear.



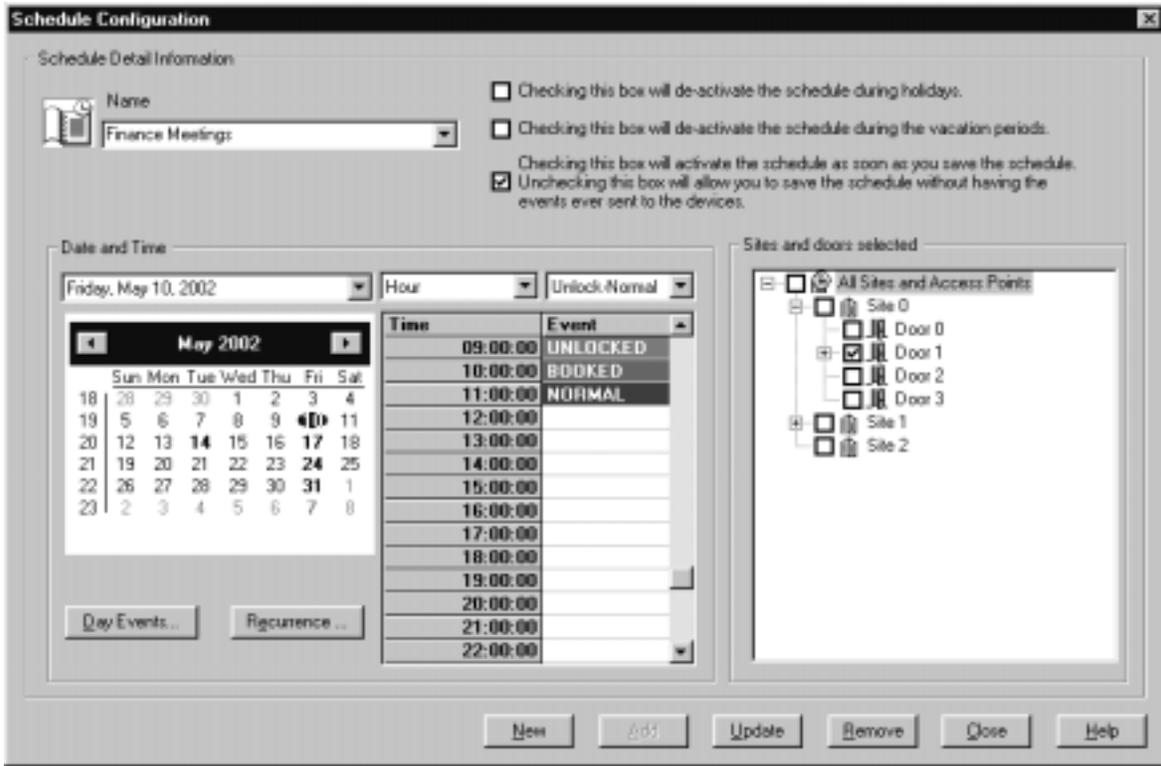
8. The software calculates the dates of all recurrences and then confirms your selection, describing the recurrences and telling you that your reserved time slots are completed.

9. Click on

10. To return to the calendar view click on the

**IMPORTANT:** When you do this, you lose your schedule as a recurring event. It returns to a being a schedule determined by choice of calendar dates. So, if you want to make further changes to this schedule, do so by selecting calendar dates.

After you click on the  button, The main screen re-appears as below:



If you page ahead using the , you will see that every Friday appears in bold because it is reserved for the weekly Finance meeting, as in this example:

June 2002							
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
22	26	27	28	29	30	31	1
23	2	3	4	5	6	<b>7</b>	8
24	9		11	12	13	<b>14</b>	15
25	16	17	18	19	20	<b>21</b>	22
26	23	24	25	26	27	<b>28</b>	29
27	30	1	2	3	4	5	6

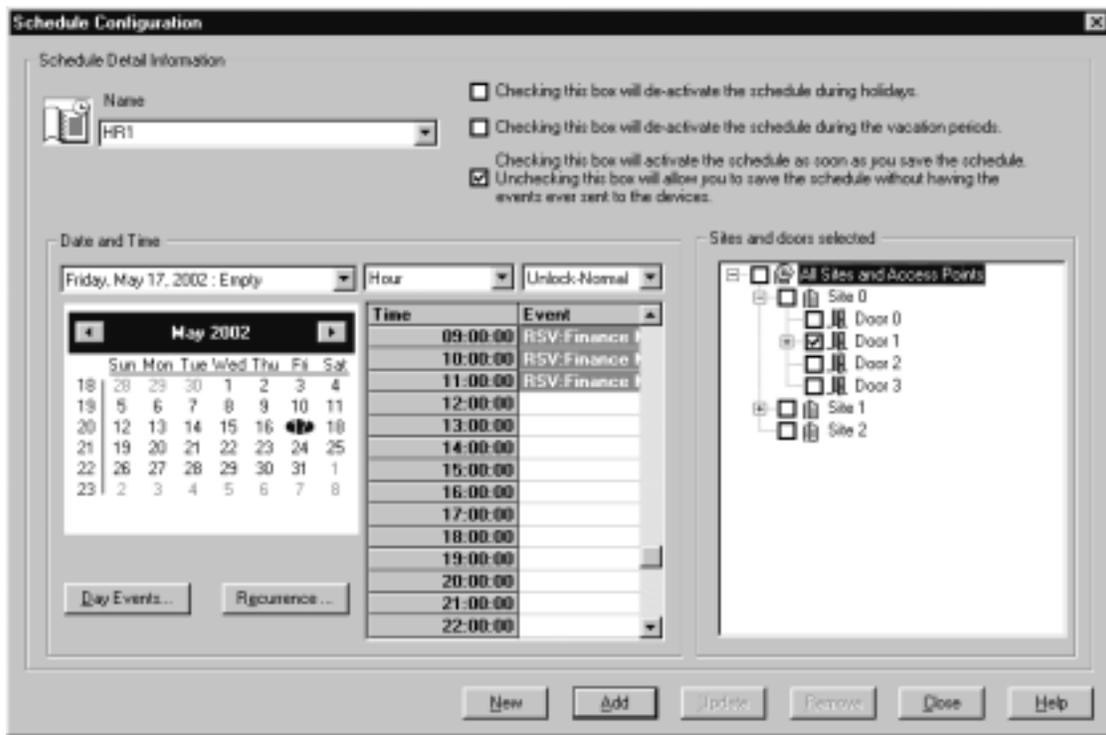
If you create another schedule that conflicts with any of your dates, you will see immediately when the date pops up that there is a conflict.

## Schedule Conflicts

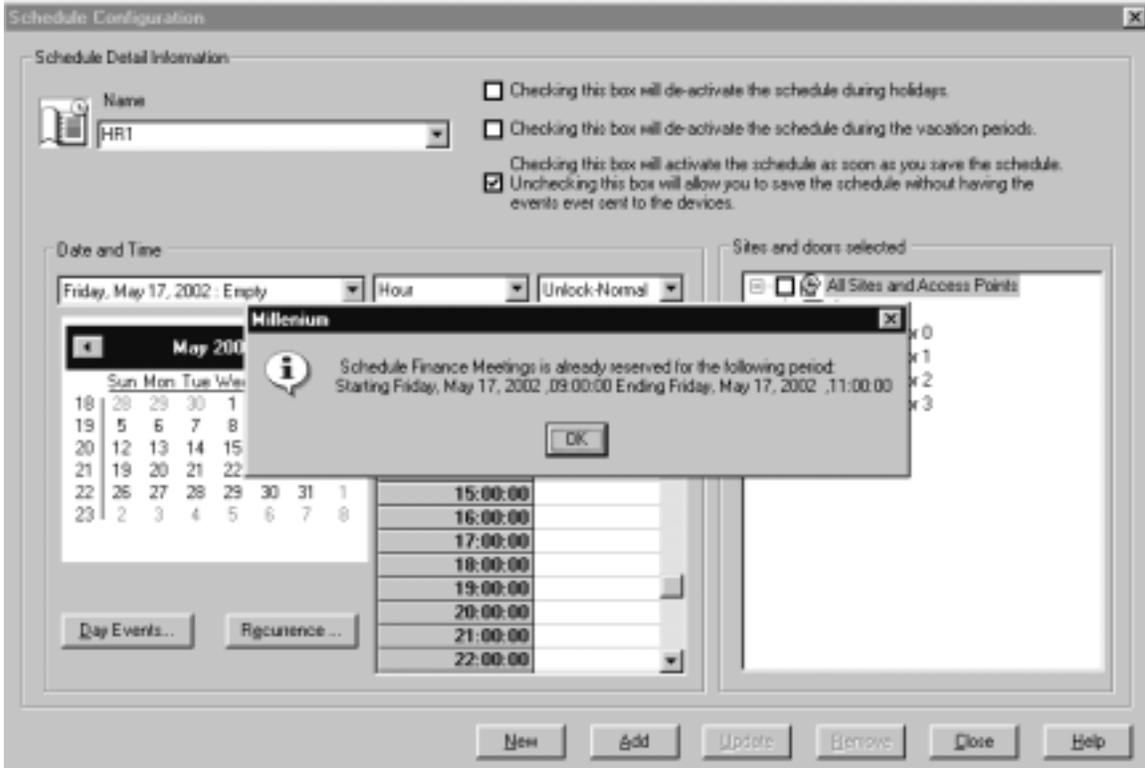
Suppose you have decided to create a schedule called HR1 that involves planning a meeting in Room 1 of Site 0 from 9:00 to 11:00 every Tuesday morning. When you get to May 17th, there is already an event booked for that room for all or part of that time.

The room will show as **RESERVED**, thus preventing you from scheduling conflicts. If you click on RESERVED, you will receive a popup message informing you that there is a conflict and providing the name of the conflicting schedule and the times involved. In the example below, the MIS Group Scheduled meeting conflicts with the Test3 schedule in that room by only one hour (9:00 to 10:00) but there is still a conflict. You must then change the room, the time, or the duration of the meeting if you want to have it on that day.

The examples are shown below:

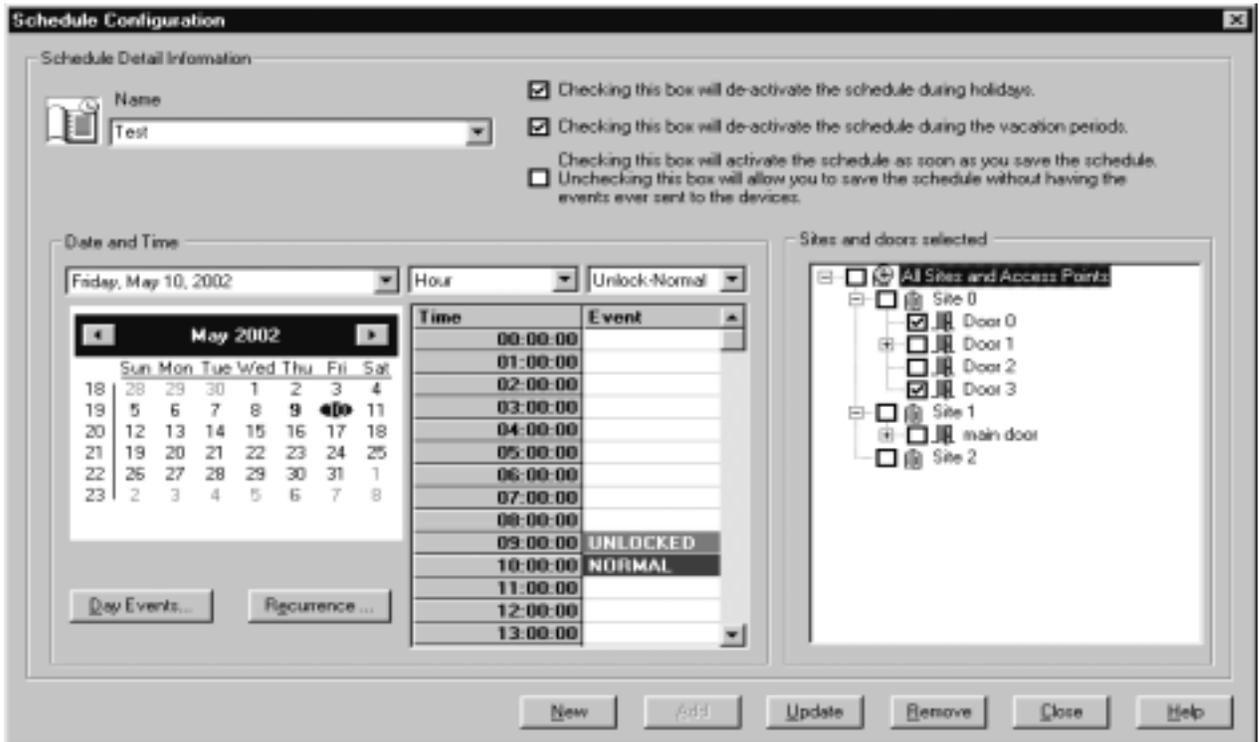


If you right-click on one of the Reserved periods, the Scheduler will tell you which schedule has booked that room at that time. If you prefer, you can then change that other schedule instead of the one you are creating now.

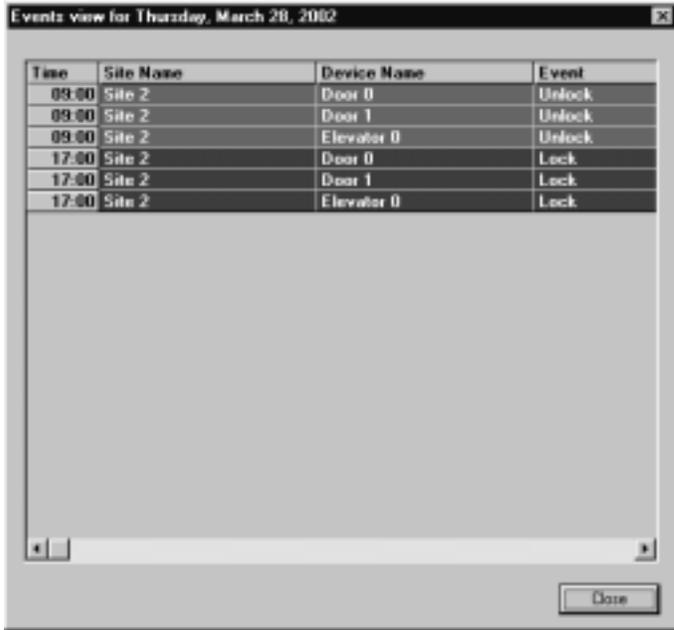


## View Daily Events

To view all scheduled events for the day, click on the **Today's Events** button at lower left.



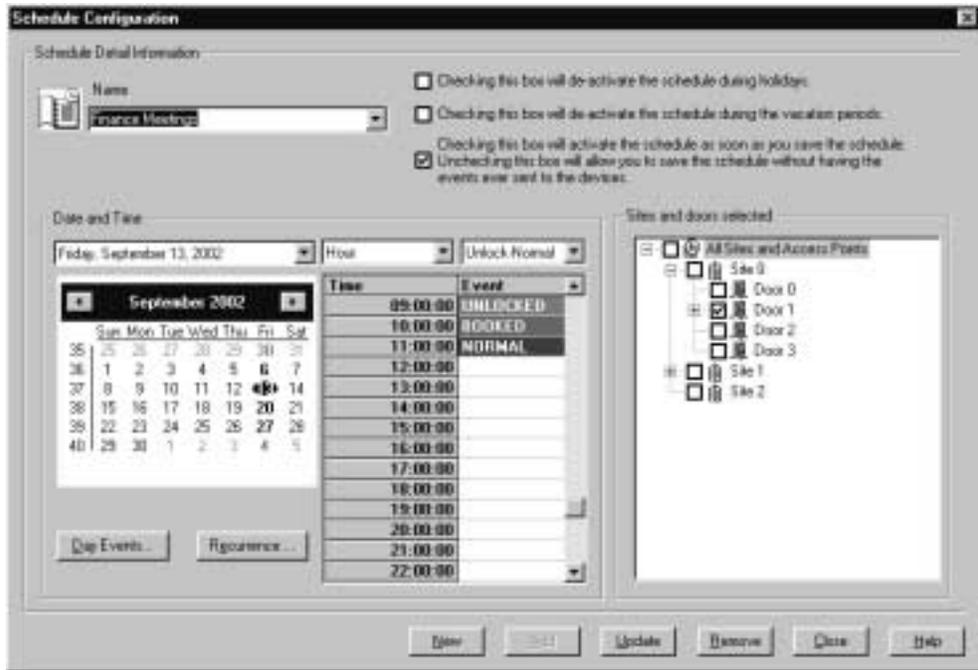
The day with all events scheduled appears



Viewing the scheduled day is a good tool to use when you are creating a schedule and want to avoid conflicts.

**How do I delete a schedule from the system?**

1. Click on the Schedule button on the Millenium toolbar .
2. The main window appears, showing the current date and time:



3. Select the schedule you want to delete by selecting the name from the dropdown list,
4. Click on the **Remove** button and the schedule disappears. All the dates and times booked for the Access points on that schedule are now available.

### **Important**

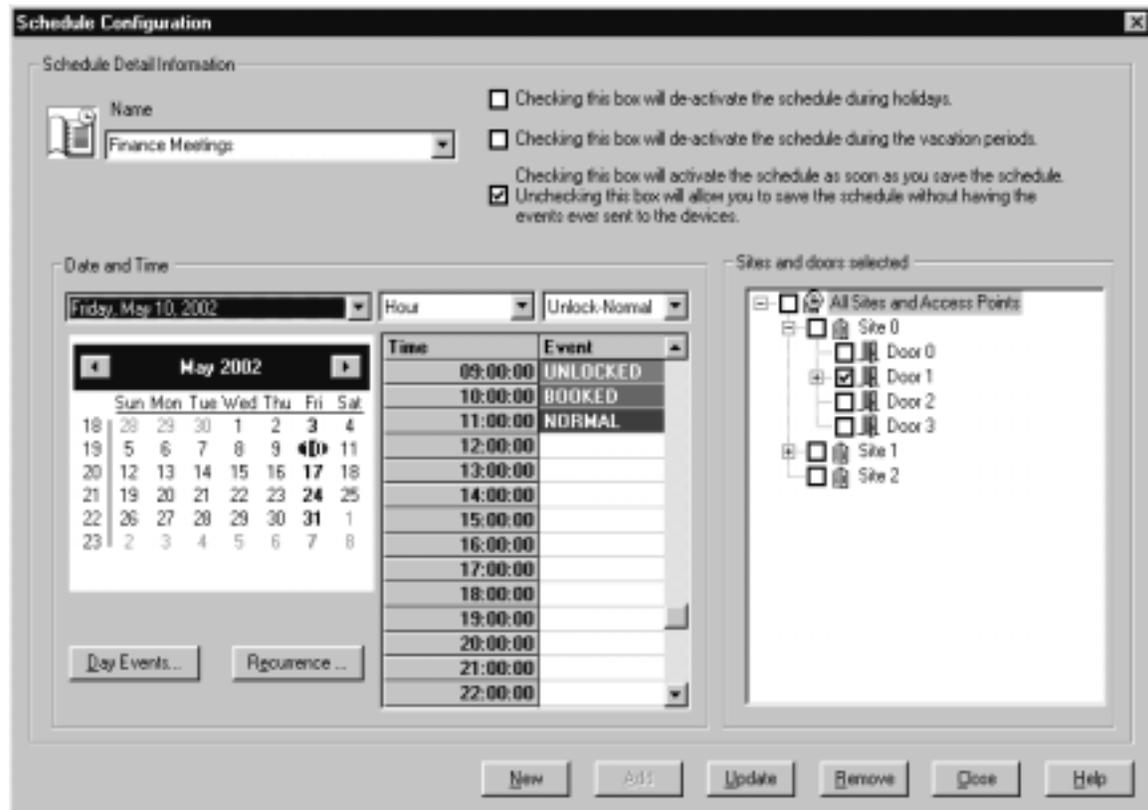
Remember that this deletes **the entire schedule** with all the dates on it. Be sure that you want to do this.

Remember that if you want to keep the schedule but not activate it yet, simply uncheck the third option checkbox at the top right of this dialog box.

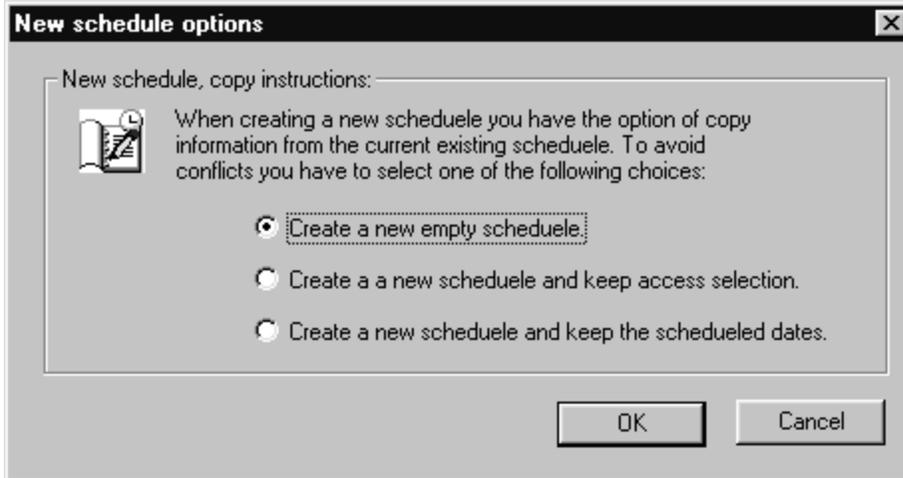
To save time, you may want to copy an existing schedule and just change the location or the dates. For example, if you have a Finance Meeting every Friday from 9:00 to 11:00 and you decide to schedule a Sales Meeting for the same day and time (every Friday from 9:00 to 11:00) but in a different location, **OR** you want to schedule the Sales meeting every Friday in the same room but at a different time.

### **How can I duplicate an existing schedule?**

1. Select an existing schedule that has the dates/times closest to the new schedule you want to create. In the example below, we have selected Finance Meetings.

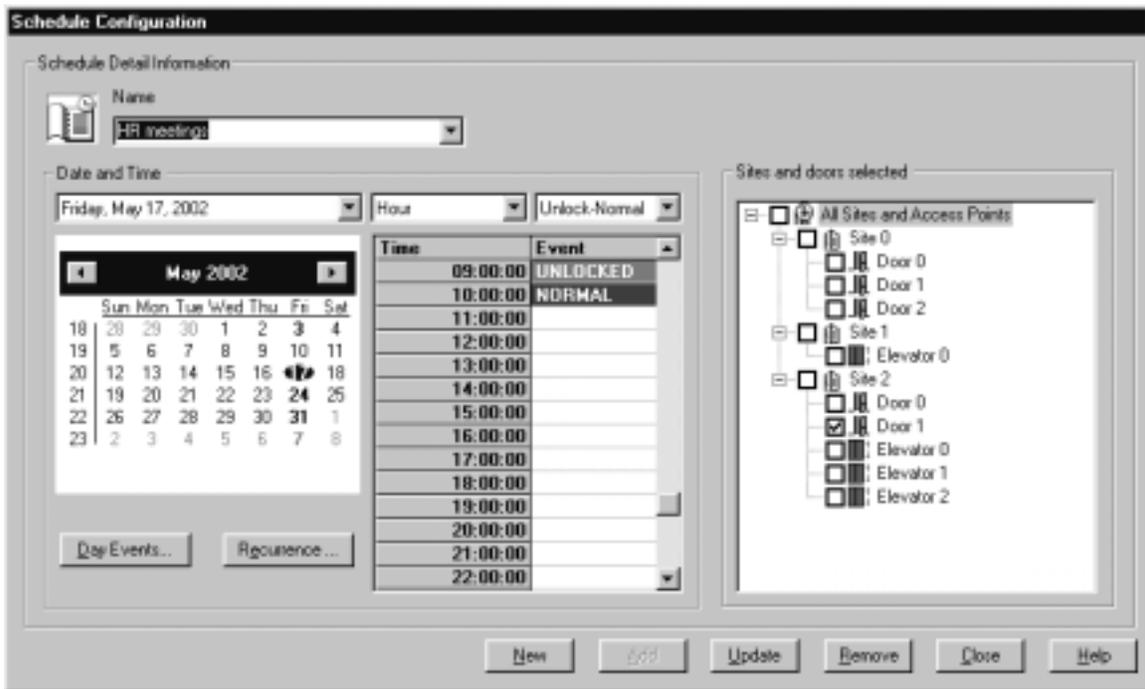
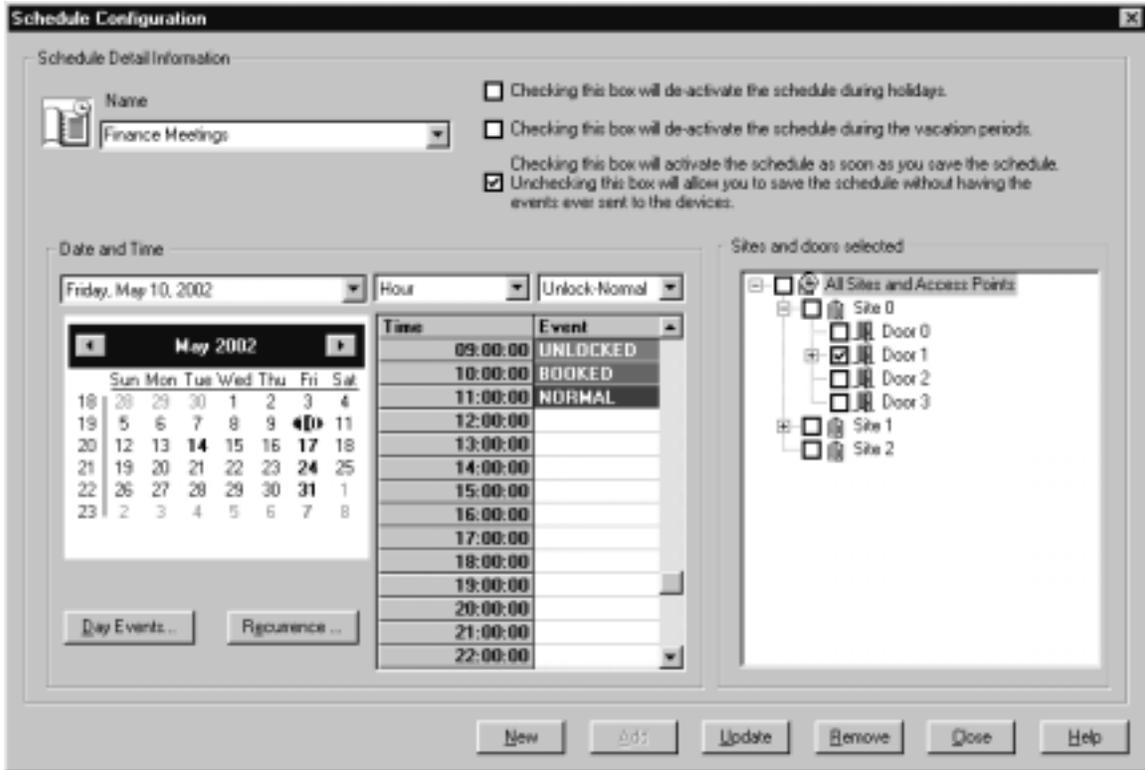


2. Click on **New** and you will see the following prompt:



3. Select the second or third options.
4. Select the schedule with the access points or dates/times you want to copy.
5. Change the name of the schedule.
6. Click on .
7. You now have another schedule that is a duplicate of the original except that the events take place in another location/s.

In the example below, we have taken the schedule called Finance, changed the room from Site 0, Door 1 to Site 2, door 1 and re-named it HR Meetings. Now all the HR meetings will take place at the same times and dates as the Finance meetings but in a different room.



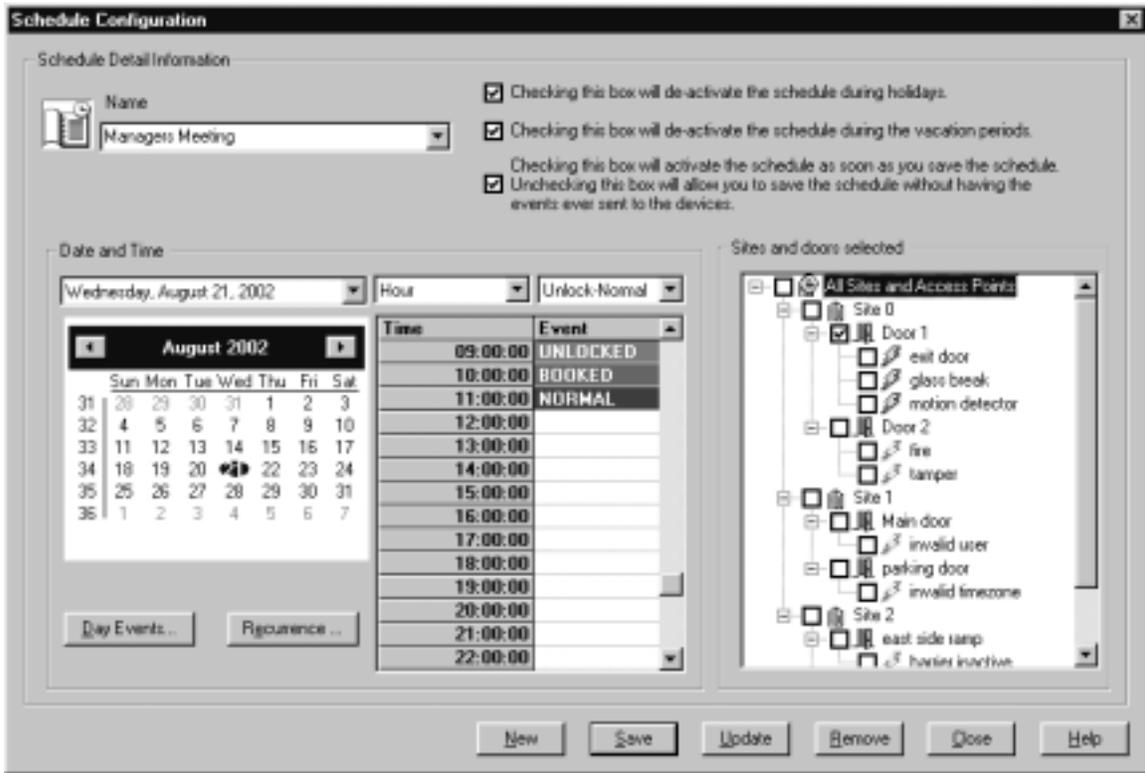
You now have another schedule that is a duplicate of the original except the events take place in another location/s.

# ALARM SHUNTING

**WARNING - Alarms connected to a door control device may or may not be associated with the access point. Shunting alarms without knowing their impact can cause a serious breach of security. Only shunt an alarm if it is known that it is affected by the access point being unlocked- a motion detector input, for example.**

Normally, unlocking a door with an alarm would trigger that alarm. Since Millenium scheduler involves remotely locking and unlocking doors through software configuration, you must make sure to turn off the alarms at the access point for those scheduled events.

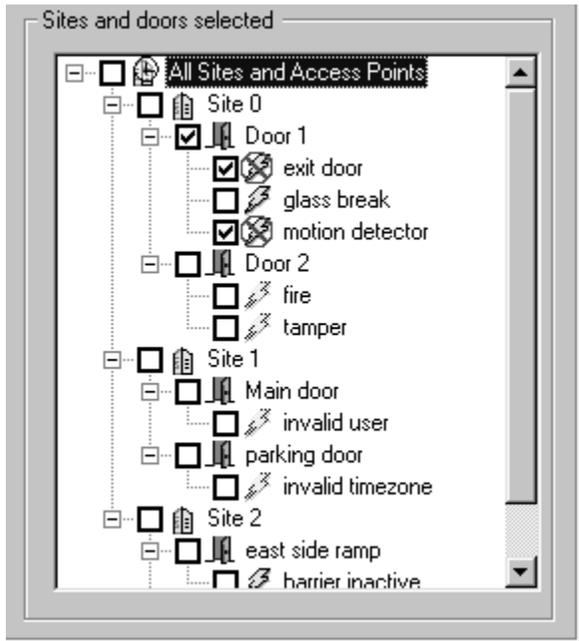
When you create a schedule involving doors with alarms, like the one pictured below, the doors that have alarms are graphically illustrated. Site #0, Door #2, for example, has three alarms - Exit Door, Glass Break and Motion Detector. You could shunt Exit Door and Motion Detector and so that no alarm would occur as people enter and exit the meeting. However, since Glass Break is an alarm that would not be affected by using the door, there is no need to shunt the alarm. Leave it active.



## How do I shunt alarms on access points for scheduled events?

1. Click on each alarm, and you de-activate it for the dates and time periods on the schedule, "Managers Meeting" in the example shown above.

2. The "alarm shunted" symbol  appears as shown below:



3. The alarm is automatically shunted (de-activated) for those periods. Therefore, it is extremely important to remember the following:
- If you cancel a meeting for one particular day, inform the responsible scheduler so he/she can delete the meeting for that day, thus locking the door again and re-activating the alarm.
  - Ensure that you have selected to de-activate the schedule (second checkbox at the top right of the dialog box above) during vacations and holidays, so that the alarm will be active if a triggering event occurs.



# Chapter 17: Reports

The picture below shows the **REPORTS** menu dialog in Millenium Expert Systems.



**To print Standard reports**, (including the Site and Device **Maps**) move the cursor to highlight one of the reports in the Standard (or Maps) listbox. Standard reports are basic lists of data.

**To print Advanced reports**, you must first make selections that determine just what History or User data you want to include on the given report.

A printer icon at the top of the preview dialog lets you send the report to the designated printer.

**Standard Reports:** Millenium Expert Systems comes with standard reports that give you a printout of data programmed into the system. For example, you can print a report on Timezones or Operators or Holidays established in the software. If you use the Tour module, you can print a list of programmed tours.

**Advanced Reports: User, History, Alarm--Incident, User Dossier, and History of Tours** reports (including archive reports for access control history and alarm activity, if applicable\*\*) involve a two-step process.

- First, the operator uses selection criteria to set up report options.
- Then the report displays on the screen and prints if you click the printer icon.

History is an audit trail of all Millenium activity.

- This history audit trail includes both access point activity and computer operator actions.
- When Millenium Expert Systems is *not* running, the audit trail of history continues to accumulate in the firmware (circuit board) of the access control device.
- For DIRECT (online) systems, history becomes part of software history the next time the computer runs the Millenium Expert Systems program. History automatically saves on the PC.
- For DIAL-UP systems, access control device history becomes part of software history the next time the site  **Download History from Site** action occurs.

Archived History lets you print a report of those history files you have archived through the **Millenium Database Utility**.

**(\*\*NOTE:** You must have run an archive and created archive files in order to see reports appear in the listbox. If you haven't created archive files, the listbox will be empty) The procedure for doing this is in the *Millenium Expert Systems Database Utility* in the on-line help and is also documented in the *Millenium Expert Systems Quick Reference Manual (PK2778)*.

- Alarm Monitor: Incident reports show all activity through the ALARM MONITOR on alarm events triggered from Millenium access control devices. Incidents are operator comments on any suspicious activity that is NOT related to alarms. Archived Alarm History report lets you print a report of those alarm and incident records you have archived through the Millenium Database Utility.
- User reports can be printed by selection criteria such as—by Access Point or by Access Group.
- User Dossier report prints an image of one user along with options to print all or some of Millenium Expert Systems' data on that user. Requires an image captured through the Millenium Expert Systems BADGE add-on. You have an option to print on-the-fly notes for the given user.
- History of Tours report prints activity for the optional Millenium Expert Systems TOUR module.

**Custom Reports:** If you have Crystal Reports™ software, you have the option to develop custom reports of Millenium Expert Systems history data. Reports come read-only to help you avoid accidentally overwriting one of the provided reports. To use an existing report, rename it before using Crystal Reports.

## Reports- Heading Toolbar

Preview and print standard reports of access control data and Millenium Expert Systems software operator actions. Reports include history of access control activity at devices installed throughout the network

Standard reports list software database information, and come ready-to-use under this toolbar button.



Examples: Timezones, Holidays, Doors, Sites, (History action) Filters, Tours, Quick User reports.

- Map reports provide a hard copy of the Site Map and Device Map available under the Map menubar.
- Advanced reports involve the operator making selection options to prepare for report generation.
- History, User, and Alarm--Incident reports require operator to make selections to determine exactly what the report should include. Access control history activity can be filtered according to such categories as sites, access points, users, operators, date/time

ranges, and more. User reports offer options such as –by access point or –by access group, plus an option to include custom user-defined fields.

- **Alarm/Incident** reports include data on triggered alarms and operator responses from the ALARM MONITOR. The Advanced listbox also includes a user **Dossier** report where a user's image (captured through the optional Millenium Badge module) displays along with selected user data. **History of Tours** report shows operator activity and/or tour checkpoint station activity for the optional Millenium Tours module.

**NOTE:** If you have created archive files of history or alarm/incident data through the Millenium Database Utility, then Advanced reports will also include options for Archived History and Archived Alarm--Incident reporting.



You can also reach the REPORTS dialog through the **View** menubar.

## Door report

- Notice the information under the some doors states:
- Relay 1 is set so strike will not activate with Request-to-Exit for this door. Alarm will be shunted.
- This note only appears when the default setting ( Allow REX to Activate Relay) is changed in the Relays dialog.
- When you remove the check ( Allow REX to Activate Relay) for specific Request-to-exit situations, the report lets you know.

## Elevator Floor Access Points report

For each programmed ECU, the report shows...

- which of the 16 possible ECU relays are programmed for access control.
- which ECU events are enabled (selected history actions to be treated as events in the Millenium Expert system,) and
- any of the four possible ECU alarm inputs that are programmed to react to a change of alarm state.

If no data is programmed, no data appears.

## Report: Alarm-Incident

The Alarm-Incident Report covers both Alarm events in the Millenium network as well as those activities recorded by the operator as "incidents."

**Alarms:** Activity from Millenium Expert Systems 'ALARM MONITOR prints through this Incident report when you select the  **Alarms** option under the TYPE section. Choose Operators, Sites, and/or Devices (Doors, RCDs) you want included in the alarm activity report.

**Incidents:** Millenium Expert Systems also enables the operator/guard on duty to record a report on an incident that occurs during the watch period. Incidents are any noteworthy activities that the operator wishes to log for the record— **other than** the alarm/event actions programmed in Millenium Expert Systems.

Activity from the Incident Report option in Millenium Expert Systems 'ALARM MONITOR prints in an Incident report when you select the **Incidents** or **Both** options under the TYPE section. The dialog where the operator records incidents is a free-form comments entry box in the Alarm Monitor. This Incident Report is a printout of those comments for the designated operator(s). Since incidents are not linked to Alarms/Events, the Sites and Devices sections will appear disabled when you only select **Incidents**.

## Tour History

The History of Tours report shows interval station activity and/or operator programming activity for all or selected tours in the Millenium Expert System Tour module. Once you've selected what you want on the History of Tours report, a report similar to the following example displays.

**NOTE:** Notice the selections options made for the individual report show across the top of the report. DELETED tours only appear if operator selects <ALL> tours in the Tour History selection dialog.

- If a station's access point has no reader assigned, no person appears in the operator/user column.
- If a user assigned to a global tour does not have a key/card for an access point in the tour, no Name/Keycard code history displays for an interval.

## Report: Date/Time Range

The screenshot shows a dialog box titled "Date/Time Range". It has two radio button options. The first option, "ALL Inclusive: (m/d/y h:m:s Thru m/d/y h:m:s)", is selected. Below it are two date and time pickers. The "Start" picker shows "May 13, 2002 06:00" and the "End" picker shows "May 27, 2002 16:00". At the bottom are "OK", "Cancel", and "Help" buttons.

Two date/range options exist in the History, Alarm/Incident, and History of Tours report selection dialogs.

### *ALL-inclusive*

Start **Time** on Start **Date**  
through  
End **Time** on End **Date**.

### *Example:*

6 a.m. on 10/01/2000 through  
23:59 p.m. on 11/01/2000

The screenshot shows the same "Date/Time Range" dialog box, but the second radio button option, "TIME Range During DATE Range (h:m - h:m ON m/d/y - m/d/y)", is selected. The "Start" picker shows "April 01, 2002 00:00" and the "End" picker shows "May 31, 2002 23:59".

### *TIME range during DATE range*

Start **Time** through End **Time**  
on  
Start **Date** through End **Date**.

### *Example:*

6 a.m. through 23:59:00 on  
10/01/2000 through 11/01/2000

You type in the date and time information the same way for both range options. The report will select data based on your choice, and the selected time-period will print at the top of the report for your reference. Depending on which date/range option you select, the report will show the report's time period as follows:

04/01/2002 0:00:00

00:00 to 23:59

through

ON

05/31/2002 23:59

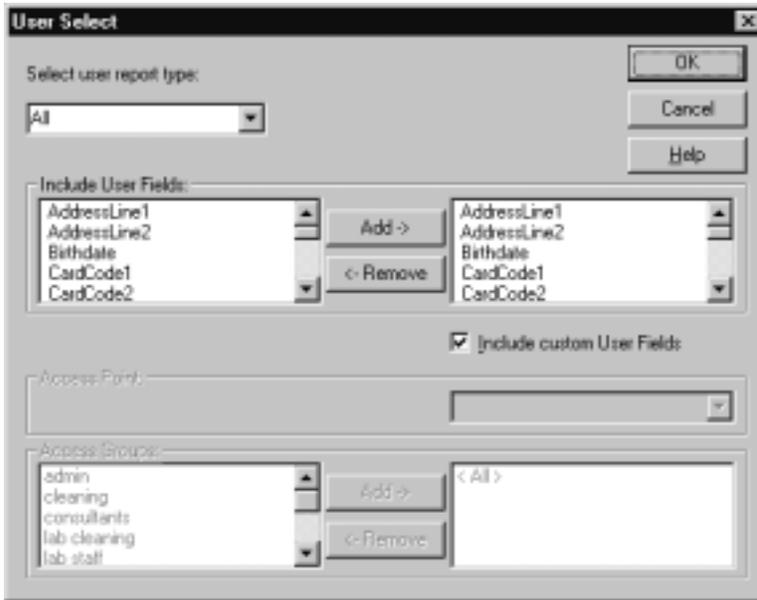
04/01/2002 through 05/31/2002

## Report: History

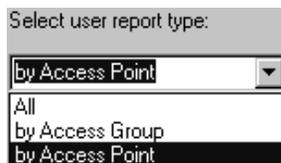
The History report is one of Millenium's Advanced reports, meaning operator input is required. An operator must select criteria to be included in the report. In most cases, you'll want to report on some portion of access control history. For example: *All history for a given date range, or all history for a given user at a specific door.*

## Report: Users

The User report is one of Millenium Advanced reports, meaning operator input is required. An operator must select criteria to be included in the report. Most likely, you'll want to report on some portion of user information. For example: *All users assigned to a given door.*



User report types give you three options:



Depending on which user report option you select, the Access Points and/or Access Groups part of the dialog become enabled or disabled.

Click **Include Custom User Fields** to print **all** custom user data fields for each user in the report.

Depending on the size and the number of custom user fields in your user database, this report can require a long time to print. Specific user reports appear in the **Standard** reports listbox for your convenience.

## Additional User Reports

Under the **Standard** reports listbox, the following User reports appear:



Single user DOSSIER report appears under the Advanced listbox

**Users--All by  
Access Group**

All users in the database grouped alphabetically under their assigned Access Group. Users with No Access appear at the beginning of the report.

**Users--All by Company  
ID**

All users in the database with the same entry in the ID field (Users dialog - Identification tab) appear alphabetically under their common ID. Users with no data in the ID field appear at the beginning of the report. For example, if you use the ID field to hold the graduation year for students, the report groups all students under their respective year of graduation.

**Users--All by  
DEPARTMENT**

All users in the database grouped, alphabetically, by Department. Users with no Department assignment appear at the beginning of the report.

**Users--All by  
EXPIRATION DATE**

All users in the database grouped alphabetically under the date their access expires. Users with no expiration date appear at the beginning of the report. **NOTE:** Once a user's access expires, their Access Group reverts to No Access.

**Users--All by READER  
TYPE**

All users in the database grouped by the type of Key or Card reader assigned to them—including lost keys or cards. Users may appear under more than one type.

## Archived Alarm or History Reports

The Millenium Expert Systems **Database Utility** lets you archive access control history. The Archived History and Archived Alarm--Incident reports let you view and print selected archives using the same selection options as the History and Alarm--Incident reports.

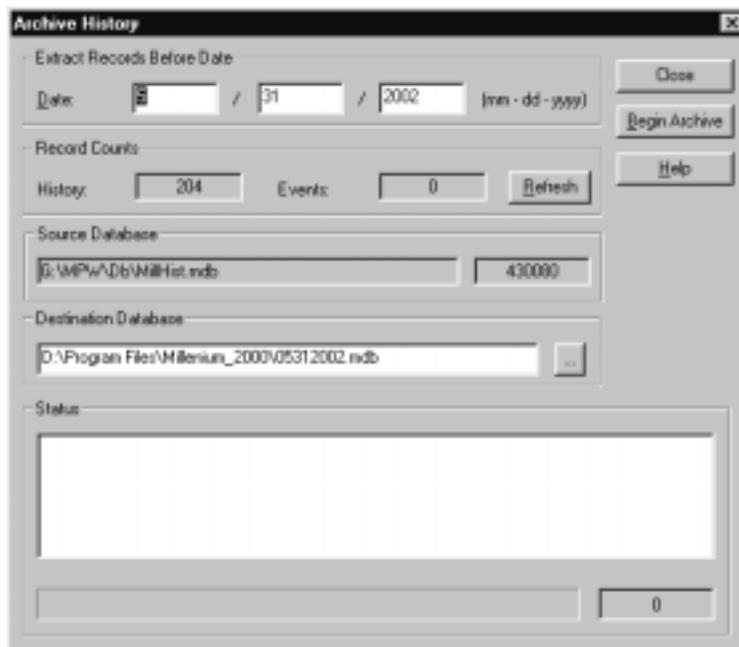
### ***Important!***

Archived reports only appear in the Advanced Reports listbox after an operator has run an archive from the Millenium DB Utility workstation. In other words, archive files must exist before Archived History and Archived Alarm--Incident reports appear in the Reports dialog.

Establish a regular policy to archive your Millenium Expert Systems history files. History files accumulate fast, so avoid letting history files grow to more than 30MB in size.

### ***How do I archive Alarm or History Reports?***

1. Both archive reports begin by having you select the archive file.



2. To verify that an archive contains ALARM data, click the **Begin Archive** button. Statistics will show you the number of history and alarm records that exist within the selected archive file.

**NOTE:** Large archived files (30MB) require more time to go through the refresh process. Recommendation is that history files be archived regularly to avoid producing files larger than 30 MB.

3. Press the OK button, The History or Alarm-Incident selection option dialog appears, depending on whether you selected the Archived History or Archived Alarm--Incident report. Select the desired report options. Make sure the date range selection covers the archive time you want included in the report.
4. Press OK to begin displaying the report preview window. The **Begin Archive** button appears black while the report is being generated.
5. Press **Print** button to print the archive report. The full pathname of the archive file prints below the report title to identify the archive data on the report.

## Dossier Report

If you use the optional Millenium BADGE add-on and have captured user images, this report prints the image along with selected user data.

### *How do I create a Dossier Report?*

1. Click the  icon.
2. From the main REPORTS dialog, select Dossier in the **Advanced** listbox.
3. If you have selected "Show find tool first", both dialogs shown below appear at once.
4. When you have found your user the first dialog disappears.



The screenshot shows a dialog box titled "Find User by Name". It features three text input fields for user identification: "Last" (containing "Baker"), "First" (containing "Bernice"), and "MI" (which is empty). To the right of these fields are three buttons: "OK", "Cancel", and "Help". The dialog box has a standard Windows-style title bar with a close button in the top right corner.

5. Use the **Add** and **Remove** buttons to scroll to the user for whom you want to print a dossier report. To locate a particular user, click the  button. To have the FIND window automatically pop up first when you open the dossier dialog, click the  option.
6. Select all or part of the user fields you want included in the report.
7. Click to include or remove the checkmark from the  option. A check means **all custom user-defined fields** will be included the report.
8. If you want free form notes to appear on the dossier report for this printing only, type in the NOTES text box.
9. Click the  button to display the report. To print the report, click the printer icon along the top of the window.

## How do I print a History Report?

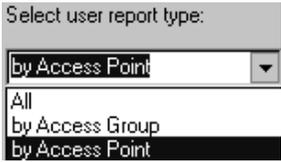


1. Click the icon  from the Millenium toolbar.
2. In the Advanced (Selection Options) listbox, highlight **History**, and click the OK button or <Enter> key. You can also double-click **History**. A History Select dialog appears.
3. Select the **Filter** to be used in gathering data for the history report. Filter defaults to ALL, however, you can create custom filters of Millenium history action through the FILTERS dialog in Millenium software.
4. Select the Date/Time Range to be used in gathering data for the history report.

5. Select any of the options to be included in the history report.
6. Options include: Users, Key/Card codes, Operators, Sites, and Devices. (A User Fields selection option appears disabled in the current software release.)
7. If you make NO selections, the report will include < All > options.
8. The selection listboxes for users and key/card codes reflect the current database of user information. If you want history for users that no longer exist in the database, you can type in exact-match data to pull history on these users. *Example:* If a name changed or was deleted, you can pull access control history on the old name.
9. Use the **Add** and  buttons to move selections back and forth between the list of options on the left and the list of selections on the right.
10. Click  to display the report onscreen. To print the report, click the printer icon across the top of the preview window.

### How do I print a User Report

1. Click the printer icon on the Millenium toolbar.
2. In the Advanced (Selection Options) listbox, highlight **User** and double-click. The User Select dialog appears.
3. In the *User Report type* field, select **All**, or **by Access Point**, or **by Access Group**.

	<p>All</p> <p>by Access Group</p> <p>by Access Point</p>	<p>Report will include all users in the database.</p> <p>Report will include all users in the Access Group(s) you specify.</p> <p>Report will include all users with access to the door you specify.</p>
	<p>by Access Point</p>	

**Include custom User Fields** Click this option to have all custom fields in the user database included in the report. This option will remain checked each time you open the User Select dialog until you change the setting. To remove custom user data from the report, click the option to remove the check mark. Custom user data appears on the USER FIELDS tab in the USERS dialog.

- If you selected **by Access Group** in Step 3, choose the group(s) for which you want to print users.
- If you selected **by Access Point** in Step 3, choose the site(s) and door(s) for which you want to print users.
- Notice that if you make NO selections, the report will include < All > Access Point or Access Group options.

Click  to display the report on screen. To print the report, click the printer icon across the top of the preview.

**NOTE:** Additional user report options can be found under the Standard report listbox. A user Dossier report option is in the Advanced report listbox.

## How can I print an Alarm-Incident Report



1. Click the  icon from the Millenium toolbar.
2. In the Advanced (Selection Options) listbox, highlight **Alarm--Incident**, and double-click. An Incident Select dialog appears.
3. Select the TYPE of report, as follows:

<b>Alarm</b>	Report will only include alarm activity from triggered devices in the Millenium network. Responses to alarms come from operator activity in the <input type="checkbox"/> Alarm Monitor.
<b>Incidents</b>	Report will only include free-form descriptions of incidents recorded by operators through the Alarm Monitor. Incidents are noteworthy comments that are <b>not</b> related to alarm events triggered from Millenium devices.
<b>Both</b>	Report will include both alarms and operator incident reports from the Alarm Monitor.

Select the Date/Time Range to be used in gathering data for the alarm or incident report.

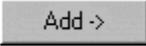
Select report options.

Options to be included in the **alarm** report:

(If you make NO selection, you get all possible options.)

<b>Operators</b>	Select specific operator(s) for whom you want to print an alarm report. Report will only include triggered alarms responded to by the operator(s) you select.
<b>Sites</b>	Select specific sites (SCUs) for which you want to print an alarm report. Report will only include the site(s) you select.
<b>Devices</b>	Select specific doors (DCDs) or relay control devices (RCDs) for which you want to print an alarm report. Report will only include the device(s) you select.

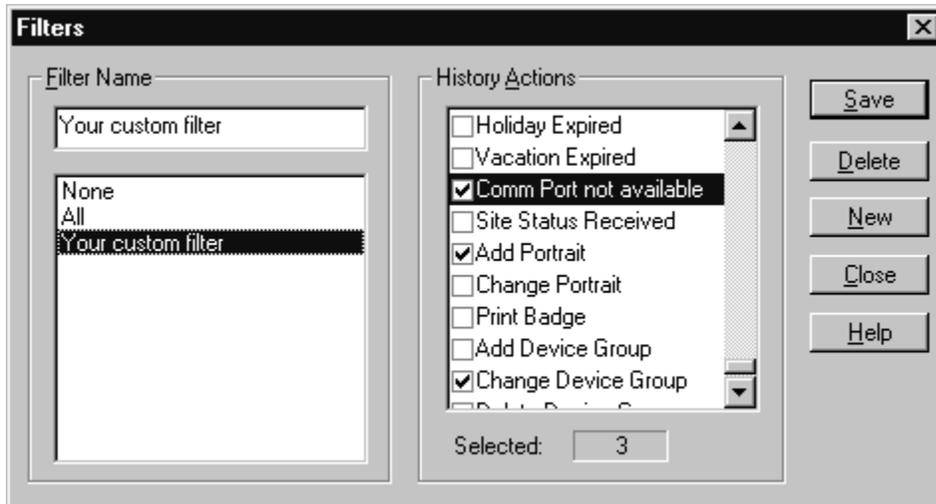
Option to be included in the **incident** report is selection of all or specific Operators. (**Make NO selection to include all operators.**) Notice all but the Operators selection listboxes become disabled (grayed out) when you select the  **Incident** TYPE.

Use the  and  buttons to move selections back and forth between the list of options on the left and the list of selections on the right.

Click  to display the report preview onscreen. To print the report, click the  printer icon along the top of the preview window.

# Chapter 18: Filters

The illustration below shows the FILTERS dialog in Millenium Expert Systems.



Operators can design custom filters that include a specific list of history actions.

1. Click the  button.
  2. Give a name to the custom filter you are establishing.
  3. Click to place a check mark beside just those history actions you want included in the custom filter.
  4. Click the  button.
- These user-defined filters are available for previewing or printing history reports. Custom filters you establish in the above dialog can also be assigned as Resident filters to control what history actions display in the application workspace and what actions automatically print to a designated printer.
  - To work with alarm information, use the special Alarm Monitor  dialog on the Millenium Expert Systems toolbar.
  - Notice the number of history actions you have selected appears below the listbox for your convenience.
  - You can print a list of all history actions through the REPORTS dialog—**Filter** report.

## Filters Toolbar Button

Filter all access control history so you can use your specific filters in setting up reports based on specific users, access points, access groups, or sites. Special "Resident" filters can also control:

which history actions display on the history portion of the Millenium window.

which history actions automatically print to the designated printer.

Two system filters—ALL and NONE—come with Millenium Expert Systems. Operators can establish custom, user-defined filters in the FILTERS dialog based on just those history actions you select.

## History actions list

**The following list shows all possible history actions recorded by Millenium Expert Systems:** You can choose to filter specific groups of items for report purposes. You can also assign custom filters as "resident," to control what actions display in the history portion of the workspace, what actions go to the Alarm Monitor, and what actions automatically print.

Tamper Alarm	Relay 3 Activated	No response (from DCD)	Change holiday
Alarm 1 (DCD)	Relay 4 Activated	Log on	Delete holiday
Alarm 2	Relay 5 Activated	Logoff	Add holiday
Alarm 3	Relay 6 Activated	Auto Logoff	Restore data
Alarm 4	Relay 7 Activated	Change Auto Logoff	Change Resident filter
Alarm 5	Relay 0 Released	Log on denied	Operator unlock
Alarm 6	Relay 1 Released	Add user	Change site
Alarm 7	Relay 2 Released	Change user name	Add site
Door Ajar	Relay 3 Released	Change key	Delete site
Tamper Alarm Reset	Relay 4 Released	Change card/other	Forgive Antipassback
Alarm 1 Reset	Relay 5 Released	Change user Expire	Change vacation
Alarm 2 Reset	Relay 6 Released	Change user access	Delete vacation
Alarm 3 Reset	Relay 7 Released	Add key	Abort override
Alarm 4 Reset	Lost DC Power	Add card/other	Override unlocked
Alarm 5 Reset	Start DST	Lost Key/Card	Override locked

Alarm 6 Reset	End DST	Delete user	Add (operator) level
Alarm 7 Reset	Cold Reset	Delete key	Change (operator) level
Unlock	Power Restored	Delete card/other	Delete (operator) level
Invalid User	Internal Reset	Change operator	Program started
Invalid Time	No Response to RCD	Delete operator	Program exited
Invalid User PIN	Auto Unlock	Add operator	History deleted
Invalid Door PIN	First User Unlock	Change Operator Password	System start DST
Passback Reject	Unlock End	Change device	System end DST
Request to Exit	Phone-in Failure	Delete device	Printer disabled
Remote unlock	Override End	Add device	Auto expire (User)
Polling Failure (from SCU/RCD)	On Line	Change events	COM port not available
Site Control Lost AC	Off Line	Change DCD relay 1	Site Status Received
Polling Restored	Lost transmit	Change DCD relay 2	Add User Portrait
AC Restored (from SCU/RCD)	Transmit restored	Change alarm	Change User Portrait
Site Clock Failed	I/O Unexpected data	Change RCD relay	Print Badge
Bypass (elevator)	Update failure	Change DCD Keypad type	Add Device Group
Bypass Reset	Checksum error (Verify)	Change time	Change Device Group
Global Entrance	No answer	Change access group	Delete Device Group
Global Exit	Busy	Delete access group	Holiday expired
Site Buffer Full (80%)	Transmit error	Add access group	Vacation expired
Relay 0 Activated (RCD)	Update complete	Change timezone	Delete alarm
Relay 1 Activated	No modem	Delete timezone	Add alarm
Relay 2 Activated	Modem restored	Add timezone	Scheduled Unlock

## History Display Sample



When Millenium Expert Systems software is running, history displays (with on-line communications systems) regardless of whether or not an operator is logged on. You may setup up an automatic pop-up of user images along with selected user unlock, invalid user or invalid timezone **history** or **event** occurrences.

## History Portion of Window

The background workspace of Millenium Expert Systems software displays on-line history of access control activity at all on-line sites. History displays in two main columns—**Time** and **History Action**. (**History Action** section includes details.)

Time	History Action	Site	Device	Name	Key/Card Code
------	----------------	------	--------	------	---------------

TIME column: Shows icon classifying type of history ACTION:

-  General history
-  Access history (Unlocks) If access is denied, the key is colorless.
-  Computer System history
-  Operator history
-  Communications history
-  Unknown (Rare) Garbled communications data could occur from communication line interference. Ignore unless frequent.
-  Access point unblocked by Millenium Scheduler

Shows TIME & DATE the action occurred.



HISTORY ACTION column:

Describes the action.

Depending on what the action is, HISTORY ACTION can include:

- Name of SITE, ACCESS POINT, USER
- OPERATOR performing the action
- Description of access control activity such as: Unlock, Add Key, Change Timezone, <Alarm name,> Invalid user.
- Key/Card code when access is granted or denied to a key/card holder.
- Image of USER (if you have (1) Millenium Badge module and (2) images captured through the Millenium Badge program and (3) screen filters set up on the RESIDENT FILTERS dialog.)
- For UNLOCK actions (Unlock, Invalid User, Invalid Time, First user unlock), selected
- Custom User Fields will display beneath each row of history for the above actions when a user performs the action. Display can be set to print to a Resident Filter printer, but will NOT be saved as part of history.
- Alarm EVENTS appear in the Alarm Monitor where an operator can be required to report on each incident.
- You can change the width of history columns by click-and-drag mouse action. Place mouse pointer over vertical line in the heading between columns. When cursor changes to a double-sided arrow, drag column to desired width. Software retains column-heading changes. You can also move a dialog box by clicking on the title band across the top of the dialog and dragging to the desired location.
- You can display a user's image at unlock attempts. When a user gains access, Millenium Expert Systems can be set to pop up a visual image of that user as part of the history display. This requires a database of images acquired through the optional Millenium Badge module. How to set up the user image pop-up feature.
- You can also display a user's image by double-clicking on a row in history row that shows an Unlock action.
- A *"Site Devices Online"* message appears whenever the system checks all devices (DCDs, RCDs) to verify they are online with the Site Control.
- If the traffic of Millenium device communications is heavy enough to affect the display of history in the workspace, the following message along the bottom of the window keeps you informed of the situation: *"Downloading history, please wait."*
- DIRECT (on-line) communications configurations display history as-it-happens.



DIAL-UP modem configurations display history after operator clicks the  button and executes one of two commands:  **Download History from Site** or  **Connect with Continuous History Polling**.

Systems with DIAL-UP communication sites display a "Site Refresh Needed" message along the bottom of the window if one or more sites need to be refreshed with the latest Millenium Expert Systems data.

## Resident Filters

At some point after your Millenium Expert Systems system has been operating for a while, you may choose to limit the amount of access control history that displays on the screen or automatically prints. You can also restrict resident filters to a specific Timezone, and you can set up an automatic display of a user image based on History or Events.

Set up or view Resident Filters through the **History** menu on the Millenium menubar.



Notice two system default filters exist—All and None. If you created custom Filters, they will appear in the filters listbox.

Three types of resident filters let you control what history actions

1. Display in the history portion of the Millenium window (Screen output device.)

### DISPLAY USER PHOTO:

If you have the optional Millenium Badge module, and have used the badging system to capture user images, the Screen Filter lets you select how user images display in Millenium software. User photo images can display based on **Events** or on **History**. Image can display for any combination of Unlocks, Invalid User, or Invalid Time entry attempts.

### DISPLAY CUSTOM USER FIELD DATA:

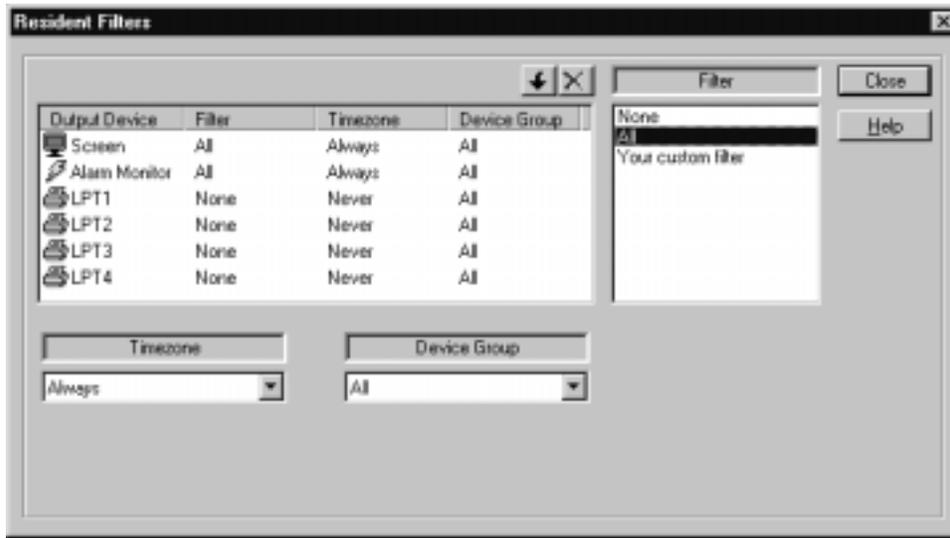
If you select custom user fields under the History menubar (Custom User Field Display option,) data from the selected custom field will display for a given user below the history action row. History displays for unlock actions: Unlock, First user unlock, Invalid User, Invalid Time.

2. Control what history actions go to the Alarm Monitor output device.

All history actions automatically save as part of Millenium access control, but you can filter those actions you want to appear in the Alarm Monitor function.

3. Go, automatically, to a specified printer (LPT output devices.)

**DISPLAY CUSTOM USER FIELD:** If you selected custom user field data to display with unlock actions in the history portion of the window, you may also set up a Resident Filter to automatically print user data when the unlock occurs.



In addition to assigning a FILTER to the resident screen, Alarm Monitor or printer, you can also limit the filter to be:

- (1) in effect during a specified Timezone, or
- (2) in effect for a specific group of Millenium devices.

Device Groups give you an option to filter what history actions go out to the SCREEN, ALARM MONITOR, or Printers (LPTs) based on selected groups of DEVICES (doors, elevator floors, site controllers, or relay controllers.)

## How do I Assign a Custom Resident Filter

1. Create a custom filter through the FILTERS dialog, if desired. System filters are **All** or **None**.



Click on the Resident Filter option from the **History** menu.

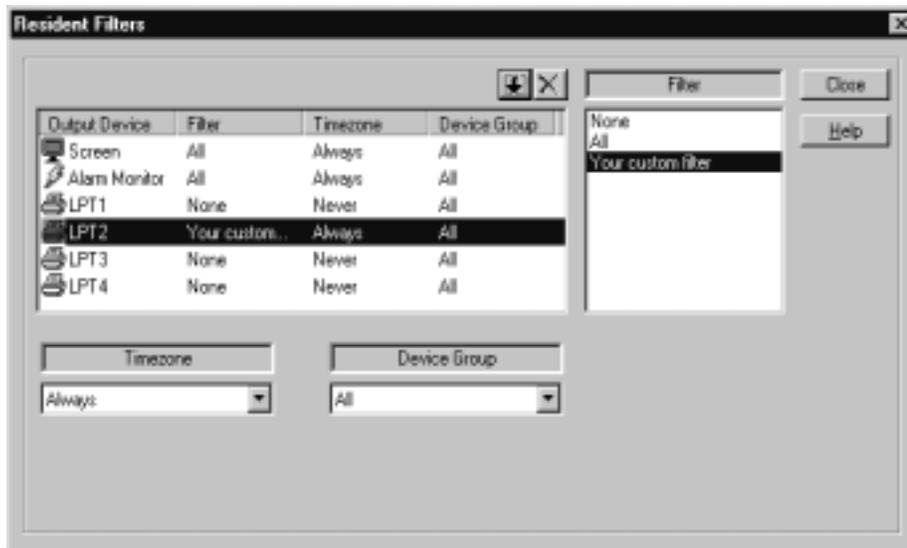
2. In the Resident Filters dialog, highlight the **Filter** you want to become Resident for one of three types of output devices:

**Screen** (history portion of the Millenium application workspace.)

**Alarm Monitor**(separate display of triggered alarm activity.)

Any **Printers** available to the PC (printers installed through Windows®.)

3. OPTIONS: If desired, highlight the **Timezone** and/or the **Device Group** you want to assign to one of the Resident Filter output devices.
4. Highlight the Output Device row to which you want to assign the filter and currently displayed filter options.
5. Click the  button to create the Resident Filter for the selected row. All currently displayed Filter, Timezone, and/or Device Group options become the resident highlighted output device.



6. To “de-select” the Filter, Timezone and Device Group, highlight the Output Device row and click the  button. All selections revert back to the defaults (shown above.)

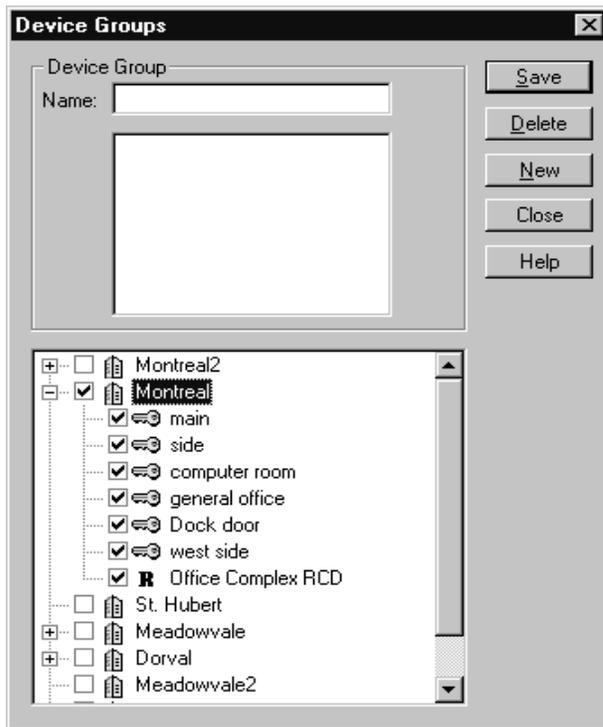
## Device Groups

The Device Groups option lets you select individual Millenium devices (doors, elevator floors, site controllers and relay controllers) and group them together under a device name of your choice. In the Resident Filters dialog, you can then assign a DEVICE GROUP to control what device history actions display on the history portion of the Millenium screen, go out to the Alarm Monitor, or automatically print on designated printers.



**Device Groups;** option appears under the History menubar.

When you select the option, the following dialog displays:



### *How do I create a Device Group*

1. Type a name for the device group you are forming.
2. Click to select the devices to be included in the named device group.
  - If you click the site name, a check automatically appears beside all devices under that Site Control Unit (SCU.)
  - If you remove the check for a site, all checks remove from devices under that site.

- Click the  button.

***Did You Know?*** Icons beside the devices identify the type of device:

-  Site Control Unit (**SCU**)
-  Door Control Device (**DCD**)
-  Relay Control Device (**RCD**)
-  Elevator Control Unit (**ECU**)
-  Elevator car Control Device (**ECD**)

## System Filters: All & None

Two filters come as part of Millenium Expert Systems, and cannot be changed by the operator.

**All** Every possible action that Millenium Expert Systems can record as history.

The default Resident Filter for history actions displayed in the application workspace is SCREEN = **All**, so all possible history displays. As you become more familiar with the Millenium Expert Systems, you may choose to set up a custom SCREEN filter with selective display actions. Regardless of your SCREEN setting, all activity saves as history.

**None** Clears all history actions (more than 140 possible selections.)



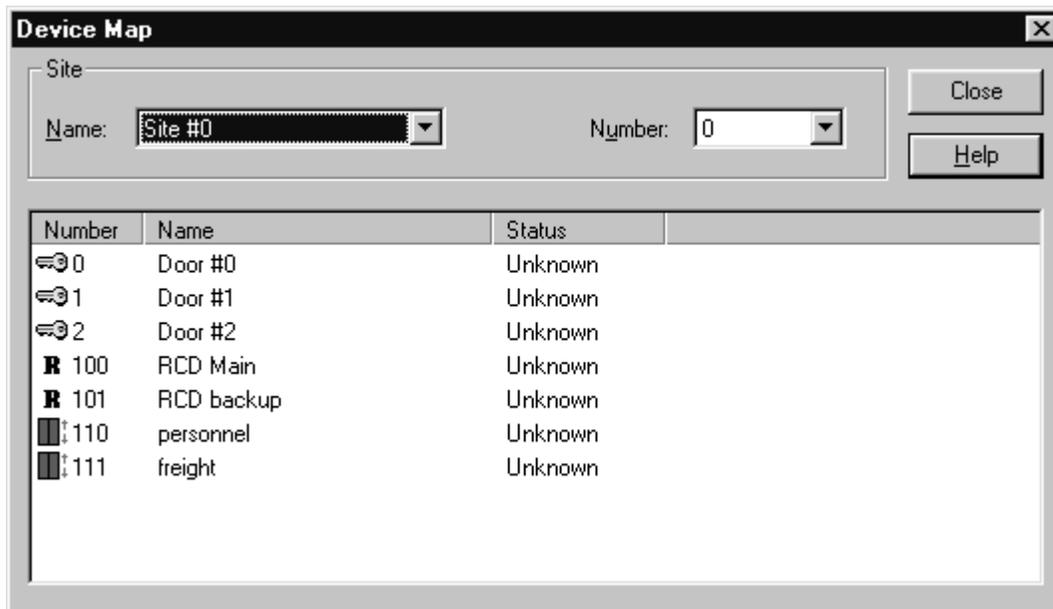
# Chapter 19: Maps

## Map (Device)

To print a Device Map, go to the REPORTS dialog.

The Device Map displays a "snap-shot" of the entire Millenium network including all devices (DCDs, RCDs, and ECUs) installed in the system. The display is site-by-site. **The map displays for your information, only—No data entry takes place in this window.**

The **Status** column lets you know whether the PC and the device are communicating (On Line or Off Line.) Unknown appears: (1) for sites that are programmed but not installed, or (2) when the Site Polling field is set to **Disabled** in the Site dialog, or (3) when you call up the Device Map immediately after logging on the software—before the Site Status check is complete.

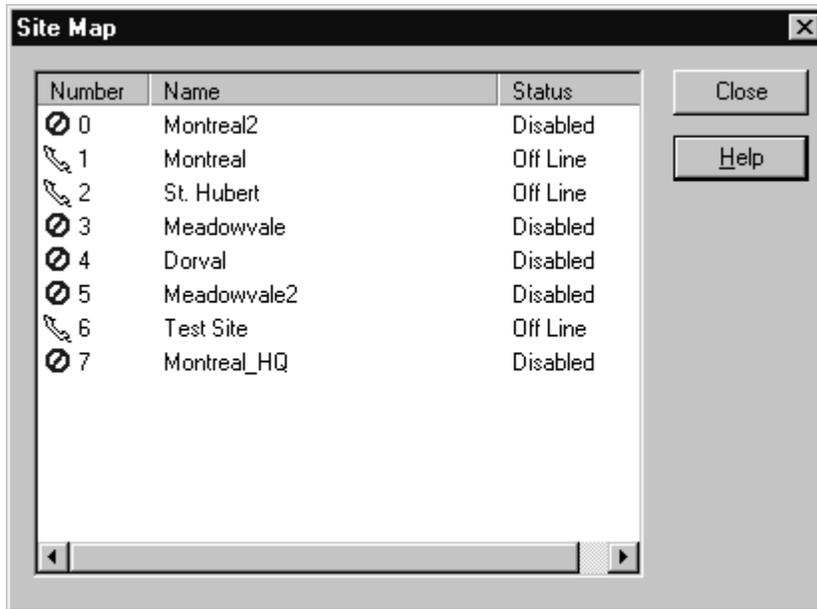


Notice a graphic at the beginning of each row identifies the type of device along with the device number. Device number for RCDs is the number plus 100. Device numbers for ECUs are 110-113 representing ECUs 0-3.

## Map (Site)

To print a Site Map, go to the REPORTS dialog.

Site Map displays a "snap-shot" of the entire Millenium network showing the individual status of all sites (SCUs) programmed and installed in the system. **The "map" is for your information, only. No data entry takes place in this window.**



**Off Line** or **On Line** status only appears when a site is ENABLED. Sites are enabled or disabled based on the polling setting in the Site dialog. Programmed devices that are not yet installed or enabled appear as off line.

**Disabled** status appears when polling is disabled in the Site dialog.

**Unknown** status comes from DIAL-UP sites that require an Update process (Dialup Connections dialog) before the status can be determined.

**NOTE:** The small ICON beside the Site Number illustrates the communication mode.

- Phone icon is solid for Online sites.
- Phone icon is hollow for Offline sites.

## DATE

Millenium Expert Systems dialogs provide two ways to enter dates in the software.

1. Pop-up calendar method - User (Identification and Access) dialogs offer the calendar date-entry method. The Timezone dialogs also offer this date-entry procedure.

Birthdate:  Expiration Date:

### How do I Select the Date Format



The default date format comes from the Windows Control Panel. The format you establish in the **Short Date Format** field will be the format you see in Millenium software. The default is m/d/yy. With the new century, you might prefer selecting the m/d/yyyy format to see future years as 20XX rather than 00 or 01.

In the date field, click the button. A graphic calendar displays, similar to the following :



Use the arrow buttons to move forward and backward through time.

- Move to previous MONTH(S)
- Move to next MONTH(S)
- Move to previous YEAR(S)
- Move to next YEAR(S)

Click on the DATE. The calendar closes, and the date displays in the dialog according to your selections in the pop-up calendar. (Date format comes from the Regional Settings control, as described in Step 1.)

2. Spin Control date-entry method

Press the <tab> key to move between segments of date data. Then either type the desired data or use the spin controls to move forward or backward through increments of date data.

End Date/Time

Example: (from Vacation tab on Timezone dialog.)

## Global message

Shows the number of times a global message is repeated. Global messages are those that affect the entire Millenium device network. Increase this count where communication lines (usually leased lines) experience frequent “noise” or interference. Higher global send counts avoid missing global message information. Default is 1. Adjust to no more than 2 or 3, if necessary.

## System Clock

Time is a central part of your Millenium Expert Systems access control system. The computer's system clock time affects the time on each circuit board device (SCUs, DCD, RCDs, ECUs) in the network. Each time Millenium Expert Systems starts up, the system sends the current time to all devices. The current time also communicates to the circuit board clocks each time you update access control devices. Therefore, it is essential to keep system clock time accurate.

Millenium Expert Systems uses the system clock setting established through the Windows **Control Panel's Date/Time Properties** dialog.

1. To check the current PC system time within Millenium software, click the **Clock...** button in the TIMEZONE dialog. The following dialog pops up:



2. The current computer system time displays.
3. The Time Change Options reflect the current Standard versus Daylight Savings Time condition. (This time-change setting also comes from the Windows Control Panel's *Date/Time Properties* dialog.)
4. If necessary, press the **Update** button to send the current PC system time to the Millenium devices.

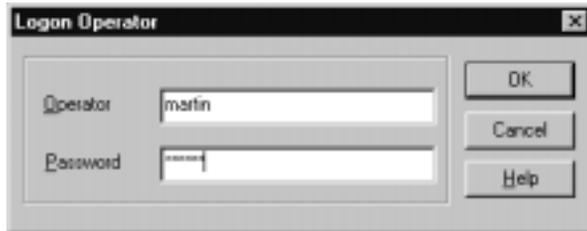
**NOTE:** You would only use this update action if a site had been offline during a session or if you noticed the computer time was inaccurate and you wanted to send the current time immediately. Otherwise, the software automatically sends the current time the next time you start the program.



# Chapter 20: Database Utilities

## Login to DB Utilities

1. Select DB Utilities from the Start Menu and the following dialog box will appear:



2. If you have not yet created an Administrator in your Millenium application, use **kaba** as the Operator and **expert** as the password.
3. If you have an operator, use his/her name and password as in the example above.
4. The DB Utilities Module can be closed without logging off.

## Millenium Database Utility offers the following functions:



**Import** User data from an external database into Millenium database.



**Export** User data from Millenium database to a tab-delimited ASCII file.



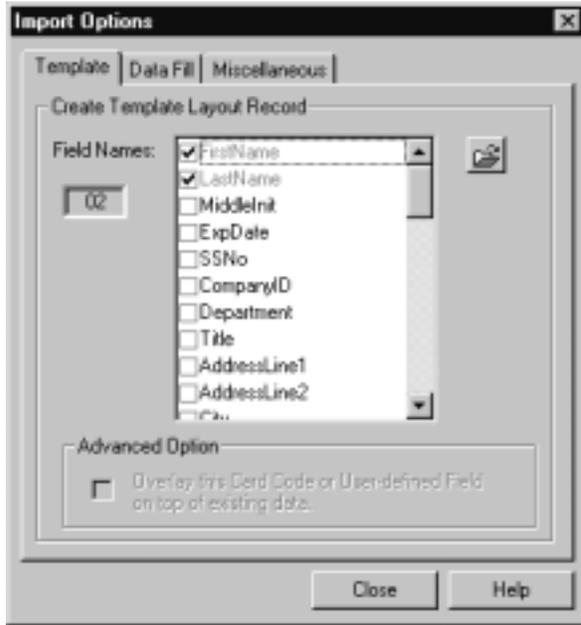
**Archive Millenium** history to and remove it to a compressed storage file.



**Export 900** creates an Import.dat file of Millenium Expert Systems USER data for ILCO System 900.

## Import Users

The import database utility lets you import user data from external ASCII database files. To import more than just a user's first and last name, the utility requires that you set up the heading columns in the import file. The headings must exactly match field names in the Millenium database. Therefore, the utility offers an option to create a TEMPLATE import file with point-and-click heading selection.



### *How do I import user data with the Millenium Database Utility?*

1. Click the database import icon from the Millenium DB Utility toolbar.
2. Use the import Options, as applicable.

**NOTE:** The Template tab on the Options; dialog lets you create and save a sample import text file complete with selected headings. You then place the data to be imported under the headings in the import file.

3. Check the settings on the Miscellaneous tab.

**NOTE:** Settings on this tab save from one import to another. One default setting comes with the system—Allow empty import fields to remove existing data in database. Use this option with care, as you cannot undo the process once an import that has empty data fields has replaced existing data with blank fields.  
A Data Fill tab lets you set the database utility to generate a unique field to be used as a user's identification code.

4. Click the file folder icon to select the import file to be used.
  - The default location is in the \mpw directory.
  - For your convenience, template header fields that are in the selected import text file

display in the Template Fields listbox.

- Test the import for errors.
- Once the import template is made, any data fill or special options are selected, the template is saved, and data exists under the template column headings, you can test the import. Press the Test Read button to generate the import WITHOUT actually overwriting the Millenium database. The STATUS window fills with a line-by-line record of the import test run. If errors exist, the test run brings them to your attention before writing to the database.
- Recommendation: Use this test procedure to check for data errors before actually performing the import. A command-line option to automatically run this test import is available, if desired.
- When the test read is successful, press the Begin Import button to populate the data under the selected Template Record field headings and import the data to the Millenium Expert Systems database.

### ***Important!***

- If you import blank fields, the import replaces existing fields in the Millenium Expert Systems database with blank fields.
- Click to see how to change this default setting.
- On very large database imports, you can press a Stop Import button that replaces the BEGIN button. This allows you to interrupt the import process. Records up to the point of interruption are already in the Millenium database as either added records or updated records. Other records remain as they were before the interrupted update.
- Import action always produces an Import.log file entry.
- Any critical errors from the import action append at the end of an MpwDbErr.log file
- Comments - You may record comments in the import file such as a label at the beginning. Use semi-colon (;) in front of the comment line and a hard return at the end of the comment line. Repeat the semi-colon at the start of each new line of comment.

**Importing selected user data**

Enable Support for [DeleteUsers] Keyword

**Importing a User Access Code, Access Group and/or UserPIN**

Automatically Send Users with a New Access Group Assignment, Access Code or User Pin to MPW

Allow Empty Import Fields to Remove Existing Data in Database  
 Note: This option does not apply to Key/Card or Access Group Assignments.

Automatic Import by Command Line

Convert to ABA Code

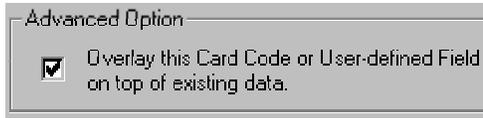
Enable Support for [DeleteUsers] Keyword

**Template tab**

The Template tab on the Import Options dialog lets you create a sample text file to be used for the import. The Template tab contains field names for column headings. The field names reflect the exact syntax of the Millenium Expert Systems database tables. Two fields—User's *FirstName* and *LastName*—are required.



1. Click to select any additional fields to be included as header columns in the sample import template. (Click again to de-select.)  
 Checked fields become the header columns for the sample import file.  
 Press the  button to name the template header file.
2. **Advanced Option:** Selected fields (*CardCode1* & *CardCode2* and custom user fields—*UserFlds 1-10*) enable an Advanced Option that makes imported data overlay existing data.



- 3.
4. To have the data being imported overlay existing data for the selected fields(s), click the advanced option checkbox.
5. Once checked, this option remains in effect—globally— for any future imports of the eligible fields. All overlaid data is left aligned. If the new data has (1) the same number of characters as, or (2) more characters than the old data, new replaces old. Shorter data overlays existing data, beginning flush left.
  - If existing field is 1000 and new field is 100011, imported field is 100011.
  - If existing field is 1000 and new field is 200, imported field is 2000.
  - If existing field is 1000 and new field is 200022, imported field is 200022.
  - If existing field is 1000 and new field is 11, imported field is 1100.



The Save button (  ) lets you create and name a sample template for the import file with the Field Names and Advanced Option as they appear.

***Important!***

You must select the appropriate template Field Names when using such import options as Data Fill, Data Fill with conversion to 9-digit ABA code, Access Group assignment, or Access Code import.

**Template Layout Record (import file)**

To import more than just a user's first and last name, Millenium 's Database Utility requires that you select or create additional heading columns in the import text file. The Template tab option lets you select column headings and create a sample **Template Layout Record** file with the headings in place. The advantage of using the Template tab to create a sample import file is that the syntax of the database field name in the HEADER will exactly match the Millenium database names.

Header	FirstName	<tab>	LastName	<tab>	MiddleInit	<tab>	<selected field> or <typed field name>
Import data	Randy	<tab>	Myers	<tab>	A	<tab>	<data>
	Amy	<tab>	Andrews	<tab>	<space>	<tab>	<data>

**Import file conventions:**

Import file headings are the first line in the import file.

All data follows the header record in **tab-delimited** order. If a field in the importing database is blank (and it is not a required field), you must still press the <tab> key to satisfy the field and move to the next field in the import.

### Recommendations—

- Insert a <tab> followed by a <space> to make a blank field easier to spot.
- Only include those import file headings that you plan to use.
- Headings must exactly match field names in the Millenium Expert Systems database.

Therefore, the  button on the IMPORT dialog takes you to a Template tab where you select the exact field names to be used as the import file headings. You can then save the template and use it as the import file—with Header column names already in place.

If you add comment lines to identify an import file, they must appear at the beginning of the import file. Comments must be ignored in the import process. Use semi-colon ( ; ) in front of the comment line and a hard return at the end of the comment line. Repeat the semi-colon at the start of each new line of comment.

## How do I import a Marlok Key, ABA card or Wiegand access code?

Millenium Expert Systems Database Utility includes a feature by which the operator can import user data from a tab-delimited **ASCII** file. The Field Names listbox in the  dialog, (Template tab) lets you use the point-and-click method to select from the following fields. You can then save the checked fields as column headings in a sample import file.

<input checked="" type="checkbox"/> FirstName	<input type="checkbox"/> City	<input type="checkbox"/> PrintCount	<input type="checkbox"/> UserFld1	<input type="checkbox"/> AccessGroup
<input checked="" type="checkbox"/> LastName	<input type="checkbox"/> State	<input type="checkbox"/> Operator	<input type="checkbox"/> UserFld2	<input type="checkbox"/> MarlokKey
<input type="checkbox"/> MiddleInit	<input type="checkbox"/> PostalCode	<input type="checkbox"/> ImageDate	<input type="checkbox"/> UserFld3	<input type="checkbox"/> ABACard
<input type="checkbox"/> ExpDate	<input type="checkbox"/> HomePhone	<input type="checkbox"/> ImageID	<input type="checkbox"/> UserFld4	<input type="checkbox"/> WiegandCard
<input type="checkbox"/> SSNo	<input type="checkbox"/> WorkPhone	<input type="checkbox"/> BadgeStatus	<input type="checkbox"/> UserFld5	
<input type="checkbox"/> CompanyID	<input type="checkbox"/> Birthdate	<input type="checkbox"/> BadgeStyle	<input type="checkbox"/> UserFld6	
<input type="checkbox"/> Department	<input type="checkbox"/> Sex	<input type="checkbox"/> UserPIN	<input type="checkbox"/> UserFld7	
<input type="checkbox"/> Title	<input type="checkbox"/> CreateDate	<input type="checkbox"/> CardCode1	<input type="checkbox"/> UserFld8	
<input type="checkbox"/> AddressLine1	<input type="checkbox"/> ChangeDate	<input type="checkbox"/> CardCode2	<input type="checkbox"/> UserFld9	
<input type="checkbox"/> AddressLine2	<input type="checkbox"/> PrintDate		<input type="checkbox"/> UserFld10	

Three types of user data listed above carry special import features:

<input checked="" type="checkbox"/> Automatically Send Users with a New Access Group Assignment, Access Code or User Pin to MPW
---

### Import an ACCESS GROUP assignment.

- Access Group must already exist in Millenium Expert Systems software.
- Add the **AccessGroup** as a column heading in the import file. Add the heading manually or select it in the Template tab and name a new import template.
- Record the exact Access Group name for each user in the import file **as it appears in Millenium Expert Systems, including the spacing**.

### Import user ACCESS CODES.

- Add the **MarlokKey** and/or **ABACard** and/or **WiegandCard** as a column heading in import file. Add the heading manually or select it in the Template tab and name a new import template.
- A special import option lets you import automatically generated random codes using the Data Fill tab.

### Import a user PIN (for Keypad Combination Readers only)

- Add **UserPIN** as a column heading in the import file, either manually or through the Template tab.

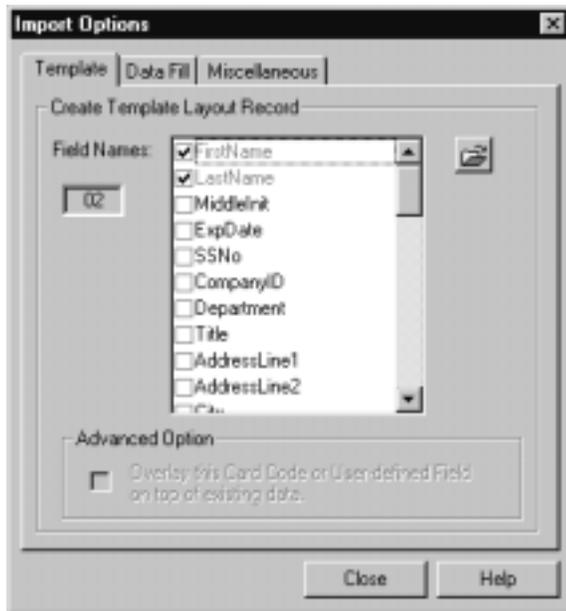
**NOTE:** If you leave the AccessGroup field blank, the import will NOT replace existing group assignments with blank fields. Even if you keep the import option to Allow Empty Import Fields to Remove Existing Data, the replacing option does NOT apply to importing Access Group assignments or Key/card access codes.

## *How do I import User ACCESS CODE, ACCESS GROUP, and/or User*

## ***PIN data with the Millenium Database Utility?***

The User Import feature can accept **Marlok Key** and **Wiegand** and **ABA** card access codes as part of the ASCII import utility. The import can also include the user's **Access Group** assignment and **User PIN**. An option also exists on the main Import Users dialog to create a 9-digit ABA card code for a user.

1. Click the database import icon  from the Millenium DB Utility toolbar.
2. If you don't already have a tab-delimited import file prepared, use the **Template** tab of field heading names to select just those database items under which you will import data.
3. Press the **Options** button  to pop up the **Create Template Layout Record**.



4. To add ACCESS CODES to a sample import text file, scroll down to the bottom of the Field Names listbox, and select *MarlokKey*, *ABACard*, or *WiegandCard*, as appropriate. Include any other database fields to be part of the import process.
5. To add *AccessGroup* and or *UserPIN* as column headings in the import file, select them from the Field Names listbox. (*UserPIN* appears higher up in the listbox.)
6. Press the button and give the template header file a name.
7. If you already have a tab-delimited import file prepared, add the appropriate access code column to the header row. Take care to use the exact syntax of the database table: *MarlokKey*, *ABACard*, *WiegandCard*, *AccessGroup*, and/or *UserPIN*, as appropriate.
8. In the ASCII import file, record the valid ACCESS CODES (or Access Group or User PIN) for each new or existing user, before performing the import.

FirstName	LastName	it	MiddleIn	MarlokKey	WiegandCard
Randy	Myers	A		3AD4C2	125-49231

- Click the file folder icon  on the main import dialog to select the import file being used. Default location is the **mpw** directory.
- Read over the notes below before performing the test or the live import as outlined on the main import dialog.
- Remember these import files are <TAB> delimited, so follow conventions outlined in the Template tab topic in this help file.
- If you leave the **MarlokKey** or **WiegandCard** (or ABACard or Access Group) field blank, the import will NOT replace existing access code or access group assignments with blank fields.
- Even if you keep the import option to Allow Empty Import Fields to Remove Existing Data, the replacing option does NOT apply to importing Access Group assignments or Key/card access codes.
- If the User already has an Access Code of the type you are importing, the new code **replaces** the old one. Example: 3AD4C2 in the above example will replace 3AD15C for Randy A Myers.

### **Important!**

- To import Wiegand or ABA card codes, you must **first** define the DISPLAY FORMAT in Millenium Expert Systems Setup (setupmpw.) The import utility rejects any access code that does not match the setup format.
- The utility will not import any access code that is **currently in use** by another user OR one that is **reported LOST** in the Millenium Expert Systems database.
- Key and Card access codes are **not** automatically communicated to doors or elevator floors as part of this import utility.

### **Two options exist:**

- An operator must perform an **UPDATE** in Millenium Expert Systems software to send this data to Millenium access control devices, or
- Import Options-Miscellaneous tab  **Automatically Send Users with a New Access Group Assignment, Access Code or User Pin to MPW** option must be checked.

## Automatic User Import - Command-Line Option

A command-line option exists to automatically run the user import utility  function at a pre-determined time. The option requires an external scheduling program such as *Microsoft System Agent* that comes with Microsoft Plus!

Once you set up the time and enter the command line (see below) through your scheduling program, the TEST READ of the user import function will automatically take place at the scheduled time. The Millenium operator then reviews the **Import.Log** file to determine if any errors occurred during the import users test run.

Example: `/(space)<import test file source path>`  
`c:\mpw\mpwdb.exe /I c:\mpw\users.txt`

If no errors appear in the log, the operator can proceed to run the actual import of users into the Millenium Expert Systems database.

**Warning!** This Automatic User Import feature is intended for advanced operators that can accept the consequences of unintentional changes to User data. As with any import function, you should backup the database BEFORE you begin working with the database utility.

- The Automatic User Import command line utility first performs the  function to insure that no errors or warnings occur in a dry run of the process.
- If an error or warning is detected, the import stops and a message goes to the **Import.log** file.
- If no error or warning is encountered, the actual import runs and adds/updates USERS in the Millenium Expert Systems database.
- All Import Options will apply during the automated import.
- After the process is complete, the Millenium Database Utility closes.

`/I2(space)<import test file source path>`  
`/I2 c:\mpw\users.txt`

Example from the Windows95 Start Menu—  
 RUN option:

`c:\mpw\mpwdb.exe /I2 c:\mpw\users.txt`

Again, remember there is no "undo" for this automatic import option except to restore the backup.

## Data Fill Tab

The Data Fill tab on the Import Options dialog offers an option to have the database utility generate a **unique field to be used as a user's identification code**. (The generated text string contains 6 fixed digits, 9 random digits, and one (1) checksum digit.) You select the **one** field from the listbox that will be filled with generated random data patterns.



The **Select a Field to Data Fill** section contains certain Field Names—*CardCode1*, *CardCode2* along with the ten custom user-defined fields (*UserFld1-10*) available in Millenium Expert Systems' User database.

**NOTE:** *CardCode1* and *CardCode2* are text fields on the User dialog's BADGE tab. Custom fields come from the User dialog's User Fields tab in Millenium software.

### **Important!**

For this random data fill feature to work, you must have selected the corresponding Field Name in the Template tab, or have the corresponding Field Name in the Import File HEADER.

- Six prefix (fixed) digits are required for the auto-generated data pattern.
- If you make no entry, the system will use all zeros.
- If you fill in *two* prefix digits, the system will finish the prefix with *four* zeros.
- The Import utility **ignores** the data fill option in the following situations:
  - The fill field to be used was not selected on the Template tab and therefore does not exist in the import file header. Example: If you select *CardCode2* (Data Fill tab—above,) you must also have selected *CardCode2* in the Template tab or have the *CardCode 1* or *CardCode2* headings in the import text file.
  - The database already contains data. The Data Fill feature will never replace existing data. This means you can repeat an import without fear of modifying the

selected Data-Filled field.

**Convert to ABA Code** gives you an option to have the import utility automatically convert the random data to a 9-digit ABA card code for a user in the specified data file field. This option requires that you have (1) the ABA Display Format field set to nine characters (DDDDDDDDD) in setupmpw, and (2) the ABACard field selected in the Template Header Record.

## Generate 9-Digit ABA Code

After you select the **one** field to be filled with a random data code, the  **Convert to ABA Code** option becomes enabled. Click the option to have the import utility create a 9-digit ABA code for a user.



### Requirements for the ABA conversion option:

- Correct ABA Display Format must be set in Millenium Expert Systems Setup (setupmpw.) Display Format must be nine data digits (DDDDDDDDD.)
- ABACard field must be selected in the Import Options Template tab (to create a template for the import file), or you must add *ABACard* as one of the column headings in the import file.



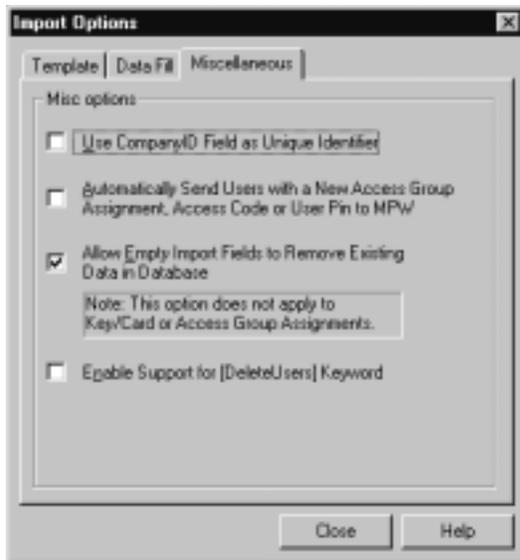
If you try to click the  **Convert to ABA Code** option without the correct ABA Display Format in setupmpw, the above message displays.

The import **ignores** the ABA Conversion in the following situations:

- Correct ABA Display Format has not been recorded in Millenium Expert Systems Setup (setupmpw.)
- Regular Data Fill feature did not generate a random digit sequence (as described under Data Fill topic – ignores section.)
- ABA Card field was not specified in the header record of the import file.
- ABA Card field in the import file contained valid data.
- User already has an ABA card assigned.

## Miscellaneous tab

The Miscellaneous tab on the Import Options dialog offers settings to perform specialized data import utility functions.



### Unique Identifier:

**Use CompanyID Field as Unique Identifier**

Millenium Expert Systems uses a combination of the LastName + FirstName + MiddleInitial as the unique identifier of users in the database. This means you cannot have two users with identical names. The first option lets you change the unique identifier to the CompanyID field so a duplicate name will be added as a new record. Instead of updating the matching record, the import process will slightly modify the last name by appending a digit beginning with zero.

### User Access Updates:



With this option, user ACCESS GROUP, ACCESS CODE, and/or User PIN information automatically updates to Millenium access control devices for those users with **changed** data in these three fields.

### ***Important!***

- An operator or database administrator can assign users to-be imported to existing ACCESS GROUPS in Millenium Expert Systems software.
- If this option were left unchecked, an operator would need to execute the UPDATE action through Millenium software's (Site dialog) to send the three types of access data changes to Millenium access control devices.
- This automatic send option only applies if you set up the import file to include ACCESS GROUP or Access Code or User PIN assignments.
- Two other conditions must exist:
  - (1) Millenium software must be running, and
  - (2) Only users for whom the Access Group, Access Code, and/or User PIN data has changed will be automatically updated.

### Empty Import Fields:



- This option makes the import function replace the field in the Millenium Expert Systems database with a blank field if the field in the import file is empty.
- **By default, this field is checked.**
- Remove the check to make the import utility skip blank fields and retain existing Millenium data.
- Exceptions— Access Group and Key/Card access codes. An empty Access Group or access code field will NOT replace existing data with blank fields.

### ***Important!***

Make sure you understand this option before using it because there is no "undo" of an import other than restoring the data.

## Removal of users through the Import option:

Enable Support for [DeleteUsers] Keyword

This option lets you remove users from the Millenium Expert Systems database based on the **User Name** or the **Company ID** fields. To use this option, check it on this Miscellaneous tab and include the keyword [**DeleteUsers**] in the import record header. Once the [DeleteUsers] keyword appears in the header, the utility will remove all exact matches from the Millenium database. This is a permanent procedure — no UNDO exists.

## Use Company ID Field as a Unique Identifier

- To identify users in the database, Millenium Expert Systems uses a combination of the *LastName + FirstName + MiddleInitial* as the **unique** identifier.
- This means you cannot have two users with identical names.
- When the import process comes to a duplicate name, the second record is considered an UPDATE of the first record. The importing record overwrites the existing record.
- A  Use CompanyID Field as Unique Identifier option lets you make the import program look at the *CompanyID* as the unique identifier instead of the user name combination. The CompanyID field could contain something like a Student Number or a Social Security Number.
- When the import process comes to a duplicate name with the "Use CompanyID Field as Unique Identifier" option, the utility checks for a unique *CompanyID*. If the *CompanyID* is unique, the program slightly modifies the user name by appending a digit to the *LastName*.

**Example:** If three identical names come up in the import process, (and you have checked the Use CompanyID option and assigned unique CompanyIDs in the import file,) the duplicates come into the Millenium database as follows:

	Name Combination	CompanyID
<b>Existing record</b>	Lane, Penny A	1025
<b>Imported record</b>	Lane0, Penny A	1026
<b>Imported record</b>	Lane1, Penny A	1027

If the import runs into a duplicate CompanyID, the import would UPDATE the existing name and record with the record being imported.

	Name Combination	CompanyID	
Existing record	Lane, Penny A	1025	...the rest of the record
Imported record	Harvey, Penny A	1025	...the rest of the record

First, however, the import program checks that the importing name does not exist elsewhere in the database. If the name does already exist, the utility appends the last name of the record being imported to maintain the inherent database requirement for unique name combinations.

	Name Combination	CompanyID
Existing record	Lane, Penny A	1025
(Importing record	Harvey, Penny A	1025 )
Existing record	Harvey, Penny A	903
Imported record	Harvey0, Penny A	1025

## Automatically Send Users During Import

- An operator or database administrator can assign to-be imported users to existing ACCESS GROUPS in Millenium Expert Systems software. The import can also include Access Code or User PIN data.
- The Millenium Database Utility IMPORT OPTIONS dialog (Miscellaneous tab) includes an option to:



- When checked, this option makes the database utility notify Millenium Expert Systems to send user data out to Millenium access control devices **when an individual user's ACCESS GROUP, KEY or CARD CODE, or USER PIN assignment has changed.**
- The IMPORT STATUS box and IMPORT LOG will include a line to indicate the user was sent to Millenium Access Management System

**Example:** Line#: 000002 Sending Myers, Randy A.

### **Important!**

- Millenium Expert Systems must be running.
- This automatic send option only applies if at least one of the three field types exists as a column heading in the import text file and if an individual user's ACCESS GROUP, ACCESS CODE, and/or User PIN has **changed.**

- This feature does not work during TEST IMPORT.
- Avoid activity in Millenium Expert Systems while the import takes place. Millenium Expert Systems **must** not be doing a site or door UPDATE while using this feature.

## Allow empty import fields to remove existing data

On the Miscellaneous tab of the Import Options dialog, an operator or database administrator can change the import function's default setting. Instead of stripping pre-existing Millenium Expert Systems data when an import field is left **blank**, you can click to de-select this option and have the import utility skip blank fields.



When check is removed, the import utility does **not** replace existing data with a blank field when a Template field is empty.

### ***Important!***

This option does not apply to existing data in the following two fields:

- ACCESS GROUP data
- Key or card ACCESS CODES in Millenium software.

Use this setting with care as you cannot undo the process once the import has replaced existing data with blank fields. A restore from data backup would be required.

## Use Import Utility to Delete Users

As part of the Import option, the Millenium Database Utility supports removal of users from the database by using a keyword in the Import Template file's header record. The process is permanent, so it must be used with care.

### ***Step-by-Step: Deleting Users by means of Import Utility***

1. Enable the option on the Miscellaneous tab of the Import Options dialog.



2. Include the keyword [DeleteUsers] in the Import Template file's Header Record that contains the Name(s) or CompanyID(s) of the **users you want to delete**.
3. Place the keyword anywhere in the header row. If you place it at the beginning, you must insert a <tab> after the keyword. If you insert it at the end, no tab is needed. In addition, the file is easier to look at with the delete field at the end because the data lines up better under the header columns.

<tab>

Example:	[DeleteUsers]	FirstName	LastName	MiddleInit	MarlokKey	WiegandCard
		Randy	Myers	A	AD4C2	125-49231

Example:	FirstName	LastName	MiddleInit	MarlokKey	WiegandCard	[DeleteUsers]
	Randy	Myers	A	3AD4C2	125-49231	

- Once you have enabled the Delete Users option and placed the keyword in the header of the Import Record file, the [DeleteUsers] keyword appears in the main Import dialog Template Fields listbox.
- The process looks for the User Name field first. If you want the user record deleted based on CompanyID, do not include any user names.
- The process allows you to use any existing import file and just add the [DeleteUsers] keyword. If other field data is included, the process just looks at the fields in search of User Name (Last Name, First Name, Middle Initial) or CompanyID data.

### **Important!**

- The delete users utility does not have an UNDO command. Deleting a user will permanently remove that user from the database.
- Use care with this option:
- Name the tab-delimited text file clearly so you know it contains the [DeleteUsers] keyword.
- Press the  button and scroll to make sure you are looking at the actual contents of the Template Header file that will be used for the import.
- To delete users, the DeleteUsers option must be enabled on the Miscellaneous tab of the Import Options dialog. If the option is not checked, but the selected tab-delimited text file contains the keyword, the process ignores the [DeleteUsers] keyword. No error message generates.
- In other words, it is critical that you know what you're working with before you perform an import. If you disable the delete users option, but perform an import on a file that contains the [DeleteUsers], **the import continues as a normal import, and therefore could affect your database according to existing import settings.**
- Example:* If the default  **Allow Empty Import Fields to Remove Existing Data in Database** is checked, any empty fields in the import file will remove data in their corresponding fields in the Millenium database.

Following a large delete, we recommend you compact the database.

## Updating:

- If Millenium Expert Systems software is running, DELETED users are automatically broadcast to Millenium devices (doors, elevator floors.)
- If Millenium Expert Systems is not running, an operator must perform a Site or Door update to remove the users from access control devices.
- Deleting users is a slow operation. Performance will vary depending on network speed and whether or not the application is broadcasting to Millenium Expert Systems devices.

To delete based on CompanyID:

- Do **not** include the User Name.
- Realize that the delete option removes the *first occurrence* of the CompanyID. (The CompanyID can exist multiple times in the database.)
- If you delete based on User Name, the utility option searches for the unique combination of Last Name, First Name and Middle Initial.

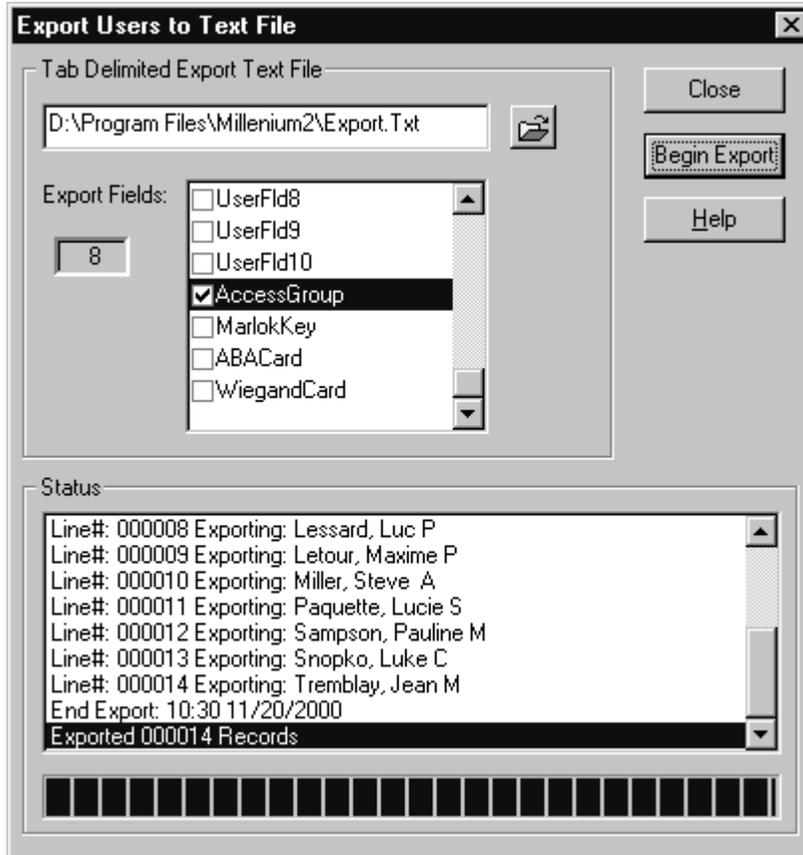
## Export Users Main Dialog

The export database utility lets you extract user data from Millenium Expert Systems' in **ASCII** tab-delimited format. You can then easily import the **ASCII** file into an application such as Microsoft Excel. Headings in the export record must exactly match those in the Millenium database, and are listed in the Export Fields listbox for your convenience.

The exported file automatically includes identification information at the beginning of the file as indicated by the semi-colon (;) in front of each comment line. The comments describe the contents of the export file and the date the export was generated.

## How do I Export User data from the Millenium database?

1. Click the database **ASCII** export icon  from the Millenium DB Utility toolbar.
2. The following screen appears.



- 3.
4. Give the export file a name.

**NOTE:** The utility automatically applies a .txt extension to the name you type.

5. If you want to browse to place the export file in a specific location, press the SaveAs  button.
6. Click to select those user fields from the Millenium database that you want in the export file. Fields you select will become the header record for the export file.

7. Click the Begin Export button  to generate the export file.

### ***Important!***

- If an export file already exists, the export process overwrites the existing file.
- It may be necessary to remove the comment lines at the beginning of the exported file, so another application such as a database program can read the file.
- Writing to a text file is not a speedy process. On average, you can expect about two user records per second.
- Run the export utility at a time when the Millenium database is **not** being modified.

The export utility writes an **export.log** file in the Millenium Expert Systems directory. This file summarizes what took place during the export process. Should the utility encounter a fatal error, the error appears in the **MpwDBerr.log**.

### **NOTES**

#### **Null columns in the database**

Some columns in the database allow null meaning the field may contain no data. For text or data types of data, the export will put one space in the output file to represent the field. As a result, when you process the export file, you should take the option to **skip fields that just contain spaces**.

#### **Timestamp columns in the database**

Export fields that contain timestamp data will be formatted according to the Windows settings established in the Windows Control Panel - Regional Settings, Date tab (short data style.)

Example: Output = 07/31/1998 12:15:18 (data and time components) may appear as 7/31/98 based on your setting in the Control Panel.

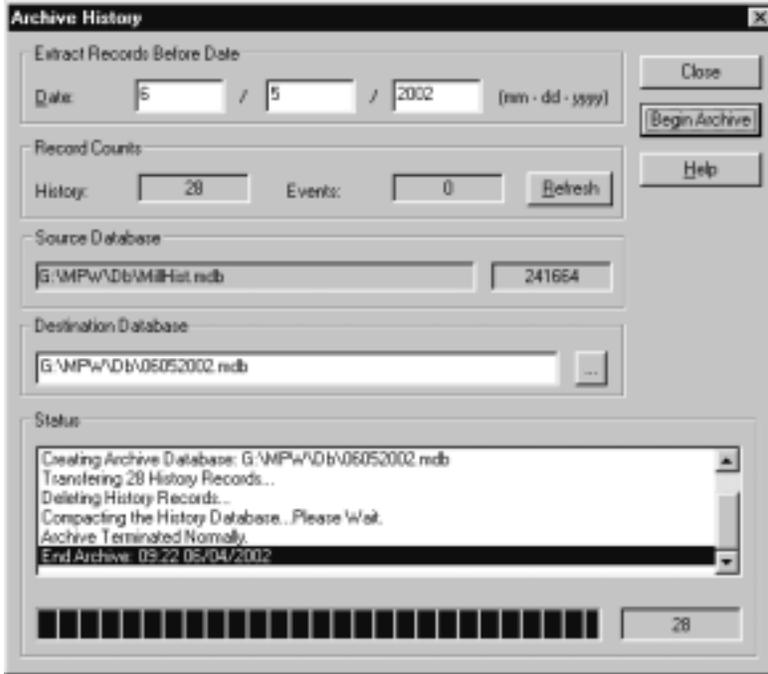
Birth date data does not contain the time component.

### **Archive History**

The Archive History utility lets you remove history from the Millenium database and save it in a compacted file. After you create a history or alarm/event archive, Millenium reports will include options to print archived history records.

### ***Important!***

Please make at least one BACKUP of your current **MillHist.mdb** file.



## How do I archive history data using Millenium Database Utility?



1. Click the archive button  on the Millenium DB Utility toolbar.

**NOTE:** The compacting step will not work if other applications are using the History database.

2. **Record Counts:** If the archive is less than 30MB in size, the Database Utility will automatically display the number of History records and how many of those records are Events. If the archive is too large to display the counts in a reasonable amount of time, a "Skipping Initial Record Count Due to Database File Size" message appears. The **Refresh** button recalculates the record count on demand.
3. **Extract Records Before Date:** Set the date **up to** which you want to extract history records. The date you record in the Extract Records Before Date field becomes part of the default name of the archive file (DESTINATION DATABASE–below) to help you identify the archive. All history records **before** the date you set will be removed from the Millenium Expert Systems database and stored in the DESTINATION DATABASE.

*Example:* The archive in the dialog graphic (above) will include all history records through the last minute (midnight) of 9/29/1997.

### Source & Destination Databases:

- The Source Database field displays the location of **MillHist** in your Millenium Expert Systems directory.
- A browse button lets you select or create your own Destination Database path and name where the extracted history records are to be stored.
- The destination includes a filename that will identify the history archive for future

reference.

- Each time you perform the archive procedure, the Millenium DB Utility retains the DESTINATION DATABASE path and defaults to name the archive file based on the current date.
  - When you type a date in the EXTRACT RECORDS BEFORE DATE field, the archive filename automatically comes from your DATE entry.
4. Click the **Begin Archive** button to start the process. Progress is displayed on the progress bar and by messages in the Status listbox, as well as by a count of history records being processed.
  5. The messages also appear in an **Archive.log** file. If a critical error occurs, the error records in a file named, **MpwDbErr.log**.

### ***Important!***

- Again, always make at least one BACKUP copy of the current **MillHist.Mdb** file before beginning an archive function.
- Make sure you have plenty of disk drive space because ODBC will swap to the hard disk as the size of the database file increases.

Here are some rough performance/time statistics:

Archive:	<b>207,689 history records</b>	Archive:	149,242 history records
	101,648 event records		7,052 event records
	2 Hours, 8 Min.		Hour, 10 Min.
	(P133 with 32 MB RAM)		(P75 with 32 MB RAM)

## **Export to System 900**

The export database utility lets you extract user data from Millenium Expert Systems and create an **import.dat** file to import users into ILCO System 900 software.

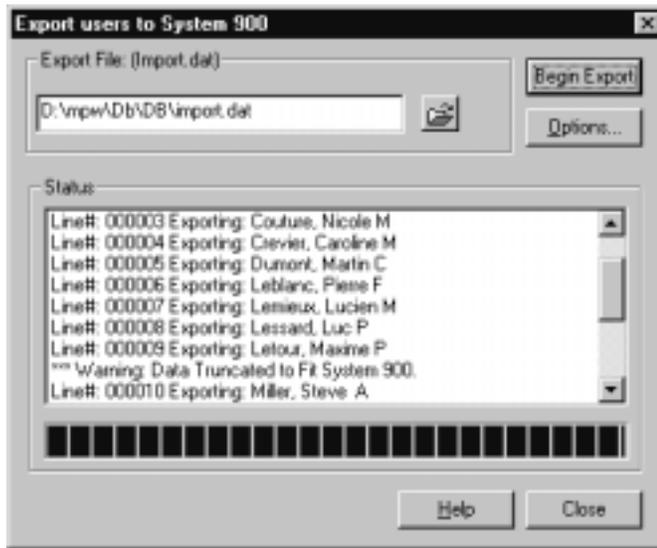


1. Click the database 900 export icon  from the Millenium Database Utility toolbar.
2. Give the export file a name.

**NOTE:** The utility automatically assumes the .dat type extension required for System 900 files.

3. If you want to browse to place the export file in a specific location, press the **Save as** button.
4. Click to select what will become the Sequence Number in the System .txt file you are about to create.
  - Selection options are a uniform sequence number (same for all users,)

- or the Millenium field from which the sequence number will be extracted for each individual user.
  - Options include Card Code 1 or 2, one of the ten user-defined fields
5. Click to select what will become the User ID in the .dat file you are about to generate. Selection options are:, or the ABA access code field.
  6. First 9 text characters from the Display Format for the Card Code 1, Card Code 2, or one of the ten user-defined fields, or Last 9 characters from the Display Format for the ABA access code field.
  7. Click the Begin Export button  to generate the export file.



The Millenium export utility creates a 900-import file in the layout required by System 900, as shown below. The export utility will truncate any data that goes beyond this fixed file format.

Field	Position	Width
UserID		9
LastName	10	15
FirstName	25	14
MiddleInit	39	
Sequence #	40	4
CLRF	44	

Millenium database, the period truncates out of the export file. A message displays and is documented in the **Export.log** file, as show below.

```

ExportLog - Notepad
File Edit Search Help
Millenium for Windows Export Utility Log File
Copyright 1997 - Ilco Unican Corporation
-----
Begin Export: 10:57 11/20/2000
Line#: 000001 Exporting: Brown, Alex A
Line#: 000002 Exporting: Carry, Joe E
Line#: 000003 Exporting: Couture, Nicole M
Line#: 000004 Exporting: Crevier, Caroline M
Line#: 000005 Exporting: Dumont, Martin C
Line#: 000006 Exporting: Leblanc, Pierre F
Line#: 000007 Exporting: Lendoux, Lucien M
Line#: 000008 Exporting: Lessard, Luc P
Line#: 000009 Exporting: Letour, Maxime P
*** Warning: Data Truncated to Fit System 900.
Line#: 000010 Exporting: Miller, Steve A
Line#: 000011 Exporting: Paquette, Lucie S
Line#: 000012 Exporting: Sampson, Pauline M
Line#: 000013 Exporting: Snopko, Luke C
Line#: 000014 Exporting: Tremblay, Jean M
End Export: 10:57 11/20/2000
Exported 000014 Records
000001 Errors or Warnings
000001 Lines with Truncated Fields

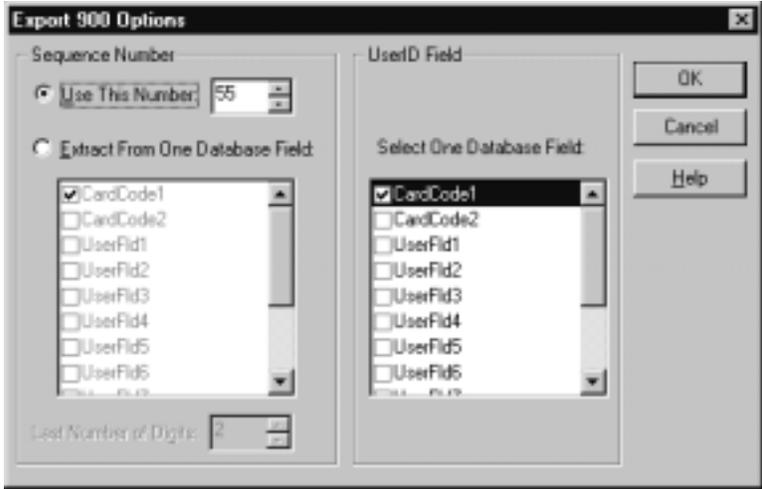
```

- The warning about user number 000009, Maxime Letourneau, occurs because the name Letourneau is too long and has been truncated to Letour.
- The exported **.dat** file is ready to be imported through ILCO System 900 software, according to System 900 requirements.

## Sequence Number

Millenium Database Utility offers two options for the Sequence Number that will be produced for KABA ILCO System 900. The sequence number appears in the "Lost Card Number" field in System 900.

- Sequence Number options appear on the left panel of the following dialog.
- Use a universal sequence number from 0 to 99.
- The same number will be applied for every user in the export file.



- Extract sequence number from a Millenium database field.
- Use part of the data from **one** Millenium database field.
- Field options are:
  - Card Code 1
  - Card Code 2
  - One of the 10 user-defined fields
  - ABA access code (Utility uses the Display Format to generate the code.)

**Last Number of Digits** field lets you set the number of digits that will be used as the sequence number. The number of digits you set will be taken from the **end** of the selected database field. Options are 0, 1 or 2 digits (0 = empty sequence number field in export file—not zero.)

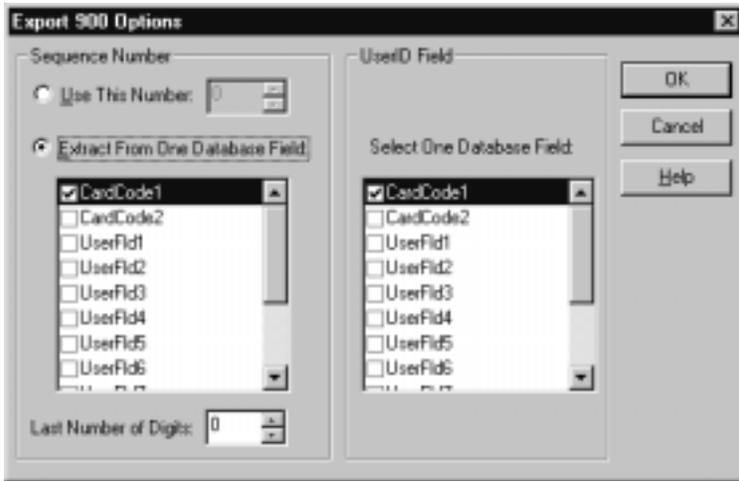
**Example:**

DB Field	Contents	Length to Extract	Actual Sequence #
Card Code 1	99123467	2	67

**NOTES:** If you extract the sequence number from a Millenium database field, you must verify that the designated field contains numeric text. In the case of the ABA code, the utility uses the Display Format to generate the text. Jump to *User ID* field for System 900 export.

## User ID in System 900 Export

Millenium Database Utility offers an option for the User ID field that will be produced for ILCO System 900. The **User ID Field** on the right panel of the dialog asks you to select the **one** Millenium database field that will be used as the User ID in System 900.



The utility produces a User ID field as follows:

### DB Field

Card Code 1  
 Card Code 2  
 User Flds 1-10

ABA Card

### Actual UserID #

**First 9** text characters from Display Format

**Last 9** characters from Display Format.

## Compact Database

The Millenium Database Utility includes a repair and compact function.

### Important!

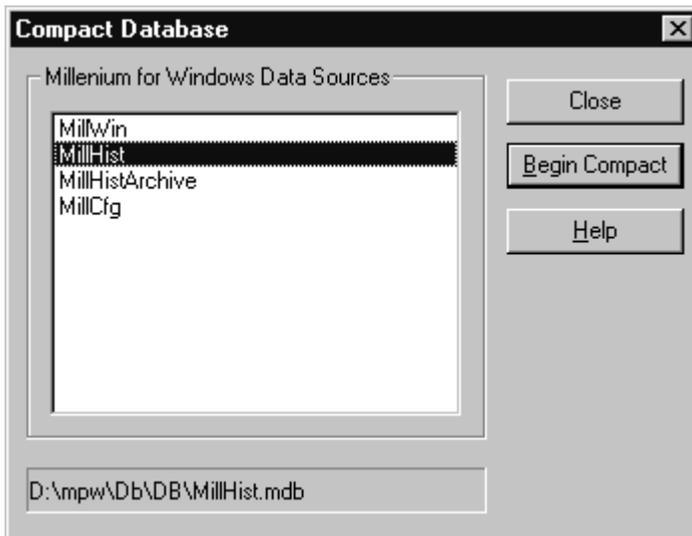
- The database operations are for stand-alone Millenium Expert Systems software configurations.
- If your Millenium Expert Systems system runs in a NETWORK configuration, DO NOT PERFORM THESE DATABASE OPERATIONS.
- See your database administrator for instructions.

**NOTE:** The Millenium Database Utility function automatically compacts the history database as part of the process. You do not need to use the compact utility on the MillHist database as a separate step.

- The upcoming database utilities need not be a regular routine. Only special situations call for the repair or compact procedure, as directed by Technical Support.

### *How do I compact the database?*

1. Make sure you have a current backup of the database before performing any repair or compact procedures.
2. From the Millenium Program Group, click on the Millenium DB Utility program.
3. Click the Compact button on the Millenium DB Utility toolbar. The following dialog box shows Millenium databases:



- MillWin is the main Millenium Expert Systems database.
- MillHist is the history database of all activity from access control devices and Millenium software programming.

- MillHistArchive is the database of archived history records.
  - MillCfg is the configuration database of settings that control how Millenium Expert Systems is set up.
1. Highlight the Millenium database to be compacted. The above example shows the main database– MillHist – highlighted.
  2. To compact the Millenium database, click the Begin Compact button.
  3. A warning reminds you that it is critical to have a current backup of a database file before performing any repair or compact functions:
  4. Click the OK button to begin compacting, or click the Cancel button, as appropriate.
  5. The dialog lets you know when the process is finished.
  6. Press Close to close the dialog, or continue to compact another database.

**NOTE:** You can also perform database functions using the Windows ODBC Administrator for standalone applications. When you use the ODBC Administrator, the utilities let you know, at the beginning whether or not your selected database is in use. In Millenium Database Utility, the repair or compact function will fail and give you a prompt suggesting that the database may be in use.

## Repair Database

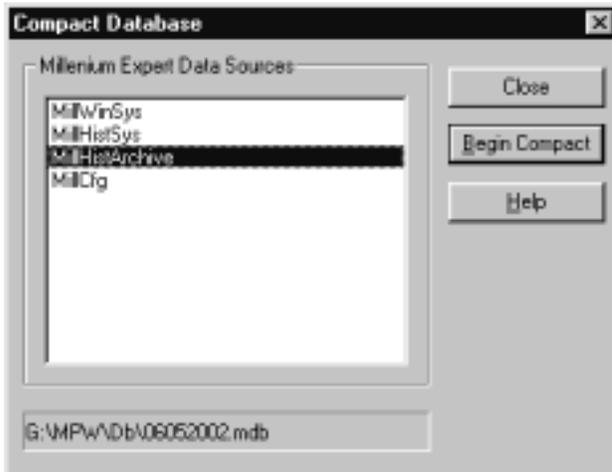
The Millenium Database Utility includes a repair and compact function. These utilities may also be performed through the Windows ODBC Administrator for stand-alone applications.

The upcoming database utilities **need not be a regular routine**. Only special situations call for the repair or compact procedure, as directed by Technical Support. We recommend that you repair databases first, then compact them. However following this order is not essential.

### *How do I perform database repair?*

Make sure you have a current backup of the database before performing any repair or compact procedures.

1. From the Millenium Program Group, click on the Millenium DB Utility program.
2. Click the Repair icon/button on the Millenium DB Utility toolbar. The following dialog shows the Millenium databases:



- MillWinSys is the main Millenium Expert Systems database.
  - MillHistSys is the history database of all activity from access control devices and Millenium software programming.
  - MillHistArchive is the database of archived history records.
  - MillCfg is the configuration database of settings that control how Millenium Expert
3. Highlight the Millenium database to be repaired. The above example shows the main database– MillWin – highlighted.
  4. To repair the Millenium Expert Systems database, click the Begin Repair button.
  5. A warning reminds you that it is critical to have a current backup of a database file before performing any repair or compact functions:
  6. Click the OK button to perform the repair, or click the Cancel button, as appropriate. The

dialog lets you know when the process is finished.

7. Press Close to close the dialog, or continue to repair another database.