MILLENNIUM ENTERPRISE

User Guide

MILLENNIUM
SECURE YOUR WORLD

MGI 2932 04/11

A publication of Millennium Group, Inc.
16 Tech Circle
Natick, MA 01760
Printed in USA, 2011

The information contained in this publication is accurate to the best of Millennium Group's knowledge.
Specifications are subject to change without notice.

MGI 2932 04/11

Table of Contents

Version 4.5 Addendum Pages Following Chapter 20.

Chapter 1: Overview

Minimum System Requirements

Millenium Application Server
- Pentium IV class minimum (Network-ready if using workstations)
- 1 Gig RAM minimum
- Hard Drive
- CD ROM drive
- 800 X 600 16 bit color VGA card
- Serial Ports (optional- for use with direct wiring to sites)
- Accurate Clock (1 to 5 minutes per year)
- Windows XP (SP2 or higher) Windows 2000 (SP 4), Vista, Server 2003, Server 2008, 7
- Microsoft SQL Server 2005 (minimum)

Millenium Workstation
- Network-ready Pentium IV PC minimum
- 1 Gig RAM
- Hard Drive
- CD ROM drive
- 800 X 600 16 bit color VGA card
- Accurate Clock (1 to 5 minutes per year)
- Windows XP (SP2 or higher) Windows 2000 (SP 4), Vista, 7

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

Millenium Enterprise Features

Millenium Enterprise is the most wide-ranging product in a suite of Access Management applications designed to administer and manage electronic security at a facility.
- Your facility can be a single location or multiple locations with as many as 100,000 access points.
- Multiple locations can include directly connected remote sites.
- Millenium Enterprise software receives your programming data for all the access points and users, communicates the data to all the electronic devices in the network and then displays and stores Access Management activity back at the Application Server.
- Users on a network can view the status of the other workstations and the server by using the Map>Network command from the main menu.
- Users on the network can also communicate with each other, using the Network Messaging facility.
- Users on the network can store common files such as floor maps in one location and be able to retrieve the files as needed.

Table of Features

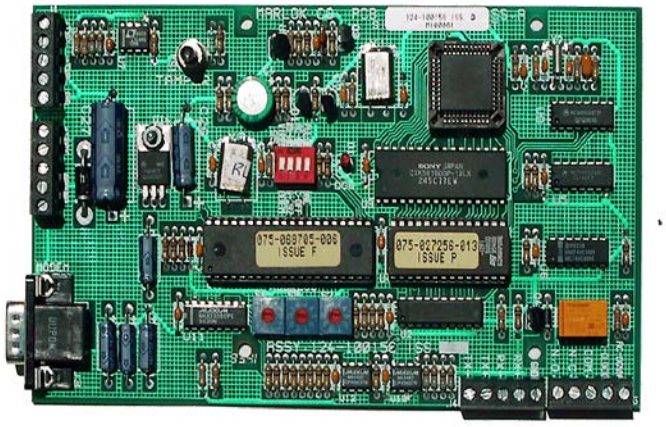
Graphical Alarm Editor	• Allows prioritization of alarms. • Lets Millenium Enterprise operator create a link from graphics to alarms.
Graphical Alarm Monitor	• Displays graphical location of the individual active alarm • Can be set to require optional security personnel responses before alarm can be reset. • Can include a pop-up photo of the user with unlock events (this requires the BADGE add-on.)
Alarms	• Up to seven programmable alarms with four alarm states – see page 87.
Relay Modes	• 7 RCD modes • 6 DCD modes
Find Users by Name	• A Find User button appears on the USER dialogs NOTES, USER DEFINED, BADGE and ACCESS tabs so you can look up a user by typing the first few letters of a name.
Import/Export Options	• Database information can be imported or exported. Consult your loca Millenium dealer for assistance.
Encode an ABA Card	• The Operator can encode up to a 14-digit ABA card. • Requires an optional Ilco System 800 encoder and settings configured in setup.
Multiple Card Formats	• Millenium Enterprise handles two different card formats (Wiegand and ABA) including the option to set up custom formats in both. Consult your local Millenium dealer for assistance.
Security	• Restrict Operator rights • Logon modules added to all dialogs for extra security.
TCP/IP to Sites	• Millenium Enterprise can communicate to Site Control Units (SCUs) using TCP/IP protocol through a Site Ethernet Interface (SEI). • Up to 32 workstations per system can also be configured with optional Server and Workstation modules.
Network Viewing and Messaging	• User can view the network status of the server and workstations. • User can send messages to selected workstations or broadcast a message to the whole network
Elevator Access Management	• Access Management for elevators. • This control feature requires you to have at least one Elevator Control Unit (ECU) and an Elevator Car Device (ECD.)
Status Check of Installed Device	• The Operator can check the status of a particular DCD, ECU or RCD device installed in the Millenium Enterprise Access Management network. • Requires a minimum EPROM level of Issue U for the SCU.
Reports	• Standard and customizable • Exportable to other formats (Excel, Word, etc.) • Prints user's image along with all or selected data if you have the image in Millenium Enterprise Badge

Optional Badge Add-on	• Integrated photo ID • Badge Layout
Millenium Enterprise Tour	• An add-on application that works with Sites and Doors established in Millenium Enterprise software. • A tour is a sequence of doors at which assigned personnel must arrive within a specified time (delta.)
Plug-and-Play	Uses standard Windows dialogs to set up and operate printers.

The Millenium Enterprise Family of Devices

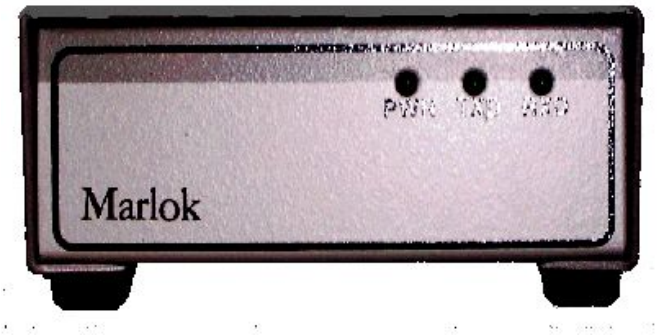
- Site Control Unit (SCU)
- Door Control Device (DCD)
- Relay Control Device (RCD)
- Elevator Control Unit (ECU)
- Elevator Control Device (ECD)
- Site Ethernet Interface (SEI)
- Trunk Interface Unit (TIU)
- Power Supply w/Line Conditioner (PS1)

Site Control Unit



The SCU supervises and maintains communications to its connected devices. It takes inbound RS232 or RS485 communications protocols and routes them to the necessary pieces of equipment on the system.

Trunk Interface Unit

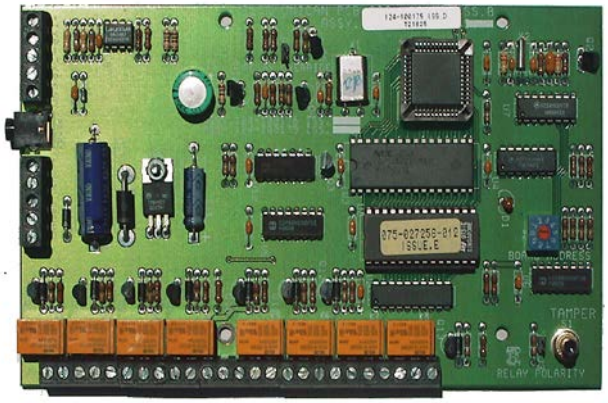


The TIU is an RS232 to RS485 converter box. Use the TIU when the SCU is more than 50ft away from the main PC or when using more than 1 SCU.

Door Control Devices (DCDs)

The DCD is the heart of the Millenium System.
This 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)



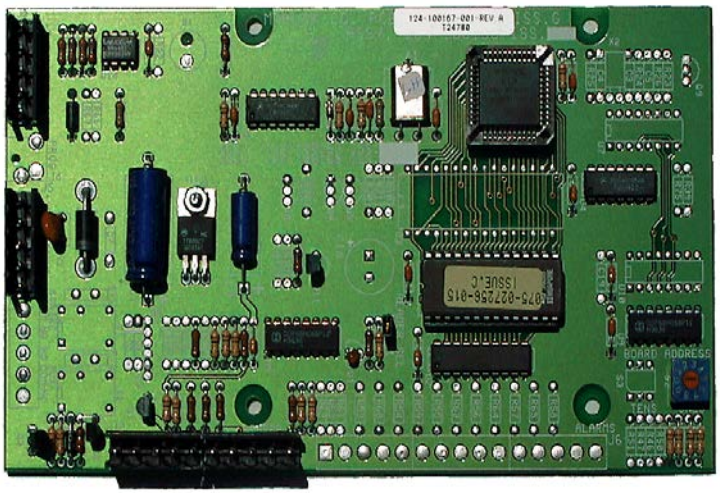
The RCD is an optional (8) relay output board that is employed within the system if additional relays are required to operate external devices.
Each RCD board (Relay Controller Board) has eight programmable relays, with a maximum of 10

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

Elevator Control Unit(ECU)

The ECU is used to interface the Millenium for Windows 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.

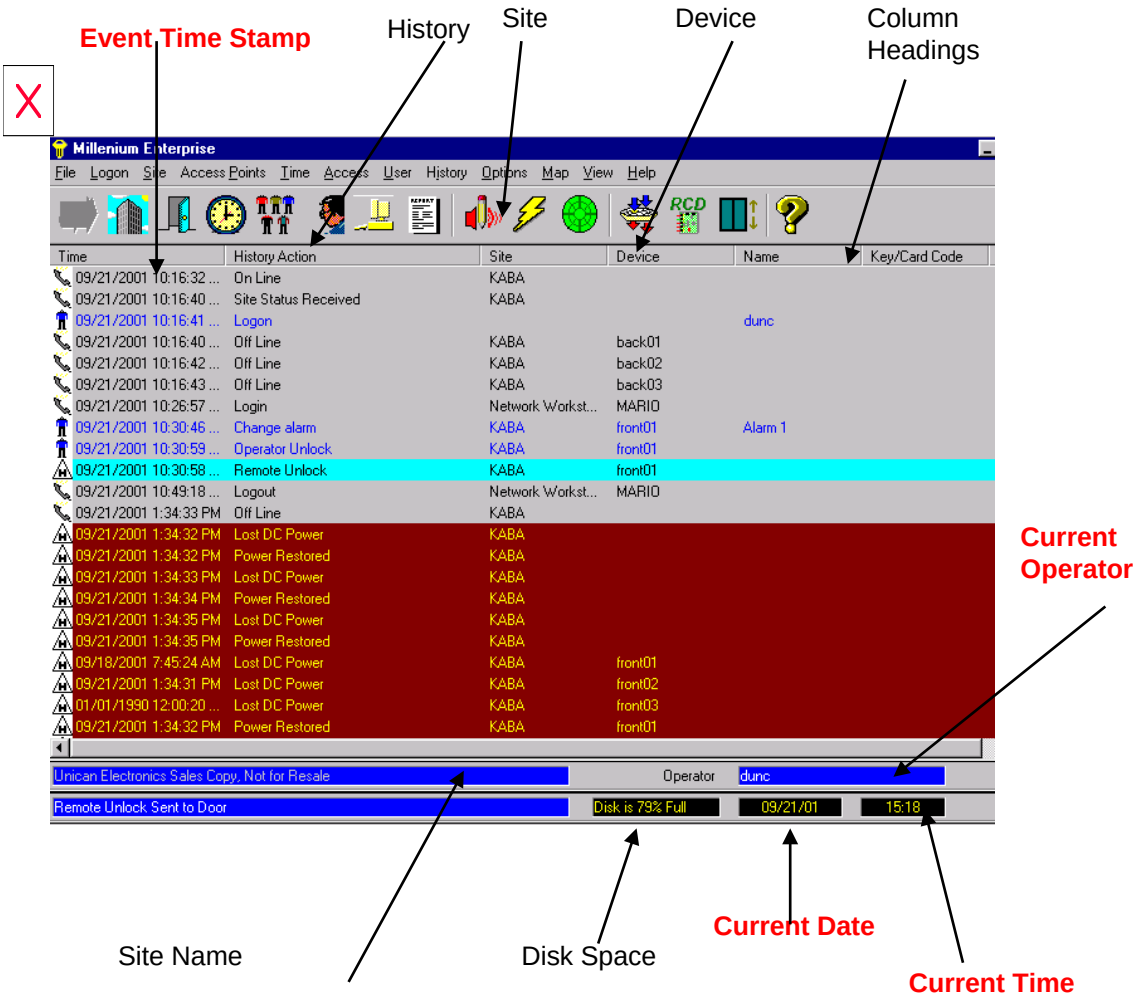
The Millenium Enterprise Family of Software add-ons

- Millenium Enterprise Integrated Badging
- Millenium Enterprise Network License (server/workstation)

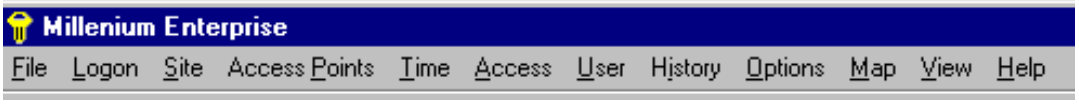
Basic Window Components

Millenium Enterprise offers both a file menu bar and toolbar buttons to open dialog boxes. In these dialog boxes, you enter and edit programming data for the electronic Access Management network. Access Management history is displayed in the background (application workspace.)

Main Millenium Enterprise Window



Menu bar



Toolbar

Menu Bar

Millenium Enterprise menu bar appears along the top of the application workspace, just above the toolbar buttons.

Millenium Enterprise Toolbar

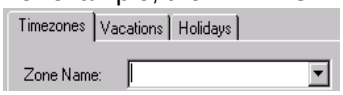
Each toolbar icon corresponds to a topic in the help file.

- Some topics contain one dialog where you create and program a part of your Millenium Enterprise Access Management network.
- Some topics contain multiple TABS that display additional dialogs you can jump between to create and program a part of your Millenium Enterprise Access Management network.

For example, the TIMEZONE icon displays a dialog with two additional TABS: Vacations & Holidays.
Main focus field in a dialog

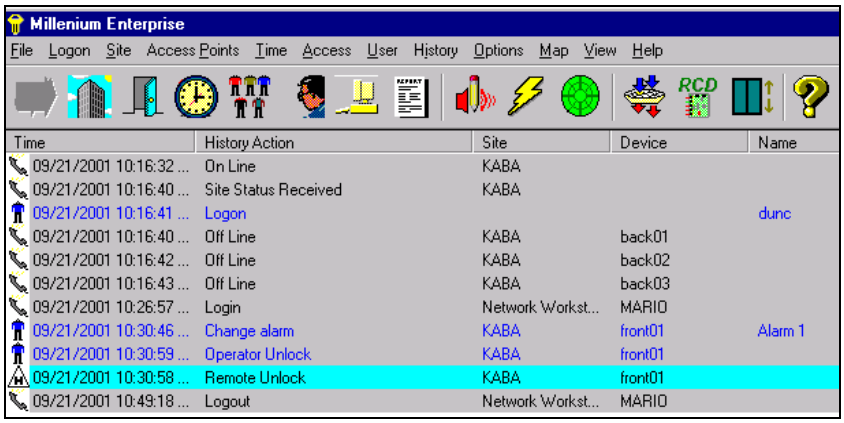
Tabs

Millenium Enterprise uses the index tab method where you can switch between additional windows of information on the same general subject. The tabs in Windows serve the same function as a tab index where you flip quickly between index cards with different segments of information.
For example, the TIMEZONE dialog includes three tabs:



TAB #1 = TIMEZONE: Name and overall settings.
TAB #2 = VACATIONS: Special vacation information that applies to Timezones.
TAB #3 = HOLIDAYS: Special holiday information that applies to Timezones.
The ACCESS POINTS dialog involves two “tabs:”

Application Workspace



Column Headings in the Application Workspace

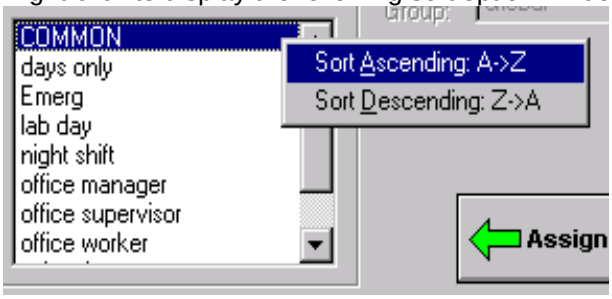
Notice the column headings for the segments of history information. You can adjust the column widths, and the program will retain the preferences set at your PC.

Sorting

Millenium Enterprise offers the option of sorting listbox data in ascending or descending order. This can be useful if, for example, you have a huge number of doors at a site and want to see the doors in alphabetical order rather than in the order by which you added them in the software. Also, with a large number of timezones or access groups, it can be helpful to list them in alphabetical order.

To sort a listbox:

1. Move the mouse anywhere inside the listbox you want to sort.
2. Right-click to display the following sort option window:



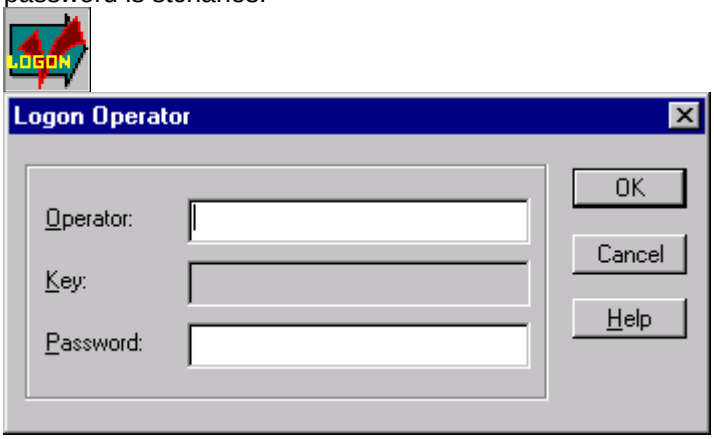
3. Highlight the sort option you want to use, and press ENTER, or double-click the desired sort order.

- The sort order remains until you close the dialog.

Chapter 2: Logging on to Enterprise

Once software is installed and at least one Level One operator has been created through Millenium Enterprise, log on using the assigned Operator ID and Password.
If you have a Marlok key-based system, you can disable manual logon (through **SetupMpw, see Chapter 3**) and insert your Marlok key in the wedge-shaped key reader unit connected to the PC.

If Millenium Enterprise is already running, click the Logon icon on the Millenium Enterprise toolbar, and type your Operator Logon ID and Password.
If this is the first time you are running Millenium, the default operator name is marlok and the password is stcharles.



If you have a Marlok key and a wedge key reader beside the PC, just insert the key and type your password.
NOTE: Only **Level One** operators can: log on to the setup program to modify overall system configuration settings or add operators to the system.

Login ID

The Login ID is a name the operator uses to log on to Millenium Enterprise. The ID should be brief to minimize the number of keystrokes required, but it must be at least two numbers or letters long. Each Login ID must be unique.
This Login ID will identify the operator in Millenium Enterprise history and in the Alarm Monitor.
A Level 1 operator establishes the Login ID in the OPERATORS dialog.

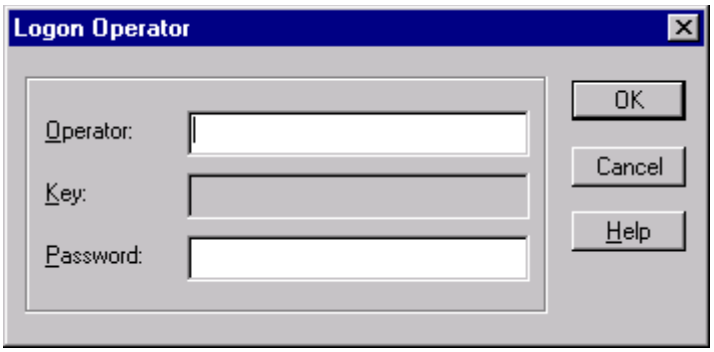
Initial Login ID

If you are entering the system for the first time, use marlok as the ID and stcharles as the password. Then add operators, following the procedure on page 93.
NOTE:
Limit the 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.

Logging On/Off the Software

When you first open the Millenium Enterprise software, a **Logon Operator** dialog box appears. The system requires a valid logon before it will permit you to exit the software. It is important to follow the proper exit procedure to avoid damage to your Millenium database.

- To log on to the software, use the default or type your operator Logon ID, as established in the Operator dialog.



NOTE: Once you open Millenium Enterprise, a logon is required before you can exit the application.

Once an operator is logged on, the logon button is disabled (grayed-out).

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 logon button becomes enabled and all other Millenium toolbar buttons are disabled. The history is displayed in the application workspace (for DIRECT communication configurations.) The system now requires a valid operator logon.

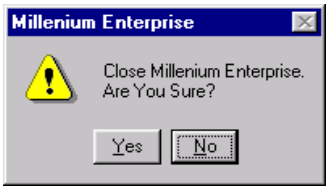
- **To log off the software**, click the LOGON menu item. Then select the **Logoff Operator** option.

Millenium Enterprise remains ONLINE (in DIRECT communication applications) with system history displaying, “as-it-happens,” in the application window.

Except for the Logon toolbar button, all Millenium Enterprise software toolbars remain disabled until another valid operator logs on (described above.)

Exiting Millenium Enterprise Software

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



Closing the software is the same as taking the software off-line from the Millenium Enterprise Access Management devices (DCDs, SCUs, RCDs, ECUs, and ECDs.) Devices continue to retain history of Access Management activity.

DIRECT communication systems will download accumulated history at the next initial logon.

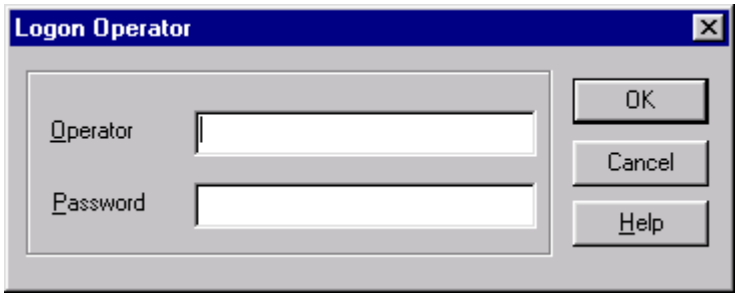
Chapter 3: Setup

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 Enterprise Setup

The Millenium Setup requires a separate login.

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



- If you have not yet created an Administrator in your Millenium Enterprise application, use marlok as the Operator and stcharles as the password.
- If you have an operator, use his/her name and password, as in the example above.

The Setup Module can be closed without logging off.

Default Settings

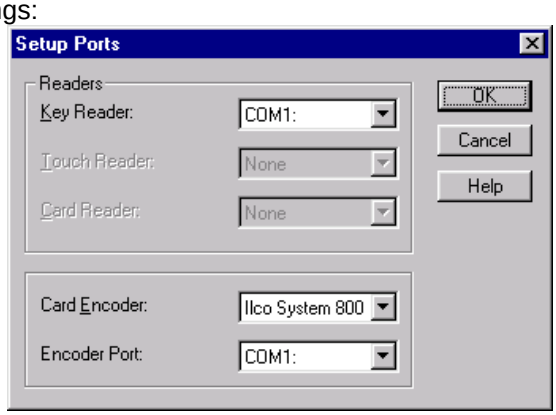
Millenium Enterprise Systems is configured with default settings that should be checked after installation and following upgrades to software or control devices. Some of these defaults MUST be modified depending on your individual access control installation.

Configuring Millenium Enterprise Setup

SETUP affects the following portions of Millenium Enterprise Systems:

Setup PORTS

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



1. **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**.

2. **Com port assignment for making ABA cards on an ILCO System 800 encoder,** if applicable.

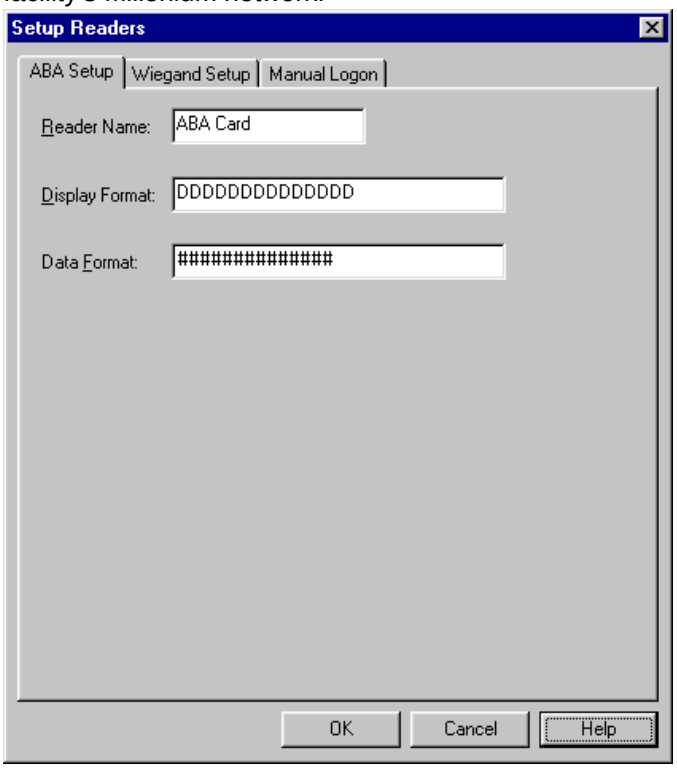
Click on Ports menu and the following dropdown menu appears, enabling you to configure two things:

3. **Serial port assignment for Millenium console key reader**, if applicable. – same dialog box as above
4. **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

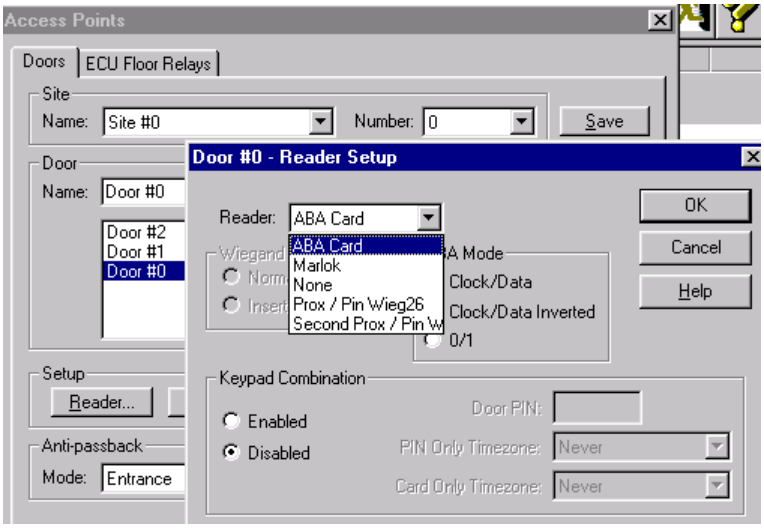
Click on the Reader button  . The following dialog box shows important settings you must make depending on the types of access control CARD READERS installed in your facility's Millenium network.



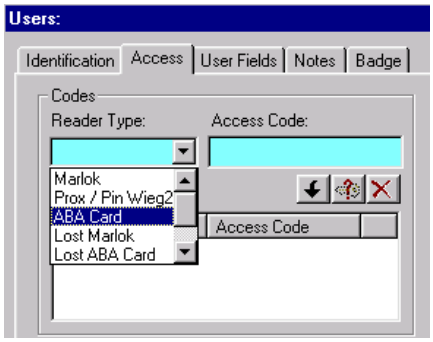
The READER NAME you type in here in Millenium Setup will be the option that appears in the door's READER field in the Access Point Dialog in the Millenium Enterprise main application.

Access Point Dialog

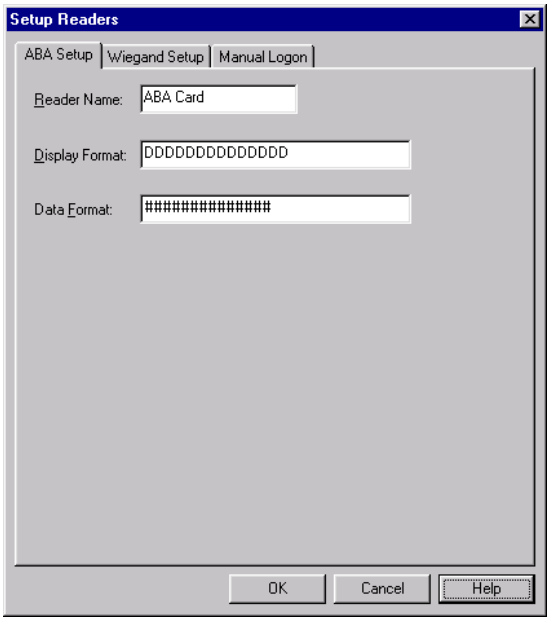
In the dialog, click on the Reader... button. The Reader Setup dialog pops up.



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

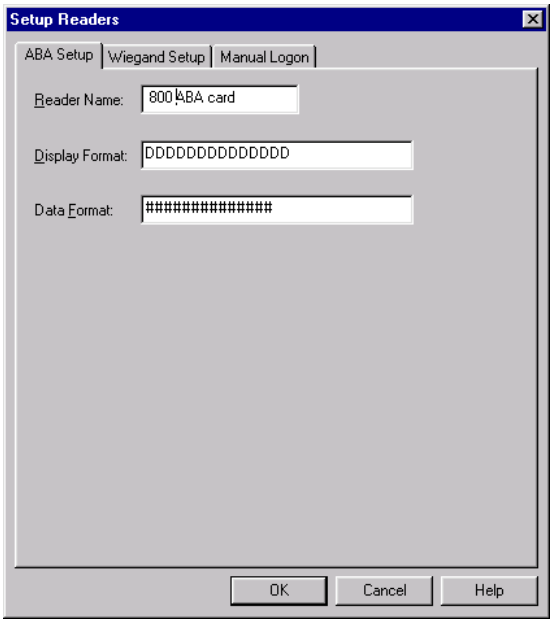
Use the following symbols when creating a custom **DATA FORMAT** for ABA cards:

SYMBOL	*REPRESENTS*	*THE SYMBOL Means*
#	**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.

Step-by-Step: Set up ABA for Use with System 800 Encoder

Millenium Enterprise 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 setupmpw.)
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:

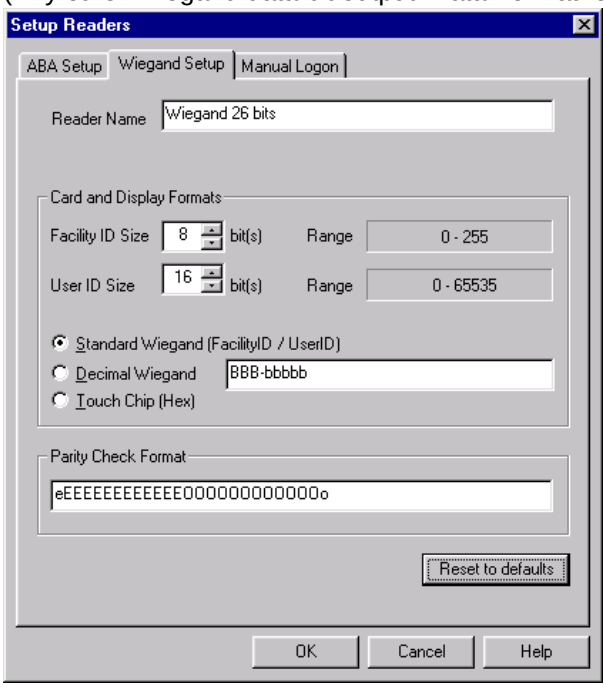
(1.) **DDDDDDDDDDDDD**
(2.) **DDDDDDDD** (or you could include separators: **DD–DDDDDD**)

Once you have completed the steps in setupmpw, you are ready to make cards through the main Millenium Enterprise 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.



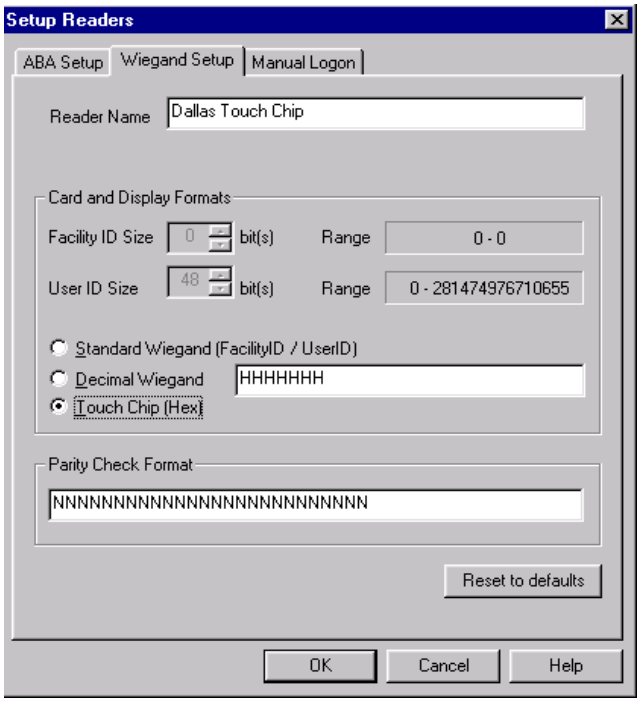
Three possible display options (DISPLAY FORMATS) exist for the **default** 26-bit Wiegand output shown in the second illustration below:

1. **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:

2. **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.



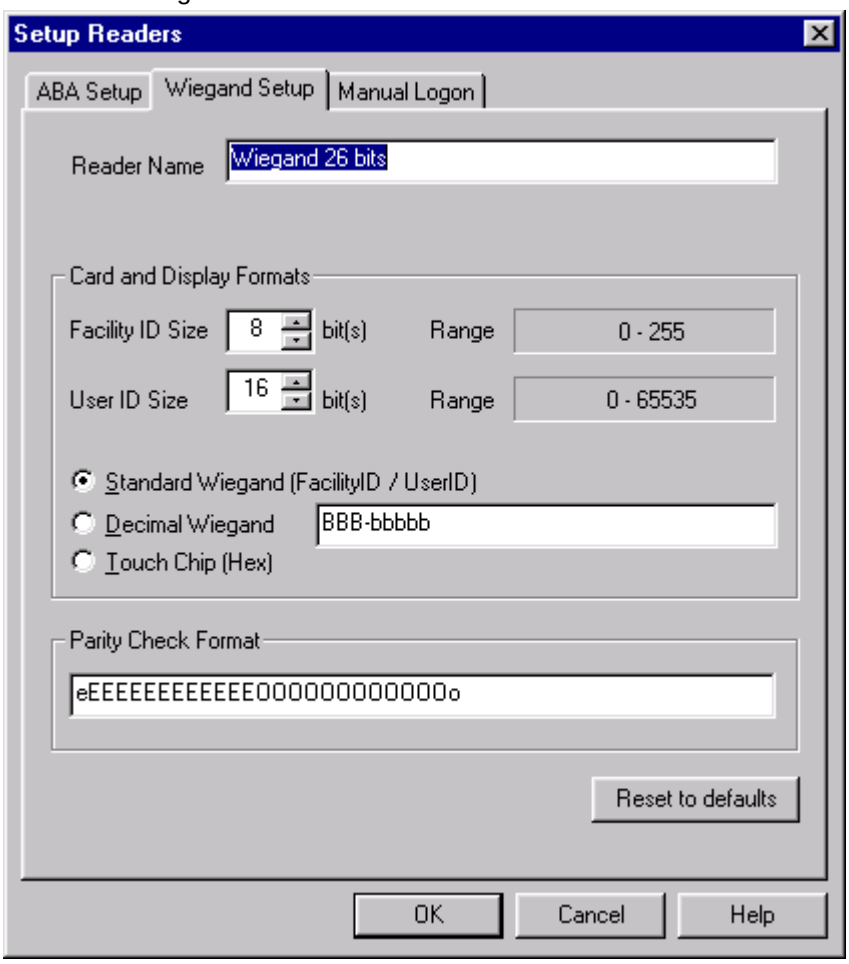
Wiegand Data Format

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

SYMBOL	***REPRESENTS***	***SYMBOL MEANS***
o	ODD parity bit	This exact position in the DATA FORMAT will be an *odd* parity bit character.
e	EVEN parity bit	This exact position in the DATA FORMAT will be an *even* parity bit character.
O	Data-making ODD parity bit	This exact position in the DATA FORMAT will be an *odd* 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 *even* 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 Millenium supplied) are proprietary and are not the responsibility of Millenium. 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.

3. **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.

Step by Step: Setting up Wiegand

1. Select Setup from the Start menu
2. Log in, using your Millenium Enterprise 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.

5. 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.
6. 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 where you enable users who operate Millenium Enterprise Systems software to logon to the PC by manually typing their **Logon ID** and **Password**.

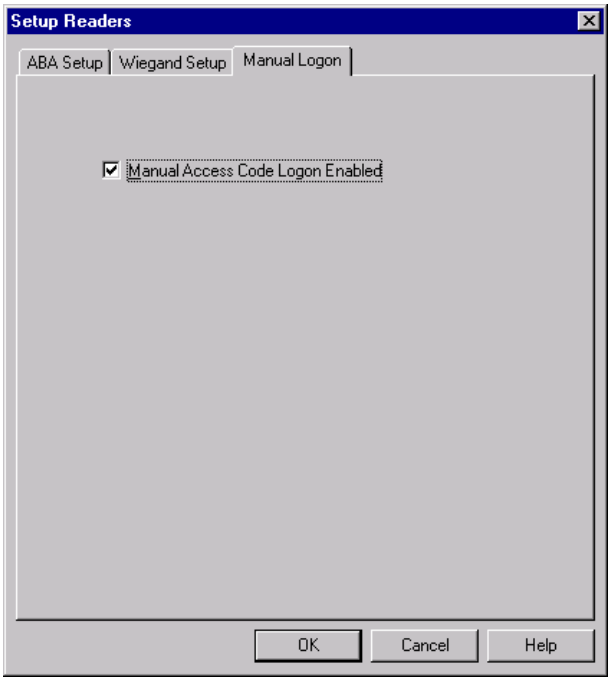
Also, when assigning cards to a USER (on Access tab in USERS dialog in the software,) the operator types in the Access Code. The access code either comes from printing on the card, or from placing the card in a reader and noting the access code as it displays in the software.

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.



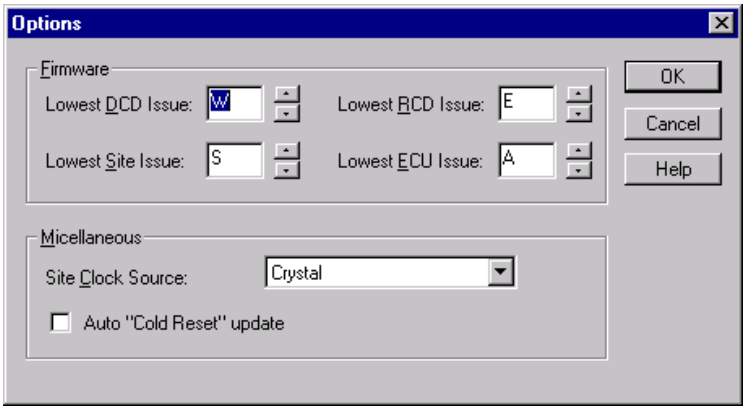
Setup OPTIONS

 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.



All access control devices in the Millenium network must be at least the issue level listed as lowest for Millenium Enterprise 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.

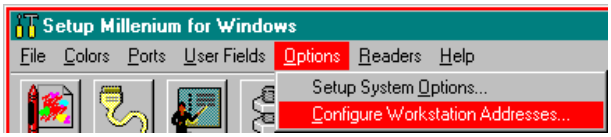
Options Menu

Click on Options in the menubar and Setup system Options will bring up the same dialog box as above.

Network SERVER & WORKSTATION (Network License) add-on option

Installations of Millenium Enterprise that have network SERVER and WORKSTATION add-ons installed have an additional choice under the Options menubar. Click **Options** to record either the server or workstation IP addresses and assign a "name" to more easily identify the IP address.

1. If you are on the SERVER machine, record all workstation IP addresses and give each workstation a name.



2. If you are on a WORKSTATION machine, record the server's IP address and name.

Setting up TCP/IP Network

If you purchased the **network Server/Workstation add-on options** for Millenium Enterprise and installed the add-on software, one of the options described below appears under the OPTIONS menubar.

On the server, you will record the IP Addresses for all workstations.

On the individual workstation, you will record the IP Address for the server.

The IP Addresses you record in these dialogs are the basis for communication between the server and the workstations.

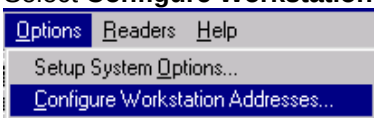
Step-by-step: Setting up TCP/IP Network

Depending on whether the machine being set up is the SERVER or the WORKSTATION:

On the SERVER:

Click **Options** on the setup menubar.

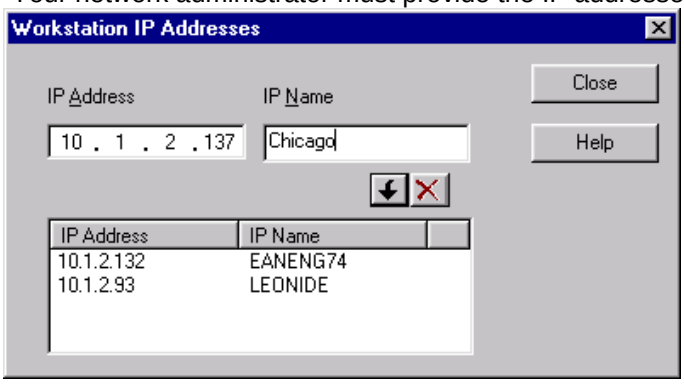
Select **Configure Workstation Addresses**



In the Workstation IP Addresses dialog, record the exact **IP Address** for each WORKSTATION machine that is to communicate with this server.

Important!

Your network administrator must provide the IP addresses.

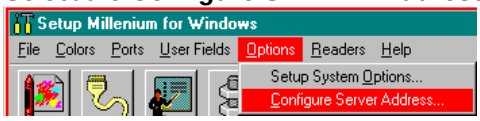


In the **IP Name** field, type a name for each machine that will clearly identify it in the Millenium system.

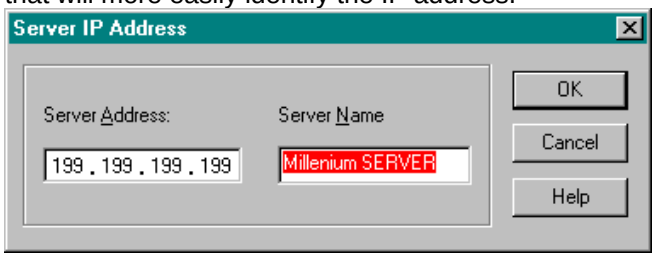
Click the  button to save the address and name. (To delete an IP address and name, highlight the address and click the  button.)
Press CLOSE.

On the WORKSTATION:

Click **Options** on the setup menubar.
Select the **Configure SERVER Address** option.



Record the IP address for the SERVER (**Server Address**) and assign a **Server Name** that will more easily identify the IP address.



Click the button.

NOTE: After adding a workstation IP address into the server, Millenium must be restarted to load the new address into memory and allow communications with the workstation.

Setting up TCP/IP to Sites

TCP/IP communication to sites requires installation of two items:

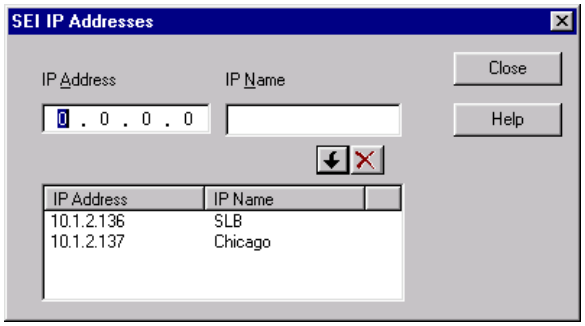
- Ethernet card in the PC
- Site Ethernet Interface (SEI) unit in the Millenium device network

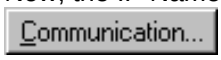
The exact IP Address of the Site Ethernet Interface (SEI) unit must be recorded as described below.

Step-by-step: Setting up TCP/IP to Sites

1. Click **Ports** on the setup menubar.
2. Select **SEI IP Addresses**

3. Record the exact **IP Address** of all Site Ethernet Interfaces (SEI) installed. **NOTE:** PC must have an Ethernet card installed.



4. Give each SEI an **IP Name** the operator will recognize in the Millenium Enterprise' Site dialog (Site Communications sub-dialog.)
5. Click the  button to save the address and name. (To delete an IP address and name, highlight the address and click the  button.)
6. Click the CLOSE button.
7. Now, the IP Name(s) you just set up will appear in the Site dialog. When you press the 

button, a Site Communications sub-dialog displays. You then select the SEI's **IP Name** for the given site from the Com Port drop-down listbox.

TCP/IP to sites

Millenium Enterprise can communicate to Site Control Units (SCU) by TCP/IP protocol.

- Communication from PC is via a built-in Ethernet card.
- Site communication is via a device called a **Site Ethernet Interface** (SEI) unit.

Important!

TCP/IP setup requires naming of SEIs and assigning IP addresses in setupmpw. The name you establish for each IP address recorded in setup appears to the operator in the Site dialog, as follows:

1. Click the 

button to display the Site Communications dialog.
2. Click the drop-down listbox for the COM PORT field.

3. Select the SEI name. (The SEI name is associated with an IP address through Millenium Enterprise' setup.)

Server/Workstation add-on options also use TCP/IP communication protocols.

IP Addresses

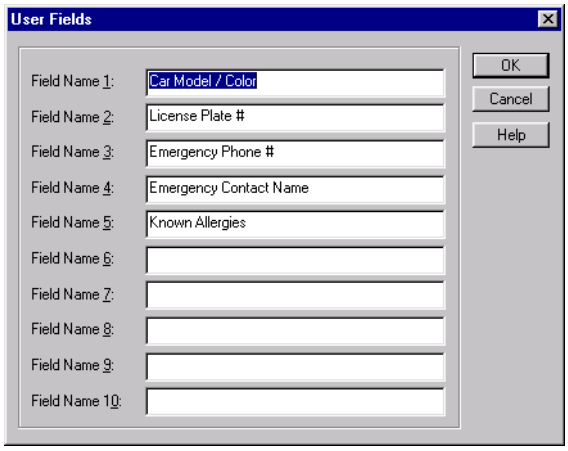
To setup IP addresses for TCP/IP communications protocols, record the exact IP addresses (as provided to you by your network administrator) in Millenium Enterprise setup. Both the following options include an **IP Name** field where you can identify an IP address by a text name that is easier to recognize in Millenium Enterprise software.

Time Differences in Millenium Networks

Two fields on the Site Communications dialog handle situations where a Site Control Unit (SCU) exists in a time zone that differs from the main Millenium Enterprise computer with the server.

Setting up Custom User-Defined Data Fields

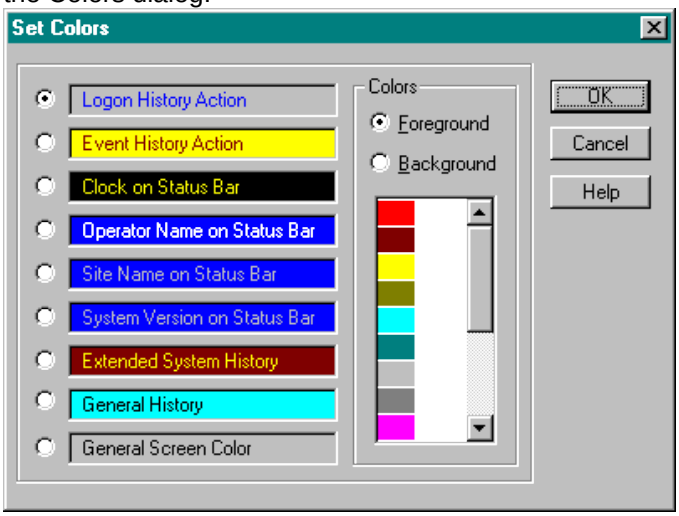
Click on the icon shown at left and the following dialog box appears:



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 above graphic shows the COLORS setup function in Millenium Enterprise Systems.

Chapter 4: Tenant Feature

Overview

Please read the following carefully before attempting to create Tenant Groups. See Adding Tenant Groups for the procedure of creating Tenant Groups.

Why do I need the Tenant Group Feature?

The Tenant feature allows specific entries in the database to be seen and manipulated only by certain "Tenant Groups". When the database is divided into spheres of control in this way, operators in a given group (each one is called a "Tenant Group") will control data such as sites, doors, users, and access groups for their own group only. The database itself is all there, but parts of it are masked so that what the user can view, add, modify, or delete is limited by the Tenant Group they belong to as well as by Operator level. The key to working successfully with this feature is to set up the Tenant Groups properly at the beginning. It is important to read the documentation, think the process through and decide just how you want the Tenant Groups to work.

Benefits of Tenant Groups

Here are some examples of applications where Tenant Groups are useful:

1. To create independent spheres of access within the Millenium Enterprise system.

Example: A branch office building - the branch office Tenant Group is under the independent control of the management's tenant operators. No other software operators can see or program data for the given doors. Operators can add or remove users from Access Groups and Doors that belong to the operator's Tenant Group. Operators can set when the building is open and closed. So, basically the security system of that building would be controlled by operators who work there, not by Operators at the Bank HQ.

2. To restrict operator views of users.

Example: workers and management - these Tenant Groups are only applied to users - not to sites or access points. A worker assigned as an operator to create employee badges cannot look at data on executives.

Important!

Do not experiment with tenant groups by creating some and assigning them to data.

> Once you assign a tenant group to a data item, you cannot simply change the tenant group assignment. Instead, you must **delete the data item** and re-create it with the desired tenant group assignment.

Read the documentation, think through the process and plan just how you want the tenant groups to work.

You must plan the tenant group setup before programming the software. Then, begin by adding global items to the database. (The Global Tenant Group is described below.)

Read the following table carefully and then review the topic links below to ensure that you have a good knowledge of the Tenant Group Feature.

Tenant Group Case Study

Tenant Group	Operator Levels	Configuration/Administration	Change and Edit	Alarms and Events	Comments
Global	System Operator Level 1	Create User-defined Tenant Groups, Users, Sites, Common Access Group, Access Points, Operator Levels.	Users, Sites, Operators, Operator Levels, Timezones, holidays, vacations, Device Groups.	Create Alarms and select Events to be reported to all Access Points in System.	Global does not have operators. It is accessed and edited by System Operator. Accessed and viewed by Tenant Group operators. All doors created in a Global Site are Global. User-defined Tenant Groups can add Access Points for their Group. Has only one Access Group – Common.
	User-defined Tenant Group Operator, Level 1	View all data, create Users, Access Groups, Access Points, Operator Levels for own tenant Group.	Cannot edit Global data.	Create Alarms and select Events to be reported to all Access Points for own Tenant Group.	
System	System Tenant Group Operator Level 1	Create User-defined Tenant Groups, create operators in System Tenant Group, create Users, Sites, Access Points in System Tenant Group. View all other Tenant Groups and Global Items.	Modify Users, Sites, Access points in System Tenant Group, change Users from one Tenant Group to another, change User's Primary Access, Assign Users to Master Access Group.	Create Alarms and select Events to be reported to all Access Points in System.	View all other Tenant Group and Global items.
User Defined	User-defined Tenant Group Operator Level 1	Create User-defined Tenant Groups, Users, Sites, Access Groups, Access Points, Operator levels and Operators for own Tenant Group only, If User –defined Tenant Group is deleted by System Operator. All items controlled will convert to System.	Modify Users, Sites, Access Groups, Access Points, Operator Levels and Operators in own Tenant Group only.	Create Alarms and select Events to be reported to all Access Points in own Tenant Group only.	View but not edit items from Global Group. See only Users, Sites, Access Points, etc. that belong to their own Tenant Group, plus Global items. Can see several Tenant Groups if user has multiple Tenant Group assignments.
	User-defined Tenant Group Operator Level 2	Access and view own Tenant Group.	Access and view own Tenant Group.	Access and view own Tenant Group.	Access and view own Tenant Group.

See all of the following for further information:

- Operators and tenant groups on page 40
- Users and tenant groups on page 41 .
- Access Groups and tenant groups on page 77.
- Sites and tenant groups on page 38.
- Doors and tenant groups on page 41.
- Tenant Groups Case Study on page 29

Two Default Tenant Groups

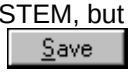
Global Tenant Group

The main purpose of the GLOBAL tenant group is to hold data that appears to operators in any tenant group.

- All operators can view, but not edit Global data
- Only operators in the SYSTEM tenant group can create Global items.

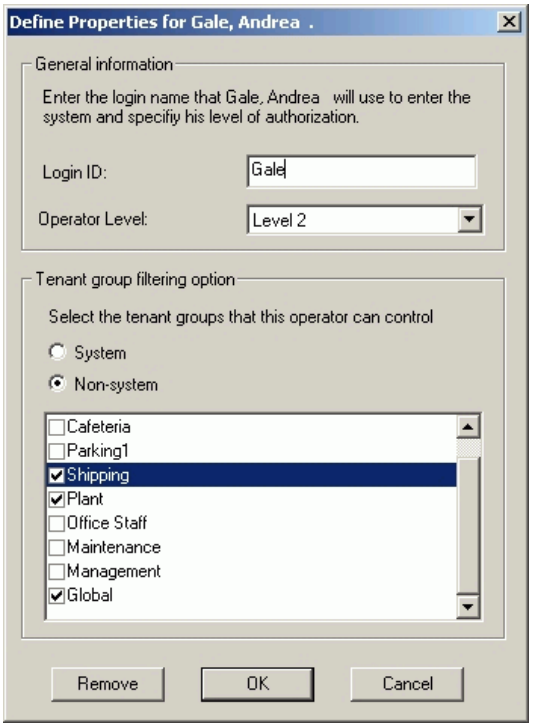
Some pre-defined items belong to the Global Tenant Group:

- Operator Levels
- Timezones
- Holidays
- The "GLOBAL" Access Group
- Relay Control Devices
- Filters
- Resident Filters
- Tours

If a Site is Global, an operator from any non-system tenant group can add a door **for their tenant group** to that site. If the operator is a SYSTEM tenant operator, the new door will default to SYSTEM, but can be changed by the SYSTEM operator up until the time the operator presses the 

button.

The GLOBAL tenant group is already in the system, but operators must be given rights to it just like any other tenant group. The Level 2 operator, Gale, has been given rights to Global in the illustration below.



System Tenant Group

The main purpose of the SYSTEM tenant group is to hold operators that create and oversee **all** non-system tenant groups.
Only operators in the System tenant group can:

- Perform **all** operations on **all** data items in the Millenium Enterprise database (based on operator level rights.) In other words, only a SYSTEM tenant operator can create any item in any tenant group. Non-system tenant group operators can only create new items or edit existing items **in their own tenant groups.**
- Assign a user to the **"MASTER"** Access Group. This group permits access to all doors at all times. There should only be one or two members in this **"MASTER"** Access Group, since they have such sweeping powers of access.
- Items in the SYSTEM tenant group are not visible to operators in non-system tenant groups.

Non-System Tenant Groups

Level 1 operators in the SYSTEM tenant group create all non-system tenant groups (all tenant groups other than GLOBAL and SYSTEM.)
Operators in non-system Tenant Groups can perform the following (based on their Operator Level:)

- **View GLOBAL items**. (See all items in the software that have a Tenant Group assignment of GLOBAL.)
- **Create and edit items in their own tenant group**. When operators from a non-system tenant group logon to Millenium Enterprise software, the operators only see users, sites, doors, etc. that belong to their own tenant group plus items in the GLOBAL group.
- **View users** with multiple tenant group assignments:
  - must have been created by SYSTEM tenant group operators

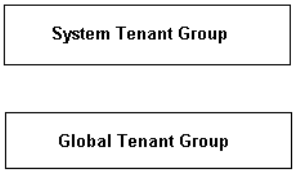
    OR

- must have been created by the non-system tenant operators and **then** assigned to additional tenant groups by a SYSTEM tenant group operator.

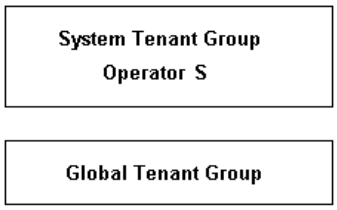
Important!

When a SYSTEM operator deletes a non-system tenant group, all items owned by that group are automatically placed in the SYSTEM tenant group.

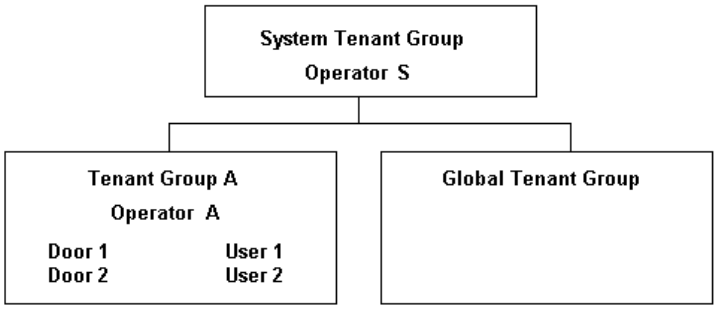
Multiple Tenant Groups Feature - Overview



There are two predefined tenant groups, System and Global. They cannot be altered or deleted, although objects can be assigned to them. Indeed, objects must be assigned to the System Tenant Group; if it is empty, nothing can be done whatsoever, since there is no operator to do it. In order to make the database useful, we need to create a System Tenant operator.



Now that we have an operator in the System tenant group, we are free to create other database objects as required. Millenium Enterprise can be deployed using only the System tenant group, but in doing so the operator forfeits some powerful access control features that come with tenant group use. More typically, the System tenant will remain very exclusive, and will thus have little in the way of users and access points. These objects will be created in other Tenant Groups for management by other operators. In this case, our System operator (Operator S) needs to create tenant groups as required for the people who need access to any assets in the database.

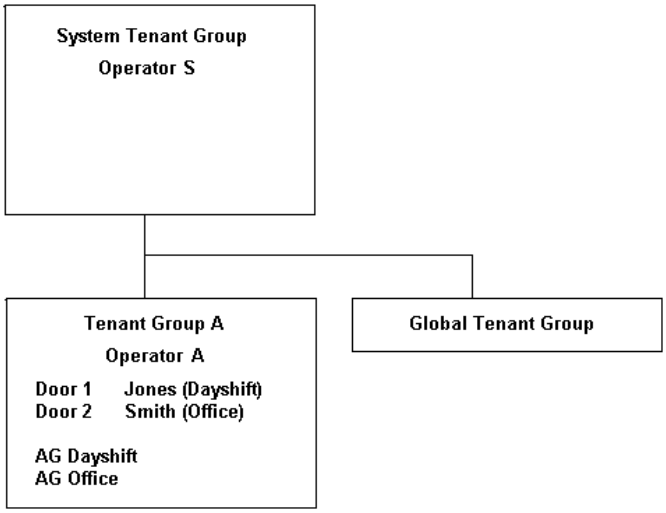


At this point we have doors and users in a tenant group, but no one has access to anything yet. To assign access, Operator A creates Access Groups. Each Access Group is a list of all doors in the Tenant Group, with a predefined timezone assigned to each. Let's say that the operator sets up two Access Groups as follows:

	AG TGA: Dayshift	**AG TGA:Office Staff**
Door 1	08h00 - 16h30	05h00 - 20h00
Door 2	12h00 - 13h00	12h00 - 13h00

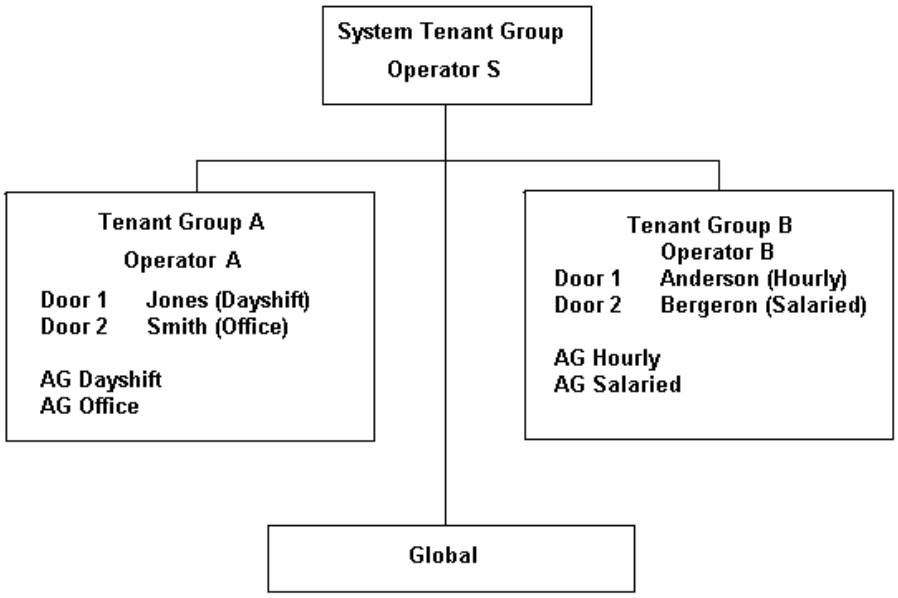
Then he can assign access to his users by assigning each user to an access group. The operator must create a separate Access Group for each unique combination of timezones to doors that he wishes to employ. Now say that the operator assigns access as follows:

User	**Access Group**
User 1	AG Dayshift
User 2	AG Office Staff



Now all users have designated timezones during which they can access any door in the Tenant Group. User Jones, for example, can access Door 1 from 08h00 to 16h30, because he is in the Dayshift Access Group.

This setup is fully functional but barely takes advantage of the Tenant Group concept. The only difference between this and a purely SYSTEM (that is, no Tenant Groups) setup is that Operator A cannot create other Operators or Tenant Groups. The tenant concept becomes more interesting and useful when we have more than one non-system tenant. Suppose, in a manner similar to what we have done already, the System operator creates another tenant - Tenant Group B. He also creates a TGB Operator, Operator B, who enters doors and users, and assigns access as required by his own configuration.



Tenant Group A	**AG Dayshift**	**AG Office Staff**
Door 1	08h00 - 16h30	05h00 - 20h00
Door 2	12h00 - 13h00	12h00 - 13h00

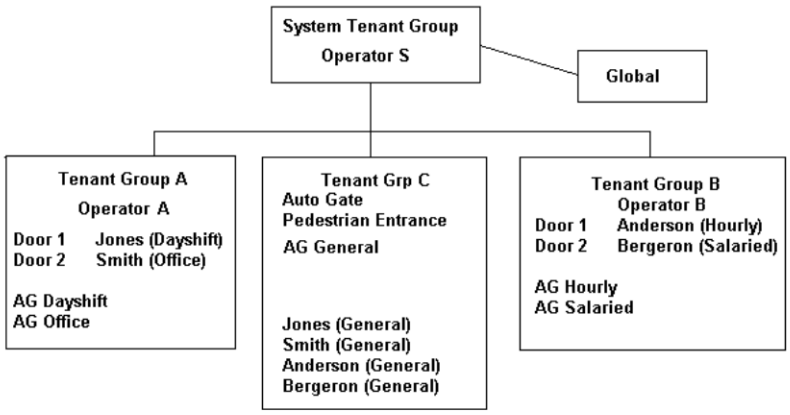
User	**Access Group**
Jones	AG Dayshift
Smith	AG Office Staff

Tenant Group B	**AG Hourly**	**AG Salaried**
Door 1	07h30 - 16h00	07h30 - 16h00
Door 2	06h00 - 20h00	06h00 - 20h00

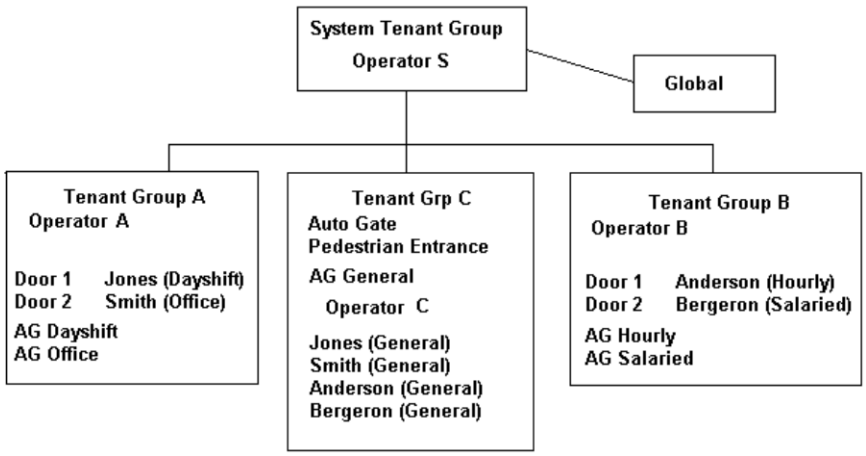
User	**Access Group**
Anderson	AG Hourly
Bergeron	AG Salaried

This is a basic example of Tenant Group use. In this configuration though, there is no provision for a resource being shared by more than one Tenant Group. For instance, if both tenants use the same parking facility, there may be a common gate and a pedestrian door that would be used by both tenants. One door cannot belong to more than one tenant group, but users and operators

can. The easiest way to set this up therefore is to make the parking facility a tenant group in its own right, and make all four of our users part of it.

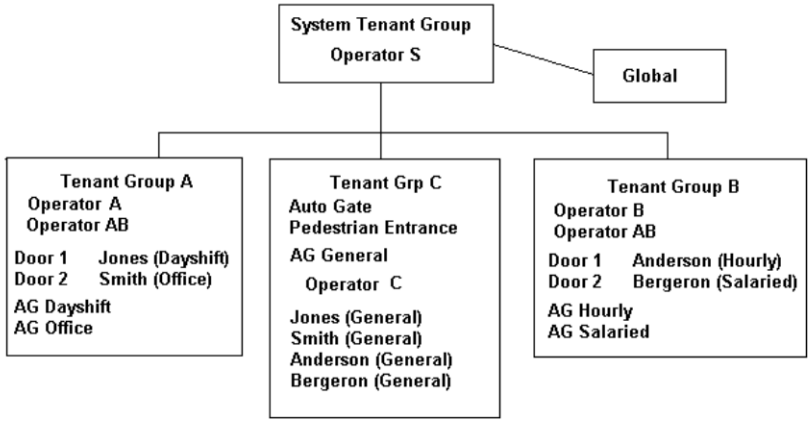


Now we can see that a new tenant group C has been created, with a gate for the cars and a door for pedestrians. Tenant group C has a single Access Group, General, whose specific details are not important for this discussion. Since operators and users can access multiple tenant groups, we were able to assign all users to Tenant Group C. Now we have a problem though; if we assign Operators A and B to tenant group C, each will have access to the other's tenant group assets. E.g., Operator B would then be able to delete the user Jones; thus tenant groups A and B would be effectively combined into a single entity. A better configuration would be as follows, where Tenant Group C will have its own operator, but with reduced operator rights:



Now the System operator has created an operator C who has access to all Users of TG C, which in this case is all of our users in the system. He can assign each user access to the two doors in the parking facility. He cannot however, delete or otherwise modify any of the users. That responsibility will be left to Operators A and B.

Now that we are making full use of multi-tenant users, the only remaining feature to illustrate is that of multi-tenant operators. (Note that even though all operators are users, there is no relation whatsoever between tenants to which the user is assigned and tenants to whom the operator has access). Like a user, an operator can be granted access to any combination of tenant groups. We may desire, for example, an operator who can work in both tenant groups A and B, but has no jurisdiction over TG C. We would ask the System operator to create an operator AB, as follows:



If desired, Operator AB can have full Operator rights; otherwise, he can be configured with restricted rights by the System Operator. Operators can be set up with any combination of Tenant Group access and Operator Rights, resulting in an improved degree of flexibility that has never before been available.

The last point to mention is the pre-defined Global Tenant Group. It exists largely for legacy purposes, as well as for possible future enhancements. In the current version of Millenium Enterprise, Global is just another Tenant Group, to which any operator, user or access point can be assigned by any operator with sufficient rights. The only difference is that it cannot be renamed or deleted.

Adding Tenant Groups

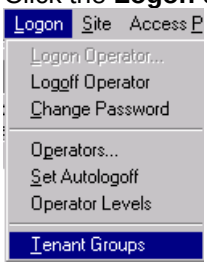
Important!

The Tenant feature has a far-reaching effect on your Millenium Enterprise database. It is essential that you read and understand the feature, and plan Tenant Groups carefully before adding them to the software.

Tenant feature overview

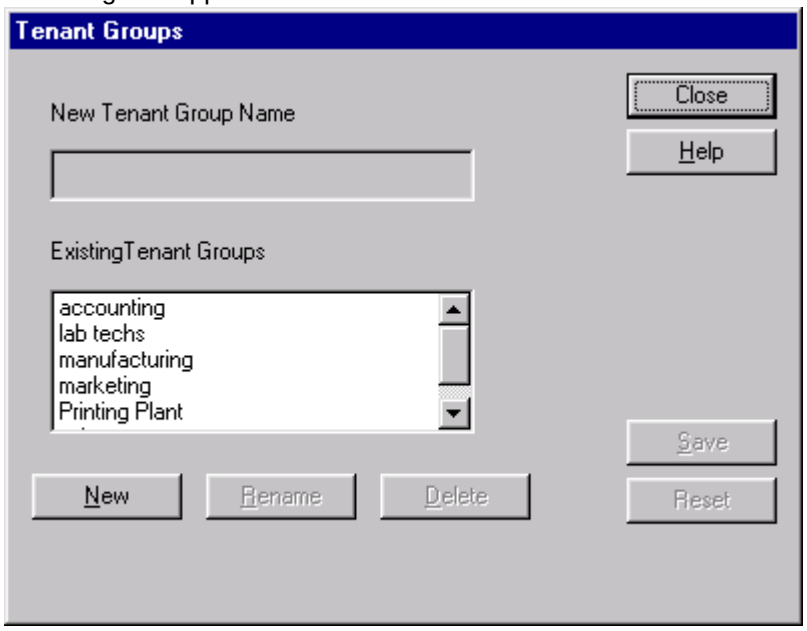
Step-by-step: Creating Tenant Groups

1. Read up on the tenant feature and plan tenant groups for your specific installation.
2. Click the **Logon** option from the Millenium Enterprise menu bar.

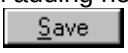


3. Select the Tenant Groups option from the drop-down menu.

The main dialog box appears:



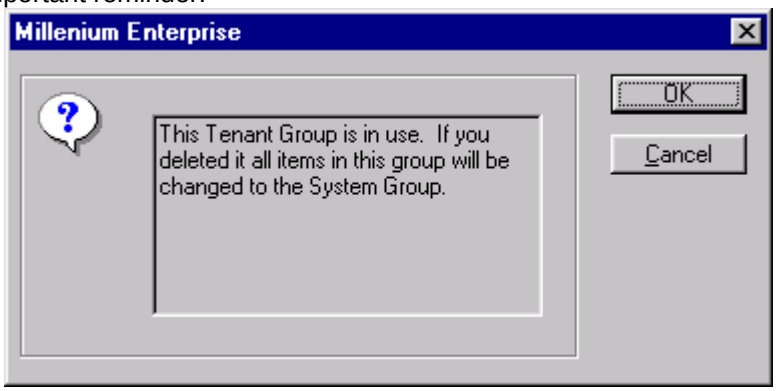
4. Click the 

button.
5. All buttons are then grayed-out until you enter a name for a new Tenant Group as in the example below.
6. Begin adding new tenant groups.
7. Click 

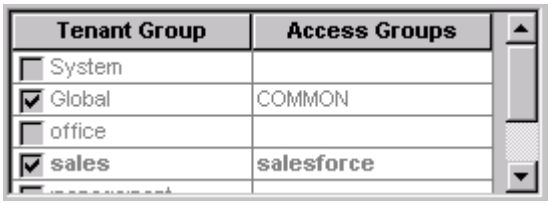
each time you create a new group.
Note that if you select an unavailable name you will receive a message that the name has already been taken.

Renaming a Tenant Group

1. Click on the Rename button to select an existing Tenant Group and rename it if you wish.
2. If you change your mind when adding a group, click the Reset button .
3. Select an existing Tenant Group and delete it if you wish. You will receive the following important reminder:



The tenant groups you have created will now appear in the Tenant Group listboxes throughout Millenium Enterprise dialogs. The example listbox below appears in the Access tab of the main User dialog.



In most cases, the Tenant Group field will appear disabled because, once assigned, a tenant group cannot be changed. The item must be deleted and re-created with the desired tenant group. Only SYSTEM Tenant Group operators can assign any item to any tenant group.

Next, create GLOBAL items.

Tenant Groups (Site dialog)

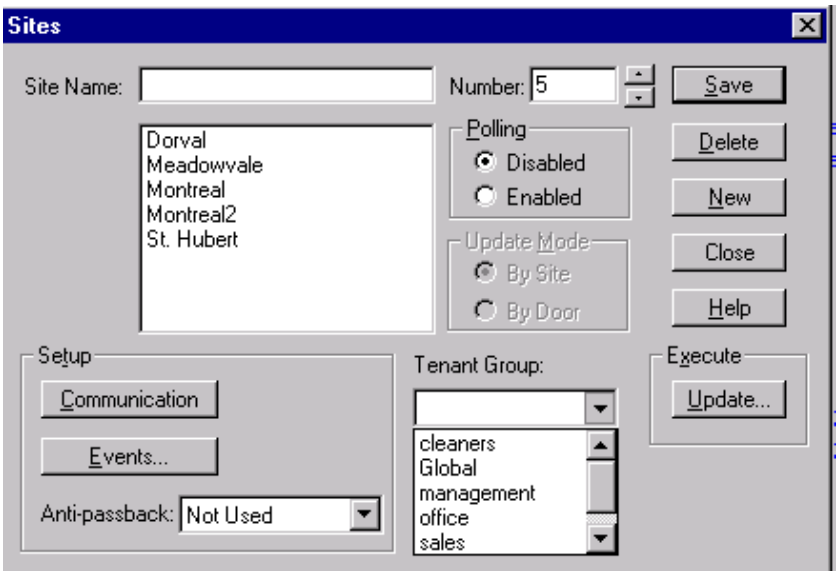
Tenant Group assignments in the Site dialog determine which sites appear to which Millenium Enterprise software operators. The site tenant group assignment not only affects which sites appear, but also affects the doors under the given site.

- SYSTEM sites only appear to operators in the SYSTEM tenant group.
- GLOBAL sites appear to all tenant operators, but can only be added or edited by SYSTEM tenant operators.

Sites with non-system tenant groups only appear to:

- operators from the specific tenant group(s), and
- operators in the SYSTEM tenant group.

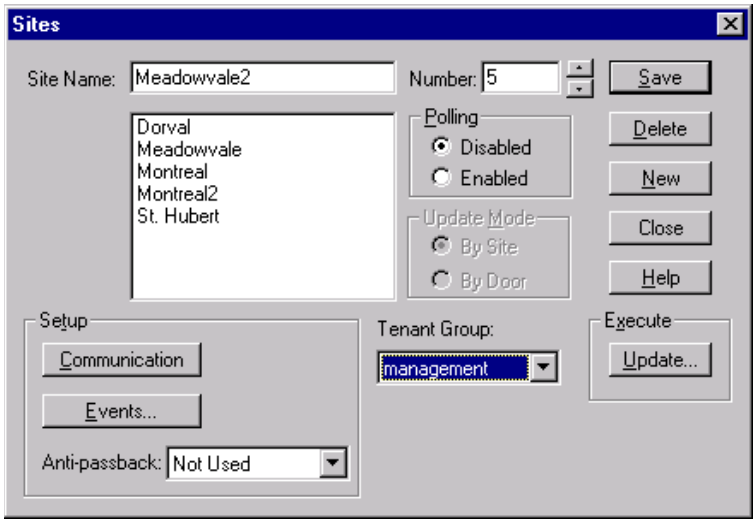
When a SYSTEM operator adds a new site to the software, the Tenant Group field display appears as follows:



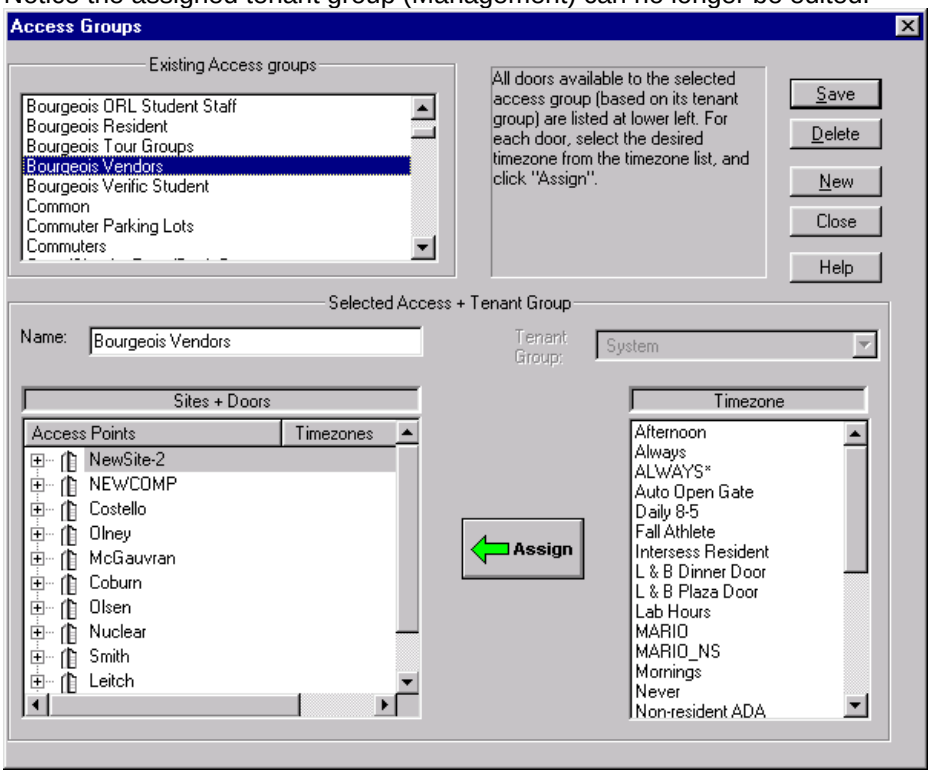
A SYSTEM tenant operator can assign the new site to any tenant group.

WARNING: Once saved, however, the site's tenant group assignment cannot be changed. Instead, the site must be deleted and re-created with the desired tenant group. If doors are programmed for the site along with users and access groups, the impact of deleting a site is far-reaching. All doors under that site will be deleted in the process.

Once a new site is saved, the site dialog appears as follows:



Notice the assigned tenant group (Management) can no longer be edited.



The above site will appear to operators from all tenant groups, but can only be edited by operators from the SYSTEM tenant group.

Operator Levels and Tenant Groups

Operators are those users who operate the Millenium Enterprise software. A Level 1 administrative operator assigns each operator an OPERATOR LEVEL in the OPERATORS dialog. 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. An operator who tries to perform a function that he doesn't have the right to perform will experience one of the following:

- Unauthorized functions do not appear
- A prompt appears informing the operator of insufficient rights to perform the function.

Operator Levels and Tenant Groups control two different areas in Millenium Enterprise.

- Operators control data in their own Tenant Groups to the extent allowed by their assigned operator level.

- Tenant Groups restrict access to data (doors, sites, users, etc.). An operator in a Tenant Group(s) can only view and manipulate items controlled by that group or those groups to which he belongs.

- Operator Levels restrict access to program features. An operator can only view, modify add or delete according to the rights he/she has.

To put it another way, as an operator who is a member of a Tenant Group(s), you only have access to the doors, relays, alarms, ECUs etc. under your Tenant Group(s) control. As an operator in the group(s), your Operator Level determines what you can do with the doors, relays, etc. - whether you can add, change, delete or save information.

There are two general categories of operator Tenant Group:

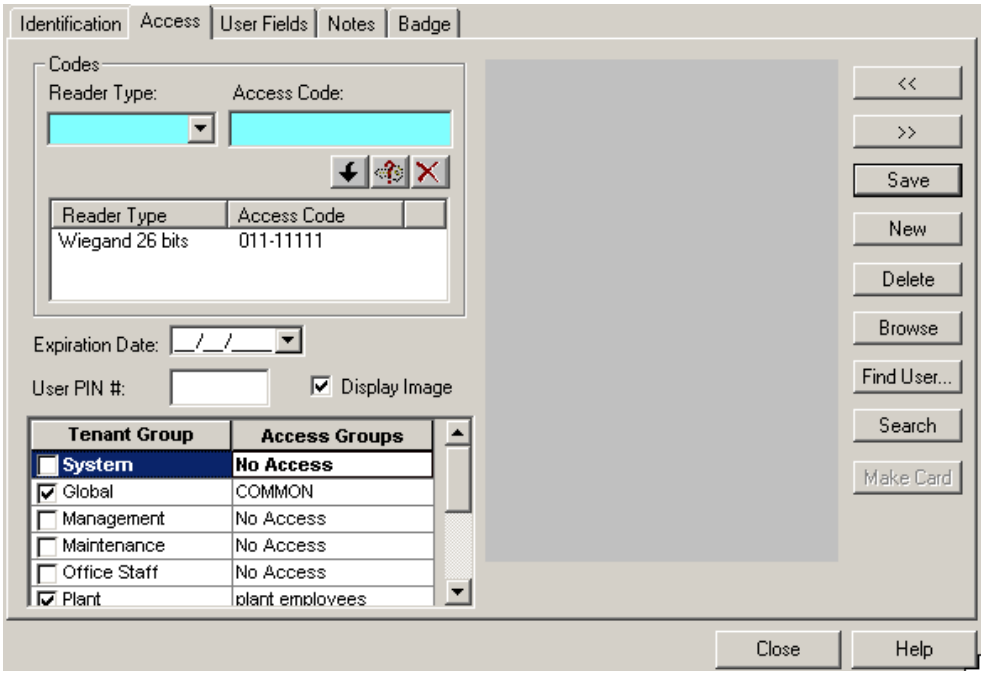
- the special SYSTEM tenant group
- all other non-system tenant groups. No operators belong to the GLOBAL tenant group.

Level 1 has Rights to all Program Features in Millenium Enterprise PLUS the SPECIAL FUNCTIONS described on page 96.

To assign Tenant Groups to Operators, see Adding an Operator on page 93.

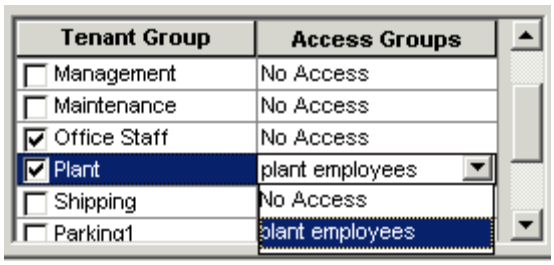
Tenant Groups – User Access

Tenant Group assignments are shown in the Users dialog (Access tab). The box at the bottom left lists the Tenant Group(s) to which the user belongs. For each Tenant Group, the user is assigned an Access Group. The following sample dialog shows the access section as it might appear to a SYSTEM tenant operator:



Facts about Users and the Tenant Group Feature

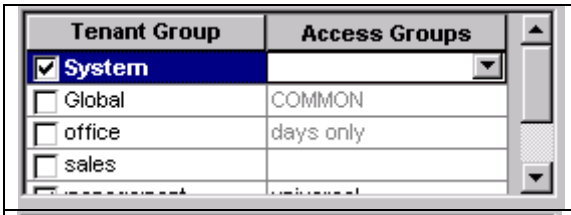
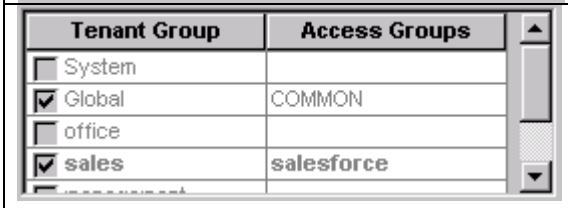
Tenant groups that have no assigned Access Groups read No Access. To assign or change the access group, move the mouse into the Access Group field until the down arrow button appears. Click the down-arrow button to display the drop-down list of all available Access Groups.



Users may belong to multiple tenant groups.

System tenant operator view.

The first example below shows how the access section might look to an operator logged in from the System tenant group .
The second sample shows how the access section might look if the logged-in operator does not belong to the System tenant group:

	System tenant operator view
	Non-system tenant operator view. If operator removes checkmark, user is removed from the tenant group and no longer appears when operators from that tenant group log on.

Important

Only a System Tenant Group Operator can access the Millenium Tour module.

Non-System Tenant Group operators:

(1) Can only see users who belong to their tenant group(s).
If a user belongs to other tenant groups, those tenant groups appear checked, but disabled (grayed-out.)

(2) Can only change the Access Group for users in their own tenant group(s).
In the first two examples above, operators in the Sales tenant group can only change the Access Group for users who belong to the Sales tenant group.

(3) Can only change user data (name, birthdates, etc) for users whose tenant group(s) is/are the same as the operator's own tenant group(s).

Adding new users

When a SYSTEM tenant group operator adds a new user, the user's access appears as shown at the right;
The newly added user's tenant group automatically equals the tenant group of the operator who added the user, System in this case.

Only a SYSTEM tenant operator can assign a user to multiple tenant groups.

System tenant group Level 1 operators may add to or change new user's tenant group(s) by going to the User Dialog, Access tab and checking the desired tenant group(s). (Se illustration above.)

A new user also automatically belongs to the GLOBAL tenant group.

A new user's access group in the GLOBAL tenant group defaults to the "Common" access group. Being in this group allows the user to access all Global access points (usually main doors, washrooms, etc.).

Chapter 5: Sites

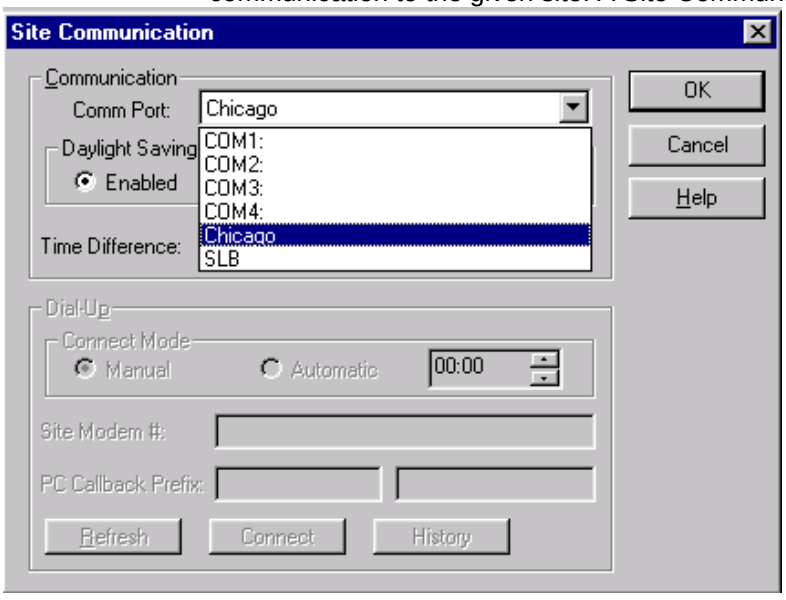
Adding a Site (SCU)

Every Millenium Enterprise network has at least one Site Control Unit (SCU.) 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 for Site Ethernet Interface (SEI) units or installation of a modem though 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.

Step-by-Step: Adding Sites

1. Logon to Millenium Enterprise, and 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.
3. Type in 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 Management devices (SCUs, DCDs) are installed and ready to communicate with the software.
   - 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."
5. SETUP:

Communication... Click this action button to set up the COM Port being used for DIRECT communication to the given site. A Site Communications dialog displays.



Continue programming DIRECT as for sites below:

Alarms... Click this action button to select those DCD Alarms and site-specific actions to be tagged as Site Events for this site. **NOTE:** You should set up DCD alarms and DCD Events for doors (ACCESS POINTS dialog) **before** selecting Site Events.

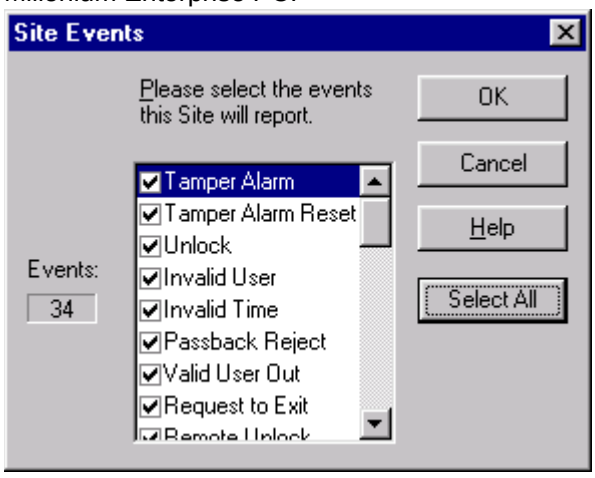
- Anti-passback If this site uses the anti-passback protection feature, select the type of anti-PASSBACK in use.

Press the Add -> button to add the new site to the database.
Assuming all Enterprise devices are installed and ready-to-go:

- Once a DIRECT site is ready to go ONLINE, and polling is ENABLED, this action immediately communicates to the SCU.

Setting up Site Events

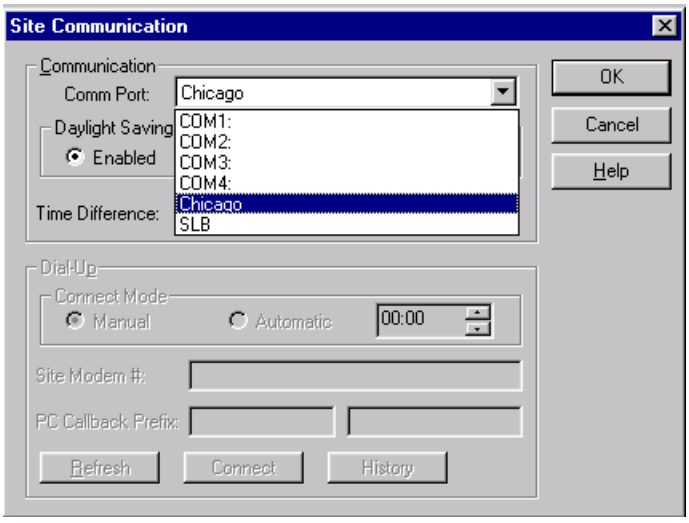
Site events are those actions that will be treated as "events" and cause the SCU to report to the Millenium Enterprise PC.



The Site Events dialog includes some site-specific items such as *Polling Failed* and *Lost AC* in addition to the same list of event options shown for doors (in the DCD events dialog.) Click on an item to select the alarm (and, when applicable, the corresponding reset) to be treated as an “event” for the given site.

Site Communications Dialog

When you press the Communication... button in the SITE dialog, the following dialog displays:



The **COM Port** drop-down selection listbox shows all serial COM ports available through Windows on your computer. The selection you make from the listbox will show the communication connection for the given Site Control and its Millenium Enterprise Access Management devices.

Select one of the following from the COM Ports listbox:

- **COM Port** where the Millenium computer connects directly to the Site Control. Direct connection can also be through such devices as a Trunk Interface Unit or a leased-line modem or TCP/IP to sites.
- **IP Name** (for Site Ethernet Interface (SEI) units)

Before IP Names for Site Ethernet Interface units appear in this listbox, the following must occur:

- Install a Site Ethernet Interface (SEI) unit to communicate by TCP/IP to sites.
- Record the TCP/IP address and "name" (Chicago, in the example above) for the SEI unit through setupmpw.

The names given to individual TCP/IP addresses for all SEIs will appear in the COM Port listbox.

Network communications set up occurs through Millenium Enterprise 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.

Site Ethernet Interface (SEI)

An SEI is an optional, modem-sized device that takes serial output from PC data and converts it to RS-232 output (used by Site Control Units.) The PC must have an Ethernet card installed.

When a Site Ethernet Interface unit is installed with a Site Control Unit (SCU,) Millenium Enterprise can use TCP/IP protocol to communicate to sites.

Setting up an SEI

To see the options described below, you must select SLB as your port setting in the Site Communications dialog.

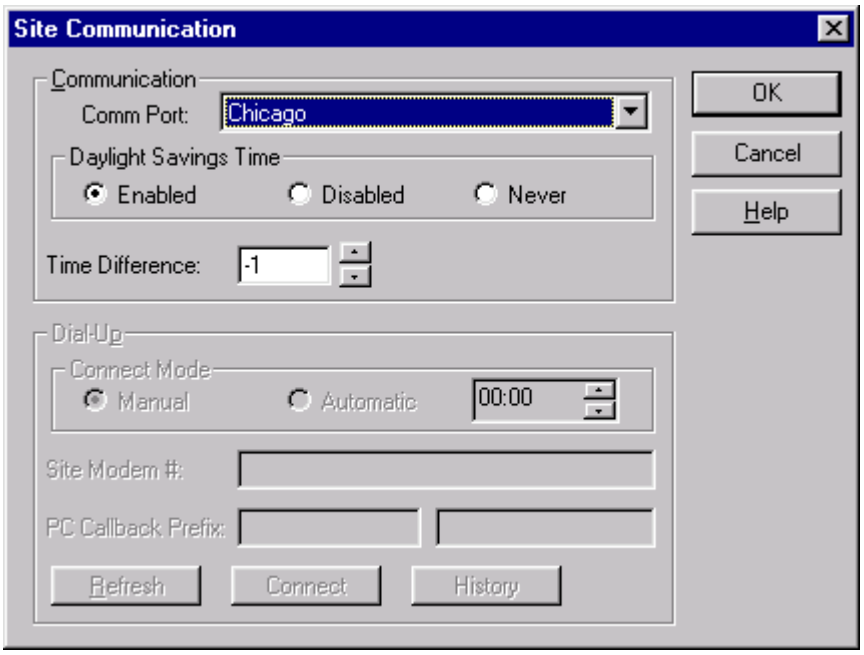
Daylight Savings Time

If the location where this Site Control operates falls under Daylight Savings Time and Standard Time changes, you can enable this option and use the next field to record the Time Difference between the main Millenium Enterprise computer and this site. **Enabled** means the system will compensate for Daylight Savings Time changes by increasing or decreasing the number of hours set in the Time Difference field, below.

Time Difference

If this Site Control Unit (SCU) is located in a region that operates under a different international time zone from the main PC, use this field to record the time difference in hours. Remember that you must always set the **time difference from the Server,** not from another workstation on the network.

Example: Assume the main PC with the server is located in the Chicago and the given Site is located in the East. The Time Difference field entry would be 1, meaning the Eastern site is one (1) hour earlier than the Millenium Enterprise server in the Midwest.



Direct Communications

On-line, “as-it-happens” communication.

Connections between PC and Site Control Unit (SCU) are through Windows-recognized serial ports or through Site Ethernet Interface (SEI) IP addresses. Select the COM port or Site Ethernet Interface (SEI) in Millenium Enterprise's SITE dialog by pressing the 

button.

NOTES:

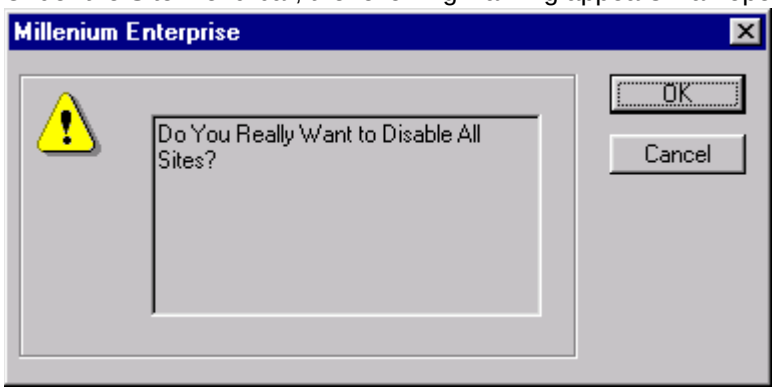
- Set up TCP/IP to sites through Millenium Enterprise Setup (setupmpw.) Requires optional Site Ethernet Interface (SEI) installed through Windows HyperTerminal and an Ethernet card in the PC.
- Set up networked server/workstation configurations through Millenium Enterprise Setup (setupmpw.) (Requires optional server and workstation add-on software.)

Can include connection configurations such as: hard-wired, fiber optic lines or using Trunk Interface Unit (TIU.)

History from DIRECT sites automatically downloads when an operator first logs on to Millenium Enterprise software.

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 Enterprise network.

Only operators with EXECUTE rights can perform this operation.

Important!

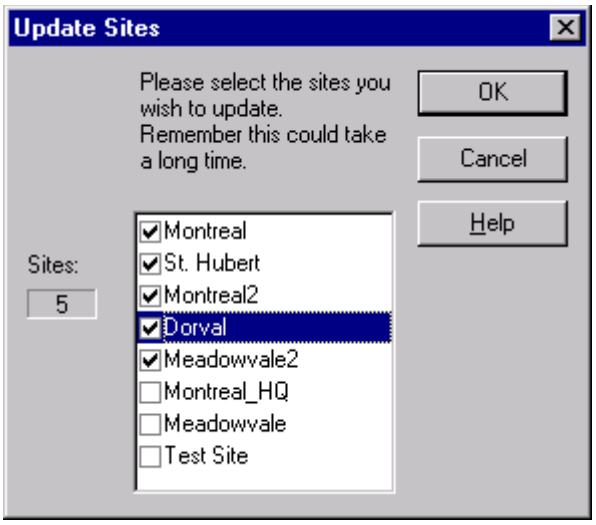
The **Disable All Sites** function is only intended for specific troubleshooting purposes, such as to stop polling all Millenium Enterprise devices to troubleshoot overall network problems. This function is rarely used.

Update Site

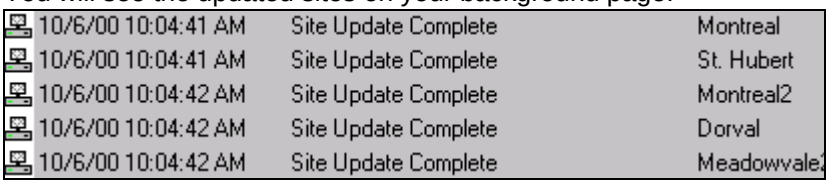
The 

action button on the SITE dialog sends all programming data out to Millenium Enterprise Access Management devices for one or more specified **Direct** sites.

Sites must have Polling Enabled on the main SITE dialog.



You will see the updated sites on your background page:



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.

Updating Millenium Enterprise Network Devices

Millenium Enterprise network updates occur when the Millenium Enterprise computer programming data goes out to devices (SCUs—Sites, DCDs—Doors, ECUs—Elevator Control Units, and RCDs—system-wide Relay Control Devices.)

Updates also bring Access Management history back from the device circuit boards to be displayed and stored as history on the PC.

Communication configurations for individual sites are DIRECT. DIRECT communication configurations rarely require operator-initiated updates because updates automatically occur online.

An operator can execute Updates from different places in the Millenium Enterprise system:

- action button in Site dialog box—for **all** programming data to an entire site and all its corresponding devices.

With on-line systems, this type of update would take place for a *newly installed site* after Millenium Enterprise programming is completed and after polling is enabled. On-line systems can

use manual updates after a device goes off-line for repair or replacement. Notice the update button is the “Click-for-more” type that pops up an additional dialog. Select the site or sites you wish to update.

Update... option

- under the button in the ACCESS POINT dialog
- 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.
- For elevators, on the ECU Floor Relays tab, the Update button works a little differently—it sends users for all relays along with any associated Timezone data, alarms and events—just like the Update button on the main Elevator dialog.

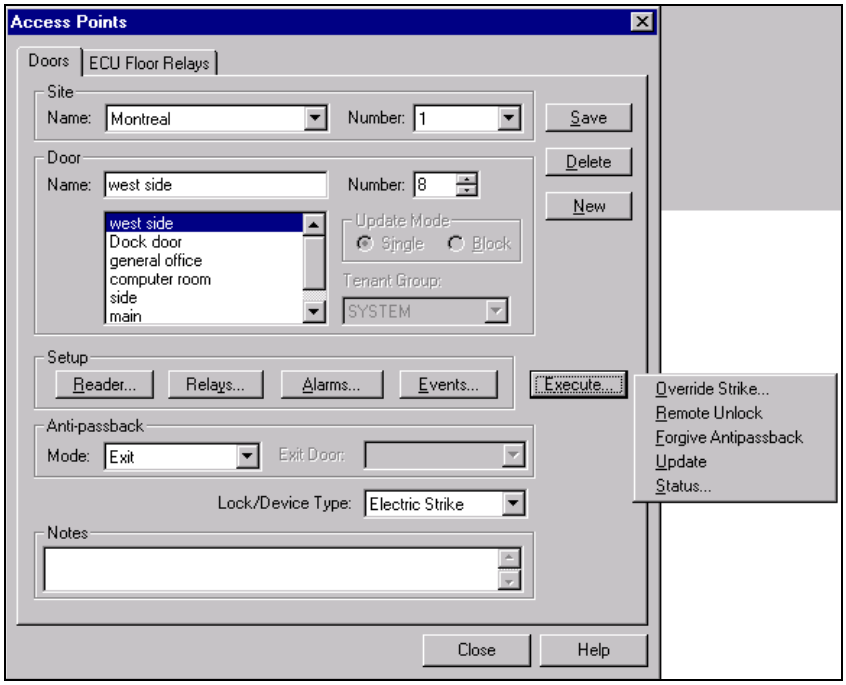
Update... option

- under the button in the ELEVATOR dialog—for updates to a specific Elevator Control Unit (ECU.) The update sends ECU alarms, events, and all users for all relays under an ECU, along with relay setup information.
- For the "master" ECU (ECU,) the update also sends ECD data for all Elevator car Control Devices under the given Site Control.

Execute button

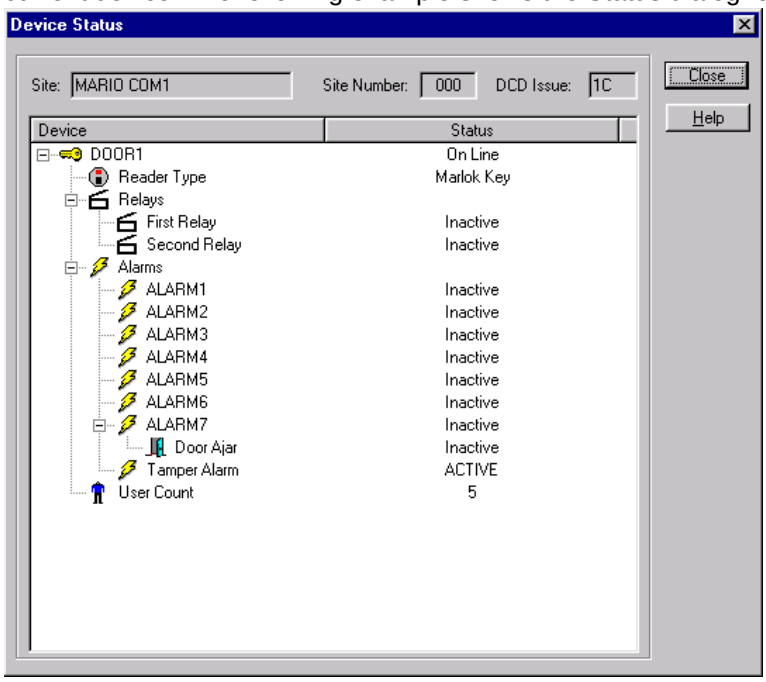
The ACCESS POINTS window (**Doors** tab) includes a special Execute... button with options to control the following door functions from the PC:

- Override Strike
- Remote Unlock
- Forgive Anti-passback
- Update Door Control Device (DCD)
- Status



STATUS of a Device (Door)

The Update... button on the Access Point dialog performs an on-the-spot status check for the current device. The following example shows the Status dialog for a door:



Device information includes a description of whether or not the device is online along with the type of reader installed at the device. In addition, the status for each relay and alarm input on a DCD is displayed, along with the number of users currently programmed in the door.

DCD Issue tells you the EPROM (Erasable Programmable Memory) Issue level for the given DCD.

Similar Device Status dialogs appear for ECUs and RCDs.

Important! This status feature requires SCU Issue U and DCD Issue Y.

Chapter 6: Timezones

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

- when user Access Groups can have access to doors within the Millenium Enterprise network
- when time-related relay functions start and stop.

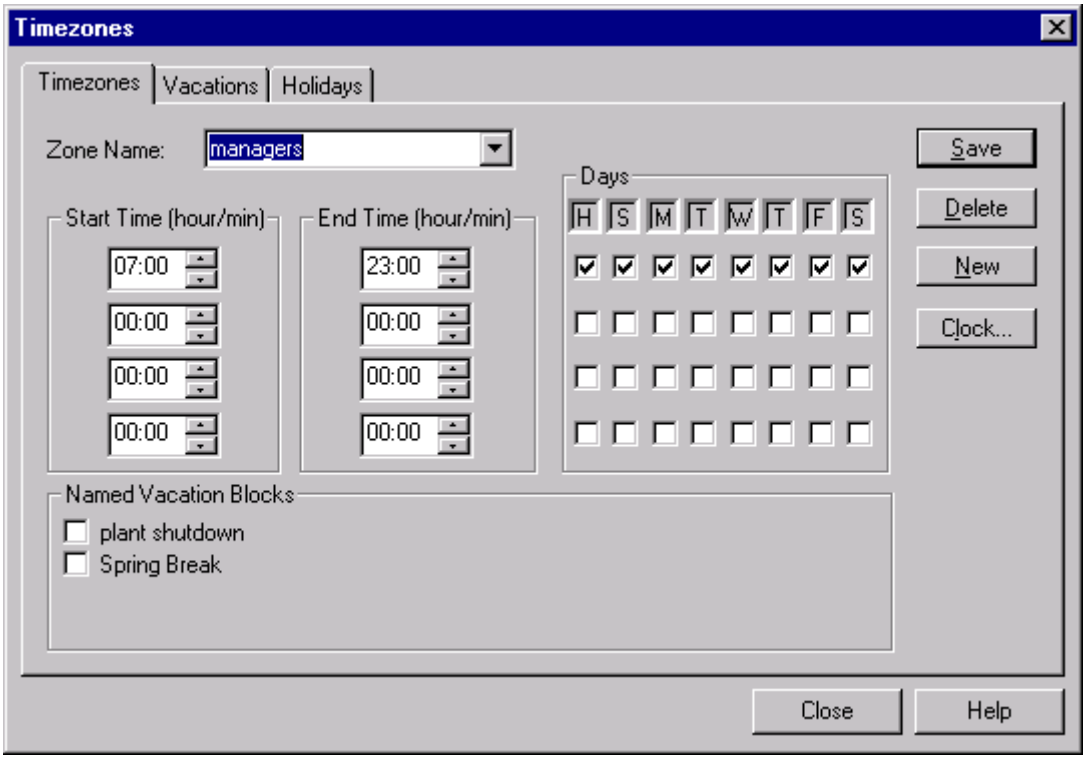
Timezone

Identify blocks of time around which your Millenium Enterprise system will operate.
ACCESS GROUPS link to specific TIMEZONES during which they may gain admission to specific ACCESS POINTS in your facility.

Timezones Dialog Box

The picture below shows the TIMEZONE dialog in Millenium Enterprise. Refer to this picture for information on how to set up or program time-period control of access to your facility. Notice this dialog has three tabs of time-related information.

Timezones Tab:



A Timezone can include up to four intervals. Each interval includes a starting and ending time, in military time.

NOTES about Timezones:

- 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.

Setting up VACATIONS: NAMED VACATION BLOCKS show those time periods you have 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.
In the example, users in the Access Group with the *Managers* TIMEZONE assigned to a particular door will still have access during *plant shutdown* and *Spring Break.*

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.

Setting up HOLIDAYS: A check in the **H** 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 that Timezone.

The example shows holidays are checked. Therefore, the **Managers** TIMEZONE will still be valid during all system holidays. Users whose Access Group has the *managers* TIMEZONE assigned to a particular door will have access to that door during established holidays. History will show access granted.

Assigning Timezones to Access Groups

Notice the button where you can verify, and, if necessary, update the computer's System Clock setting (including changes due to Daylight Savings Time.)

Setting up a Timezone

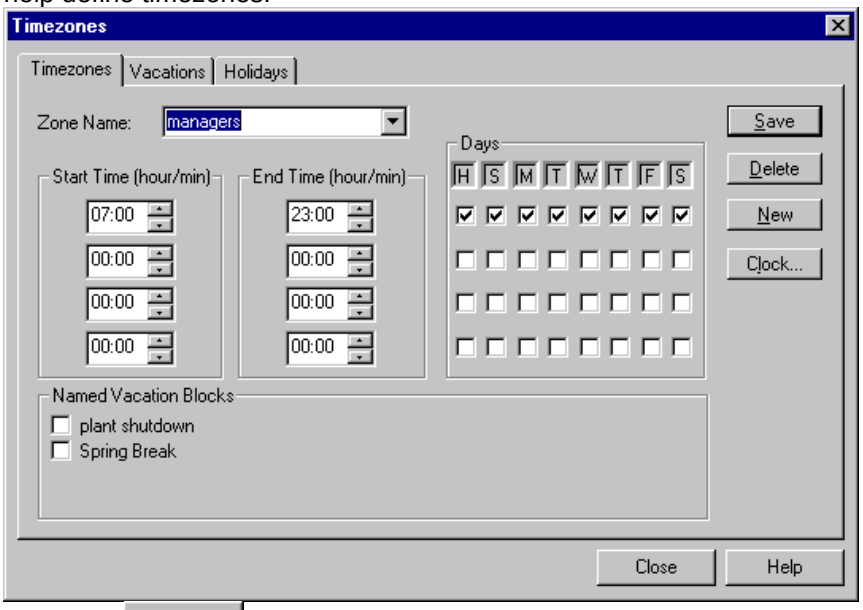
Timezones are at the heart of controlling access to your facility. For any given Access Group, one Timezone links to each access point in the facility. Then you assign each user to an Access Group. As a result, users can only have access to points in your facility during pre-determined times.

Timezones can also automatically control access points, automatically activate devices, automatically determine when a pre-defined action is handled as an event in your facility.

If you still need help, follow the procedure below.

Step-by-Step: Adding Timezones

1. Click the  icon on the Millenium Enterprise toolbar.
   The Timezone dialog appears with three tabs that hold time-related data:
2. If you have already set up HOLIDAYS and VACATIONS, then start with the main Timezones tab. Otherwise, begin by creating holidays and vacations that will be used to help define timezones.

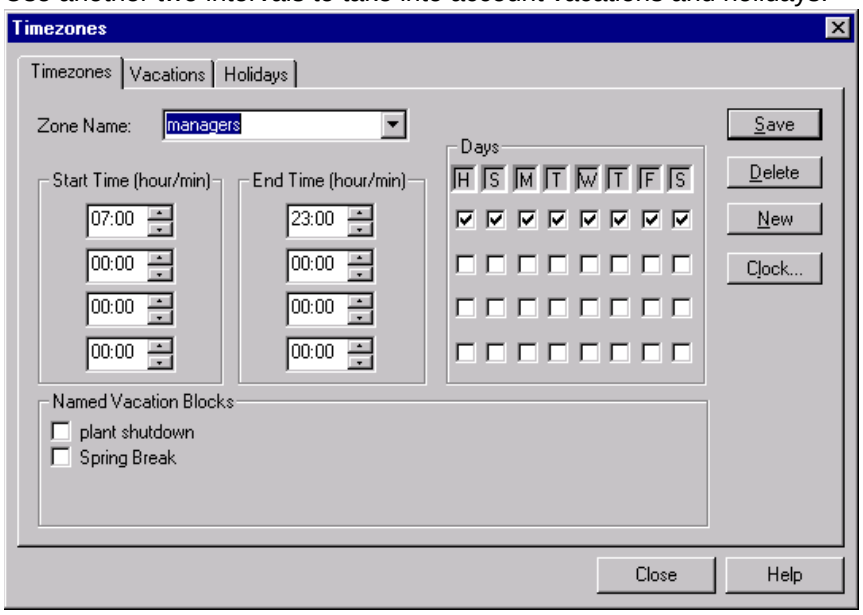


3. Press the  button to clear any field data on the main Timezones tab. Then name the Timezone you want to create. Give the Timezone a name that will have meaning to an operator when it's time to assign a Timezone somewhere else in the Millenium Enterprise software.
4. Move to the **Start Time** section of the first interval and enter it . Select or type the time of day (in military hours and minutes) the timezone begins.
5. Press the <tab> key to move to and establish the **End Time** for that interval.
6. 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.
7. Move to the DAYS section. If you have Holidays established, set the H column as follows:
   ☐ Timezone becomes invalid during **all** system holidays.
   ☑ Timezone is valid during **all** system holidays.
8. 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.)
9. 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.
   Checking the Vacation box, in effect, puts the timezone on vacation.

Timezone Interval

You can establish up to four (4) intervals within each TIMEZONE.
Use two intervals to make a Timezone take effect at different times on Mondays/Wednesdays/Fridays than on Tuesdays/Thursdays.

Use another two intervals to take into account vacations and holidays.

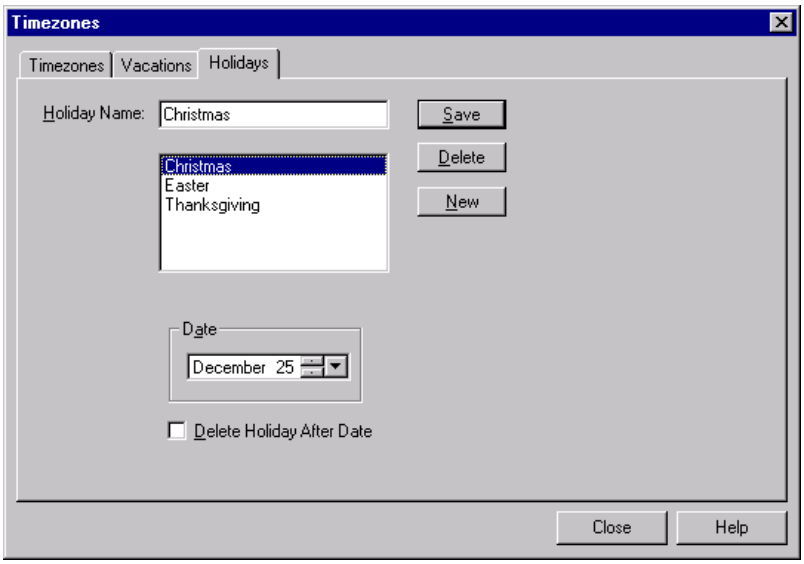


The illustration above shows that all members of the access group **Managers** can get into the doors between 7:00am and 11:00 PM all the time, including during plant shutdown and Spring Break, official holidays and weekends.

Holidays Tab

The Timezones dialog includes tabs for other time-related information such as holidays. Holidays are those time periods observed by the entire Millenium Enterprise system network.

A checkmark in the **H** column (DAYS section) of the main TIMEZONE tab means **all** holidays established on the Holidays tab are included in the given TIMEZONE — meaning the TIMEZONE remains **valid** for all holidays established in the system.



Name as many as 20 holidays observed at your facility.

Normally, the holidays do not display a YEAR data field. The system assumes all holidays are in the **current calendar year**. The drop-down calendar presents future years, but the system will NOT retain year data.

When you check the Delete Holiday After Date option, the date field expands to show the year.

Important!

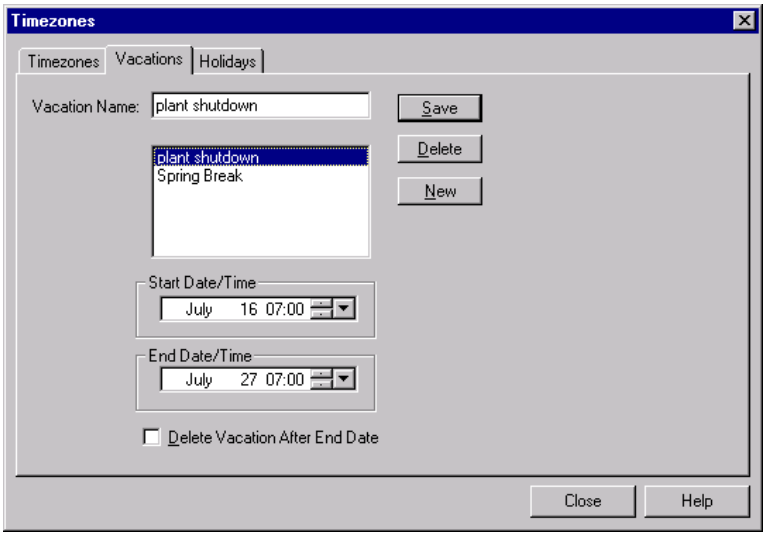
Operators must establish a procedure for updating the actual date of those holidays that change from one year to the next. Since holidays may be part of the TIMEZONES created for your system, it is important that holidays, which fall on different dates every year (such as Thanksgiving), are accurate 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.

Timezones - Vacation Tab

The Timezones dialog includes tabs of time-related data. Vacations are time periods observed by the entire Millenium Enterprise system network. 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.

Vacations Tab:



Set up as many as eight (8) vacation periods.

DATE & TIME:

Use the <tab> or the arrow keys to move between segments of the date and time field. The button pops up a calendar to help you select the MONTH and DAY. You can also use the spin controls buttons to move forward and backward through highlighted segments of the date and time field, or you may choose to type the data.

Notice that vacation periods can designate separate start and end times during the day. For example: a vacation begins at 1:00 PM on February 12TH and ends at 8:30 in the morning on February 23.

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 *Winter98* vacation from 12/18 through 12/31and a *Winter99* vacation from 1/1 through 1/8 must be established.

The 

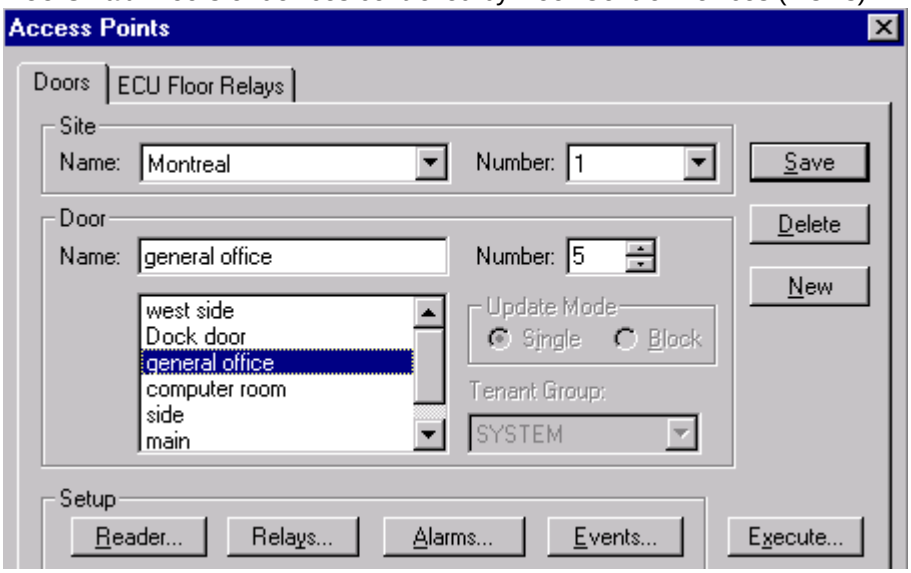
checkbox lets you set up a vacation for automatic deletion from the system after it occurs. Once you click the delete option, the Date box displays day-of-the week and the current year data. After the vacation is past, the software removes the expired vacation from the database. A history message ("Vacation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

Chapter 7: Access Points

Access points are those locations in your facility where a user requires a valid key or card to gain access.
Some examples include doors, parking gates, elevator floors, etc. where a key or card-reading device is installed to electronically read a user's identification.
A Millenium Enterprise Door Control Device (DCD) or Elevator car Control Device (ECD) electronically reads the key or card.
DCDs retain the history of all activity at the access point and Elevator Control Units (ECUs) retain the 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, respond to devices such as motion detectors or trigger an external device such as a bell, buzzer, or camera.

Access Points: Doors

The ACCESS POINTS dialog box in Millenium Enterprise is shown below. Use the image both as an introduction and as a reference for how to set up or program access points (doors) in the Millenium Enterprise network. Once you learn which options in this dialog control the features required by your facility, customize each access point according to how you want your Millenium Enterprise system to operate.
Doors Tab: Doors or devices controlled by Door Control Devices (DCDs)



Reader...	To identify type of reader device installed at a given door. To set up keypad combos. To set up Card Reader's as Wiegand or ABA mode.
Relays...	To set up DCD Relays for a Millenium Enterprise access point
Alarms...	To set up alarm inputs used on this door
Events...	To identify events to which this door will respond
Execute...	To perform door actions from the PC (includes the **Update** and **Status;** actions along with **Remote Unlock**, **Override Strike** and **Forgive Antipassback**.)
Tenant Group	If applicable, this field shows the Tenant Group to which this door belongs. The Tenant Group assignment controls what door is visible to what operator. Once a

	tenant group is assigned to an item, the group cannot be changed. Instead, an operator must delete the item and re-create it with the desired tenant group assignment.
Anti-passback Mode/Exit Door	Select Antipassback mode and Exit Door depending on that selection (see Antipassback)
Lock Device Type	Select lock device type from the dropdown menu.

Access Points Toolbar Button

Clicking this button brings up a dialog box with two tabs. 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, this 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 Enterprise settings. Access Points:

Adding an Access Point (DCD)

Step-by-Step: Adding an Access Point

1. Select the ACCESS POINT icon  .
2. Highlight the SITE NAME for which you want to create Access Points.
3. Type a DOOR NAME that identifies this door (Door Control Device - DCD.) Avoid using symbols such as apostrophes.
4. Use the **Setup** section of action buttons:

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

    - To set up either of the two relays on the DCD, click the Relays button.
    - 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.

- To trigger a secondary device based on system 

, set up the ALARMS

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

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

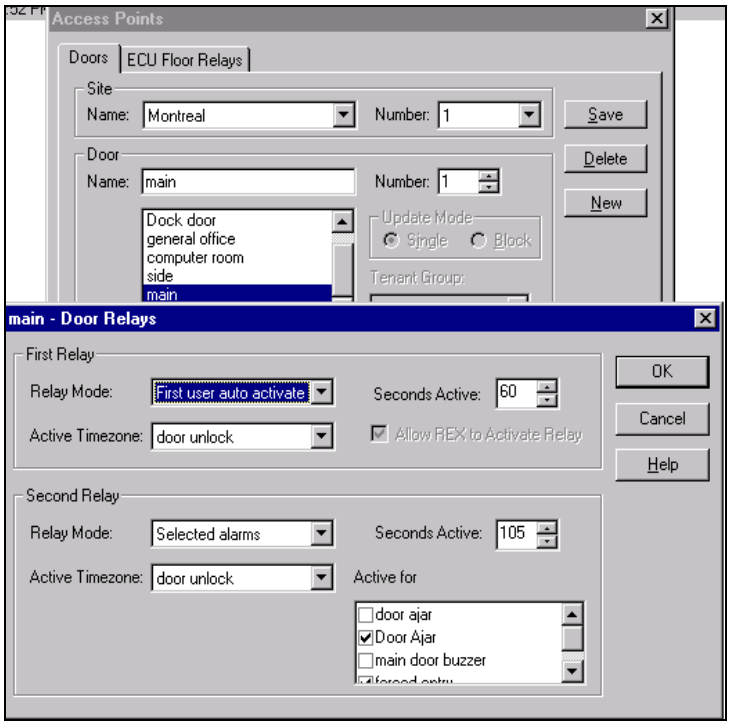
6. Select the LOCK TYPE that describes the type of hardware installed on this door. If DCD only uses its relay contacts and is not connected to locking hardware, select *Other.*
7. Use the NOTES box to describe the access point, as needed. You may summarize the Setup for this door to save an operator from having to check the individual setup dialog windows.

8. Press the Save button to add the door to the Millenium Enterprise 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.
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.)

Relays Button

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.



DCD Relay Modes

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

Table of DCD Relay Modes

Auto Activate	▪ 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.
First User Auto Activate	▪ 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.
Valid User	▪ Relay contact activates for a valid user, for the designated number of seconds–only during the selected TIMEZONE.
Rejected User	▪ Relay contact activates for a rejected user (invalid key or card), for the designated number of seconds–only during the selected TIMEZONE. The relay could be wired to activate a warning device to alert a guard of the invalid entry attempt.
Any User	▪ Relay contact activates for any user (valid or invalid,) for the designated number of seconds–only during the selected TIMEZONE.
Dual Custody	▪ This relay mode is used with DCDs requiring a Marlok Key, but it requires two users to be present to unlock the door. Instead of inserting one Marlok Key to activate a relay, two Marlok keys must be inserted before any action occurs. The keys must be inserted 4 seconds apart to trigger the relay. This mode is usually set for high security doors such as safes. See Important below.

The **Second DCD Relay** includes three *additional* mode options:

Selected Alarms	▪ A second 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 is activated. The Active for Alarm(s) listbox becomes enabled, and displays only those alarms set up for the given door. Example: Assuming ACTIVE TIMEZONE = Always, and SECONDS ACTIVATED = 120: 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: (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.)**
Mirror Selected Alarms	▪ A second Relay contact activates when the selected alarm is activated. With multiple alarms, the second DCD relay is active while those selected alarms are active. The Mirror Selected Alarms mode lets you set the relay to be active not only while the selected alarm is active, but also only during the relay's ACTIVE TIMEZONE. Example: Assuming ACTIVE TIMEZONE = Always: 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.
Last Person Out	▪ The event of the last person exiting on this particular DCD triggers the relay. The door registers a count of everyone who has entered and then counts down as each person exits. When the countdown reaches one and one more exit takes place, the relay is latched. "Latched" means that it changes its state and remains in that state until another person enters, which causes it to change state again. This Last Person Out relay mode cannot be used in conjunction with Anti-passback mode. See IMPORTANT below.
R.E.X.	▪ If the door uses the Request-to-Exit (R.E.X.) reader connection on the DCD to control a device such as a motion detector (passive infrared device–PIR,) you may or may NOT want the first relay to activate the strike. ▪ When the checkmark is removed from the Allow REX to Activate Relay option, any alarm connected to the first relay will be shunted. As a result, in the PIR example, motion detection will NOT unlock the door. ▪ DCDs with EPROM issue level X or higher offer this option.

Dual Custody and **Last Person Out** modes are only available with certain issues of **EPROM**. Be sure to check your EPROM .levels on the SCU and DCD cards before selecting these features.

Features	EPROM level required for SCU	EPROM level required for DCD
Dual Custody **Last Person Out**	**Issue V**	**Issue 1C**

Alarm States

There are three possible configurations for the alarms you create on a DCD access point.

1. Alarms 1-4, supervised with 2 states: trigger/reset
2. Alarms 1-7, supervised with 2 states: trigger/reset
3. Alarms 1-7, supervised with 4 states: trigger/reset/open/short

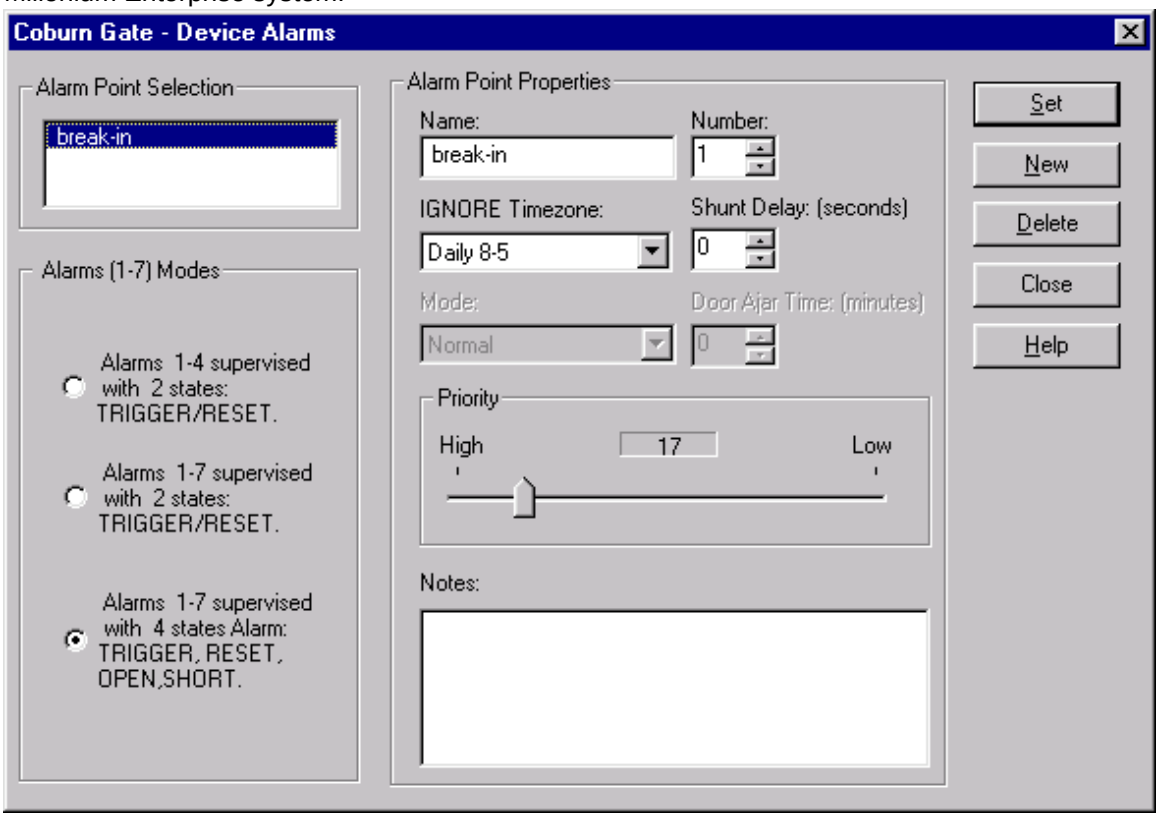
Table of Alarm States

Trigger	The alarm responds to an event such as forced entry of the door.
Reset	The alarm responds to a reset
Open	The alarm responds to a normally closed circuit being opened or an open circuit being closed.(this could be caused by an intruder cutting wires, for example)
Short	The alarm responds to a short circuit, which could be accidental or deliberate tampering with the wires on the part of an intruder.

- Shunt delay timer from 0 to 255 sec.
- Customized setup-requiring acknowledgment from monitoring personnel or offering explanations and instructions.
- Forced-door entry alarm with shunt delay timer of 0 to 255 seconds
- Door ajar alarm with programmable delay timer of 1 to 255 minutes.
- Ability to run from any workstation.

Setting up Door Alarms

Millenium Enterprise Door Control Devices (DCDs) come with seven alarm inputs. The alarm inputs are supervised alarms. Alarm input number 7 offers a special Door Ajar feature where the door can be set to respond if left propped open 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 Enterprise system:



Step-by-Step: Adding Alarms

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, see page 66.)
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 and 255 seconds.
5. Select the states for each alarm. Refer to Alarms_ Alarm States
   - Two states for alarms 1-4 TRIGGER/RESET
   - Two states for alarms 1-7 TRIGGER/RESET
   - Four STATES FOR ALARMS 1-7 TRIGGER/RESET/OPEN/SHORT
6. Prioritize the alarm in a scale from 1-100. The Alarm Monitor will use this information for display options.
7. Use the NOTES section to record any free-form text for operators about the alarm setup.
8. Press the button.

Alarms - Supervised Inputs

The J6 terminal on a DCD includes seven alarm inputs and their returns (resets.)

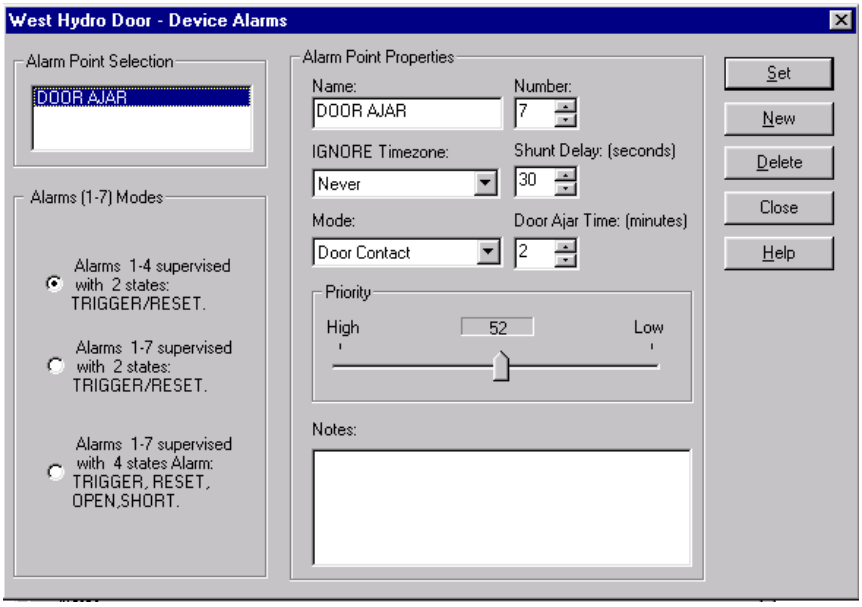
Supervised Alarms

- End-of-line (EOL) resistors come with a DCD for use on the alarm inputs.
- These resistors look for 1K Ohm resistance across the alarm inputs.
- If the resistance is not present—for example, if the alarm contact is open or if the DCD terminal pins are jumpered together by someone wishing to bypass the alarm—the alarm triggers.

Notes*:*
EOL resistors allow use of either sensor contact type on the same alarm input (Normally Open—closes to short the line, and Normally Closed—opens the line.)
Elevator Control Unit alarm inputs are unsupervised—they have no resistors.

Door Ajar Feature

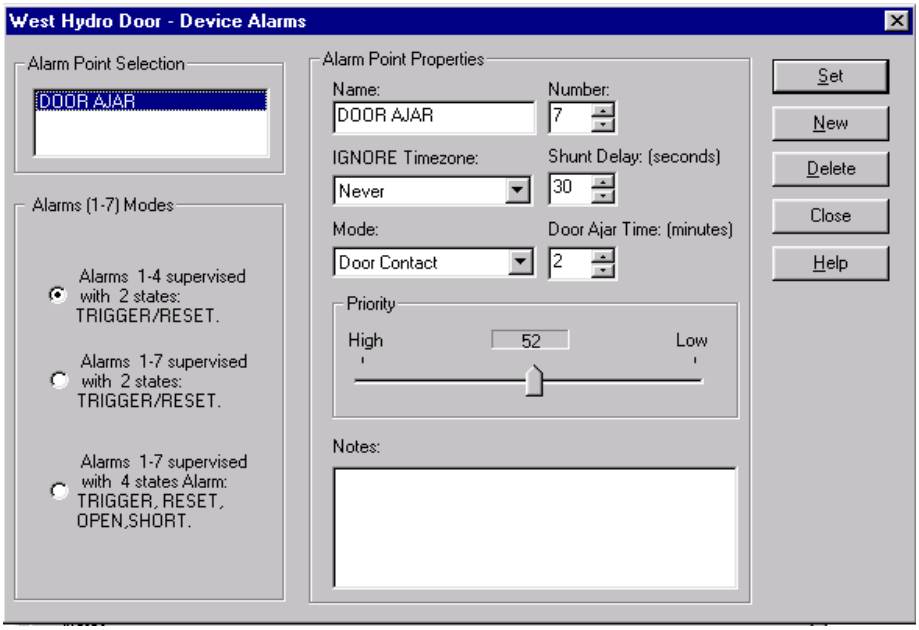
Alarm # 7 on a Door Control Device offers a special Door Ajar feature. The feature lets you set up an alarm to activate if a door is propped open, following a valid entry, for more than a pre-set amount of time.



Step-by-Step: Adding Door Ajar Alarms

1. Click on the Access Points symbol and in the main screen of the dialog box, select the DOOR WHERE YOU WANT TO PROGRAM THIS ALARM.
2. Click on the Alarms  button.

The following screen appears:



1. Give the 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 (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.
   - 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**"
   - 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**"
7. Prioritize the alarm in a scale from 1-100. The Alarm Monitor will use this information when deciding which active alarm requires attention first.
8. Use the **NOTES** section to record any free-form text for operators about the alarm setup.
9. Press the Save button.

Setting up Door Events

In Millenium Enterprise systems, an event is a pre-defined action that triggers a relay.
Once you have set up door alarms 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.

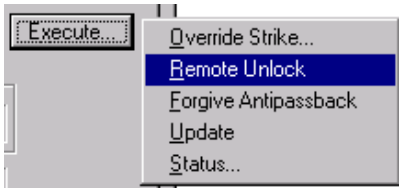
Each event goes out to the Millenium Enterprise network as data output from the DCD. In the above sample dialog, the given DCD uses one of its seven possible alarms (Dock Camera.) The Alarm and its reset (Dock Camera Reset) are designated as EVENTS. When the door opens, the Dock Camera alarm triggers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

Remote Unlock

Doors operated by electric strike can be remotely unlocked from the PC by any Millenium Enterprise operator with EXECUTE rights to the Door dialog (Access Points, Doors 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.

Step-by-Step: Executing 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.
   (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.

4. 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 is displayed earlier in history as the most recent operator to log on.

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.

Override Mode	**None**	This door is not in a temporary override mode.
	Unlocked	This door is set to temporarily unlock for the OVERRIDE TIME indicated.
	Locked	This door 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 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 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.

Antipassback

The Anti-passback feature must first be selected for the **Site**, although it need not be activated for all the doors at that site. If you select one of the two anti-passback options in the **Site dialog**, the site is ready to set up to use the anti-passback feature for its doors. Anti-passback is designed to prevent users from passing their key/card back to someone else to gain access to your facility. Operator may forgive anti-passback from the PC.

Types of Antipassback on DCDs

In setting up individual doors (Access points) you select one of the Anti-passback modes described above OR **None** if you have doors where you don't want the feature.
There are two types of anti-passback.

PAIRED	▪ A user must exit the facility by a specific EXIT DOOR other than the one used as a specific ENTRANCE before his/her key/card is valid to work again in the system. In other words, the user must enter by one and only one specific Entrance and exit by one specific Exit. If Paired is chosen in the Site dialog as the Anti-passback mode, then one entrance door and one exit door must be selected in the Access Points dialog for each door where Anti-passback is used.
GLOBAL	▪ A user must exit the facility by any door designated as a Global Exit and enter by any door designated as a Global Entrance. If Global is chosen as the Anti-passback mode, then several entrance doors and several exit doors must be selected in the Access Points dialog for each door where Anti-passback is used.

When anti-passback is enabled in the SITE dialog, the **ACCESS POINTS** dialog anti-passback fields are automatically enabled. The system will require you to set any necessary anti-passback field selections before allowing you to save the data. In setting up individual doors (Access points) you select one of the Anti-passback modes described below **OR None** if you have doors where you don't want the feature

PAIRED

- The following options appear in the ACCESS POINTS dialog when Paired anti-passback was selected in the Site dialog:

None No Anti-passback is used on this door

Entrance	Door is a designated as an entrance. When you select Entrance, the EXIT DOOR field automatically enables, and you must select an exit door to be paired with your selected Entrance.
Exit	Door is a designated as an exit. When you select Entrance, the EXIT DOOR field automatically enables, and you must select an exit door to be paired with your selected Entrance.

Forgive Anti-passback

Sites that use the anti- passback function can have Millenium Enterprise operators use the 

button (ACCESS POINTS dialog) to forgive anti-passback at a given door.

Chapter 8: Access Groups

Access Group

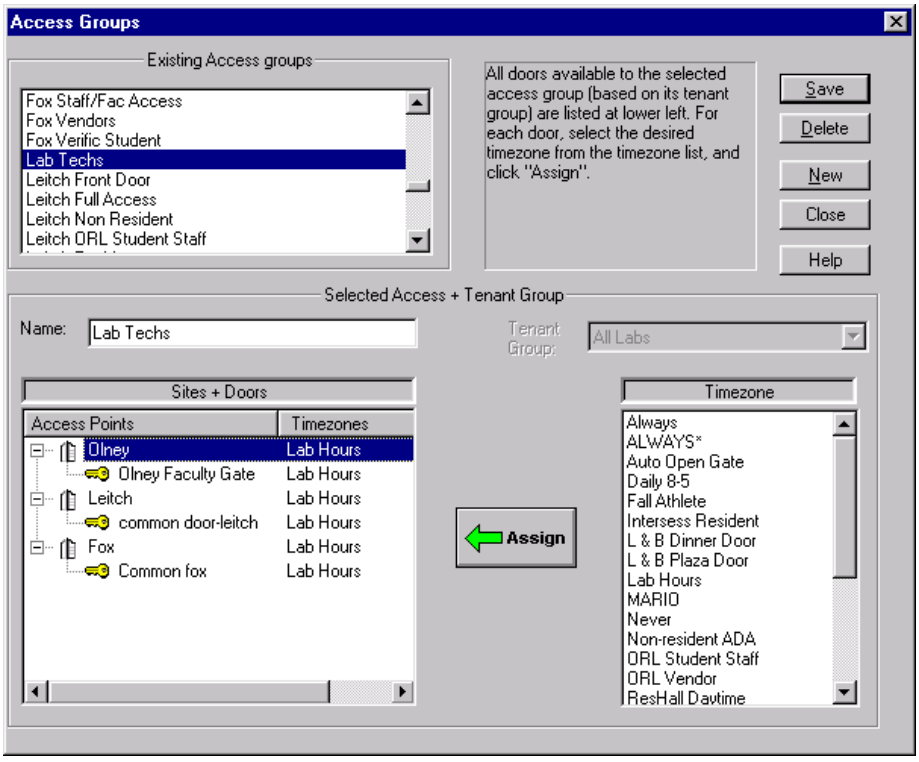
Access Groups, along with Timezones, are the basis around which the Millenium Enterprise controls access to points in your facility.

An Operator assigns Users to an Access Group.

- The Access Group has permission to access specific points (doors) in your facility.
- The Access to the doors is limited to a specific TIMEZONE.

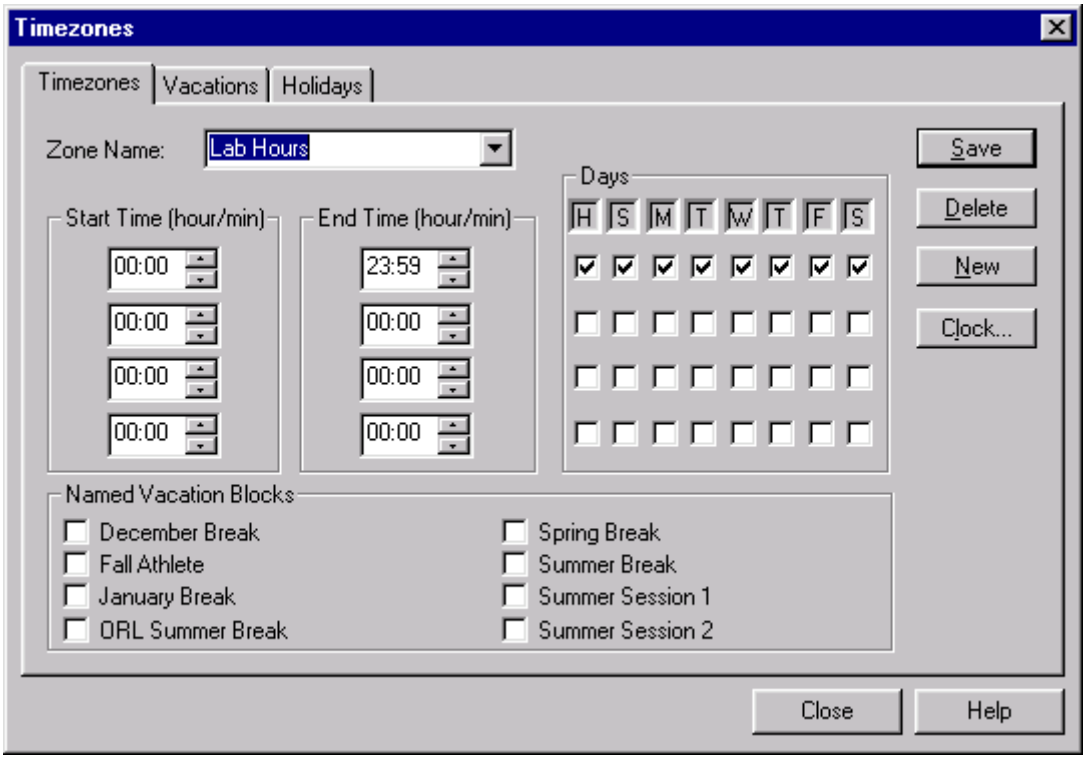
An Operator assigns a Timezone to an Access Group, taking into consideration the **Tenant Group** to which the Access Group belongs.

Let's look at the example below:



- For example, if the **Tenant Group is All Labs,** the tenants' usual **Access Group** is **Lab Techs.**
- Assign the Timezone **Lab Hours** to **Lab Techs**

Both assignments are made keeping in mind that the Lab Techs will need access to the lab doors almost 24 hours a day (the Timezone **Lab Hours** runs from midnight to 23:59).

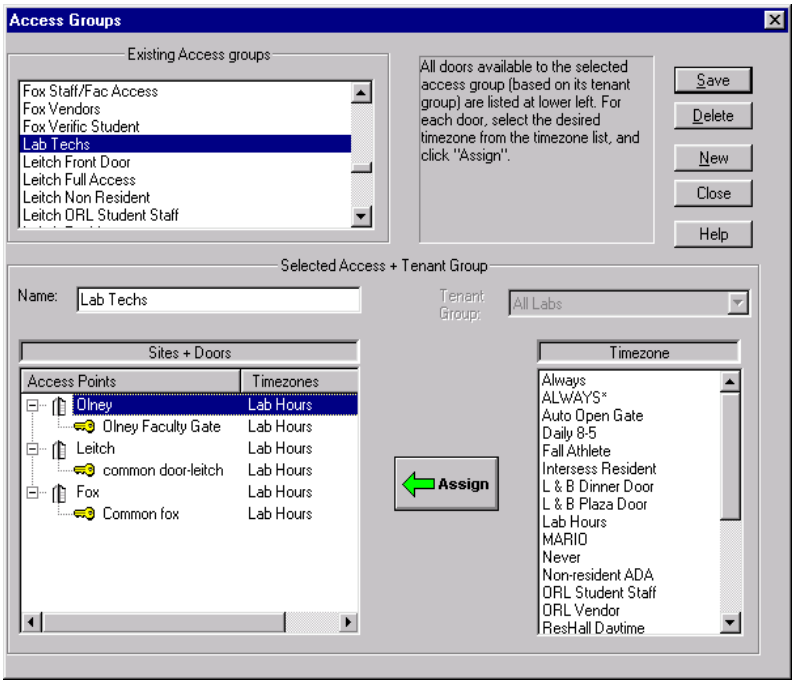


The system will only unlock a door

- when the user's valid key or card is used in a reader device on a door to which his/her Access Group has access.
- during the TIMEZONE specified for the given Access Group.

Access Groups: Create/Assign

Access groups have admission rights to specific points in your facility during specific time periods. The example below shows the **ACCESS GROUPS** dialog as it appears when you first click the Access Groups icon. Notice some of the dialog appears disabled or grayed-out until you select one Access Group from the listbox below the **Name** field.



Creating an Access Group

Before creating Access Groups, you must first have programmed SITES, ACCESS POINTS, and TIMEZONES in the software. You will use these three components to define timezone-controlled access to your facility.

If you use the tenant feature, a SYSTEM tenant group operator must have created tenant groups. Then a non-system tenant group operator can only create access groups within their own tenant group. The Tenant Group field automatically displays the name of the tenant group to which the logged-in operator belongs.

If you do not use the tenant feature, the access group defaults to the System tenant group. You can ignore the setting.

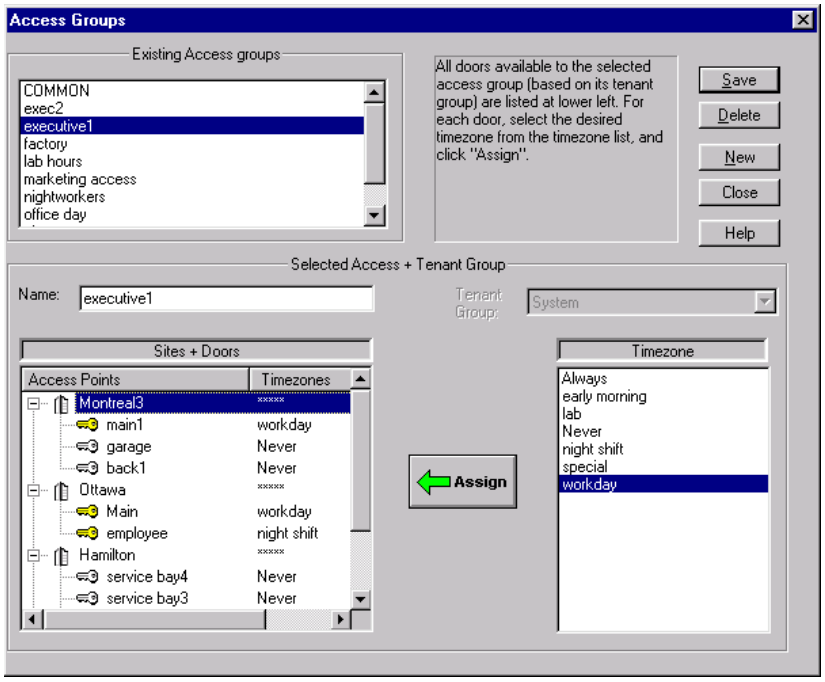
Step-by-Step: Creating an Access Group

1. Select the Access Group icon  . The dialog appears disabled with the cursor In the **Name** field
2. 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.

Important!

(For Tenant Group feature only) If the logged-in operator is a SYSTEM tenant group operator, the Tenant Group field activates and displays the SYSTEM tenant group, by default. The SYSTEM tenant operator must assign the new access group to the desired tenant group before pressing the Save button. Otherwise, the new access group will belong to the System tenant group.

3. Move to the Access Points / Timezone listbox. Notice all Sites set up in your facility appear in the left-hand column. **With the tenant group feature, just those sites that belong to the tenant group of the logged-in operator display.** A plus symbol ("+") appears at the left of each Site. If an operator selects a different access group, just the sites (and doors) for the selected group appear.



- 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 Enterprise software.

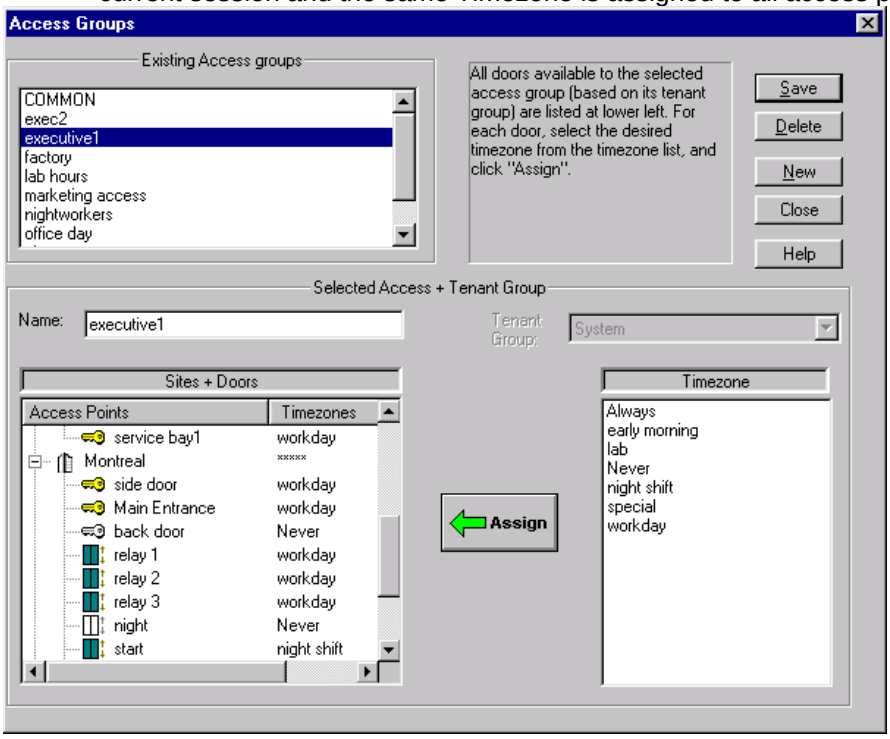
- The second column is where you **assign** one established Timezone to each ACCESS POINT.

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.

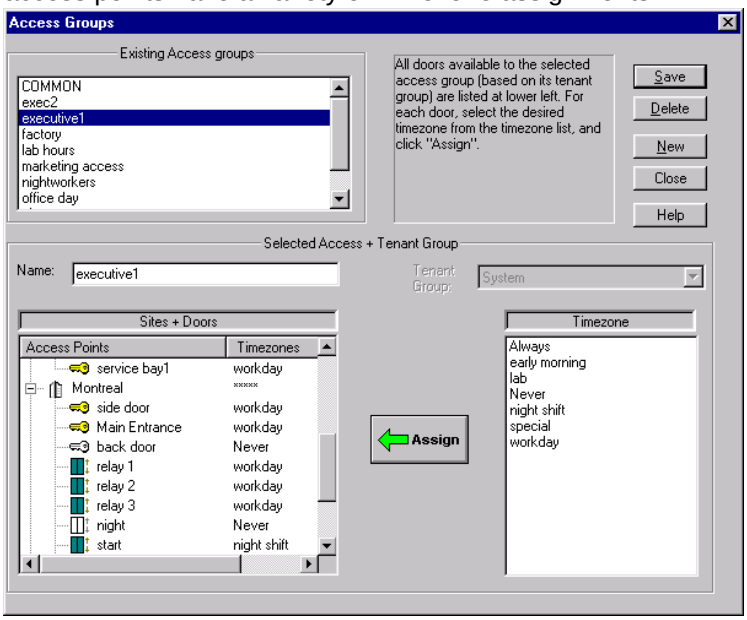
Note: To pick multiple access points, hold down the <Ctrl> key to highlight more than one individual access point. To select a group of access points, hold down the <shift> key to highlight the first and the last access point in the group.)

5. Then click the Assign 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:
   - ***** 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.
   - 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.



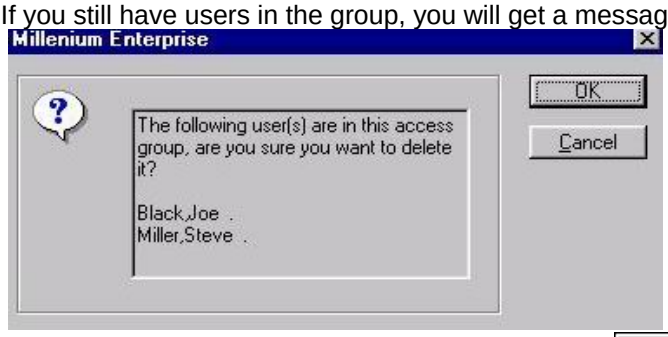
For the Executive 1 Access Group (shown above)) Montreal site has been opened and access points have a variety of Timezone assignments.



For the Exec2 Access Group (shown above Ottawa has been opened but the timezone **workday** applies to ALL the doors at the site, so the doors are not listed individually as they are for Montreal3.

How can I delete an Access Group?

1. Select the Access Group you want to delete. (Remember you cannot delete System or Global).
2. Click on the Delete button.
3. If you still have users in the group, you will get a message like the following:



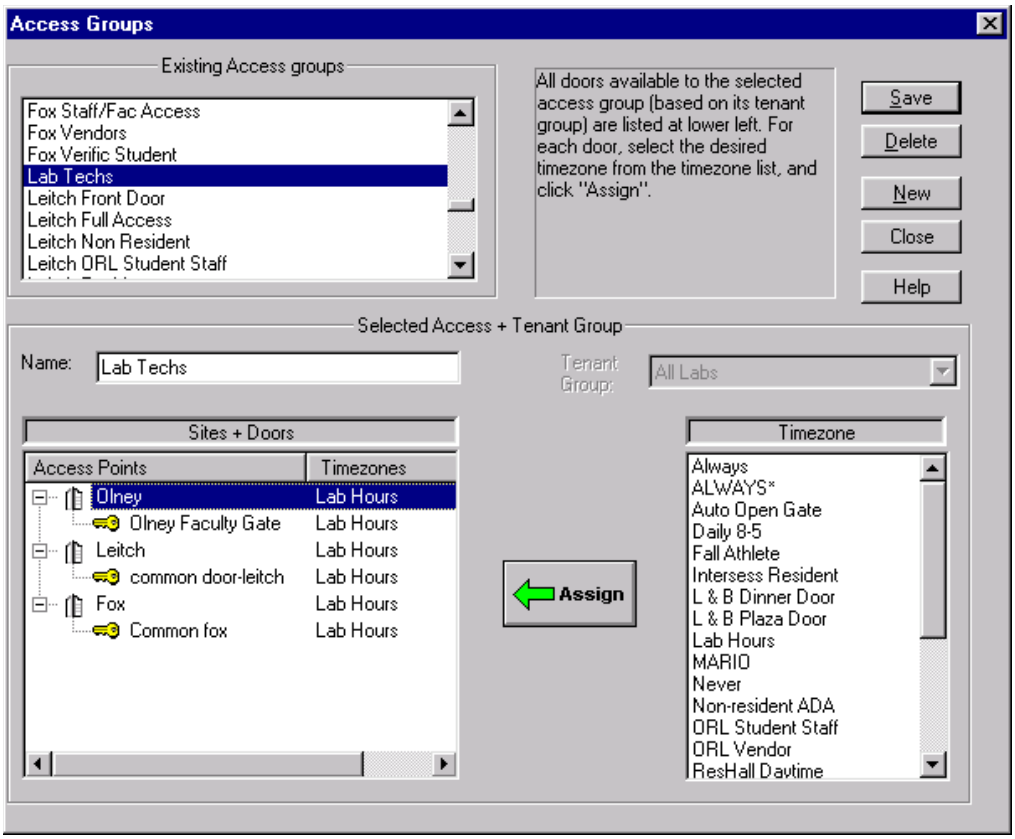
4. Select Cancel and change the users first or click on OK and the users will automatically be placed in the System Tenant Group and will have no access except for System Access Group and Common Access Group (permitting access to Global access points.)

Assigning a Timezone to an Access Group

Every Access Group in Millenium Enterprise can enter each ACCESS POINT in the system where his group has access but the group can only enter each access point during a specific timezone. 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 selected doors 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:

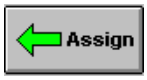
Step-by-Step: Assigning a Timezone to an Access Group

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.

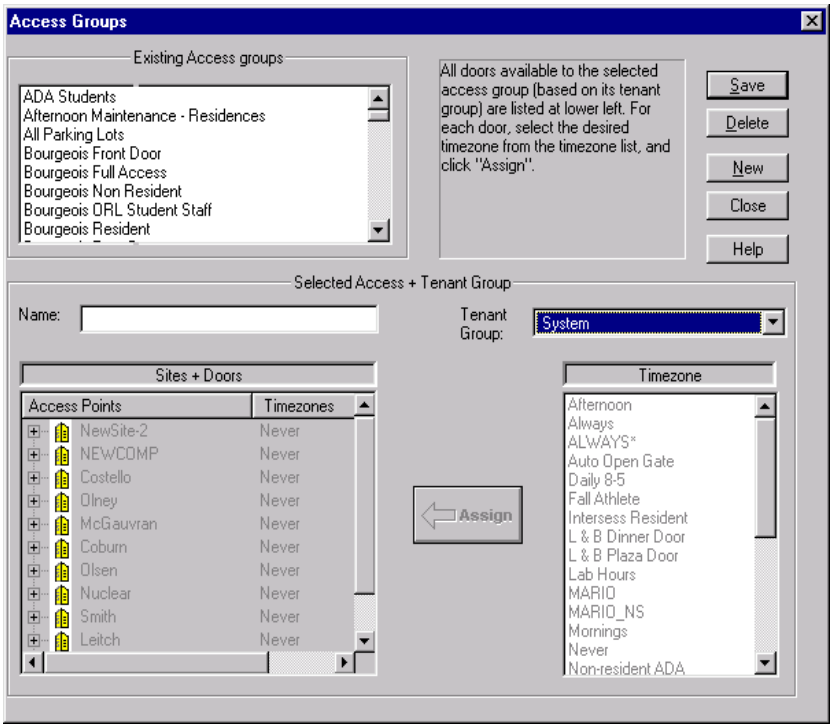
6. Now press the 

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 

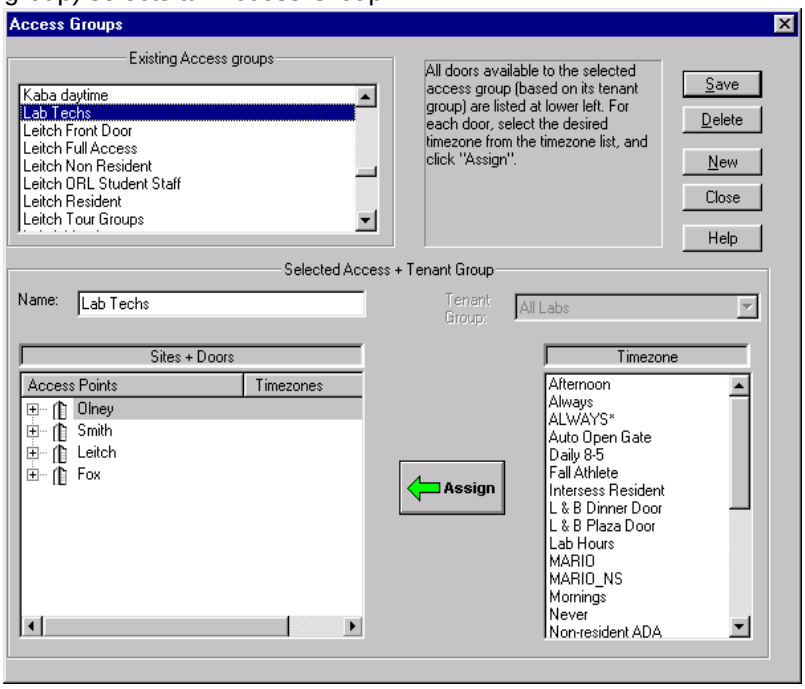
button to save each timezone assigned to an ACCESS GROUP for each door. Be sure to save before creating or selecting another access point.

Tenant Groups (Access Group dialog)

Before an operator selects an Access Group, the Access Group dialog appears similar to the following example, with the Access Points and Timezones listboxes disabled. Once you select an Access Group, the sites (and doors) that belong to that Access Group and the Access Group's Tenant Group will appear.



The following example shows the same dialog **after** an operator (from the Lab Techs Tenant group) selects an Access Group:



The above example also shows just those doors that belong to the All Labs Tenant group.

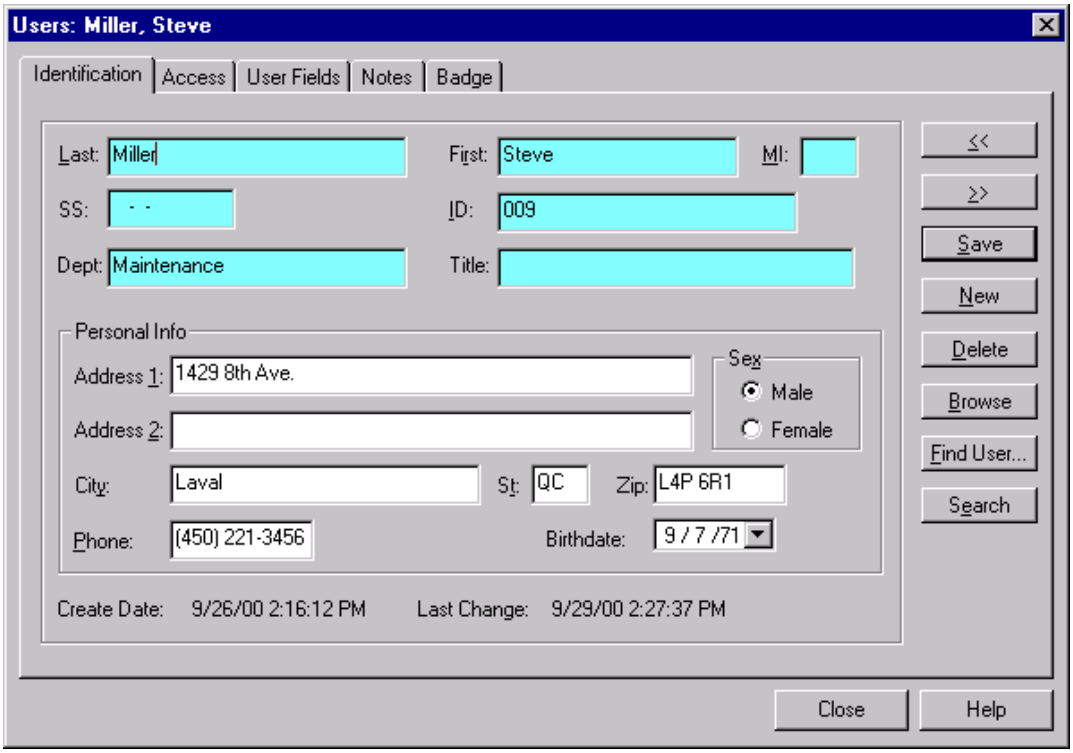
Facts about Access Groups

- In the Access Group dialog, a tenant operator can only see those **Access Groups** that belong to the operator's tenant group, plus the COMMON access group. In the example above, the operator is a Level 1 Operator in the All Labs Group, so he/she sees only the Lab Techs and Common access groups.
- In the Access Group dialog, the only **doors** that appear are those doors that belong to the Access Group's tenant group. The Labs are at the Montreal 3 and Montreal2 sites, so the doors to which the Lab Techs Access group has access are all at those sites.
- A SYSTEM tenant operator will see all Access Groups.
- When an operator makes a new Access Group selection, two areas of the dialog refresh:

Chapter 9: Users

Here is an illustration of the USERS dialog in Millenium Enterprise. Users are people who are assigned keys or cards. They use these keys or cards to access points in your facility. The USERS dialog has multiple tabs that let you switch between multiple windows of information about users. The name of the user in focus appears across the title bar of the dialog.

Identification Tab:



NOTES:

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

2. The BIRTHDATE field above, and the EXPIRATION date field on the ACCESS tab feature a pop-up calendar for ease in entering dates.
3. To add a user: press the New button.
4. To edit or change user data, make the modifications and press the Save button.
5. 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 a find a user from an alphabetical list, click the Browse 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 New

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 Search 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 New button and type complete **Reader Type** and **Access Code** data to locate the user by their access code.

Last Change: 09/20/2001 4:17:33

Date only changes when user **Access Code**, **Access Group**, or **PIN#** changes.

Adding a User

Before creating Users, you should 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) during which Timezone the user's key and/or card will be valid for that point.

Step-by-Step: Adding a User

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 Find User... button,
(b) focusing the cursor in the TITLE field,
(c) pressing the Search button,
(d) typing the first few letters matching the data you want to find such as "Vice."

Users (Access tab)

The Access tab is the place where you make three important Access Management entries in the Millenium Enterprise software. The Access tab is also where you have the option to make an ABA card.

- **Assign keys or cards** to the people who access your facility,
- **Assign an expiration date** to each user.
- **Encode an ABA card** for an individual user

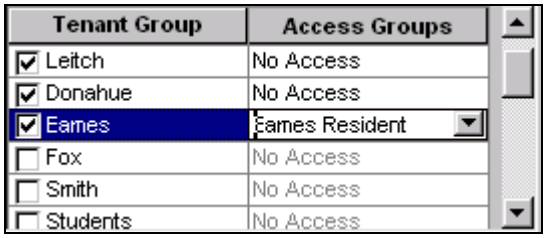
If you are SYSTEM tenant operator:

- **Assign a TENANT GROUP** to each user.
- **Assign ACCESS GROUP** to each of the user's Tenant Groups, or leave that responsibility to an operator within the user's tenant group.

If you are a NON- SYSTEM tenant operator, then all users that appear as well as any new users you create automatically belong to your tenant group.

- **Assign ACCESS GROUP** to each user in your Tenant Group.

1. You can also remove any users from your tenant group by removing the check in front of your Tenant Group name in the Access tab of the User dialog box.. That user will no longer appear when you open the user dialog.

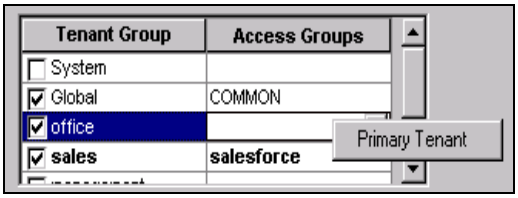


- If you are an operator from the user's tenant group(s), you can edit user data, based on your operator level.

Important!

- If you are an operator from the user's tenant group, and you delete the user, that user is deleted from the entire Millenium database.
- Users may be assigned ONE key, ONE Wiegand card and ONE ABA card each. They cannot be assigned more than one of each type.

1. Click to pop up ACCESS tab.
2. Assign the user a key or card, an optional expiration date and personal identification number (PIN.) You also have the option to display the user's image if you have the Millenium Enterprise Badge module and have captured images for your users.
3. Then assign a user to a Tenant Group and to an Access Group for each Tenant Group, if applicable.



- Have Access Groups created for each Tenant Group.
- Select the Tenant Group(s) to which this user belongs.
- Select the Access Group for each Tenant Group.

To assign a key or card to the user:

1. Select the **Reader Type** and record the **Access Code**.

- 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 Enterprise display screen, or
  - Record the code printed on the card, or
  - Record both the site identification number and the access code.
  - Record an ABA code to be encoded on a card using an optional System 800 encoder.

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.)

Press the arrow or the Save button to make assignment appear in the listbox.

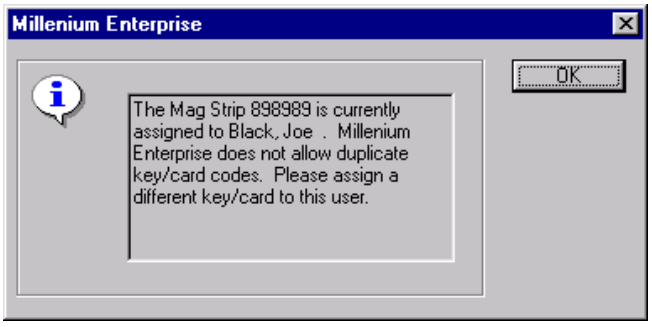
To designate a lost key or card as lost, use the button.

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

User Fields tab: Record custom, user-defined information such as License Plate No.

Duplicate Access Codes

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



Reader Type

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.

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, the first second of the designated date) type the date or use the button to select the expiration date from the drop-down calendar.

NOTES:

- When the user's expiration expires, their access group changes to <*blank*> meaning No Access.
- To remove an Expiration Date, highlight any part of the date and press the Delete key on the keyboard.
- Blue-shaded fields mean you can search for a user by **Reader Type** and **Access Code**.
- 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.

How to Encode an ABA Card

Millenium Enterprise has an option to encode a 14-character ABA card. Currently, the encoding option uses an ILCO System 800 encoder. Once you select the encoder and set up the 14-character ABA data and display formats in setupmpw, a Make Card button appears enabled in the USER dialog's ACCESS tab.

Step-by-Step: Encoding a User Access Card:

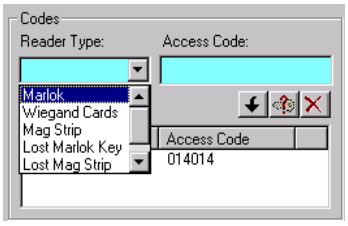
1. Make the necessary settings in setupmpw.
   (**NOTE:** In setupmpw, you can choose to place "ignore characters" in the Display Format to customize the length of the Access Code that appears in the software.)
   Open the USER dialog and select the user for whom you want to make an ABA card. Then click on the ACCESS tab.
2. Make sure the user has an ABA card assigned.
3. **NOTE:** If it is necessary to add a user or to add an ABA card to a given user, press the Save button before trying to make a card.
   Place a card in the ILCO System 800 encoder. Insert card as follows:
4. Magnetic strip side face down, strip on the right side.
5. Only insert card about 1/4TH of the way into the slot. The MAKECARD process will pull the card in the rest of the way.
6. Click the Make Card button.

NOTE: If the ILCO System 800 encoder gives you any problems, unplug the device to reset it.

Lost Key or Card

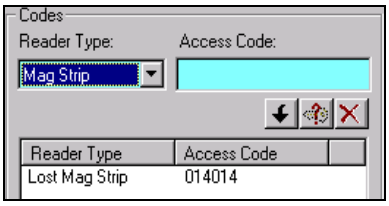
If a user loses their assigned key or card, you can tag the key or card as "lost" through the USERS dialog, Access tab. Since a user can have ONE of each type of card and ONE key assigned, this "lost" designation lets you assign a replacement key or card of the same type as the lost one.

Step-by-Step: Tagging a User Card as Lost



- Highlight the lost key or card in the Reader Type column of the listbox.
- Click the lost key button ( ).

The tag "Lost" appears in front of the **Reader Type** column of the listbox.



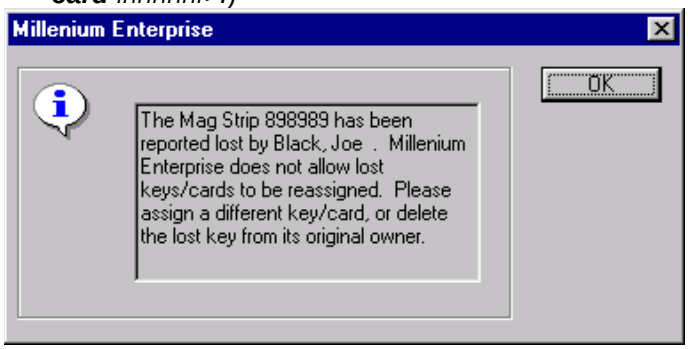
Click the Save button.

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: If you find a lost card or key, try it at an access code reader. Then, find out from history the original user's name and the access code. Another option is to go to the ACCESS tab and press the Reader... button. Then select the Reader Type and type the code in the Access Code field. Press the Search button to search for any user that has the given key or card assigned.

- 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.)

Users Toolbar Button

Add and edit names and key / card information on people who access your facility. Then give each user an ACCESS GROUP assignment. If you have the optional Millenium Enterprise BADGE module, click the BADGE tab on the USERS dialog to capture photo images and make user badges.

You can also:

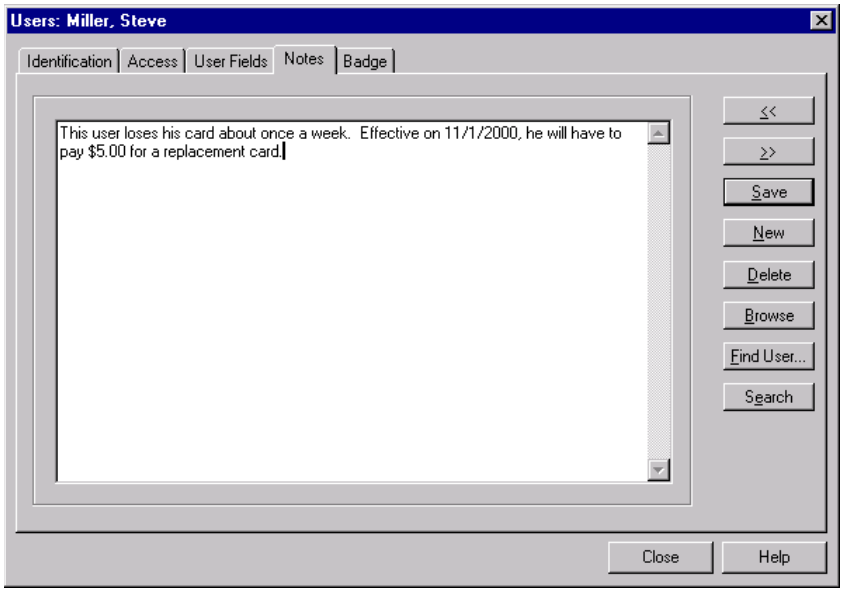
- Set a date when a user's access will EXPIRE.
- Assign a user PIN number for use in KEYPAD combination readers.
- Record when a user 's key or card is LOST.
- Display a user's image.
- Encode a 14-character ABA card (with optional Ilco System 800 encoder)
- Record free-form data about individual users for use by operators with authority to view the NOTES tab.

Important!

A person must exist as a User in Millenium Enterprise software before he or she can become an operator.

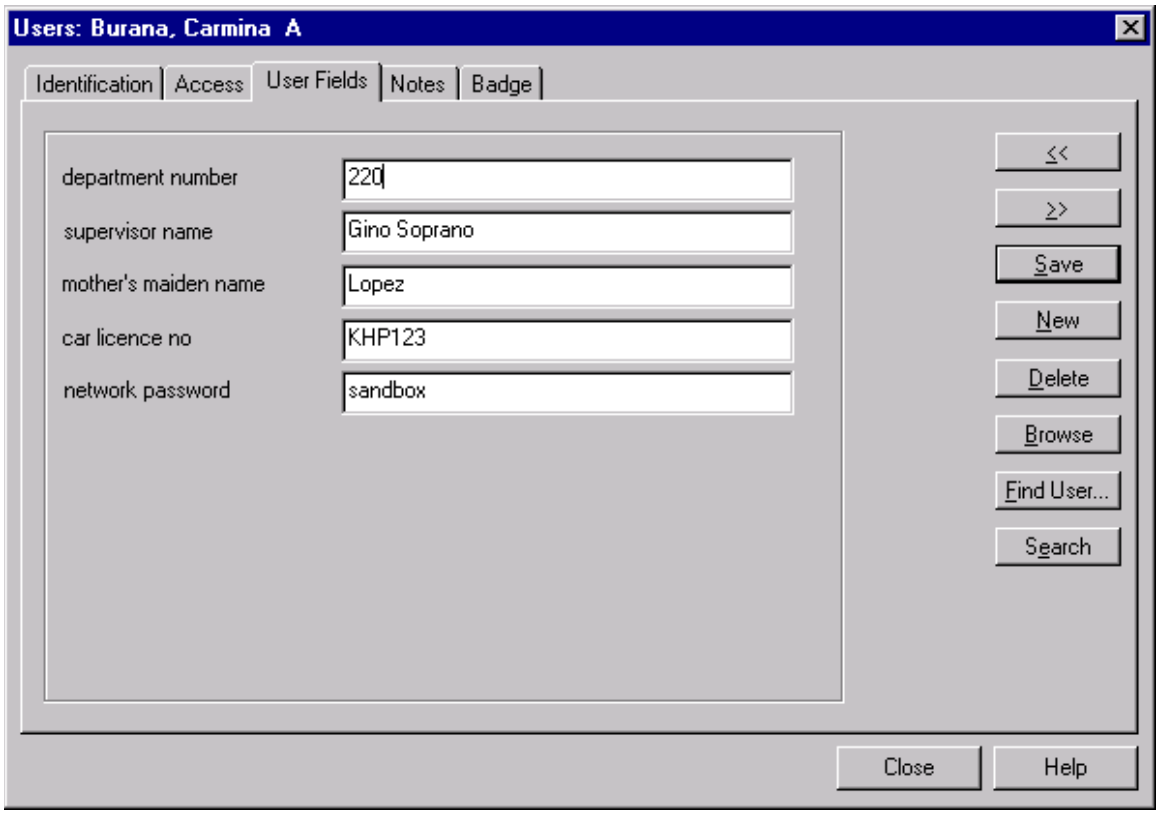
Users (Notes tab)

Use this tab to record notes you want Millenium Enterprise operators to have available for individual users.



Users (User Fields Tab)

Up to ten field names that appear in this dialog come from entries made by a Level One operator in the setupmpw program. In other words, you define exactly what custom user information you want to include in the User database.



Users (Badge tab)

Once you have users recorded in the database, the Badge tab (shown below) is the heart of the badge-making process. First, you Setup the system and Layout the badge style(s). Then, use the Capture, Preview and Print buttons to produce the badges. Each of these buttons represents a section in the ***Millenium Badge User Guide***, and is also covered in on-line help.

How to Display User photo

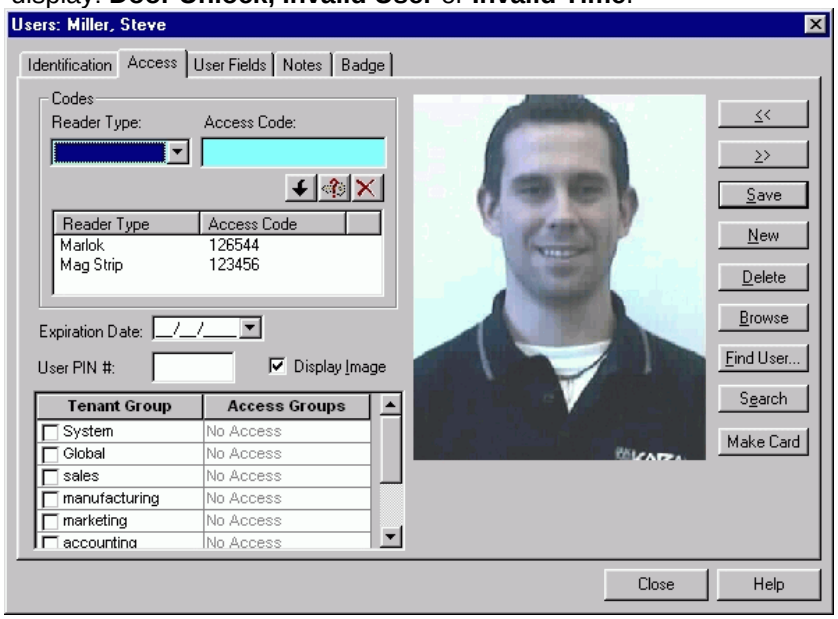
The Resident Filter dialog gives you an option to pop up a user image as part of the SCREEN filter features. The image triggers by an EVENT occurrence or as a result of selected HISTORY actions. The display can show two users at a time.

This option requires that you have captured user photo images through the Millenium Enterprise Badge system.

Step-by-Step: Displaying a User Photo

Highlight the Screen resident filter in the OUTPUT DEVICE / FILTER / TIMEZONE / DEVICE GROUP listbox of the Resident Filter dialog.

1. Highlight your choice from the Filter, Timezone, and Device Group listboxes.
2. Determine whether you want the user photo to display based on pre-determined **Events** or based on **History** (History portion of Millenium Enterprise workspace.)
4. Then select one or more of the three actions for which you want a user photo to display: **Door Unlock, Invalid User** or **Invalid Time**.



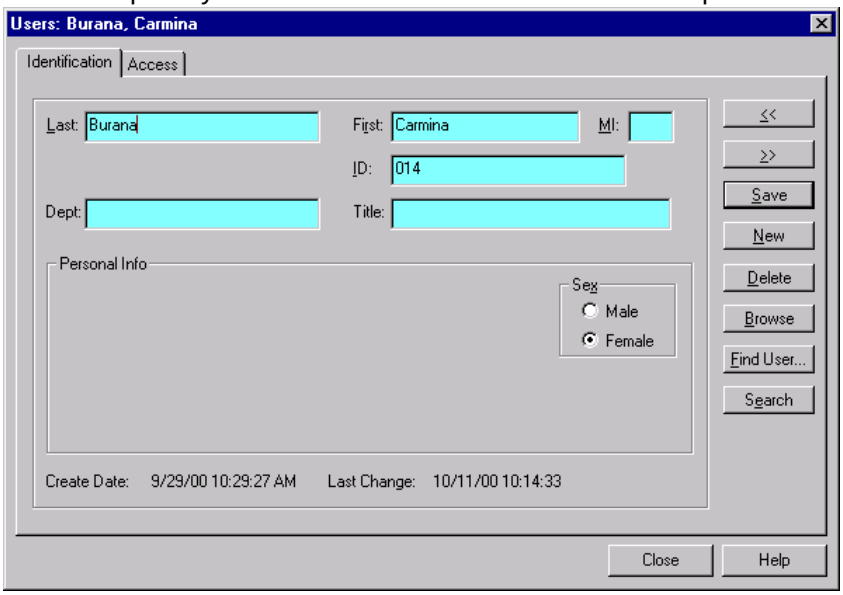
- When based on *Events*, the following selections will only display a user photo if the actions are selected as Site or Door .

- 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 are not recorded or displayed as events for elevators.

- **Note:** You can display a user's image by double-clicking a row in the Millenium Enterprise 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.
- 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.

Keeping Some User Information Private

The following dialog shows the USER Identification dialog with some user data removed from view. This privacy of selected user information can be set up based on a particular operator level.



Four fields may be removed from view based on a custom operator level that you set up.

- Social Security Number **User: Social Security No**
- Address **User: Address**
- Phone **User: Phone**
- Date of birth **User: Date of birth**

The screen shows the view right removed for all four types of personal information for the operator level currently logged in Millenium Enterprise. The Custom Operator Level dialog for this example will have **V**iew rights to **Users: Identification** (the main USERS dialog) but NO view rights to the four personal user fields.

Chapter 10: Operators

Operator Definition

- People who access your facility are called *users*. A user must first be recognized as a user in the software before becoming an operator.
- People who administer Millenium Enterprise software are called *operators*.
- A Level One *operator* determines the types of software actions the other users can perform.
- Operators also control access to the computer for such functions as changing programming data for the Access Management devices or just viewing and printing data and history.

Operators Toolbar Button

You can do the following through the Operators Toolbar button:

- Make a Millenium Enterprise USER into a Millenium Enterprise software operator
- Assign a password
- Select which operator level reflects the new operator's authority to perform system functions.

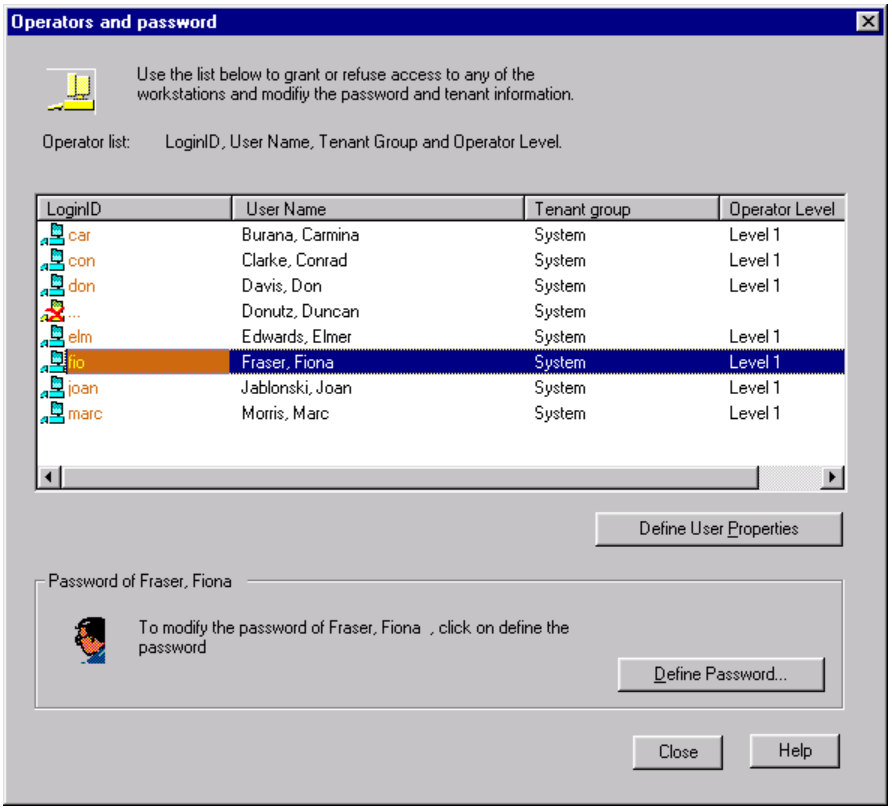
Two pre-defined operator levels come with the system - Levels 1 and 2.. A Level One operator has the option to create custom operator levels.

Important!

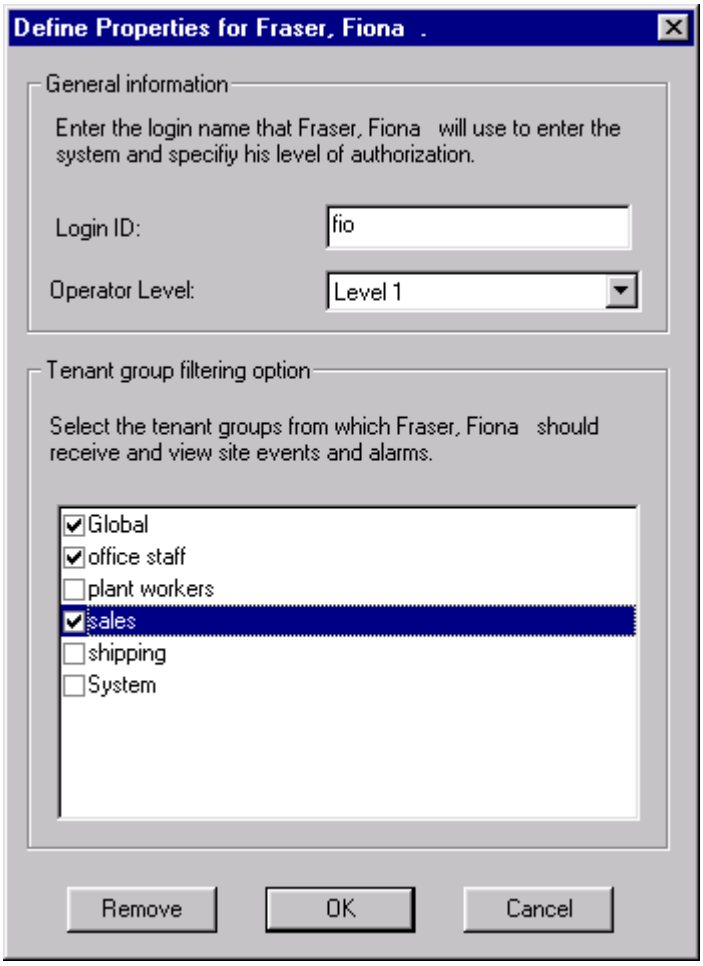
Only a Level One operator can change operator settings or add operators to the Millenium Enterprise System or use the Setup Millenium Enterprise program.

Operators and the TENANT GROUP feature.

The illustration below shows the OPERATORS dialog in Millenium Enterprise. Only Level One operators have access to this dialog.



When you click on Define the user's properties, the following screen appears:



1. Select the login name, level of operator and Tenant Groups that you want the operator to view.
2. Click OK
2. If you wish to remove a User as an operator, click Remove. That user will no longer be an operator, but remains on the list of users in the system.

When you click on Define the Password, the following appears:

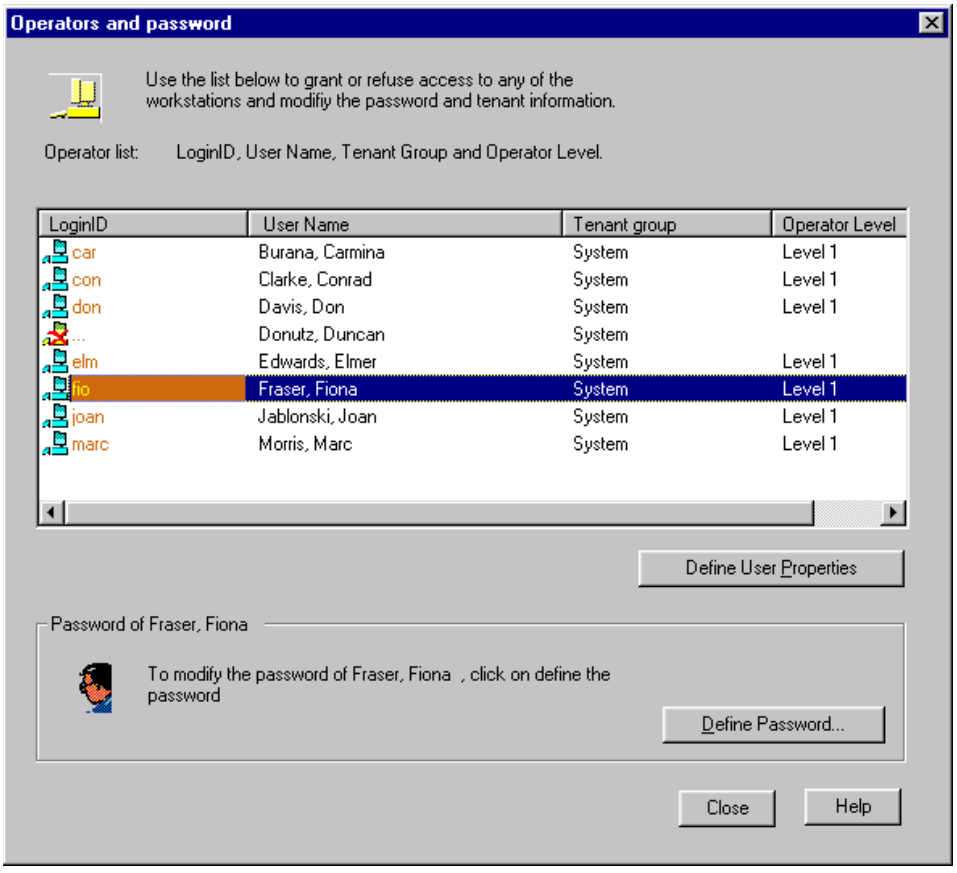
A Level 1 operator can change any operator's password from this dialog. Valid operators can change their own password through the Change Password dialog (Logon menu.)

Adding an Operator

To add a user as an operator of Millenium Enterprise, follow the procedure below.

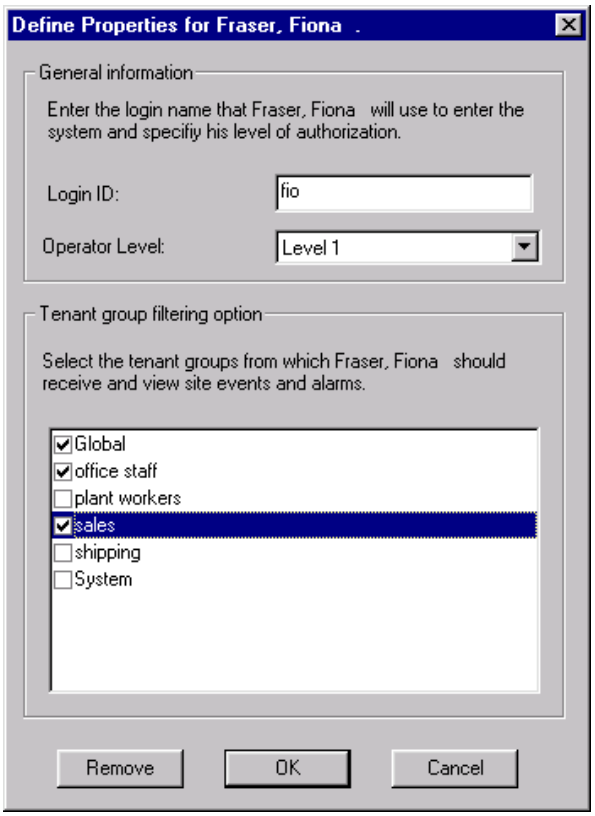
Step-by-Step: Adding an Operator

3. Make sure the person already exists as a User in the USERS dialog.
4. Click the  button.
5. The Operator Dialog Box appears.



6. Click the  button.
7. Scroll to the Name of the user you want to add as an operator. The Tenant Group to which the user belongs automatically displays in the Tenant Group field. (A user's tenant group assignment comes from the Users dialog/ACCESS tab.)
8. Click on 

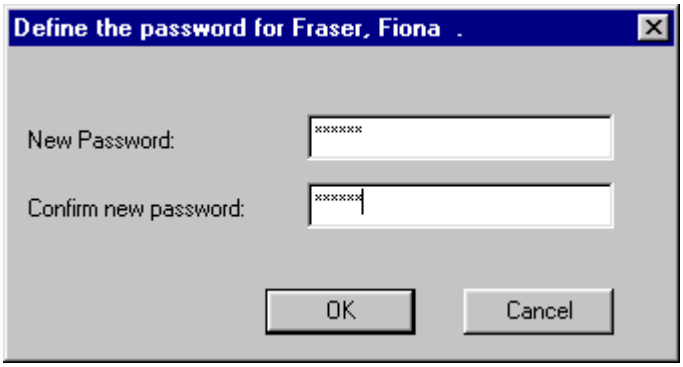
9. The following dialog box appears



10. Select the **Operator Level** to be assigned to this new operator by selecting from the dropdown list.
11. 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.

12. Select the login name, level of operator and Tenant Groups that you want the operator to view.
13. Click OK
14. If you wish to remove a User as an operator, click Remove. That user will no longer be an operator, but remains on the list of users in the system.
15. When you click on Define the Password, the following appears:



16. Type a **Password**.
17. Re-type the password to confirm the first entry.
18. Press the button.

Note: The button switches to an ADD button after you type in **all** operator data.)

Important!

Only a Level 1 operator has the 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 password, but a Level 1 operator can also change operator passwords through this OPERATORS dialog.

Level 1 System Operators have full rights to the system including management of:

- Tenant Groups
- Non-System Tenant Group Assignments
- Hardware Tenant Group Assignments
- Millenium Setup
- Timezones
- Operators

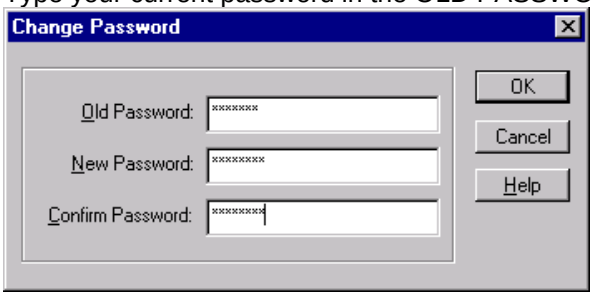
Change Password

A valid operator may change their password by the following procedure:

Step-by-Step: Changing a Password

1. Select Change Password from the **Logon** 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.
   Type the new password.
4. Press the <Tab> key (or down arrow, or <C> key) to move to the CONFIRM PASSWORD field.
   Re-type your new password.
5. Click the OK button to save the new password for your logon.

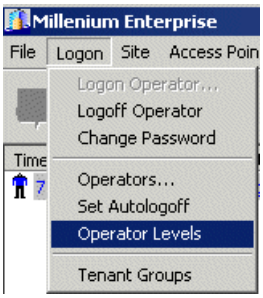
Current Operators

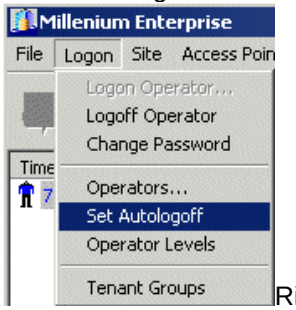
This field in the OPERATORS dialog lists the **Login ID** of all users who hold operator status, meaning they can log on to Millenium Enterprise software.

Operator Levels

Operators are those users who operate the Millenium Enterprise software. A **Level 1** administrative operator assigns each operator an OPERATOR LEVEL in the OPERATORS dialog. 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**. An operator who tries to perform a function which he doesn't have the right to perform will Unauthorized functions either do not appear, or inform the operator of insufficient rights to perform the function when attempted.

Level 1 Rights to all Program Features in Millenium Enterprise **PLUS** the following SPECIAL FUNCTIONS:

-  Rights to Setup Millenium Enterprise (setupmpw)
-  Rights to add an operator or to change operator settings. (Actions from the lower half of the Logon menu)
-  Rights to the OPERATORS dialog.
- 

Rights to create a custom operator (Operator Levels option under the Logon menu bar.)
- 

Rights to Set Autologoff.

Level 2 Rights to all Program Features in Millenium Enterprise **EXCEPT** SPECIAL FUNCTIONS of Level 1 operators (listed above.)

Notes:

1. 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.
2. 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.
3. We recommend that you always have **at least two people trained as Level 1 operators.**
4. Valid operators can change their own passwords, and a Level 1 operator can change any operator's password.

Custom Operator Levels

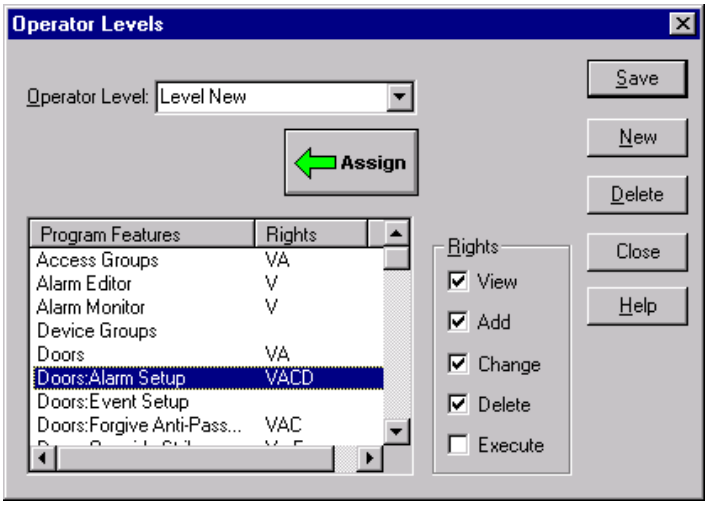
Level 1 operators have the option to create custom operator levels tailored to exactly those Millenium Enterprise menu functions they want to include. For operators logged in at their assigned level, the software only displays or enables those dialogs or menu actions to which that operator has access. 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*, *Date of birth*, or *Social Security Number* fields. See more information under **View**, below.

Click the **Logon** menu bar item to display the submenu.

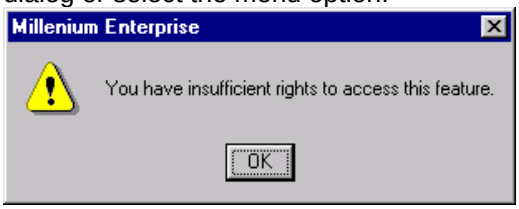
Then select the **Operator Levels** option to display a dialog similar to the following sample graphic:



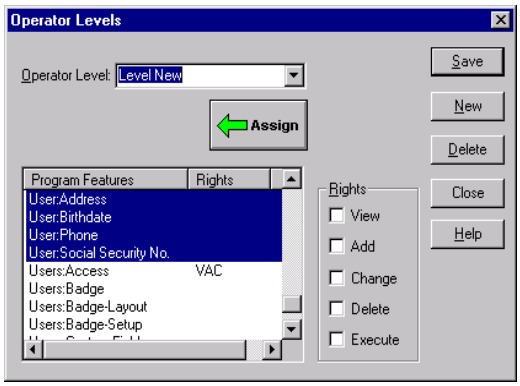
The above example shows four "rights" (***View***, ***Add***, ***C***hange and ***D***elete) assigned to the **Program Feature-**Doors (Access Points dialog, Millenium Enterprise tab) for the custom **Operator Level**, *Level New*. This example means *Level New* custom operator level can **View, Add, Change, Delete** and (Save) door data—all features on the Access Points dialog (Millenium Enterprise tab.) Without the rights to Execute, this operator cannot perform any actions that affect the entire Millenium Enterprise 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. The following four fields appear under the Program Features listbox, and may be removed from **View** and **Change** rights for a custom, user-defined operator level:



- To use this option, keep the View rights for the USERS: Identification feature and do NOT assign View rights for any or all the four personal data fields highlighted above.

Add

- Controls whether or not the button lets you add a new item to the Millenium Enterprise 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 Enterprise 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 Enterprise database.

Execute

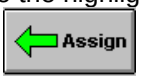
- Controls whether or not an operator can perform actions using any of the following special action buttons that affect the entire Millenium Enterprise network:
  SITE: 

and
  DOOR: 

Remote unlock, Update, Override Strike, Forgive Antipassback
  RELAYS: 

Step-by-Step: Creating a New Operator Level

1. Click the 

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 Enterprise.
2. OPERATOR LEVEL: Type a name as you want it to appear in the OPERATOR LEVEL listbox on the OPERATORS dialog.
3. Click to select the **Rights** that apply to the highlighted PROGRAM FEATURE(s) for the given **OPERATOR LEVEL**. Then press the 

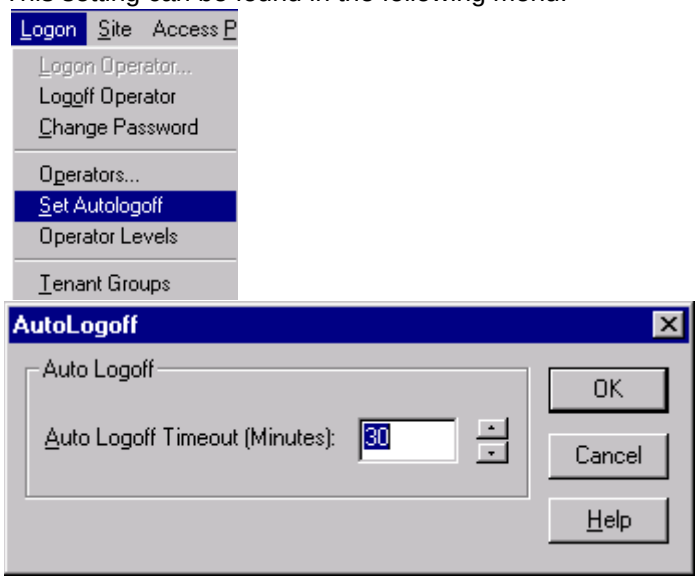
button to assign selected **Rights** to the highlighted PROGRAM FEATURE(s.) The initials representing the rights appear beside the selected features.

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.

Setting an Automatic Logoff

Millenium Enterprise 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.

This setting can be found in the following menu:



In the **Auto Logoff Timeout** field, record the number of minutes the system will allow the keyboard to remain inactive before reverting to a logon-required condition. Millenium Enterprise 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 log on again

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

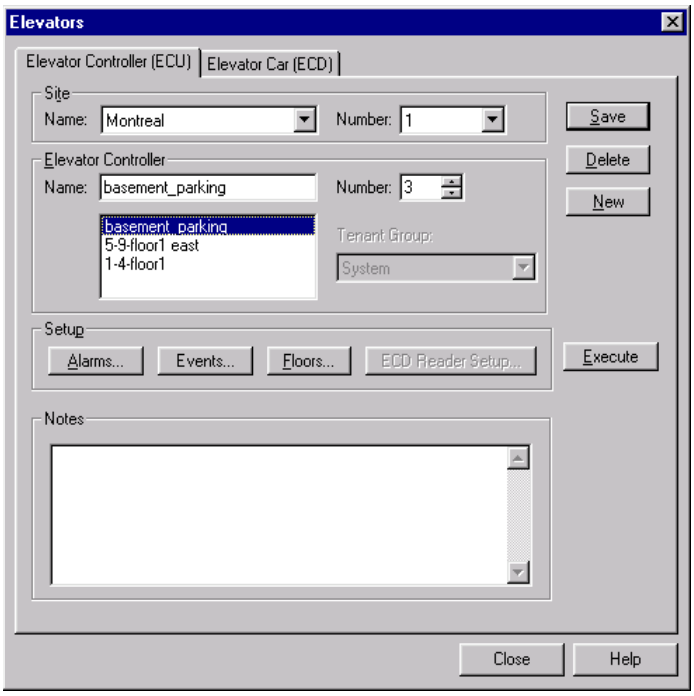
Important:

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

Chapter 11: Elevators

Elevator Controls

- Elevator control is an integral part of Millenium Enterprise software. Access Management devices required include an Elevator Control Unit (ECU), Elevator car Control Device (ECD) and reader device.
- 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 each. 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.)



19. The ACCESS POINTS dialog has an ECU Floor Relays tab where you set up or program the 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
- Alarms... button opens a dialog where you set up elevator alarms.

Events... button opens a dialog where you select alarms or actions to be treated as EVENTS for the given Elevator Control Unit (ECU.)

Reader... 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 Update button enables you to perform an update of programming data to the ECU or a status check on an ECU.

Elevator access points

The ACCESS POINTS window (**ECU Floor Relays** tab) includes a special button with options to control the following elevator floor functions from the PC:

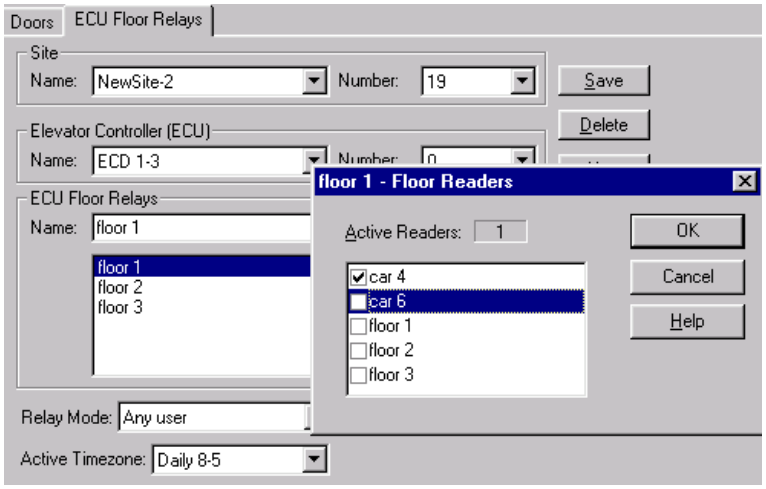
- Override Floor Relay
- Remote Unlock
- Update (Works just like the Update button on the main ELEVATOR tab.)

Press the Save button to automatically send data to Millenium Enterprise devices. The update action sends (1) all users and their access group rights to each elevator floor relay, (2) the ECU device map, and (3) alarms and events programmed for the ECU. The update is often done after a device is newly installed, repaired or replaced.

Readers Button (Elevators)

1. To program which elevator floor buttons will light up for a given floor, click the Reader... button from the ACCESS POINTS dialog ECU Floor Relays tab. The pop-up dialog lists Elevator car Control Devices (ECDs) created through the ELEVATORS dialog Elevator Car tab.

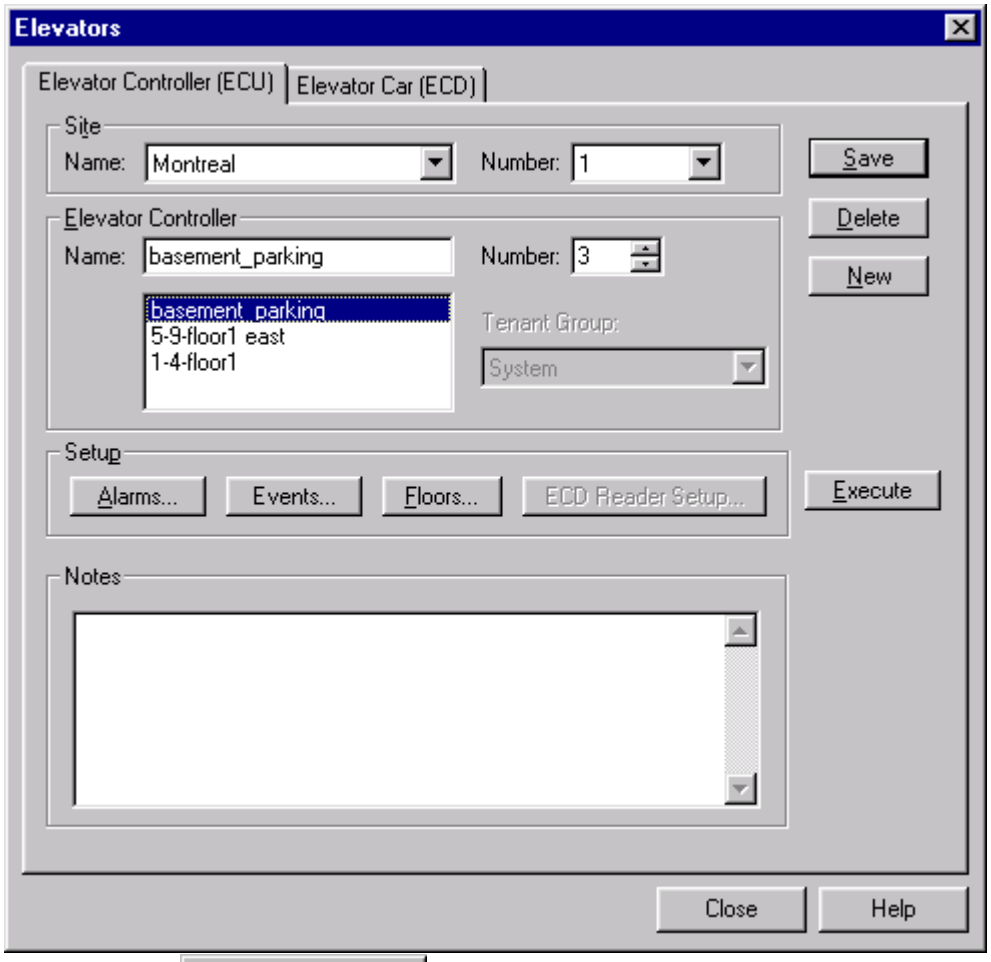
NOTE: Elevator floor access is also controlled by the individual passenger's ACCESS GROUP assignment, based on particular Elevator floors and Timezones.



2. Click to select the elevator car reader that will activate for the highlighted floor.

3. In the example, the reader selected in the pop-up dialog (—the reader wired to the ECD for Elevator Car 4—) will activate for the highlighted floor (Floor 1-Car 4.)

NOTE: To set up the one type of reader device to be used under one Site Control, go to the ELEVATOR dialog

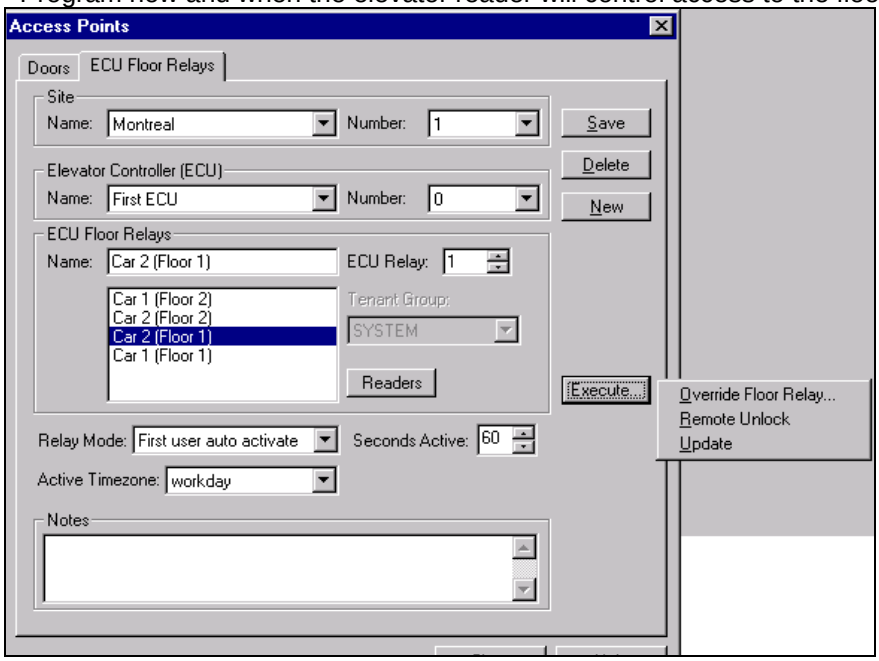


and press the ECD Reader Setup... button.

ECU Floor Relays

Use the ACCESS POINT dialog's ECU Floor Relays tab to:

- Name and assign elevator floors—each of 16 ECU Floor relays—as access points
- Select Elevator car Control Device (ECD) readers which will activate the given floor, and
- Program how and when the elevator reader will control access to the floor.

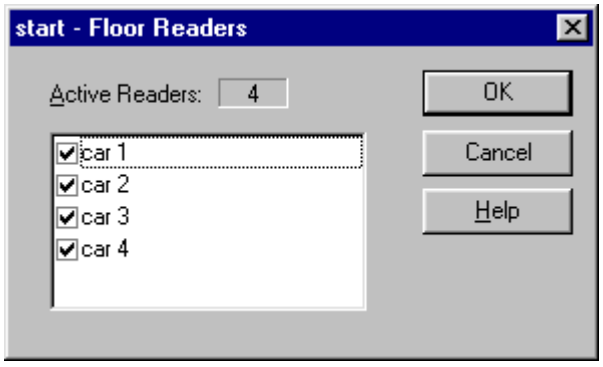


Relay Mode Controls elevator access points (floors) the same way relay modes control doors.

Active Timezone Timezone during which the given floor relay will be available to valid users. Normally the Active Timezone is only used for the Auto activate and First user auto activate floor relay modes.

Seconds Active Number of seconds you want the elevator control relay to remain active (de-energized.) The maximum is 255 seconds with five (5) seconds being an average setting.

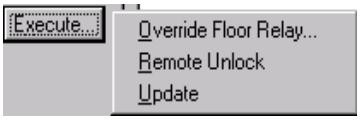
Reader... Select elevator car reader that will be active for the given floor.



The reader device attached to the selected ECD will receive a user's key or card and grant or deny access to the elevator floor. A button on passenger control panel will either light up for the given floor or remain unlit. Example (above) shows Elevator car readers for one floor.

Note: This Floor Readers dialog and the Site Floors listbox (ELEVATOR dialog's Elevator Car tab) show identical data in two different ways.

Perform one of three functions:



Elevator Relay Modes

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

No action	▪ Elevator relay does not activate for the given floor.
Auto Activate	▪ 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.
First User Auto Activate	▪ 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.
Valid User	▪ Elevator relay activates for a valid user, for the designated number of Seconds Active–only during the Active Timezone.
Rejected User	▪ Elevator relay activates for a rejected user, for the designated number of Seconds Active–only during the Active Timezone.
Any User	▪ Elevator relay activates for any user (valid or invalid,) for the designated number of Seconds Active–but only during the Active Timezone.

Adding Elevator Control Units (ECUs)

Millenium Enterprise Elevator control option programming takes place in two dialogs—

ELEVATORS dialog

A. Elevator Control (ECU) tab— add Elevator Control Units, set up one reader type per Site Control, set up alarms and events.

B. Elevator Car tab—name elevator car and assign those relays (floors) activated by using a valid key or card in the card reader device.

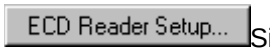
ACCESS POINTS dialog

C. ECU Floor Relays tab— name the floors controlled by elevator relays, assign floor relays, and program how the relays will control the elevator floor access.

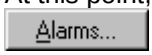
Step-by-Step: Adding an Elevator Control Unit

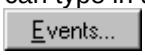
Part 1.

1. Select the ELEVATOR icon. 
2. The main Elevator dialog appears.
3. On the main Elevator tab, highlight a SITE NAME where you want to add (program) an Elevator Control Unit (ECU.)
4. Type a NAME for the Elevator Control. The first ECU at a given site must have ECU number zero (0) ECU 0 serves as the **master** elevator controller.



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 car 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.
3. Pop up Elevator Car dialog.

Part 3.

The next step is to program **ECU Floor Relays** (ACCESS POINTS dialog). Pop up ECU Floor Relays dialog. 

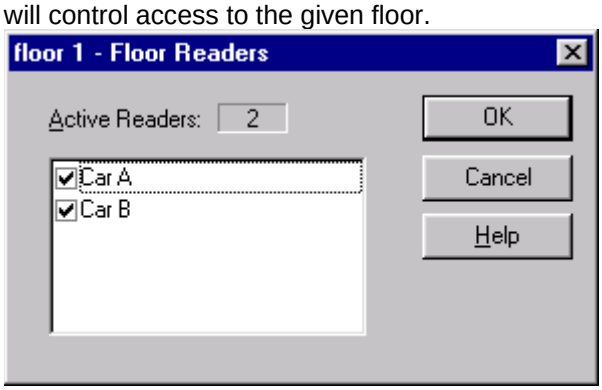
1. Click the ACCESS POINTS toolbar button, and select the **ECU Floor Relays tab**.
2. Select the ECU for which you want to name and define up to 16 relays (floors.)
3. Press the 

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 to fifteen. 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 Readers button to select the Elevator car Control Device (ECD) readers) that will control access to the given floor.



The reader device attached to a selected ECD will read 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)

6. 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

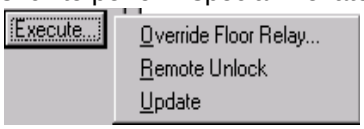
If appropriate, select the TIMEZONE during which the given floor relay will be available to valid users. The Active Timezone is commonly used with the Auto activate and First user auto activate relay modes.

Seconds Active

Time-related relay modes let you set the number of seconds you want the elevator control relay to remain active (de-energized.) The maximum is 255 seconds with 5 seconds as an average setting.

Execute...

Click 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.
- Send current programming data to the ECUs. This occurs naturally when you press the Save button, See Updating devices in the Millenium Enterprise network for more about the update function.

It is possible to have more than one Elevator car 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.

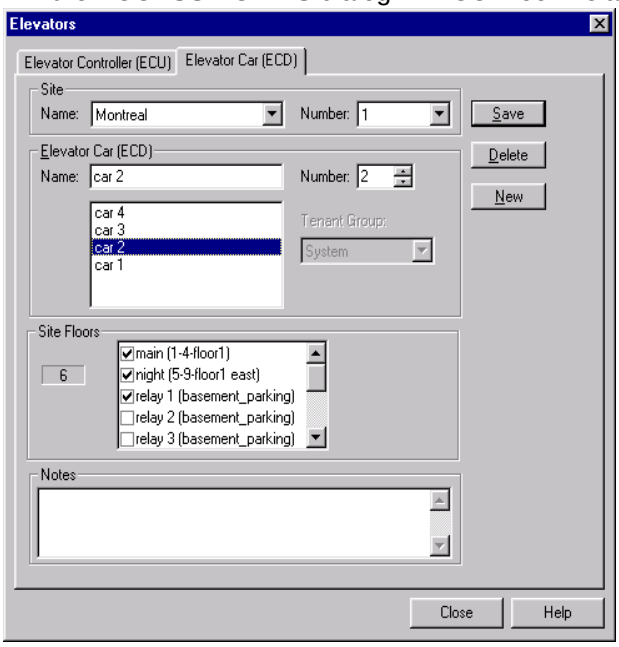
Examples:	**ECD**	**Controls**
	Floor 1 - Car 1	Front door
	Floor 1 - Car 1	Back door
	Floor 2 - Car 1	Front door
	Floor 2 - Car 1	Back door

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.

Elevator Car Tab

Use the ELEVATOR dialog's Elevator Car tab to:

- Name the Elevator car Control Device (ECD) commonly known as the elevator car, and
- 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.

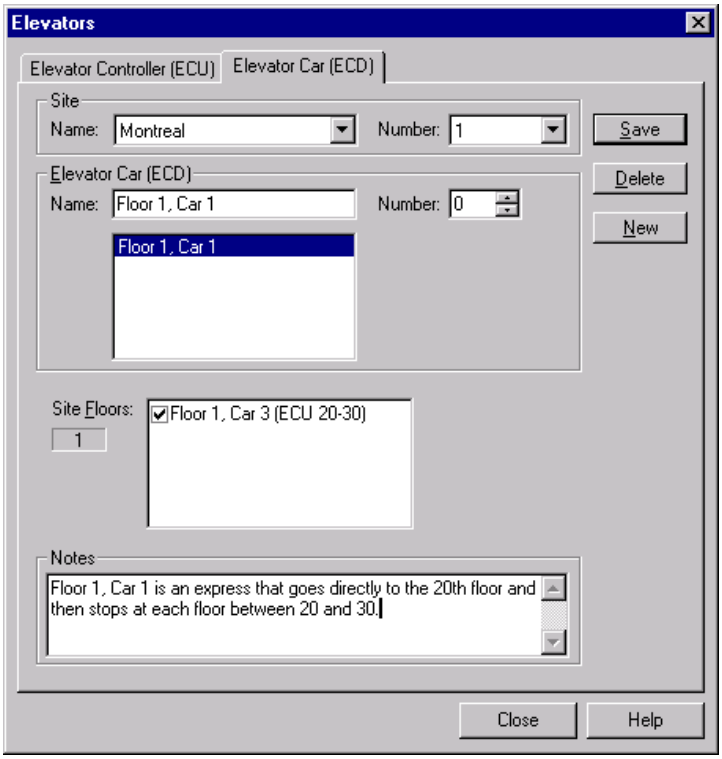


- You may select floors and elevator cars in two different parts of the software:
- In the Site Floors listbox, above, select floor relays to be activated by the highlighted elevator's reader, or
- Select the Elevator card Control Device (ECD) reader that will control access to a given floor in the ACCESS POINTS dialog (ECU Floor Relays tab.)
- Notice the ECU name appears after the name of the **Site Floor** for your reference, and that 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.

Setting up an Express Elevator

The following example shows how an express elevator setup would look to have an elevator car (ECD) only stop at the first and twentieth floors. For valid users, the reader in Elevator car 3 would only activate ECU floor relays to light up buttons for Floor 1 and Floor 20 on the passenger's control panel inside the elevator car.

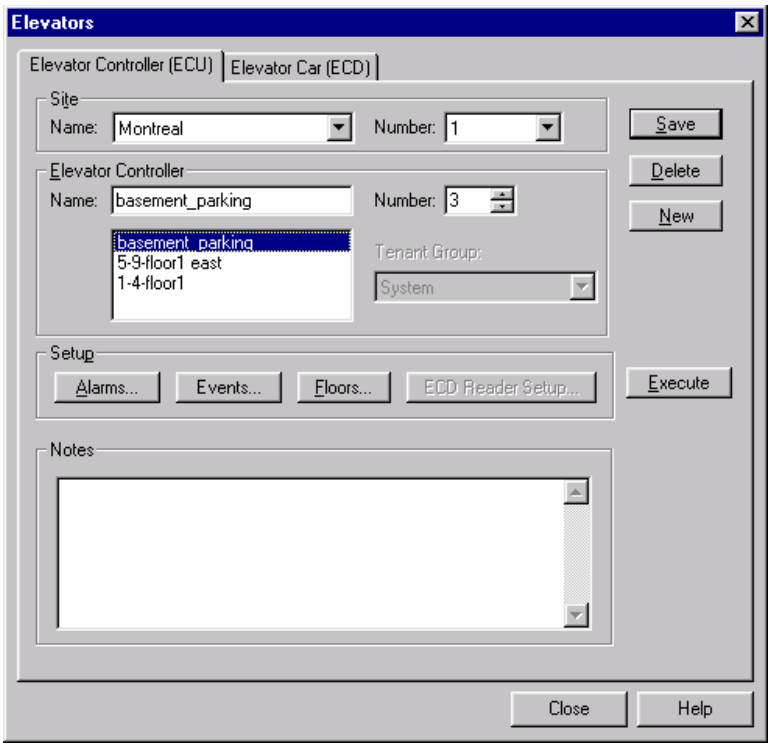


Setting up Elevator Alarms

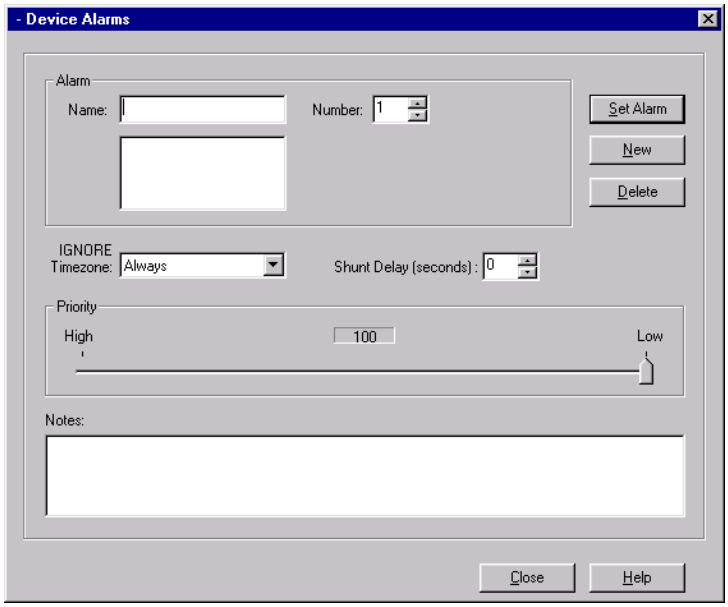
Millenium Enterprise Elevator Control Units (ECUs) come with a tamper alarm and an optional external manual bypass alarm. In addition, four unsupervised alarm inputs may be programmed through the software as follows:

Step-by-Step: Programming Alarm Inputs

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.



5. Give the alarm a descriptive name that will clearly identify the alarm in other parts of the Millenium Enterprise system such as in the Alarm Monitor, in the ECU 

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.

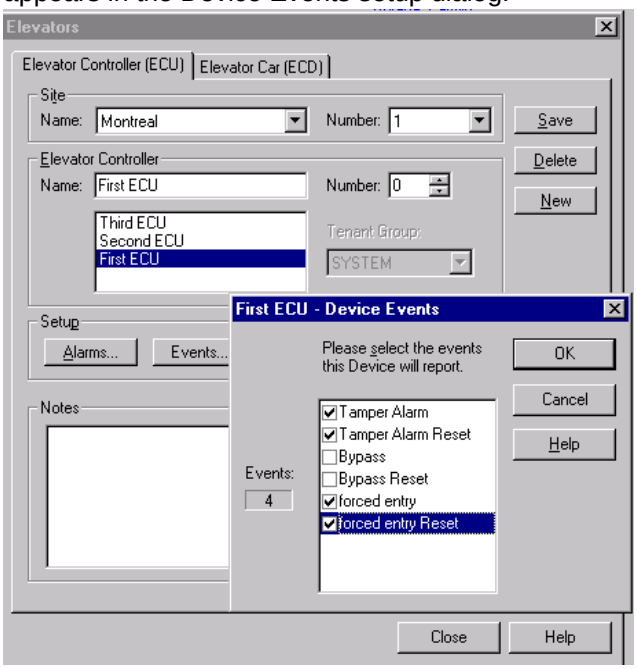
8. SHUNT DELAY: Establish a grace period before the alarm triggers. Options are between 1 and 255 seconds.
9. Prioritize the alarm in a scale from 1-100. In the Alarm Monitor, an operator must respond first to those alarms with the highest priority.
10. Use the NOTES section to further describe the alarm you are setting up.
11. Press the Save button.

Setting up Elevator Events

In Millenium Enterprise systems, an event is a pre-defined action that triggers a relay. Elevator events include tampering with the ECU circuit board device, any of the four alarms (and their resets,) and use of the manual by-pass switch.

Step-by-Step: Selecting Alarm Events

Once you have set up elevator alarms (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.



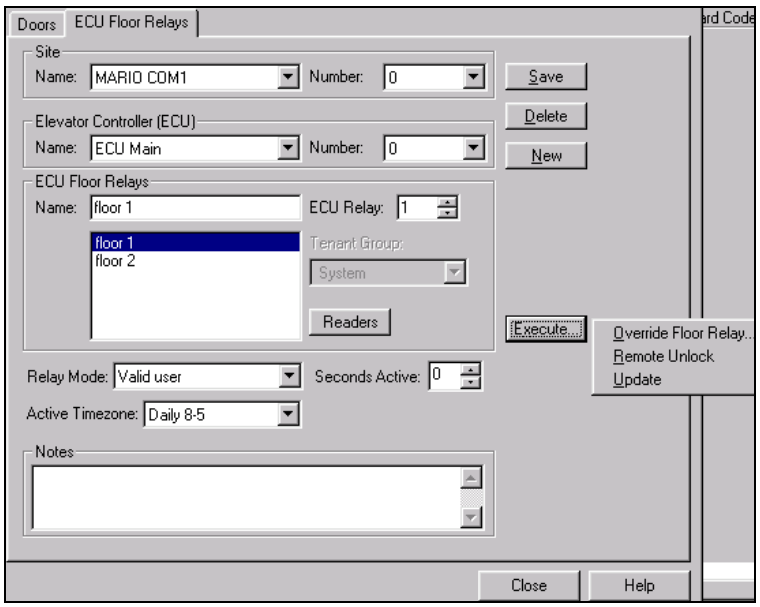
1. Click to select those alarms (and usually the corresponding reset) you want to be treated as “events” for the given elevator controller. A check mark appears beside selected events.
2. Click the button to save your selections.

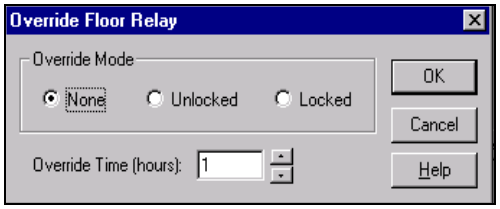
Note: Each event goes out to the Millenium Enterprise network as data output from the ECU. In the above sample dialog, the given ECU uses one of its four possible alarms (Named "forced entry" in the above ECU's Alarm Setup dialog example.) The Alarm and its reset (Forced Entry Reset) are designated as EVENTS. When a person forces the elevator door open, the Forced Entry alarm triggers whatever device you have wired to respond. When the button is released, the reset stops the responding device.

- The event will display on the PC (history portion of Millenium Enterprise's application workspace) with stand-out attributes as established in setupmpw under the COLORS option.
- Based on the setup on the left, the history event will be highlighted in yellow in the Millenium Enterprise application workspace.
- The ALARM MONITOR module displays alarm events, only, and is designed to be running continually for security personnel.
- If you use optional RCDs, the ECU event can cause an action by its respective relay on an RCD circuit board.

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.)





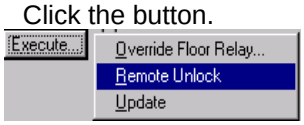
Override Mode	None	▪ This elevator floor is not in a temporary override mode.
Override Time (hours) **For auto-activated relay modes:**	Unlocked Locked	▪ This elevator floor is set to temporarily unlock for the OVERRIDE TIME indicated. ▪ This elevator floor is set to temporarily lock for the OVERRIDE TIME indicated. ▪ 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. ▪ 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.

Remote Unlock (Elevator floor)

Elevator floors can be remotely unlocked from the PC by any Millenium Enterprise operator with EXECUTE rights to the ACCESS POINTS 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.

Step-by-Step: Executing Remote Unlock for Elevator Floor

1. Open the ACCESS POINTS 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.
   (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.

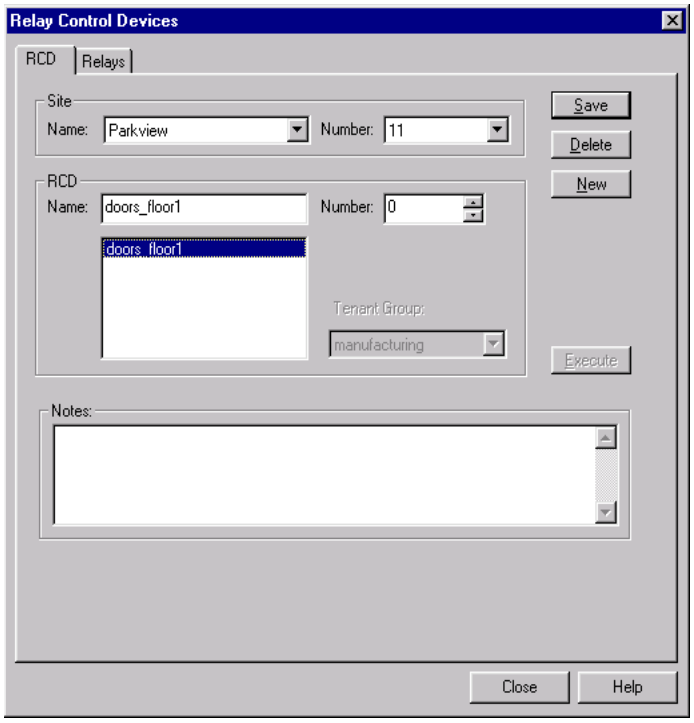
6. History reflects "Operator Unlock," and identifies the elevator floor, site, and operator ordering the action. After the remote lock actually opens, history reflects "Remote Unlock," and identifies the floor and site.

Chapter 12: Relay Control Devices

RCD Toolbar Button

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 Enterprise network. RCDs can also trigger other devices and be set to activate an auto-dialer. The illustration below shows the RCD dialog in Millenium Enterprise. 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 Timezones,
- To control optional devices such as a sprinkler systems or heating/air-conditioning in the Millenium Enterprise network
- To take advantage of a special System Supervisor function reserved for the first RCD relay.



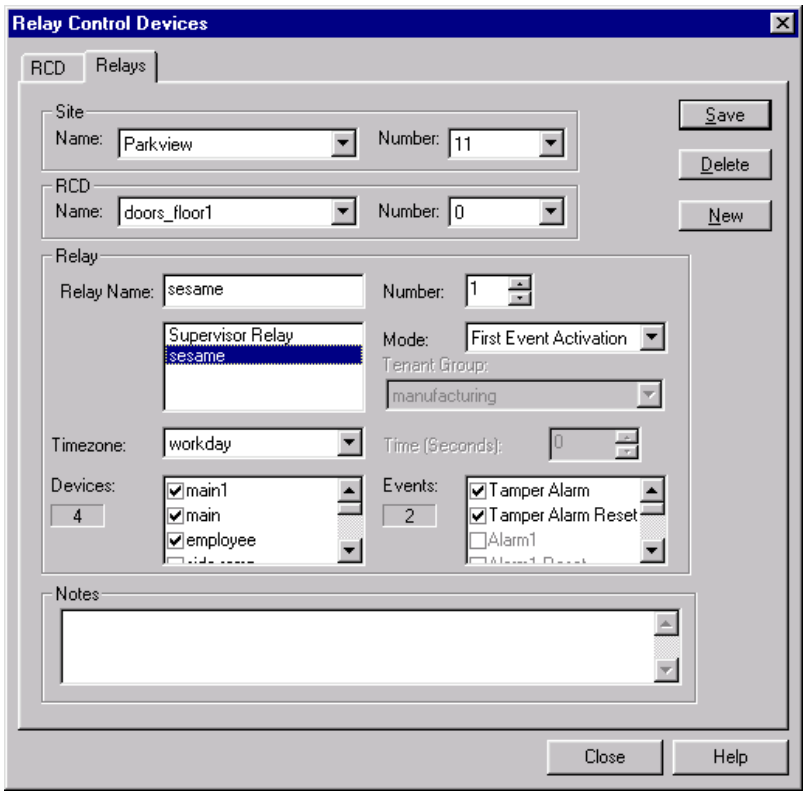
Setting up RCD Relays

Step-by-Step: Setting Up RCD Relays

1. Select the RCD icon 

.

Select the RCD tab if you have not yet added the Relay Control Device to the software. 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. The above example combines the RCD number (0) with the relay number (1.)
   Notice the **first relay** (0) 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 Enterprise handles up to 10 RCDs per Site Control Unit. 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 Enterprise 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 events) to which it will 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.

8. Use the NOTES box to enter free-form descriptions of the particular relay function being set up.
9. Click the 

button to finish the RCD relay setup process.

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 Enterprise. 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 off-line, 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 Enterprise 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.

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 at least SCU Issue **U**.

Table of RCD Modes

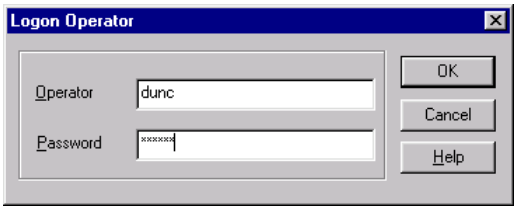
Up to seven relays (including the Supervisor Relay) on each optional Relay Control Device (RCD) can operate in any of the following modes:

System Supervisor	***(Only applies to Relay #0 on the first RCD (RCD #0) per Site Control)*** **This relay is shown by default when you open the RCD dialog box, relays tab.** Relay **activates** when PC is polling other devices on the system. If the PC and SCU go off-line, 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.
Alarm Latch	Relay changes state (activates or de-activates) until the specified EVENT resets, at which time the relay returns to normal state. You must only specify *one* event from *one* device. Event choices are: Tamper Alarm -or- Alarms 1 through 7 -or- Tamper Alarm Reset -or- Alarms 1-7 Resets
First Event Activation	Relay activates at some time during the TIMEZONE after receiving the specified EVENT or EVENTS and 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**.
First Event Release	Relay de-activates at some time during the TIMEZONE after receiving the specified EVENT or EVENTS and 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**.
Timed Release	Relay de-activates for specified length of time after receiving 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.)
Timed Activation	Relay activates for specified amount of time after receiving the specified EVENT or Events and de-activates after 255 seconds.
Timezone Activation	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**.

Chapter 13: Alarm Editor

Alarm Editor: Logon and Logoff

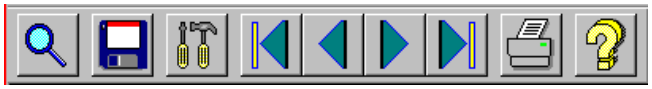
The Alarm Editor requires a separate logon.



Enter the same ID and password as you are currently using in Millenium Enterprise. If you have not set up operators in the main application yet, use the default marlok, stcharles.

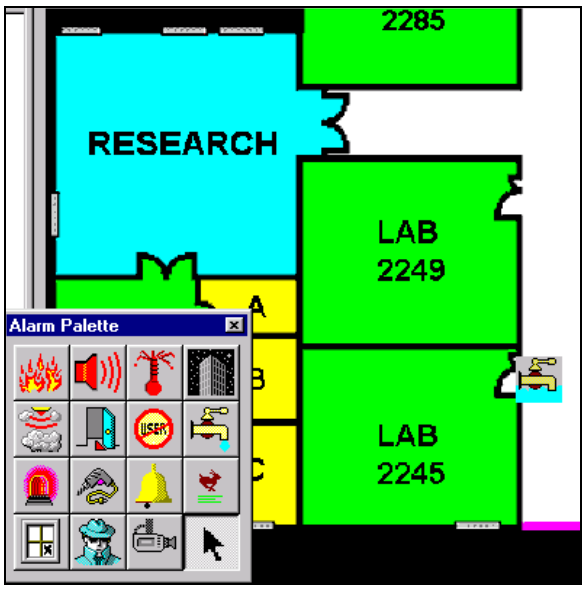
Alarm Editor: Toolbar Contents

The Alarm Editor toolbar contains tools to help you search for a particular site.



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 Enterprise database.



Displays alarm icon palette. Double-click on the icon and then click the cross-hair cursor on the location on your layout that most nearly represents the location of the alarm. An example is shown below - a water level detector is placed outside the Lab door.

Moves to the FIRST site programmed in Millenium Enterprise' 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 Enterprise' database.

Moves to previous site.

Moves to next site.

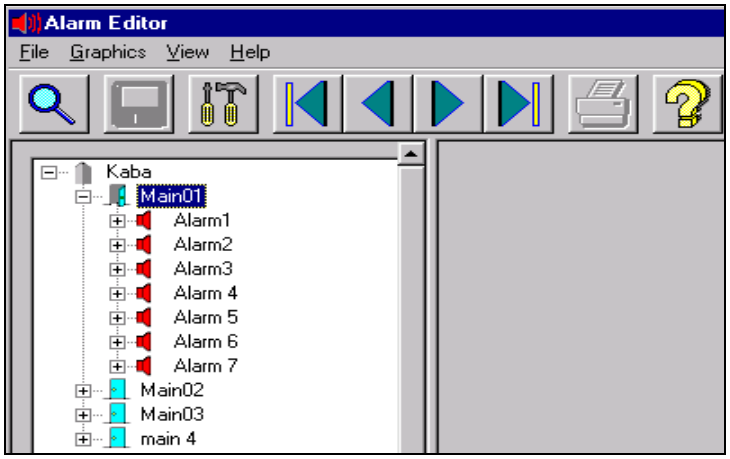
Prints the currently displayed floor map.

Displays the on-line help for the Alarm Editor. To see on-line help for an individual dialog, click the button in that dialog.

Setting up the Alarm Editor

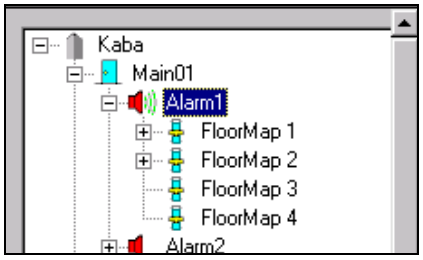
Notice the first steps are to set up the alarm and to establish the alarm as both a door event and as a site event in Millenium Enterprise software.

1. **Select the Site and Door.** Example shows "Kaba" and "Main01."

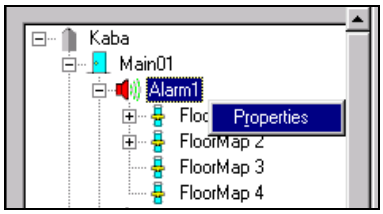


If you need help locating a particular site, use the Alarm Editor Toolbar to search. The fastest way to find a particular site among a large number of sites is to use the magnifying glass icon. Another way is to use the large arrow buttons on the toolbar to scroll forward or backward between programmed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

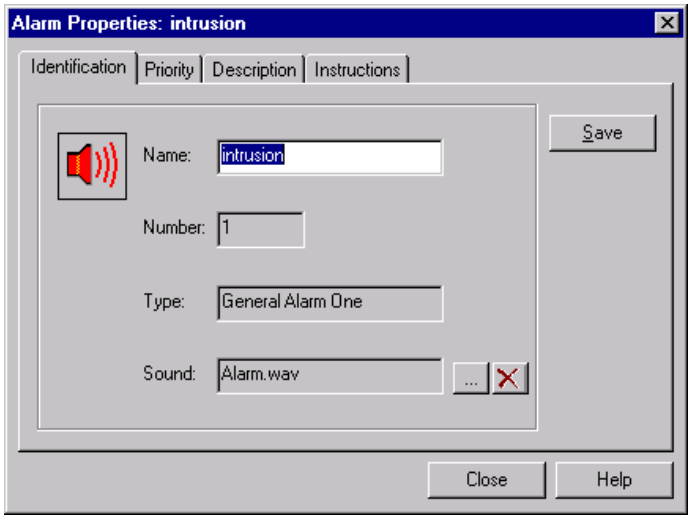
Then double-click on the alarm you want to set up:
The example shows "Alarm 1 on "Main01" DCD. After you double-click, the four possible floor maps appear.



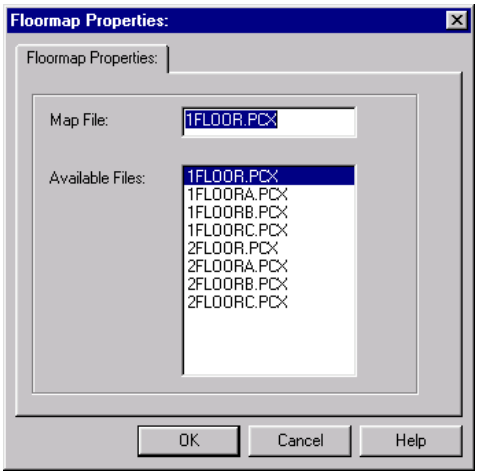
If desired, take a look at the PROPERTIES set up for the given alarm: Highlight the alarm name, and right-click. A **Properties** option appears. Highlight and click to pop up an Alarm Properties dialog. The Alarm Properties dialog includes four "tabs" of information:



- Identification
- Priority
- Description
- Instructions



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 **\mpw\Maps** folder in STEP 3.)

1. 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: The alarm icon appears as appears in the examples above. The fire icon will flash to aid the security guard in pin-pointing 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.

To **Delete** an alarm icon, click the icon and press the delete key. A verification box displays.
NOTE: Each of the four individual floor maps must have the DELETE action to remove alarm icons.

NOTE: The graphic floor plan you set up can also appear to the operator through the Alarm Monitor

Setting up the Floor Map

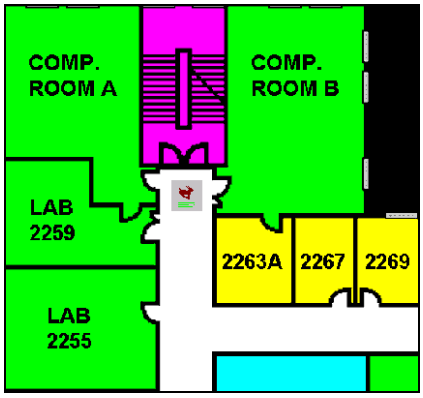
Floor Maps are graphic views of your facility that you provide. Formats can include: .pcx, .bmp, .wmf, .tif, .jpg, .pct, .tga.

Each of the seven (7) possible door alarms can have up to FOUR floor maps.

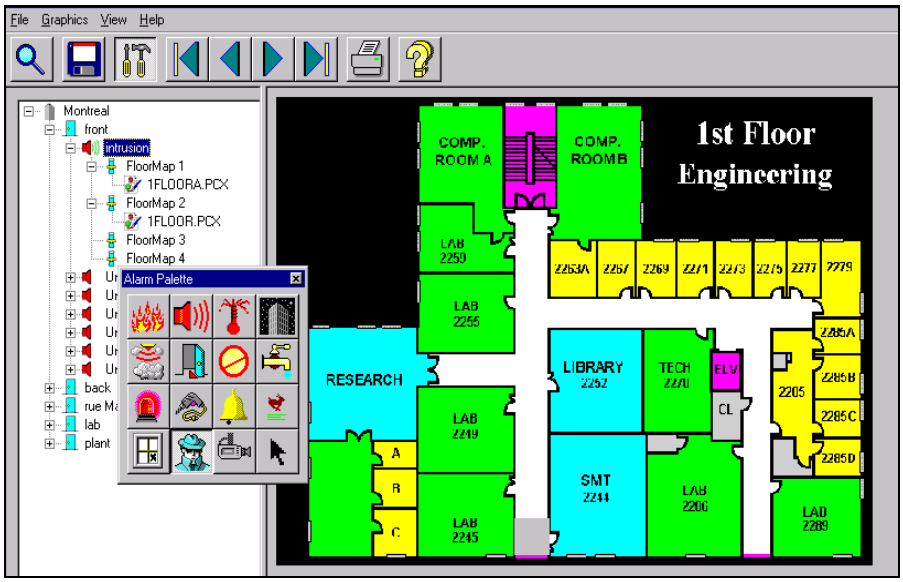
When setting up the Alarm Editor, you have the option to include alarm icons showing location of installed alarms.

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 triggers, 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.



The Alarm Editor lets you **prepare a visual display of alarms** wired in your Millenium network and programmed in Millenium Enterprise. 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 Enterprise system—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.

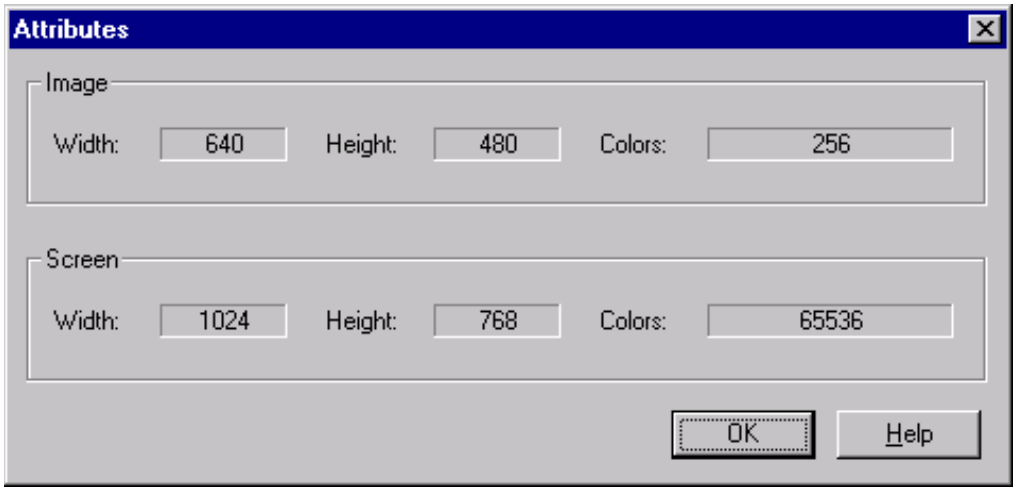
Notes: Alarms you have wired to the DCD and programmed in Millenium Enterprise appear with the name you established in the software.
The graphic floor plan you set up can appear to the operator through the Alarm Monitor

Jump to step-by-step directions.

Graphics Menu Attributes

Each time you open the Alarm Editor, the software attempts to present your graphic images in the best available way using your computer's current graphics capability. The Graphics menu bar displays your current graphics attributes.

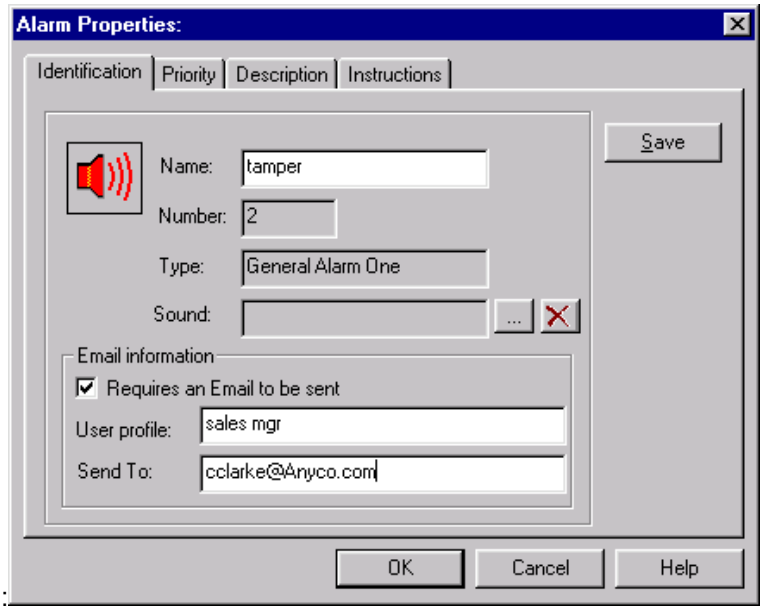
Attributes: Displays size and color information on the image and screen. This is reference information only. No editing occurs from this dialog.



NOTE: When you right-click on one of the palette icons, an attribute dialog displays the size and position of the selected icon. You can enter exact size and position settings for icon graphics.

Alarm Editor: 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 (Intrusion in the example above).
- **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.

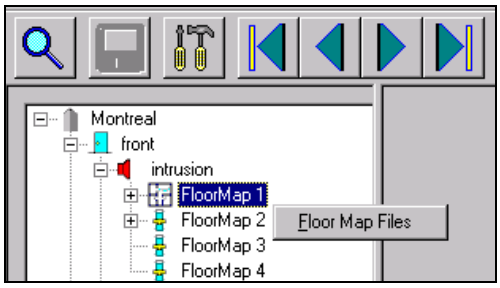
- **Priority tab:** Lets you change the priority of an alarm. This setting affects which alarms must be responded to FIRST in the Alarm Monitor. If more than one alarm triggers, the system uses your priority rating to display the highest priority alarm in RED so an operator will have no doubt as to what 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.
- E-mail Required: Fill in the name or position of the person you require an e-mail sent to. Whenever this alarm goes off, an e-mail will be sent to the address you enter, so that the relevant person is instantly notified of a particular alarm.

NOTE: Alarm Properties information comes from data you record in Millenium Enterprise ACCESS POINTS (Press setup button.)

Any changes you make in the above dialog will also affect the information in the ACCESS POINTS dialogs.

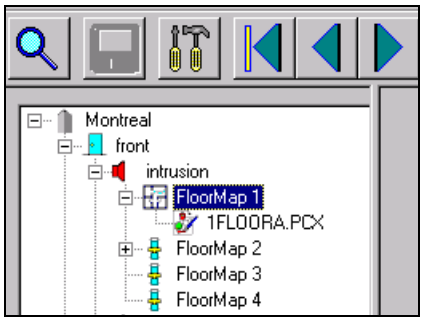
Alarm Editor: Graphic Files List

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.



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.

Graphic file selection for Floor Map 1 (above) appears in the following sample dialog:



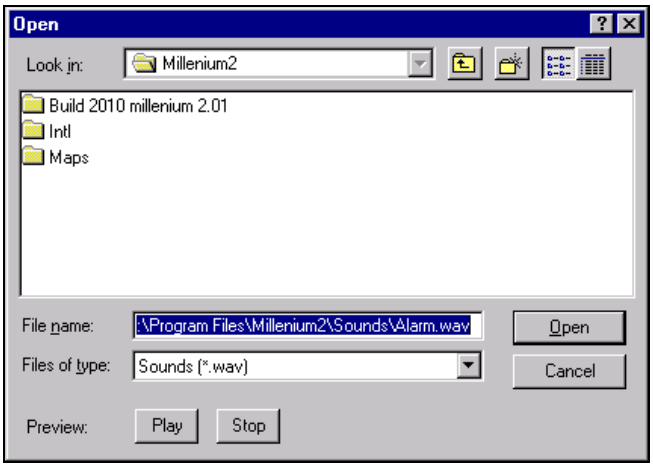
Available Files appear from the **\mpw\Maps** folder where you must place any graphic layout files to be used in the Alarm Editor.

Create the folder and then store your floor maps there

Alarm Editor can use any of the following image formats: .pcx, .bmp, .wmf, .tif, .jpg, .pct, .tga.

Sound Files

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



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

Important! For sounds to work in the Alarm Monitor, you must click the "Reminder sound" option on Alarm Monitor's Setup dialog. 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.

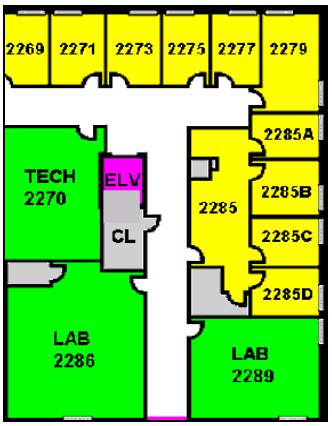
Alarm Editor Palette

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

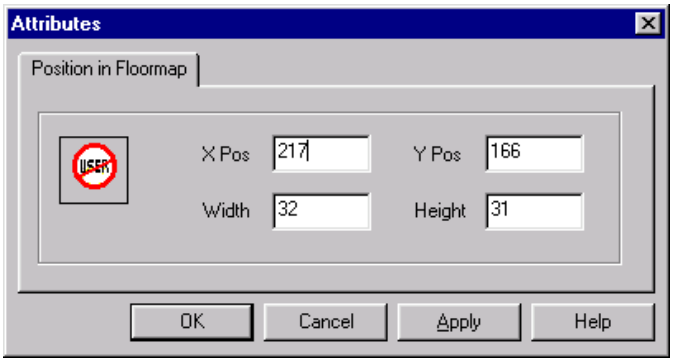
To see a word explanation of each graphic, hold the mouse pointer over the image until its "title" appears.

To select an alarm icon, just click the desired alarm image (invalid user, shown in the Attributes dialog box below).

- To place an icon, double-click the icon and then click on 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 following dialog box will appear:

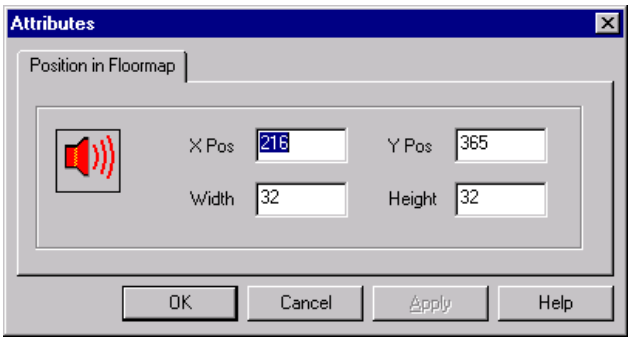


The same icon will automatically appear on each Floor map under a given alarm.

- To **delete** an icon, select it and then 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.

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.

Alarm Palette (titles)

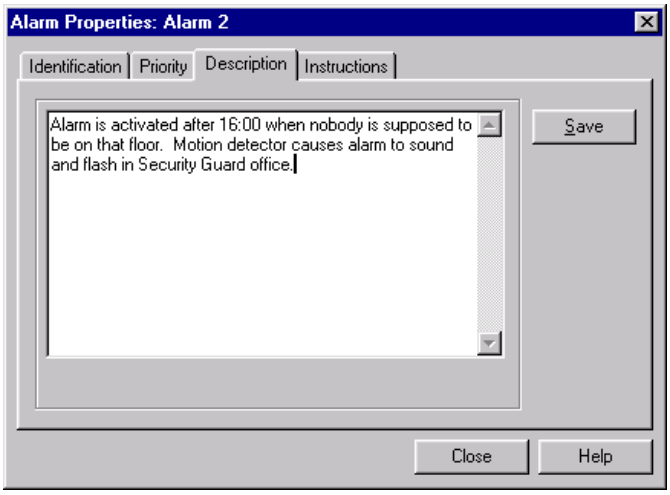
The following graphic shows the word title for the individual icons you can use to show the location of alarm devices installed in your Millenium Enterprise network:

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

Alarm Properties: Description

Description tab:

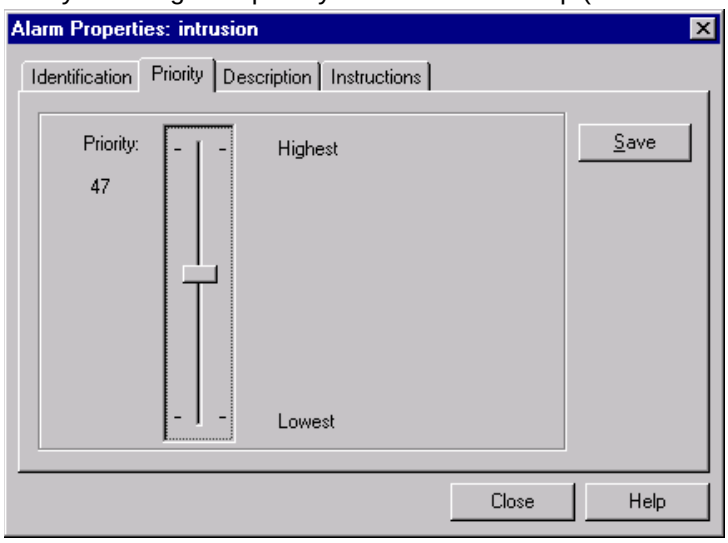
Lets you describe, in more detail, the alarm wired and programmed at this location.



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.

Alarm Properties: Priority

Lets you change the priority established in setup (ACCESS POINTS dialog.)



The system calculates priority of triggered alarms and places a 1 in the Alarm Monitor, in front of the alarm with the highest rating.

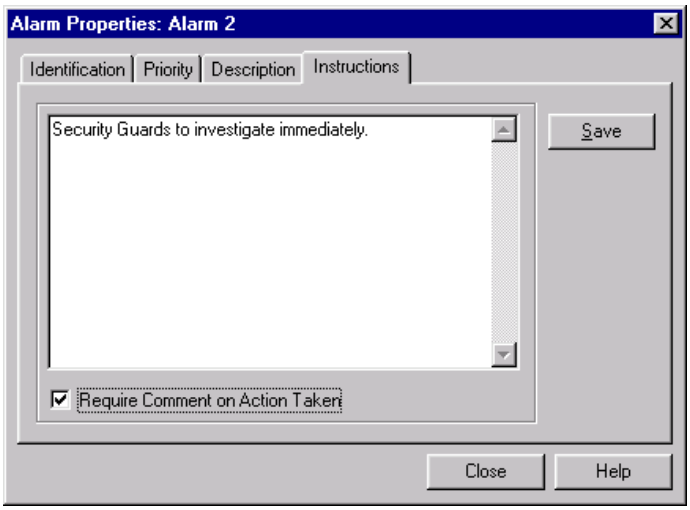
Important!

Program will not let operator investigate (double-click) an alarm with a lower priority.

Alarm Properties: Instructions

Instructions tab:

Lets you record instructions to the guard or security personnel about the highlighted alarm.



The Require Comment on Action Taken checkbox gives you the option to require the responding operator to comment on what actions he or she took in response to the alarm.

Details about the alarm, special instructions, and the operator's recorded response will appear in the ALARM MONITOR *Inspect Alarm* dialog.

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 *Inspect Alarm* dialog.
Inspect Alarm dialog will not allow the operator to close the dialog by pressing the Ignore or Acknowledge 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.)

Chapter 14: Alarm Monitor

Alarm Monitor is a graphical alarm editing application that allows a user to

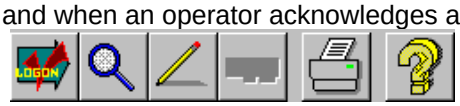
- Identify, track and report on triggered alarms
- Acknowledge and reset alarms
- locate the alarms on site maps that display the location of the individual active alarm.
- respond to alarms that require optional security personnel responses before being reset.
- respond to prioritized alarms displayed in different colors on the Alarm Monitor History screen
- include a pop-up photo of the user with unlock events
  (this requires the BADGE add-on.)

Alarm Monitor Toolbar Button

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

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

The advantage of the Alarm Monitor is that it displays alarm activity only. The history portion of Millenium Enterprise 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

Step-by-Step: Using the Alarm Monitor

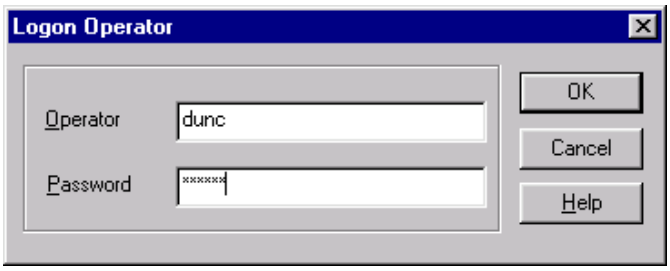
Setup		Dialog with some basic options on how you want Alarm Monitor to work.
Logon & Logoff		Alarm Monitor requires a formal logon as well as a formal logoff. Alarm Monitor is designed to run continuously on a dedicated PC, and also requires that Millenium Enterprise be running.

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

What the monitor reports		▪ Under the columns shown above, Alarm Monitor reports all alarms set up as events through Millenium Enterprise 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. ▪ The Monitor ranks triggered alarms according to their PRIORITY, and requires the operator to respond to the highest priority alarm event before any others.
Operator's Investigation of Triggered Alarm		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: ▪ expanded information about the alarm (from Alarm Editor's Alarm Properties dialog —Description tab.) ▪ instructions on how to respond to a particular alarm (from Alarm Editor's Properties dialog —Instructions tab.) ▪ operator's response to the triggered alarm (Enter Action Taken free-form entry box) ▪ This response can be required through a selection in the Alarm Editor's Properties dialog–Instructions tab. ▪ Depending on the settings in the Alarm Monitor Setup 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 required, the program will not allow an operator to remove alarms from the Alarm Monitor display without recording a response.
Operator's Incident Report		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.)
Print		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.
Help		Displays this on-line help file. A button in individual Alarm Monitor dialogs displays help on the specific topic.

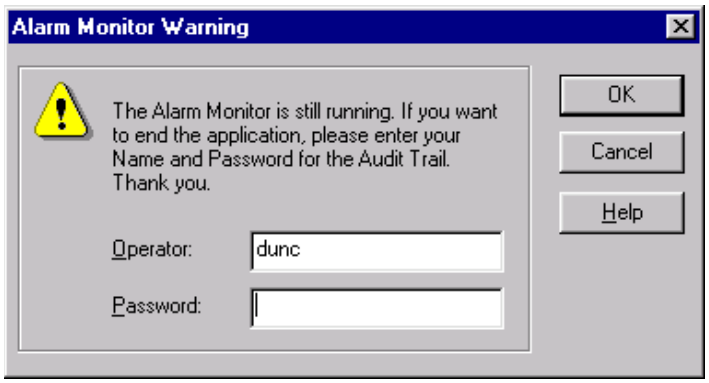
Logon and Logoff

The Alarm Monitor requires a separate logon.



Notice the ALARM MONITOR requires a logoff as well as a logon. Since the Alarm Monitor is designed to run continuously on a dedicated PC, a logoff should not be a common occurrence.

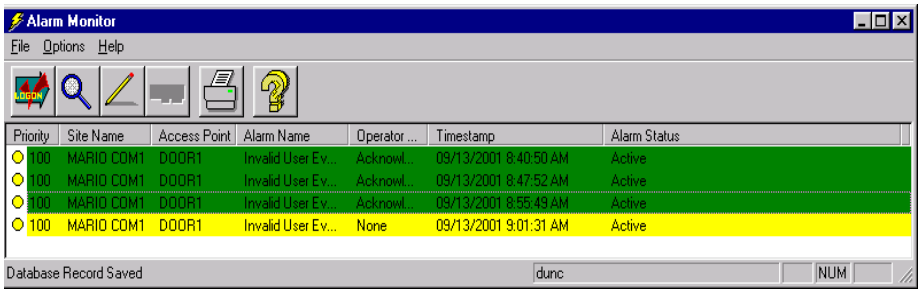
To end the alarm monitor function, an operator MUST identify himself or herself for the audit trail. If an operator decides to turn off the monitoring function, that operator is responsible for the decision.



Even if the Alarm Monitor is not running, Millenium Enterprise continues to log alarm activity as part regular history.

The screen below shows the **ALARM MONITOR** function in Millenium Enterprise. The Alarm Monitor oversees all alarm event activity in the Millenium Enterprise network. Alarm Monitor is designed for use in a security or guard station. For maximum effectiveness, therefore, the Alarm Monitor should be on a dedicated PC that is running at all times.

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



Important!

- Alarm Monitor requires Millenium Enterprise to be running before any active alarms can be displayed.
- If Millenium Enterprise is not running, active alarms stored in the Site Control's memory will display in Alarm Monitor as soon as you log on to Millenium Enterprise software.
- Alarm EVENTS must be checked (selected) in both the DCD and the SITE dialogs in Millenium Enterprise software.

Regardless of whether or not you use this Alarm Monitor, Millenium Enterprise 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 Enterprise 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.

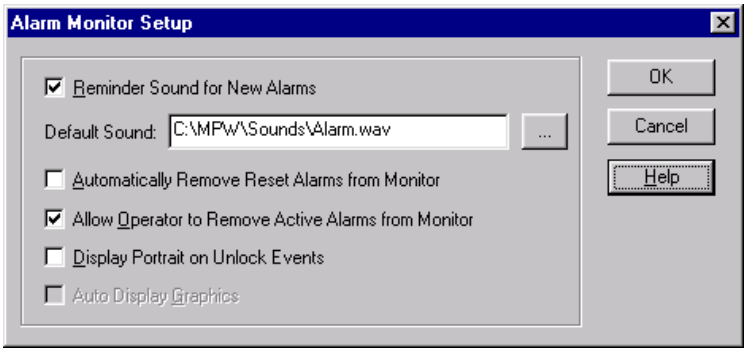
  If permitted in Setup, an operator can remove an alarm from the monitor by right-clicking and selecting the **Remove** option.

Alarms: Alarm States

Millenium Enterprise Door Control Devices (DCDs) come with seven alarm inputs. All inputs are supervised alarms. See page 65.
For the Door Ajar feature, see page 66.

Setup

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



If you want to lay out 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.

- 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 Enterprise

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 (100 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 sounds (if no Default Sound.)

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 Properties dialog, Instructions tab,) reset alarm will not disappear until operator logs a response (Inspect Alarm dialog.)

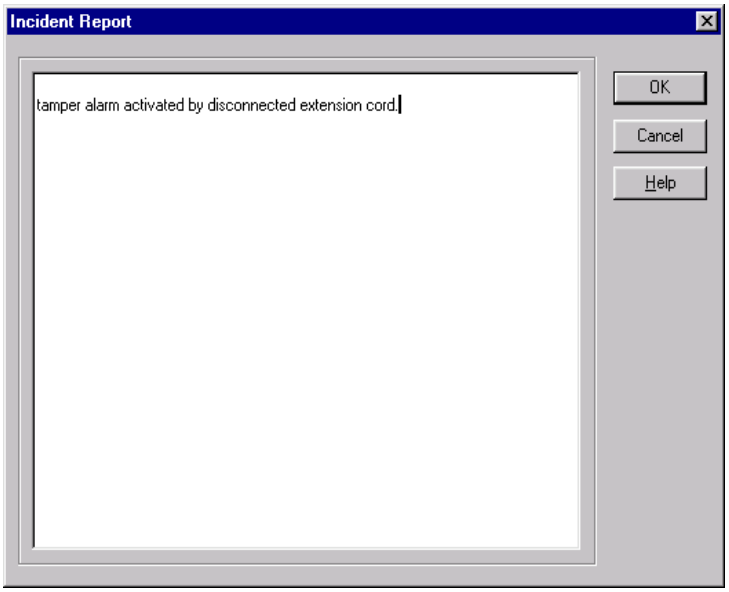
Allow Operator to Remove Active Alarms from Monitor

Operator can right-click on an alarm row in the Monitor and remove the alarm display.

Display Portrait on Unlock Events

Incident Report

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

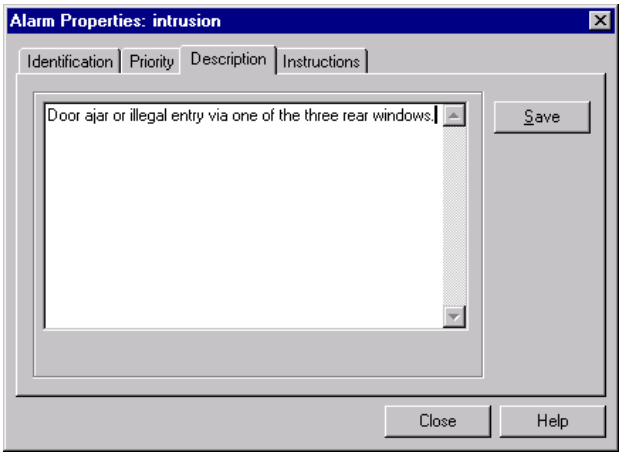


NOTE: Operator records response to **triggered alarms** in the Enter Action Taken box of the Inspect Alarm dialog. To get to Inspect Alarm dialog, either click the Alarm Monitor's inspection icon  or double-click on the specific alarm row in the Alarm Monitor display.

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.

Instructions Tab

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

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

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

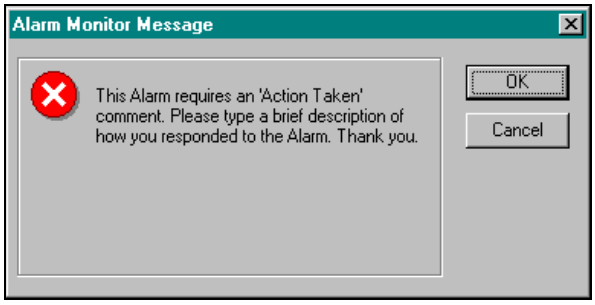
Enter Action Taken

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.

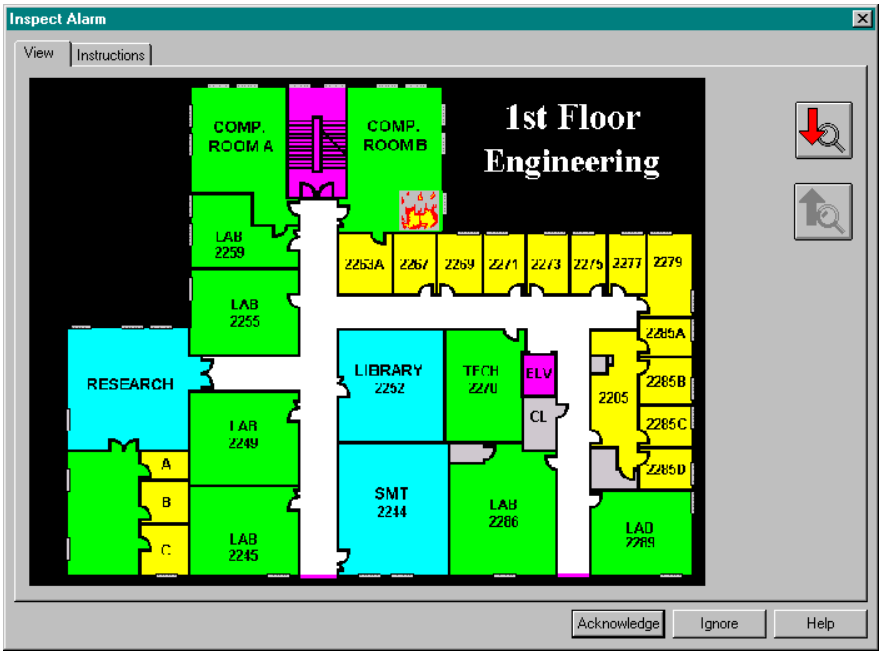
the particular alarm will not automatically be cleared from the main Alarm Monitor display when the RESET occurs. It will be cleared when the operator makes an entry.



Required entry comes from a checkbox entry on the Alarm Editor's Properties dialog—*Instructions tab*.

View Tab

Displays optional graphic image of where the triggered alarm exists. **NOTE:** You provide the graphic image and set up Millenium Enterprise' alarms on the image through *Alarm Editor*.



The graphic is designed to help a responding operator pin-point the location of a triggered alarm. Icons appear to be in motion to help 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:

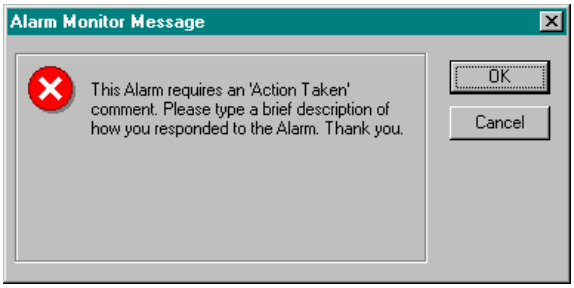
jumps to **next** Floor map file for the given alarm.

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

Ignore button

When the operator clicks this button, it means he/she 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.



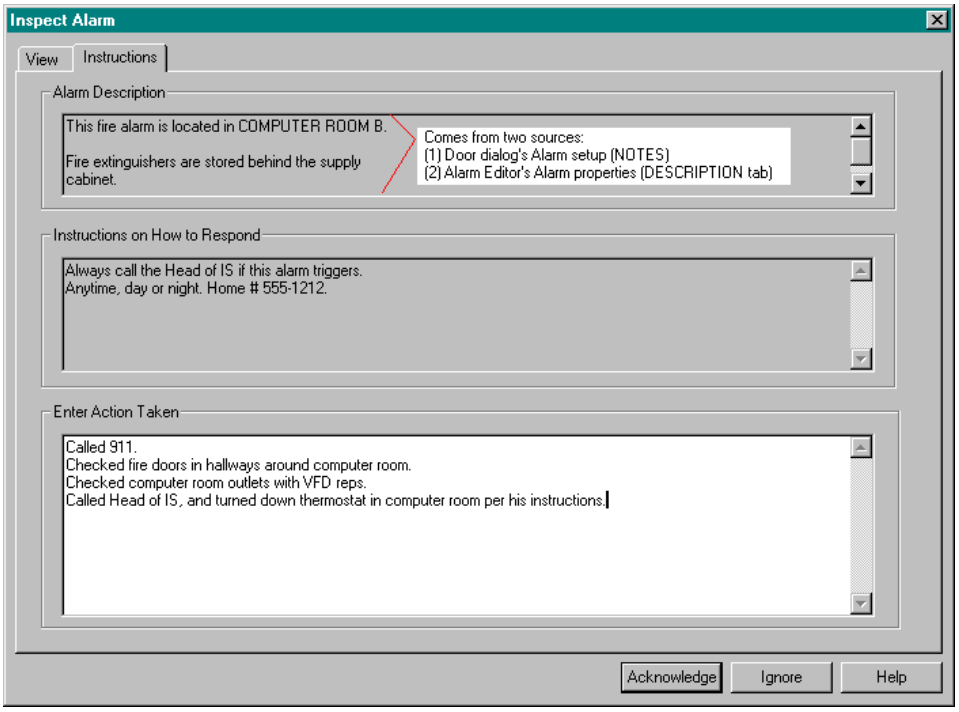
If required, operator records actions taken in response to the situation (Enter Action Taken box).

If operator tries to Ignore or Acknowledge an active alarm without completing the Enter Action Taken box, the Alarm Monitor Message appears.

Depending on your 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.

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.

Alarm Monitor Data

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

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. A 100 appears in the 

column.

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 Alarms... setup.

Operator Response Records operator response based on whether operator presses the Acknowledge or Ignore 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.

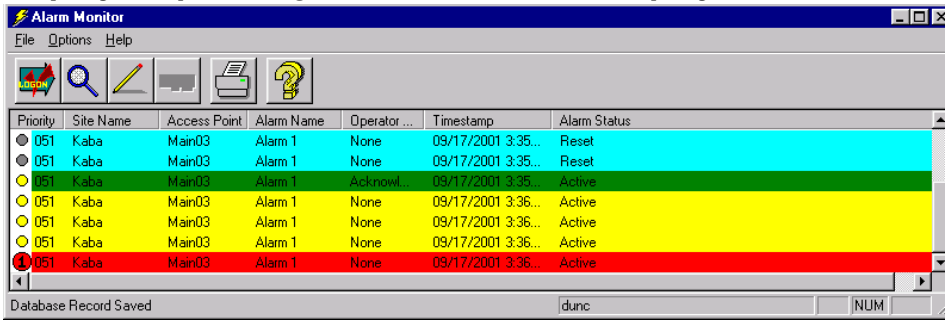
Timestamp Records the time the alarm activity occurred.

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 Enterprise History Report can produce an Alarm report according to several operator selection options.

Using the Alarm Monitor Display

Step-by-Step: Using the Alarm Monitor Display



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:

  RED - Active Alarm
  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.

  GRAY - RESET Alarm
  The triggered alarm' 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.)

  AQUA - RESET Alarm (requires an operator response)
  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.

  YELLOW - Active Alarm
  Although important, this alarm's Priority setting is NOT highest of all active alarms in the current display.

  GREEN - Incident Report
  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 (both prioritized and not prioritized) 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 notices the priority setting.

Important!

- 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 Enterprise software, you may see the following additional information on the triggered alarm:

- **Description:** Details describing the individual triggered alarm. Comes from the NOTES text field in the door's setup dialog (Millenium Enterprise ACCESS POINTS dialog.) Can also come from ALARM EDITOR Properties dialog—  *Description tabs*.
- **Instructions:** Specific directions on what the operator is to do in response to the individual alarm. Comes from the ALARM EDITOR Properties dialog—  *Instructions tab*.

If you press the print button  , details about the selected alarm row go to the local printer. Operator can then take a printout of information as he or she investigates the alarm.

Incident Report: If the operator notices activity **other than** anything displayed on the Alarm Monitor, and wishes to log a report on that activity or incident, do the following:

- 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.

Chapter 15: Tours

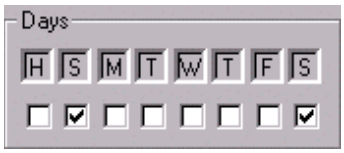
Millenium Tour is an add-on application that works with Sites and Doors established in Millenium Enterprise software. A tour is a sequence of doors at which assigned personnel must arrive within a specified time (delta.) The sequence is linear, meaning the personnel must follow a predetermined order.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

Important!

Millenium Enterprise must be running, and only one workstation should run Tour to prevent duplicate history. Millenium Enterprise continues to record access control history at the same time the single workstation records Tour activity. Only System Operators in the Millenium Enterprise software can access this Tour Module.

Day - Definition in Tour Module

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 Enterprise Timezone dialog (Holiday tab.)

Important:

Tour intervals are not designed to cross midnight from one day to the next.

Delta

Delta refers to the period of time or "leeway" available to a person to arrive at each door on his or her tour.

If the DELTA is 5 (minutes,) the person may arrive at the interval station (door) 5 minutes **before or 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 Enterprise' REPORTS dialog.

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 are displayed 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

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.

See Running a Global 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.

See Assigning an Individual Tour ;

Tour Toolbar Button

Press the tour button on the toolbar  to display a login dialog that launches the application. Millenium Enterprise Tour lets an operator set up a series of access points where a user (usually a security guard) must check in as part of touring your 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.

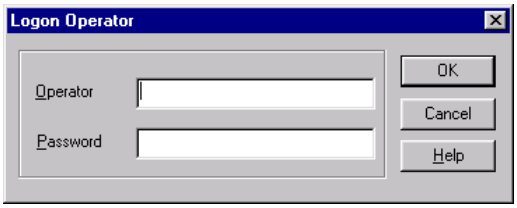
Reports for Millenium Enterprise's Tour module appear in the Report Selection dialog that displays when you click the REPORTS () button

Logging on to the Tour Module

First, log on to Millenium Enterprise.

Click the Tour icon on the main Millenium Enterprise toolbar.

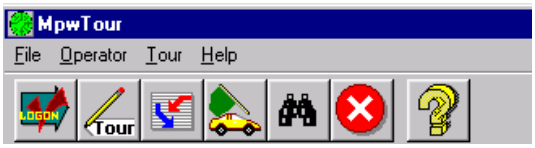
The following dialog appears where you Log on to the Tour application:



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

Click on a button in the toolbar shown above to jump to the relevant online help documentation.

Millenium Enterprise toolbar (**Click Tour icon to jump to main dialog**.)



Preliminary programming is required before you set up a tour.

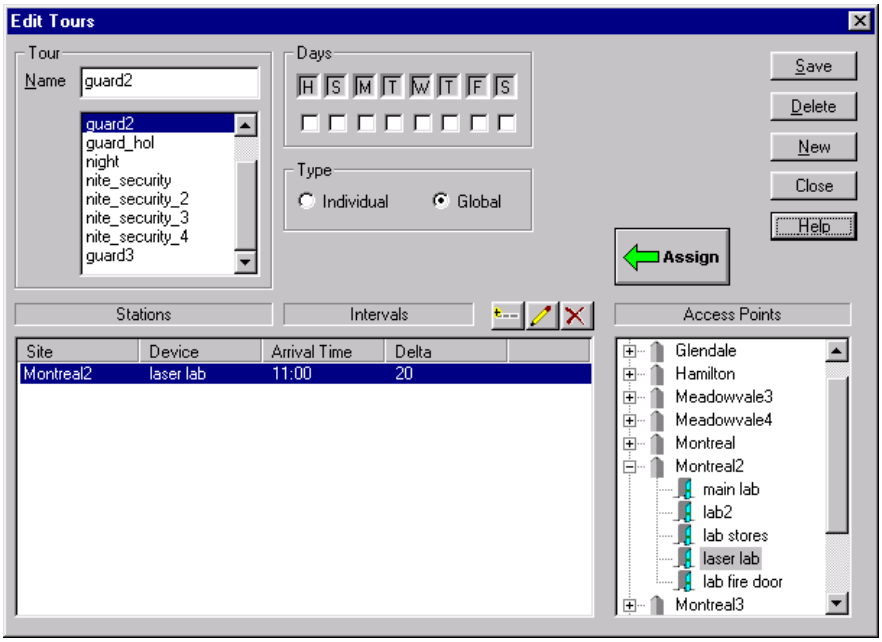
1. Have tour personnel created as USERS in Millenium Enterprise.
2. Have SITES (Site Control Unit circuit boards) installed and created in Millenium Enterprise software.
3. Have DOORS (DCD circuit boards) installed at checkpoint stations and created in Millenium Enterprise software.
4. Have Holidays and/or company-wide Vacations programmed under TIMEZONES in Millenium Enterprise.
5. Have reader device installed at each checkpoint station. Reader either can be installed as a tour checkpoint only, or can double as an access control device. That is, the reader can serve purely to log the tour personnel's arrival at a station, or the reader can also grant or deny access to a door or elevator floor based on the user's Access Group and Timezone.
6. 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 ( .)

Tour Setup

The following dialog is the main place where you establish and modify tours. You can create up to 100 named tours—each with as many as 96 **intervals**.

A Tour is a sequence of stations (access points) at which a user must insert an assigned key or card in a reader device to register arrival. Tour personnel should arrive at the checkpoint within the predetermined amount of time (**delta**.) If arrival is early or late (*outside* the delta time period,) or out of sequence, the Tour application reports accordingly.



1. After naming the tour, setting the days, and checking the type, the core step is to establish intervals.

An interval is an arrival time with a delta/leeway.

2. Then, assign access points (Site and Device "station") to each interval.
3. Finally, assign a user to a tour.

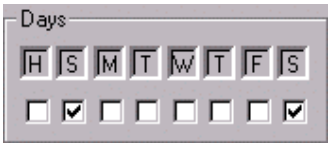
- Tour assignments are of two types: **Individual** and **Global**
- As soon as an operator starts the Tour application, all named tours with intervals load into memory and are considered **Active** or running.
- This means the software will evaluate the loaded tours —tours that have personnel assigned — every 15 seconds.
- Once the Arrival Times for all intervals have passed, the tour status switches to **Inactive** for the given day.

Step-by-step: Setting Up a Tour

Check that you have finished preliminary Millenium programming before you set up a tour.

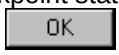
1. Log on to Millenium Enterprise software.
2. Select the Tour icon button.
3. Log on to the Tour application
4. Click the Tour setup/edit button.
5. Name the tour.

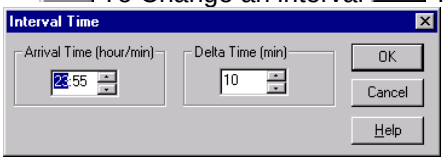
6. Select the **DAYS** of the week during which the tour is to run.



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 Enterprise' 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 Enterprise.)***

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

- Set the **Arrival Time** (in hours and minutes) at which the tour personnel should arrive at the station
- Establish the Delta Time in minutes (The Delta is the leeway the user has to arrive at the checkpoint station after the Arrival Time.)
- 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



Select the SITE and Access Point for this particular station interval. Together the site and access point will become a "station" in this tour.

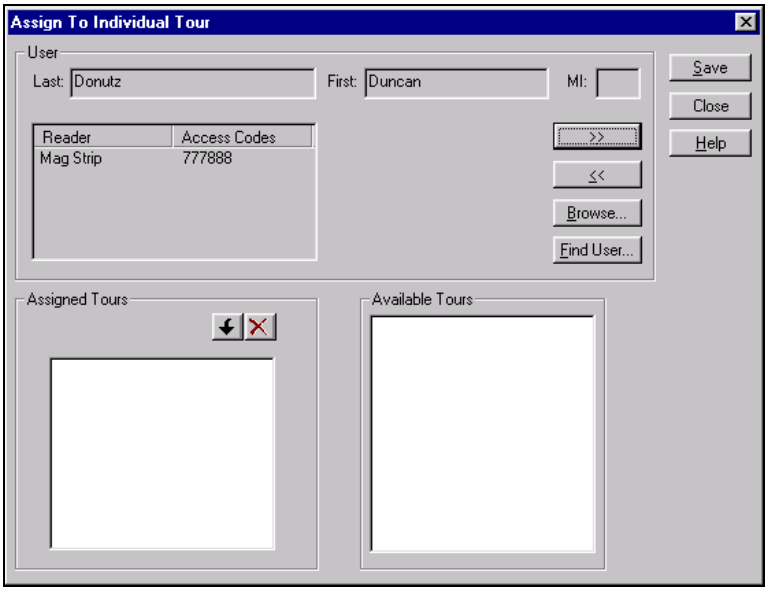
 First, click the "–" beside the SITE name. A "tree" of access points for the given site expands below.

 Then, highlight the access point to be assigned to the given interval.
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.

Tour Assignments - Individual

Step-by-Step Assigning Tours to Individuals

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



2. Select the tour personnel from all USERS set up in Millenium (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.

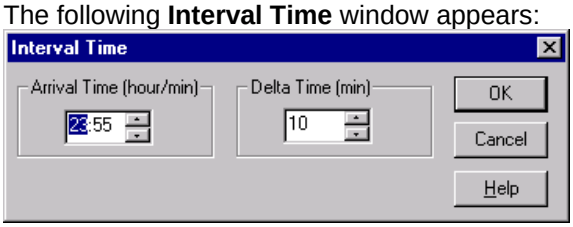
Notice, also, that each user's access key or card appears for your information. The first key or card assigned will display in Tour history.

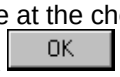
Adding an Interval to a Tour

To add an interval, click the add/edit tour button (

) and highlight a tour.

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



2. 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

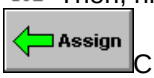
As part of creating a tour interval, first you set up the interval **arrival time** and **delta** (leeway.)

Then you assign the Site and Access Point station to the interval, as follows:

Select the SITE and Access Point for this particular station interval. Together the site and access point will become a "station" in this tour.

 First, click the "–" beside the SITE name. A "tree" of access points for the given site expand below.

 Then, highlight the access point to be assigned to the given interval.

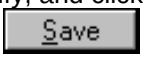


Click the Assign button (or double-click the Access Point in the previous step.)

Notice the interval row now shows both the station and interval times.

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.

Step-by-Step: Assigning a User to a Tour

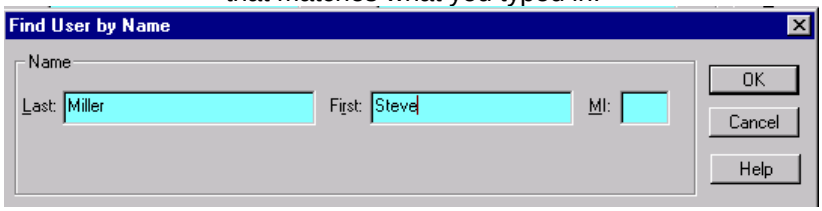
Both Individual and Global tours require that a Tour operator assign a user to a tour.

1. 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.
2. Click the Assign button.
3. Select the person who will be assigned to do the tour from all users in the Millenium Enterprise database.

4. Use the forward and backward buttons to scroll through individual users, one-at-a-time.

5. Use the browse button to select from a pop-up window list of all users in Millenium Enterprise.

6. Use the find to search for a particular user. Type the first few letters of the user's name in the pop-up dialog. The software will search for the first user that matches what you typed in.



7. In the **Available Tours** listbox, double-click the available individual tour you want to assign to the selected person.
8. (Or highlight the available tour and click the  button to place the tour in the **Assigned Tours** listbox.)
9. Click the SAVE.
   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.

Global Tour

1. Assign user to a **global** tour as part of the "run" the global tour process.
2. Click the "Run a Global Tour" button  .
3. Follow the same procedure described above, to select a person from all users in Millenium Enterprise.
4. Double-click to select one of the **Available Global Tours**.
5. Click the "run" button  .
   This global tour now becomes Active.

Tours that Cross Midnight

Important!

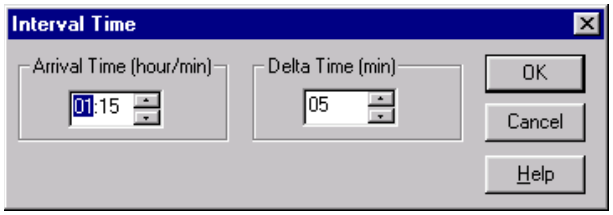
A tour cannot cross midnight. Tour days are defined as anytime between 00:00 and 23:59, and tour intervals are not designed to go past MIDNIGHT.

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.)

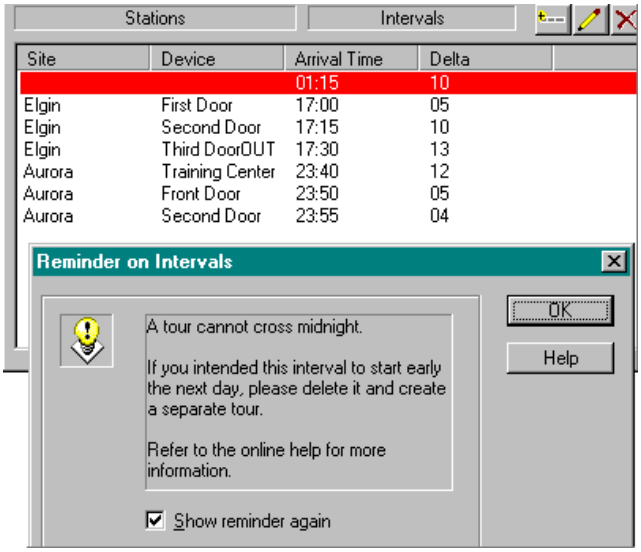
If you are creating a pattern of intervals intended to span midnight into the following day, the software will treat your time entry as follows:

- 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.



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.

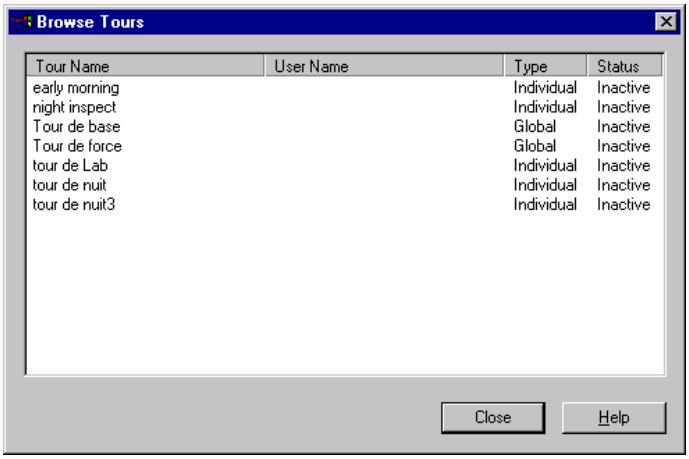
Summary– to span midnight in the example:

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

To turn off reminder for next five instances, click to remove check.

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 (.)

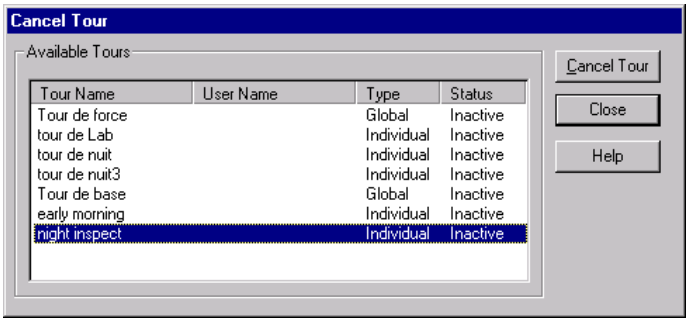
Tour STATUS shows the following:

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

Active	• 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. 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.

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.



Running a Global Tour

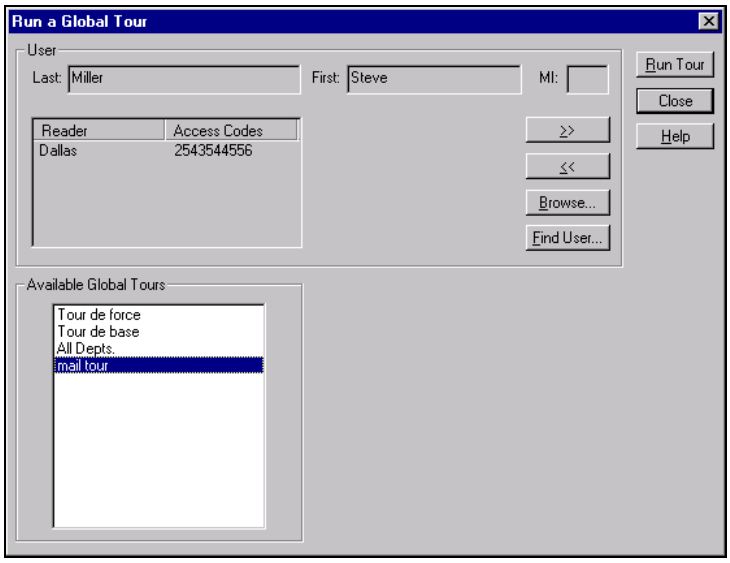
Step-by-step: Running a Global Tour

To run a global tour:

- Select a person who will be performing the tour from all users in Millenium Enterprise.
- Then highlight a global tour, and press the 

button to assign the highlighted tour to the selected person.

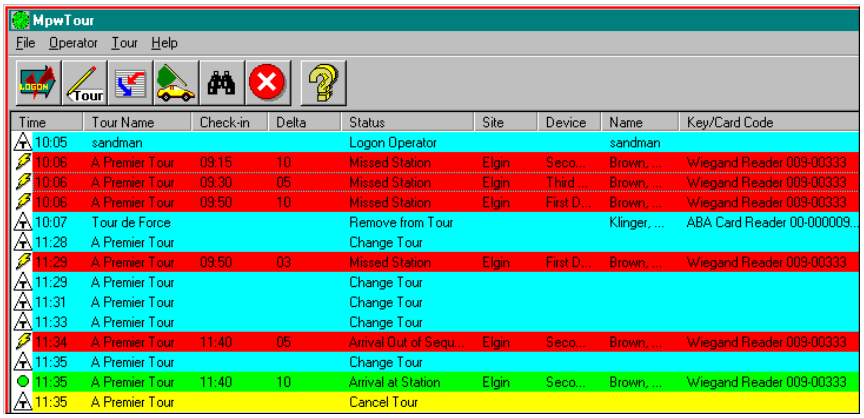
Notice each user's assigned reader access appears, as assigned in the USERS dialog of Millenium Enterprise (ACCESS tab.)



See also Assigning a user to an INDIVIDUAL tour .

Tour History

The Tour module displays its own history.



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 Enterprise 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 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.

Chapter 16: Filters

A filter allows you to view only certain portions of Millenium Access Management activity and history. You can use your specific filters in setting up history view screens or 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 Enterprise window.
- automatically print to the designated printer.

All & None

Two filters come as part of Millenium Enterprise, and cannot be changed by the operator.

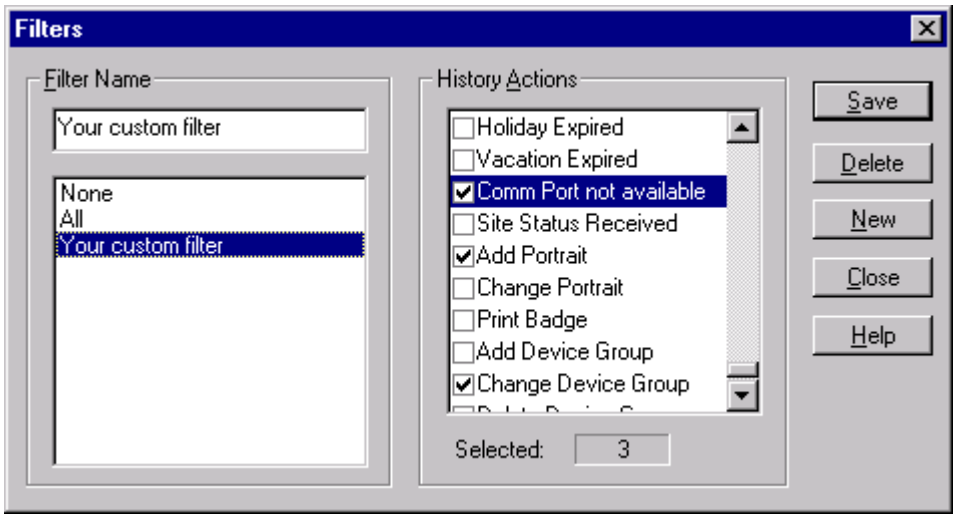
All Every possible action that Millenium Enterprise can record as history.

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 Enterprise system, 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 Suppresses display of all history actions (more than 140 possible selections.)

Filters Dialog

The illustration below shows the FILTERS dialog in Millenium Enterprise.



Operators can design custom filters that include a specific list of history actions.

1. Click the New 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 Save 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 Enterprise 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 Management 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 Enterprise window.
- automatically print to the designated printer.

Two system filters—ALL and NONE—come with Millenium Enterprise. Operators can establish custom, user-defined filters in the FILTERS dialog based on selected history actions.

Resident Filters

At some point after your Millenium Enterprise system has been operating for a while, you may choose to limit the amount of Access Management 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 Enterprise menu bar.

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 Enterprise window (Screen output device.)**
2. **Control what history actions go to the Alarm Monitor output device.**

All history actions automatically save as part of Millenium Enterprise 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.)**

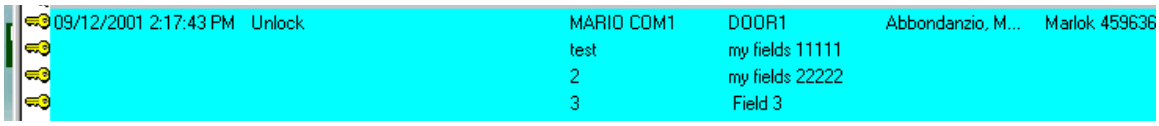
DISPLAY CUSTOM USER FIELD: If you selected custom user field data to display with unlock actions in the history portion of the window, you may also set up a Resident Filter to automatically print user data when the unlock occurs.

DISPLAY USER PHOTO:

If you have the optional Millenium Enterprise Badge module, and have used the badging system to capture user images, the Screen Filter lets you select how user images display in Millenium Enterprise 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 menu bar (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



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 Enterprise devices.

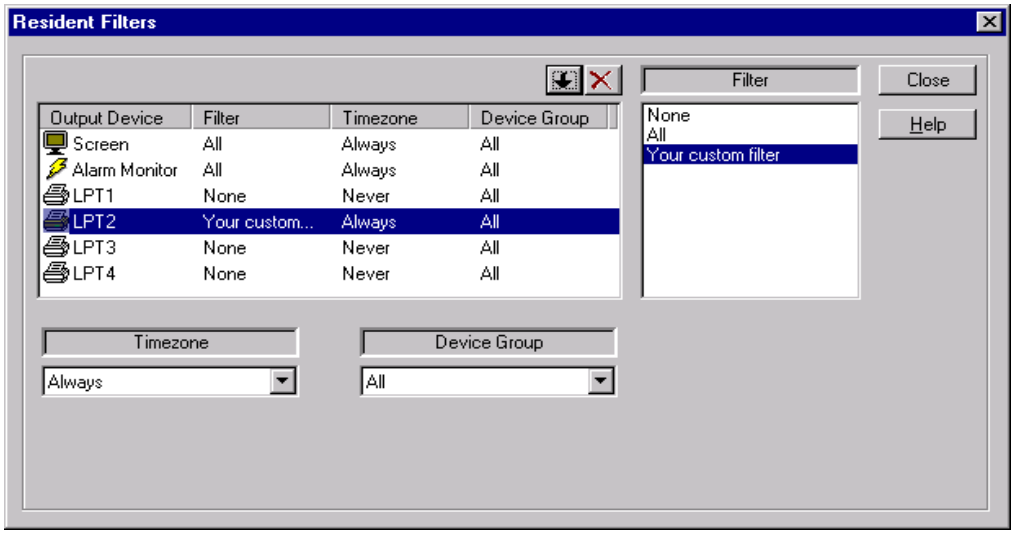
Device Groups give you an option to filter what history actions go out to the SCREEN, ALARM MONITOR, or Printers (LPT) based on selected groups of DEVICES (doors, elevator floors, site controllers, or relay controllers.)

How to Assign a Custom Resident Filter

Step-by-Step: Assigning a Custom Resident Filter

1. Create a custom filter through the FILTERS dialog, if desired. System filters are **All** or **None**.
2. Click on the Resident Filter option from the **History** menu.

3. 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 Enterprise application workspace.)
   - **Alarm Monitor** (separate display of triggered alarm activity.)
   - Any **Printers** available to the PC (printers installed through Windows.)
4. OPTIONS: If desired, highlight the **Timezone** and/or the **Device Group** you want to assign to one of the Resident Filter output devices.
5. Highlight the Output Device row to which you want to assign the filter and currently displayed filter options.
6. 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.



To “de-select” the Filter, Timezone and Device Group, highlight the Output Device row and click the ‘X” button. All selections revert back to the defaults (shown above.)

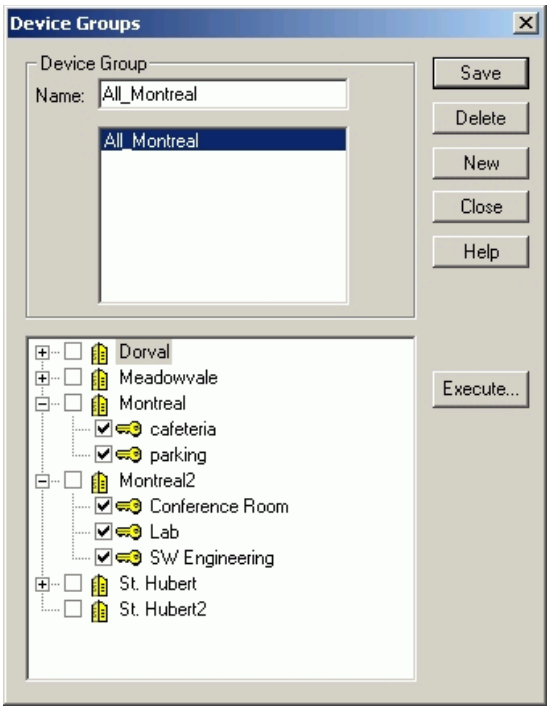
Device Groups

A 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 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.

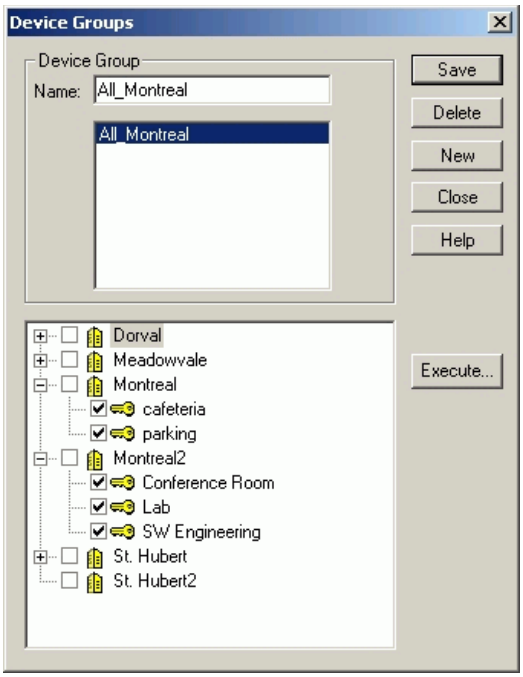
Device Group option appears under the History menu bar.

When you select the option, the following dialog displays:



Step-by-Step: Creating 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:

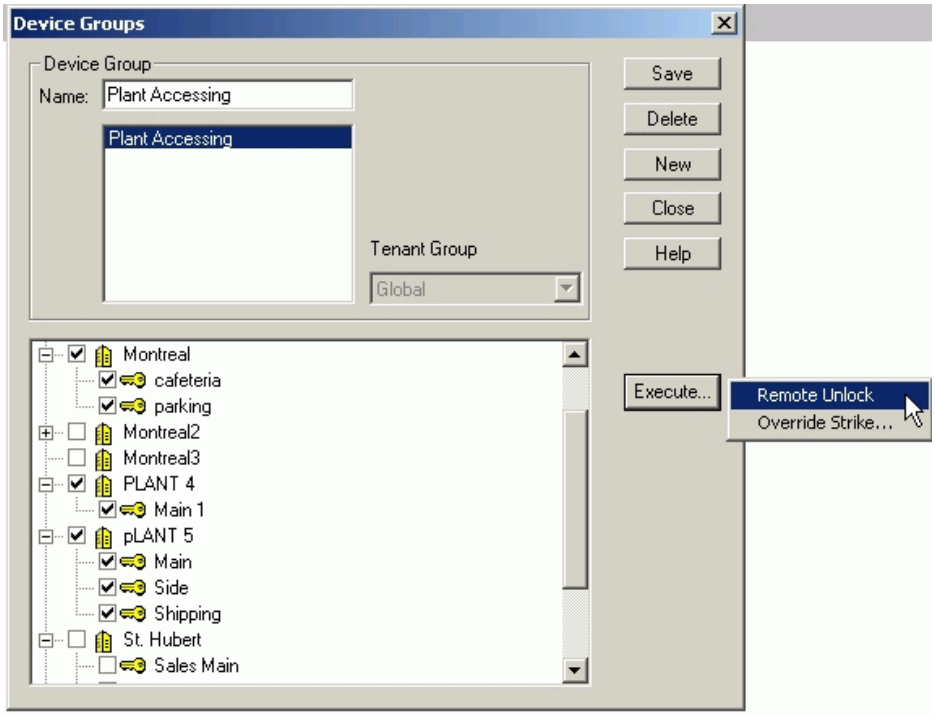
Site Control Unit **(SCU)**

Door Control Device **(DCD)**

Elevator Floor

Device Groups – Remote Unlock Feature

You can create a Device Group and then remotely unlock all its access features. This could be useful in case of fire in a remote building, for example, so that the firemen could have access before you might be able to get there. The illustration below shows a device group that contains all the devices for accessing a remote plant – doors, elevators, etc.



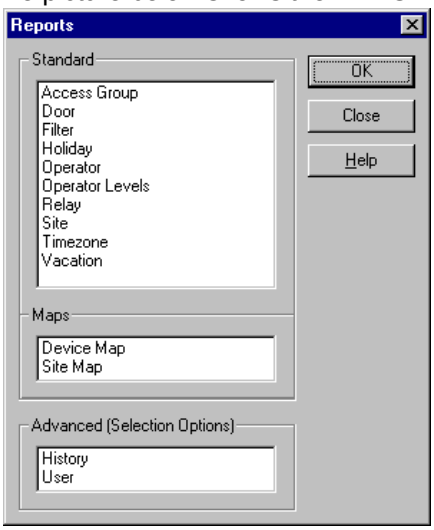
1. Select the device group.
2. Click on Execute, then Remote Unlock.
3. The doors in that Device Group have now been unlocked.

You can execute an Override Strike Command to a device Group in the same way.

Chapter 17: Reports

Reports

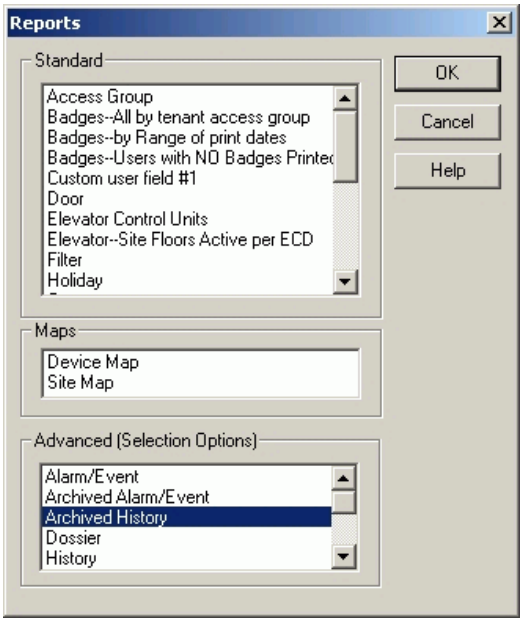
The picture below shows the **REPORTS** menu dialog in Millenium Enterprise System.



- 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.
- Click the OK button, or double-click the report name to display a preview.
- 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 System 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 Enterprise activity. This history audit trail includes both access point activity and computer operator actions. When Millenium Enterprise 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 Enterprise program. History automatically saves on the PC. Archived History lets you print a report of those history files you have archived.

(****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 an SQL script that your database manager should have.

Alarm Monitor: Incident Reports

Show all activity through the ALARM MONITOR on alarm events triggered from Millenium Enterprise 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 Enterprise Systems' data on that user. Requires an image captured through the Millenium Enterprise 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 TOUR module.

Custom Reports: If you have Crystal Reports™ software, you have the option to develop custom reports of Millenium Enterprise 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 Toolbar Button

Preview and print standard reports of Access Management data and Millenium Enterprise software operator actions. Reports include history of Access Management activity at devices installed throughout the network

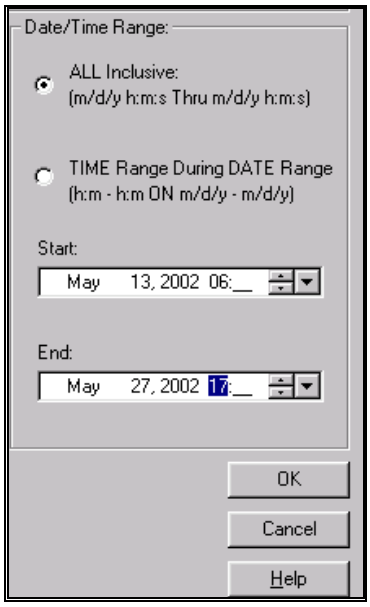
- Standard reports list software database information, and come ready-to-use under this toolbar button. Examples: Timezones, Holidays, Doors, Sites, (History action) Filters, Tours, Quick User reports.
- Map reports provide a hard copy of the Site Map and Device Map available under the **Map** menu bar.
- Advanced reports involve the operator making selection options to prepare for report generation.

History, **User**, and **Alarm--Incident** reports require the operator make selections to determine exactly what the report should include. Access Management 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 Enterprise 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 Enterprise Tours module.

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

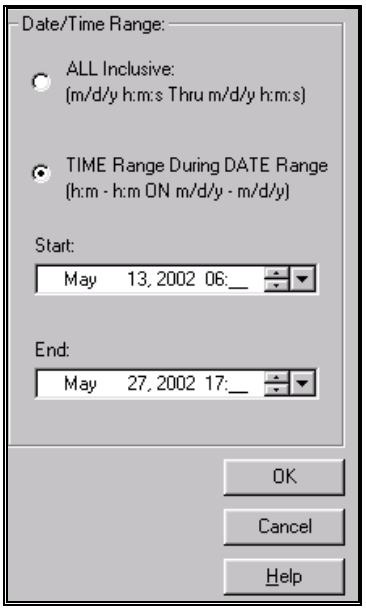
You can also reach the **REPORTS** dialog through the **View** menu bar.

Report: Date/Time Range



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:
6:00A.M. on 13/05/2002 through
17:00 P.M. on 27/05/2002



TIME range during DATE range
Start **Time** through End **Time**
on
Start **Date** through End **Date**.
Example:
6:00 A.M. through 17:00 on
13/05/2002 through 27/05/2002.

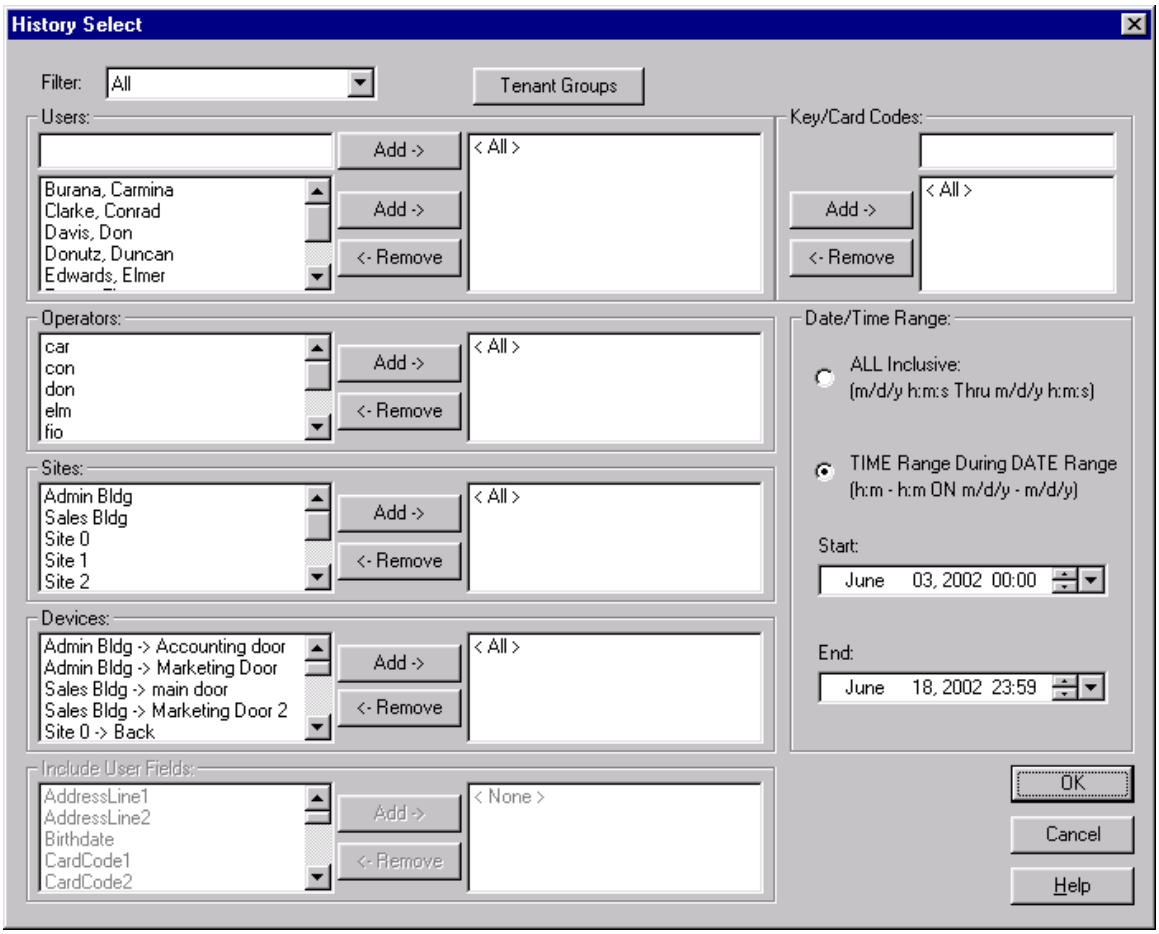
You type in the date and time information the same way for both range options. The report will select data based on your choice, and the selected time-period will print at the top of the report for your reference. Depending on which date/range option you select, the report will show the report's time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

6:00A.M. on 13/05/2002 through 17:00 P.M. on 27/05/2002

6:00 A.M. through 17:00 on 13/05/2002 through 27/05/2002.

Report: History

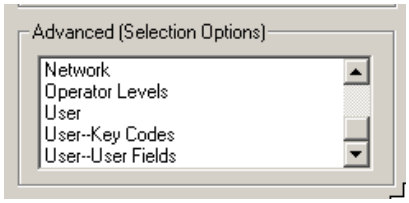
The History report is one of Millenium Advanced reports, meaning operator input is required. An operator must select criteria to be included in the report. In most cases, you'll want to report on some portion of access control history. For example: *All history for a given date range, or all history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



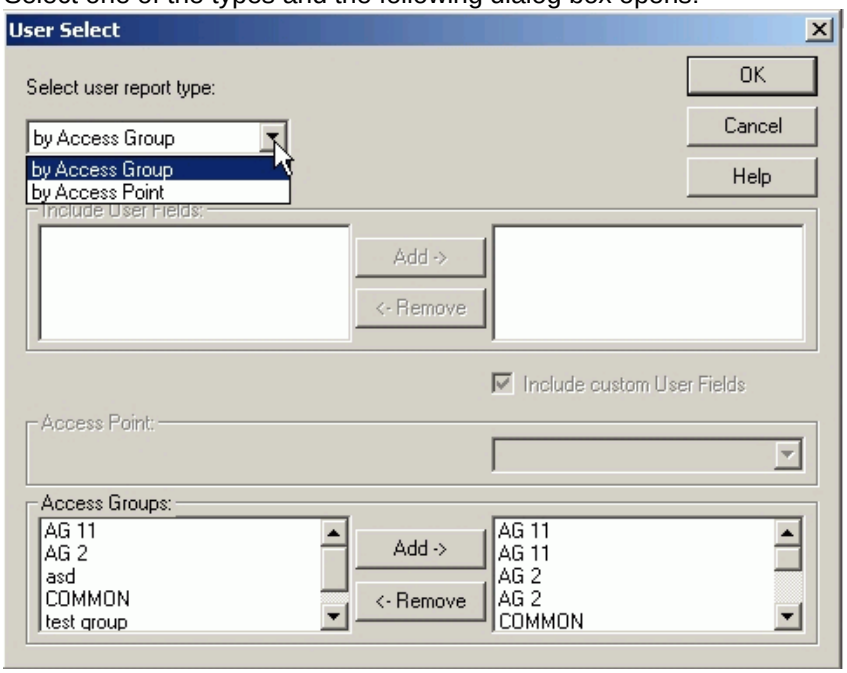
Report: Users

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: User, User Key Codes and User Fields.



Select one of the types and the following dialog box opens:

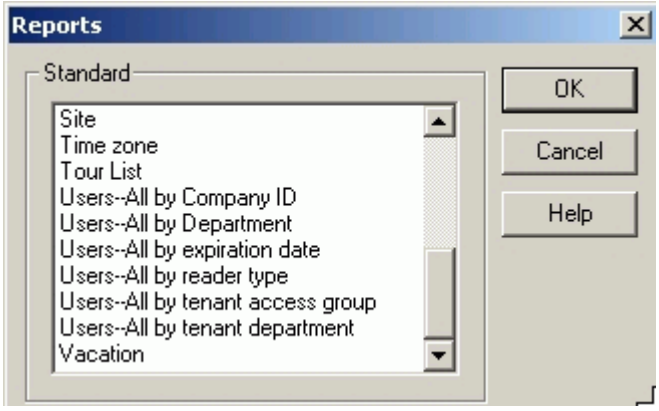


Depending on which user report type you select, the Access Points or Access Groups part of the dialog becomes enabled or disabled

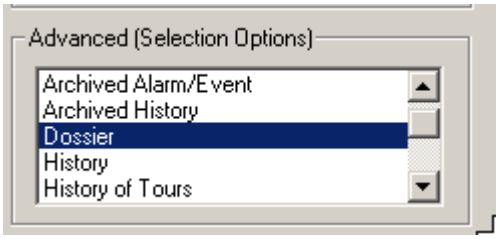
Click OK to print **all** custom user data fields for each user in the report.
Depending on the size and the number of custom user fields in your user database, this report can require a long time to print. Specific user reports appear in the **Standard** reports listbox for your convenience.

Additional User Reports

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



Single user DOSSIER report appears under the Advanced listbox



Additional User Report Types

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

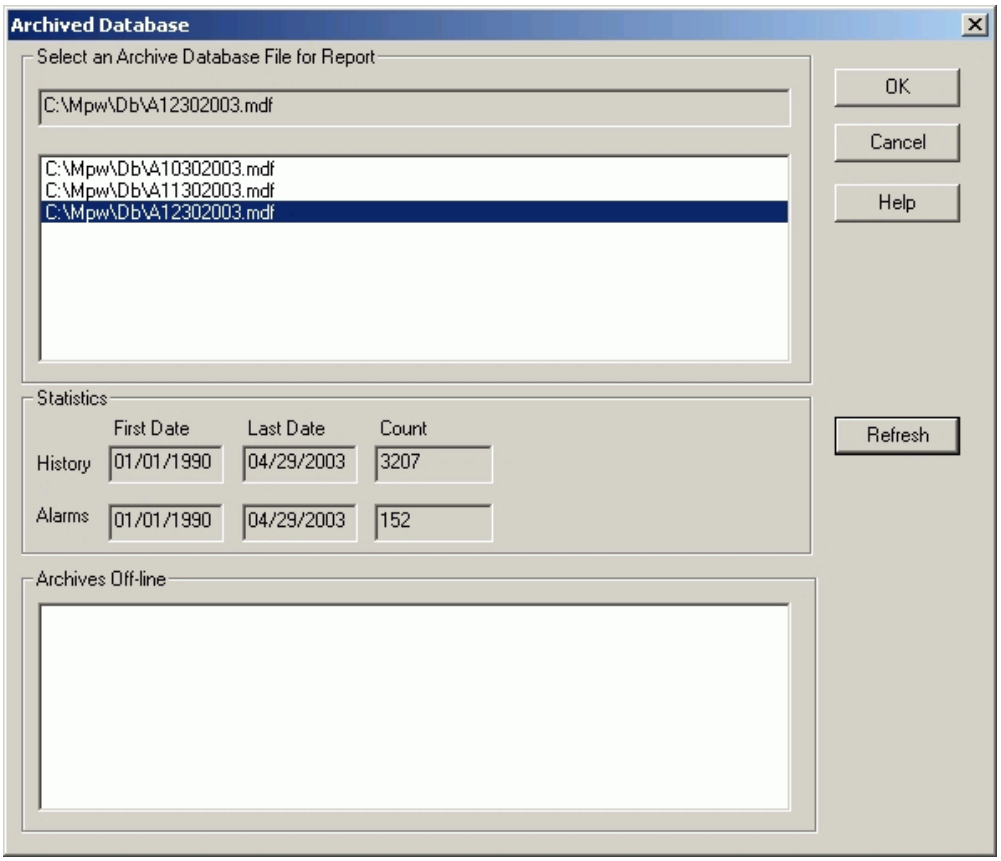
Millenium Enterprise can be set up to automatically archive history and alarm data. Your SQL database administrator can configure this option. The archive function is run on the SQL Server database itself. For more information, see the readme.htm file on the installation CD.
Establish a regular policy of archiving your Millenium Enterprise Access Management Systems history files.

Important!

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

Step-by-Step: Obtaining an Archived History Report

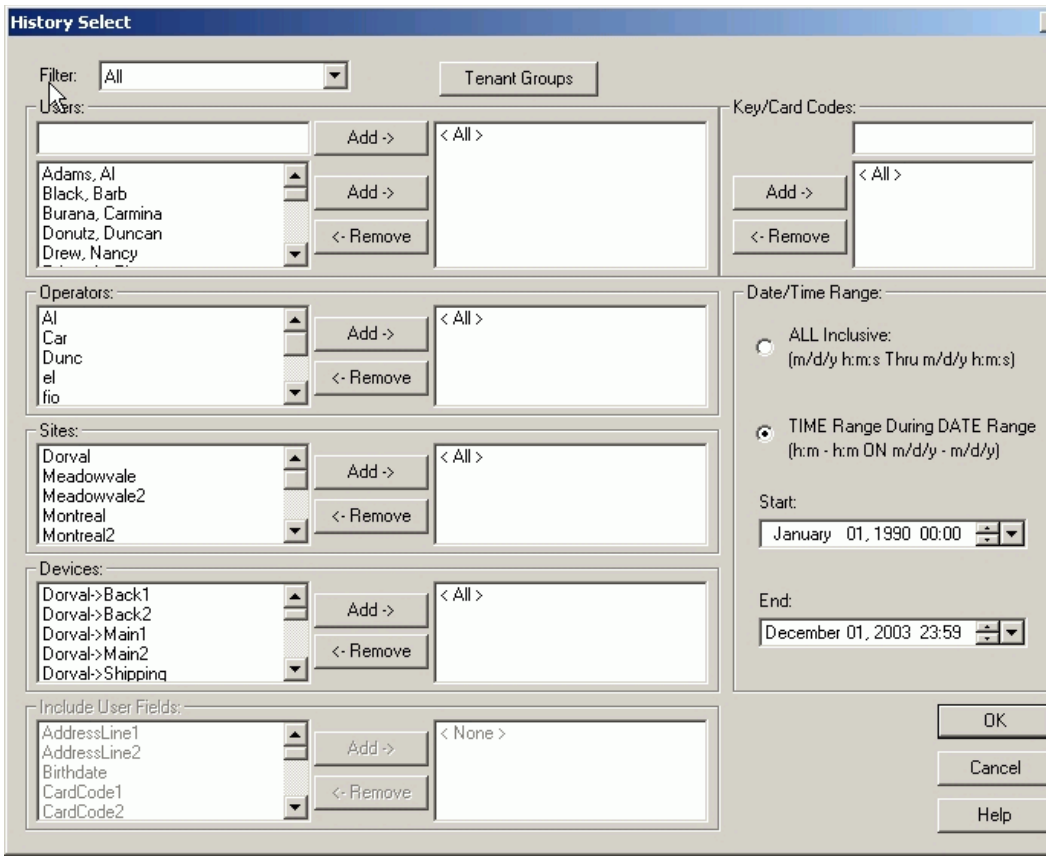
Both archive reports begin by having you select the archive.



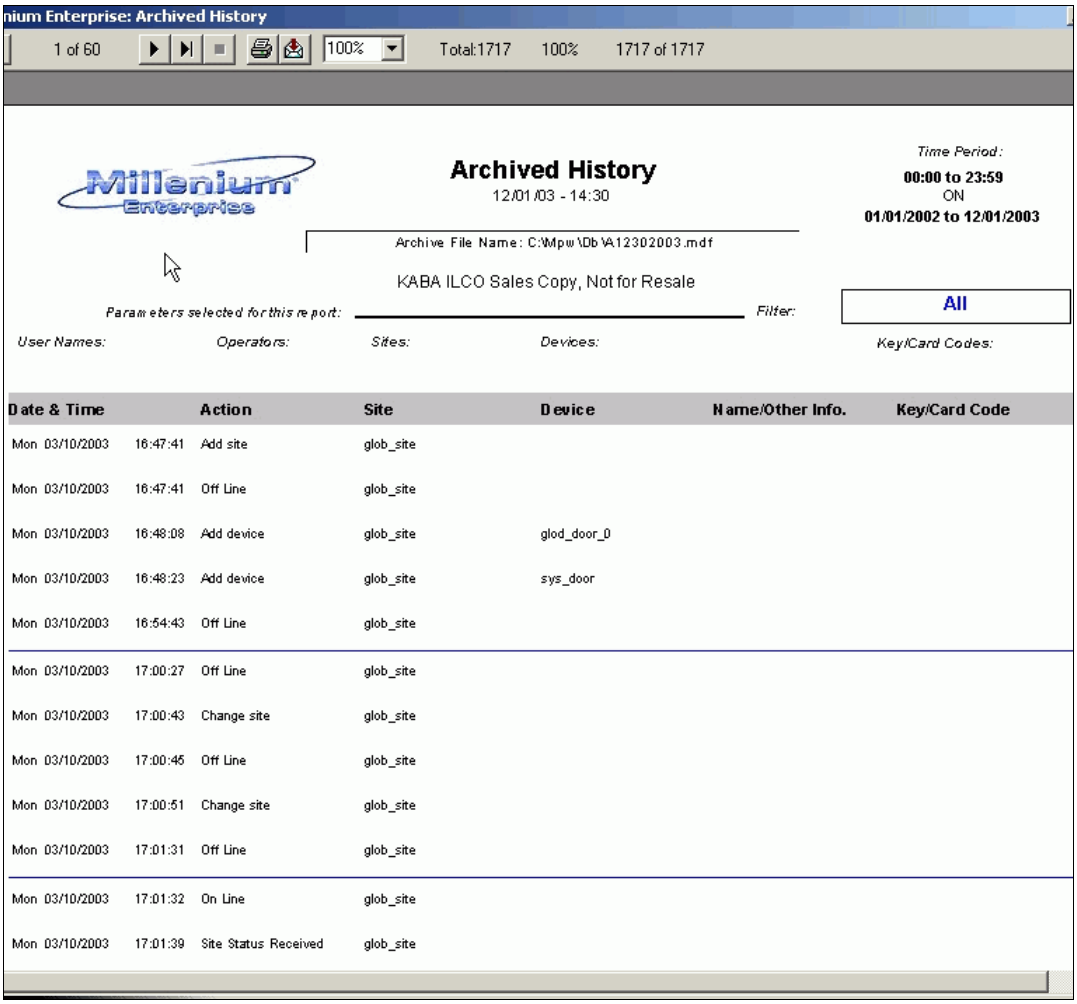
1. To verify that an archive contains ALARM data, click the button. Statistics will show you the number of history and alarm records that exist within the selected archive file.

NOTE: Large archives require more time to go through the refresh process.

2. 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.



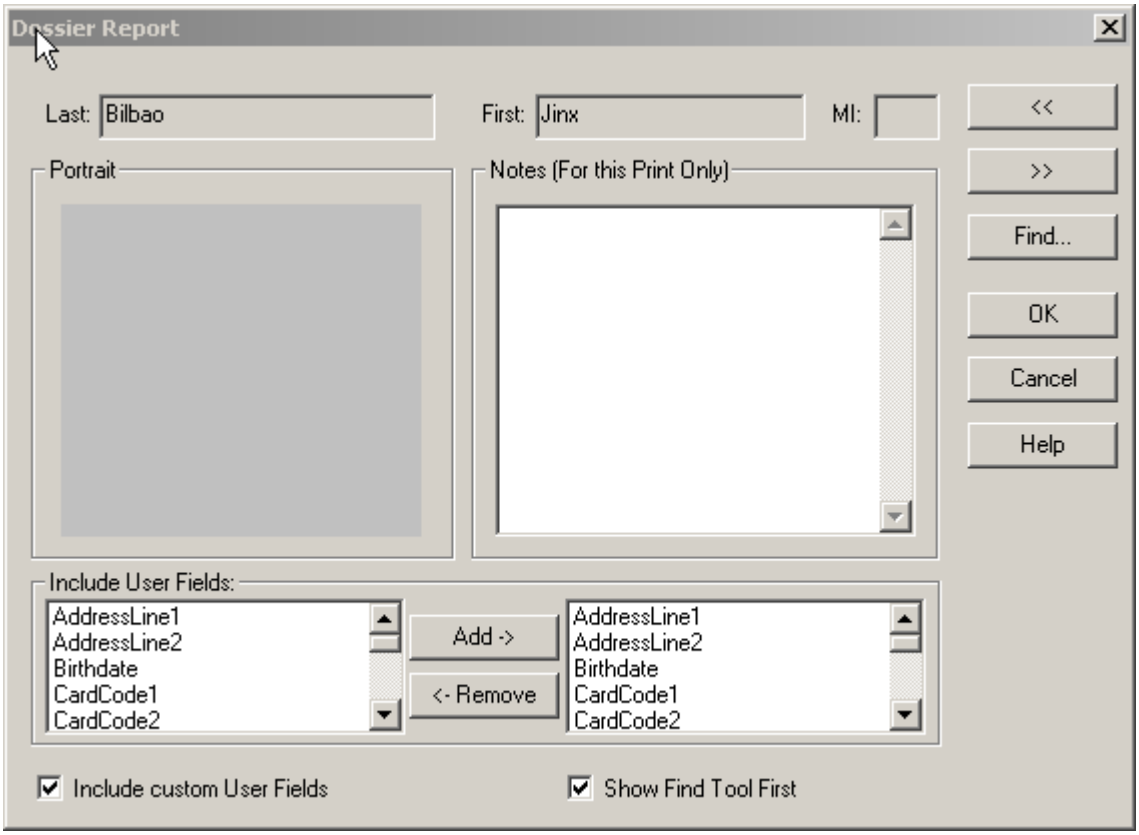
3. Press OK to begin displaying the Report Preview window.



4. Press 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.

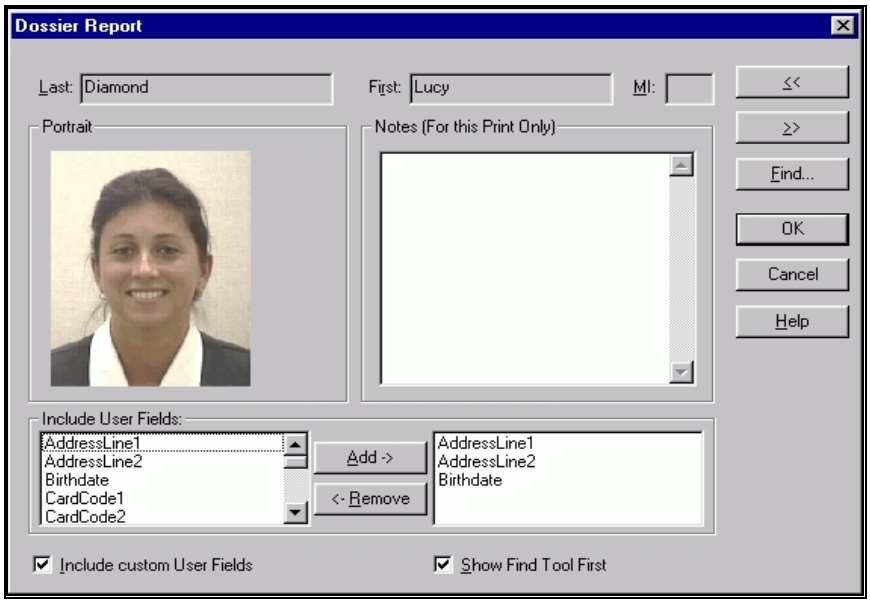
Dossier Report

If you use the optional Millenium Enterprise Badge option and have captured user images, this report prints the image along with selected user data. In the example below, the image has not been captured, so there is no portrait.



Step-by-Step: Obtaining a Dossier Report

1. Click the  icon.
2. From the main REPORTS dialog, select Dossier in the **Advanced** listbox.



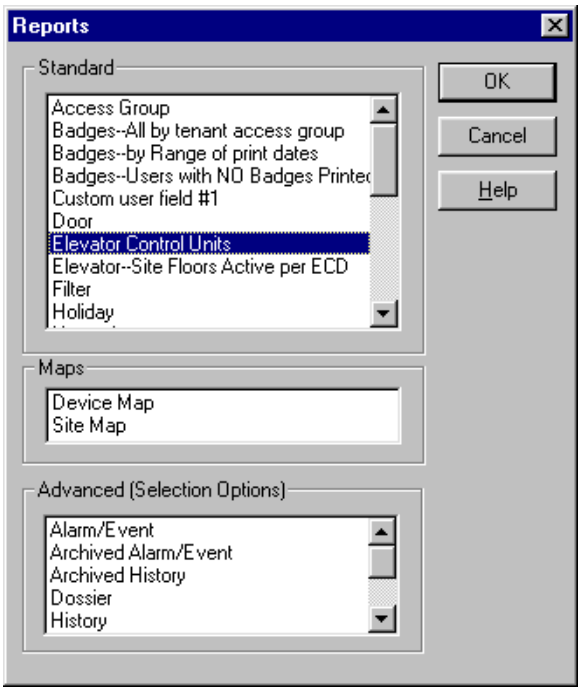
3. Use the >> and << buttons to scroll to the user for whom you want to print a dossier report. To locate a particular user, click the Find User... button. To have the FIND window automatically pop up first when you open the dossier dialog, click the option.
4. Select all or part of the user fields you want included in the report.
5. Click to include or remove the checkmark from the ☑ Include custom User Fields option. A check means **all custom user-defined fields** will be included the report.
6. If you want free-form notes to appear on the dossier report for this printing only, type in the NOTES text box.
7. Click the OK button to display the report. To print the report, click the printer icon along the top of the window.

Elevator Reports

If you use the elevator access control option, the following reports provide information on programmed elevators:

- Elevator Control Units (ECUs)
- Elevator Floor Access Points (ECU Floor Relays)
- Elevator -- Site Floor and Active Readers (ECD Floors and their active readers)

Some of the same information appears on each of the above reports. The main difference is the level of information presented by each report.



Elevator Control Units report lists ECUs and which of the 16 possible floor relays are programmed at each ECU. Report also includes:

- Programmed **alarms** and selected **events**.
- Type of reader device used by all ECUs under a given Site Control.
- Whether the ECU is the master (first ECU at a site) or a slave (one of up to three other ECUs

under an SCU.)

Elevator Floor Access Points report repeats much of the same ECU information, but goes into more detail on how each of the **16 possible floor relays** is programmed for access control.

Elevator Site Floors Active per ECD report shows:

- your selections in the **Site Floors** listbox for each Elevator car Control Device (ECD) **(Site Floors are those floor relays selected to be active** for each ECD under a given Site Control.)

the ECU for each Site Floor.

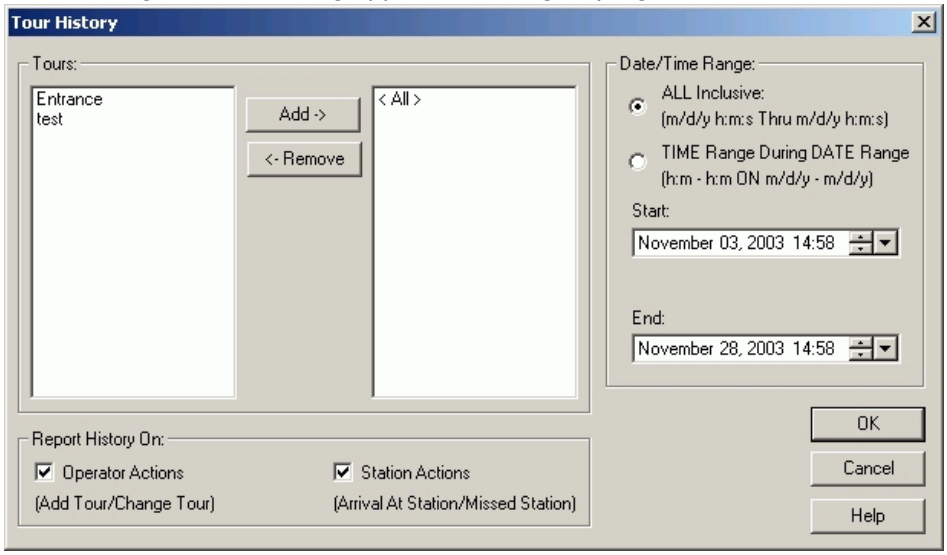
Tour History Report

Step-by-Step: Obtaining a Tour History Report

As tours run in the Millenium Enterprise software, history accumulates. To run a report of the tour activity or of the programming changes done by Millenium Enterprise operators on the tour module, follow these steps:

1. Click the  icon.
2. From the main REPORTS dialog, select History of Tours in the **Advanced** listbox.

The following selection dialog appears showing all programmed tours in the left listbox:



3. Select individual tours or leave the <All> setting to include all programmed tours in the report.

NOTES:

Deleted tours are only included when you select the <All> option.

Operator actions only include add, change, delete, and cancel if you choose selected tours. <ALL> tours are required to get such history as *Operator log on* and *Assign to tour*.

4. Click the checkboxes to report on operator activity in programming tours or tour station activity, or both. (Operator actions only include add, change, delete, and cancel a tour if

you select just)

5. Date/Time Range: Select the starting and ending dates for which you want tour history.
6. Press the OK button. The History of Tours preview displays. You can choose to view or print the report from the preview.

Tour Reports

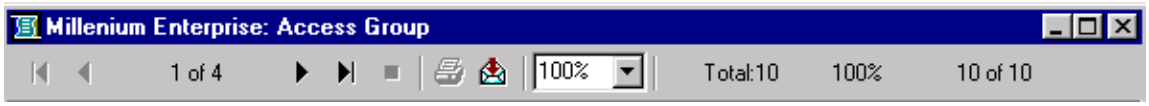
If you use the Millenium Enterprise Tour option (,) the following reports capture programmed tour data as well as recorded tour history:

- Millenium Enterprise TOUR List
- Millenium Enterprise TOUR History

Select the Tour List report from the Standard listbox in the REPORTS dialog. Below is a sample of a **Millenium Enterprise TOUR List** report:

Preview Window TOOLBAR

A toolbar across the top of the report preview window gives you information and options:



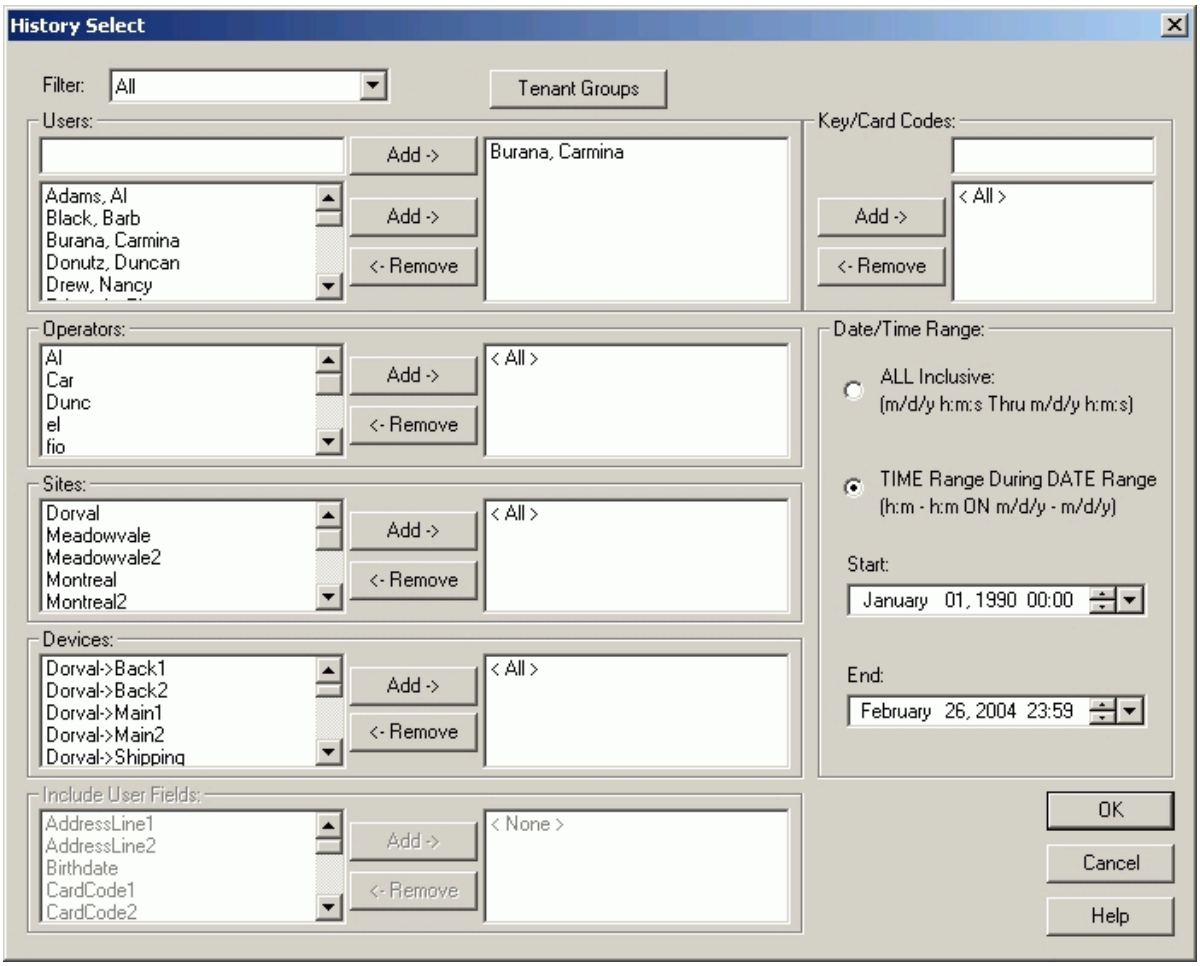
- Click the listbox selection arrow to choose among a variety of possible preview sizes.
- Send report to the default printer. Click the printer icon and select the printer, page ranges, and number of report copies you wish to print.
- Send the report to a file. Click the envelope icon and name the file. **NOTE:** Formatting is lost in many of the file type options.
- "In process" button shows a **black** square in the center when the preview window is in the process of displaying a report page. If you click this button, the report displays up to the point through which it has processed.
- "1 of 1+" shows the page currently being displayed out of multiple pages. Use arrow buttons to move back and forth between additional pages:

To check how many pages the report includes:
1) Scroll to bottom of the first page, OR
2) Click the Last page button.

1 of 2 Once you have displayed the last page of the report, the "1 of 1+" changes to show the "**current page** of **total pages**" in the report.

"Total:10" shows the total number of **items** included in the report, based on your selection criteria. The example toolbar tells you the report includes all 10 of 10 (100%) doors programmed in the software If your selection criteria only applied to some of the doors in the database, the indicator would let you know how many items this report includes. For example: 8 of 10 (80%.)

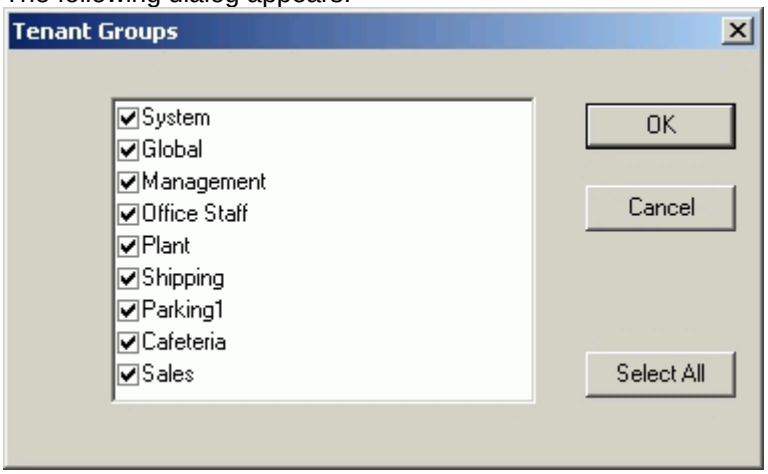
History Report



You can filter the report by selecting specific Tenant Groups also.

Click on the  button.

The following dialog appears:



Select All or click on the Tenant Groups you want to include in the History Report.
To see an example of this type of history report, go to Preview sample: History Report.

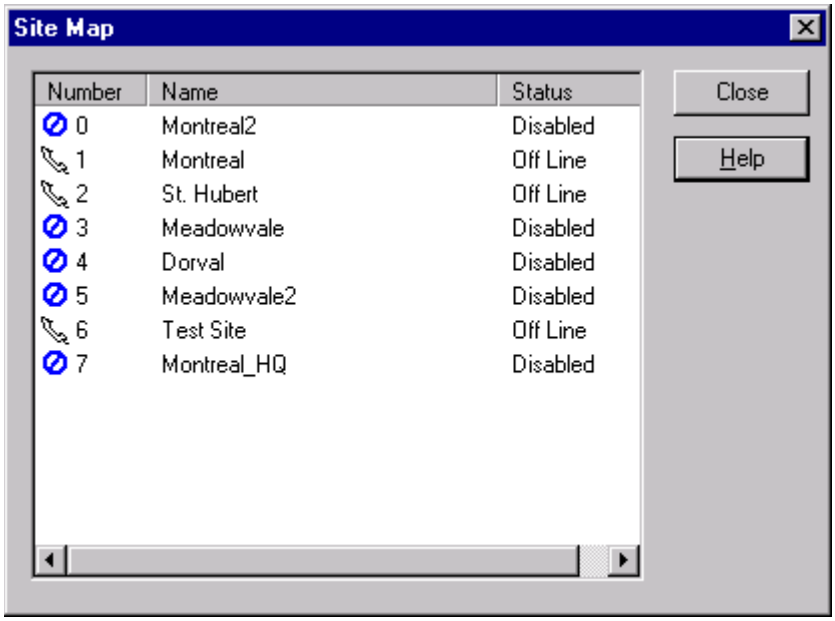
Custom Reports

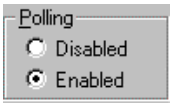
If you have Crystal Reports ☐ software, you have the opt
Millenium Enterprise Systems history data. Reports come read-only to help you avoid accidentally overwriting one of the provided reports. To use an existing report, rename it before using Crystal Reports

Chapter 18: Maps

Map (Site)

To print a Site Map, go to the REPORTS dialog.
Displays a "snap-shot" of the entire Millenium Enterprise 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.





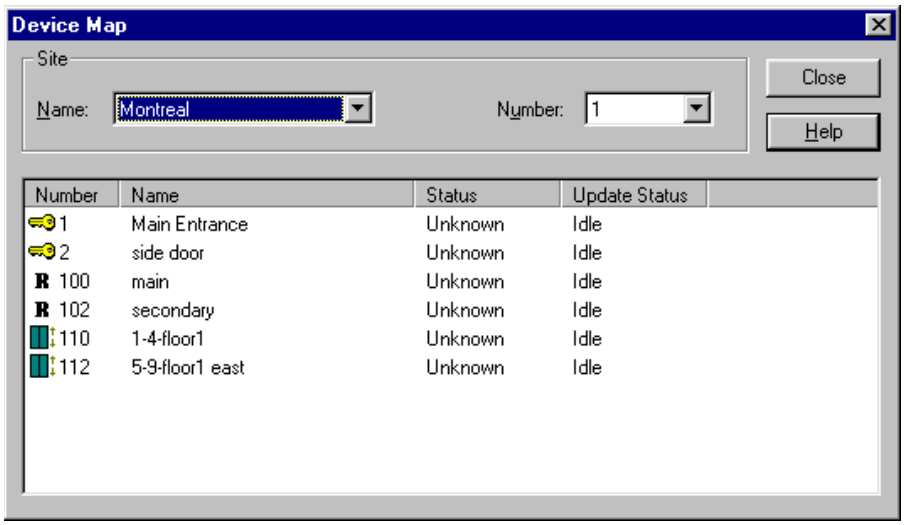
- Off Line or On Line status only appears when a site is ENABLED. Sites are enabled or disabled based on the polling setting in the Site dialog. Programmed devices that are not yet installed or enabled appear as off line.
  Disabled status appears when polling is disabled in the Site dialog.

- **NOTE:** The small ICON beside the Site Number illustrates the communication mode.
  - Phone icon is solid for online sites.
  - Phone icon is hollow for Off-line sites.

Map (Device)

To print a Device Map, go to the Map Menu item.

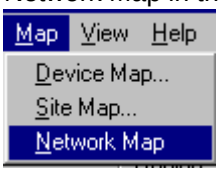
- The Device Map displays a "snap-shot" of the entire Millenium Enterprise network including all devices (DCDs, RCDs, and ECUs) installed in the system. The display is site-by-site. The map displays for your information, only—No data entry takes place in this window.
- The **Status** column lets you 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.



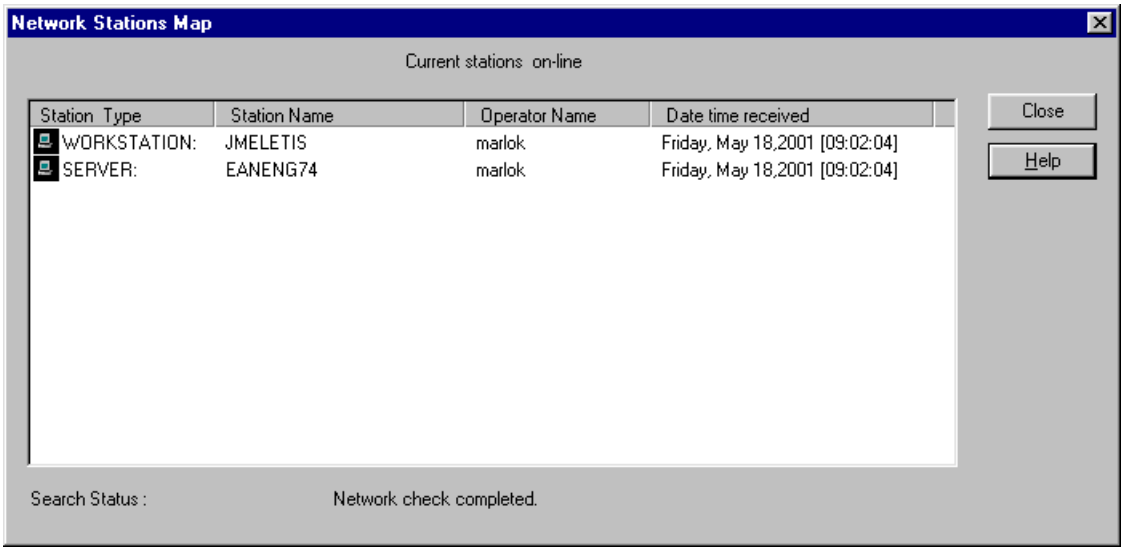
Notice that a symbol at the beginning of each row identifies the type of device along with the device number. Device number for RCDs is the number plus 100. Device numbers for ECUs are 110-112 representing ECUs 0-2.

Map (Network)

To print a Network Map, go to the Map Menu item.
If you want to know which stations are currently participating in your local network, click on Network Map in the menu for Map on the main menu.



Displays a "snap-shot" of the current stations on-line with the type of station (server or workstation) on the Millenium Enterprise network showing the operator name and date/time the snap-shot" was taken. The “map” is for your information, only. No data entry takes place in this window.



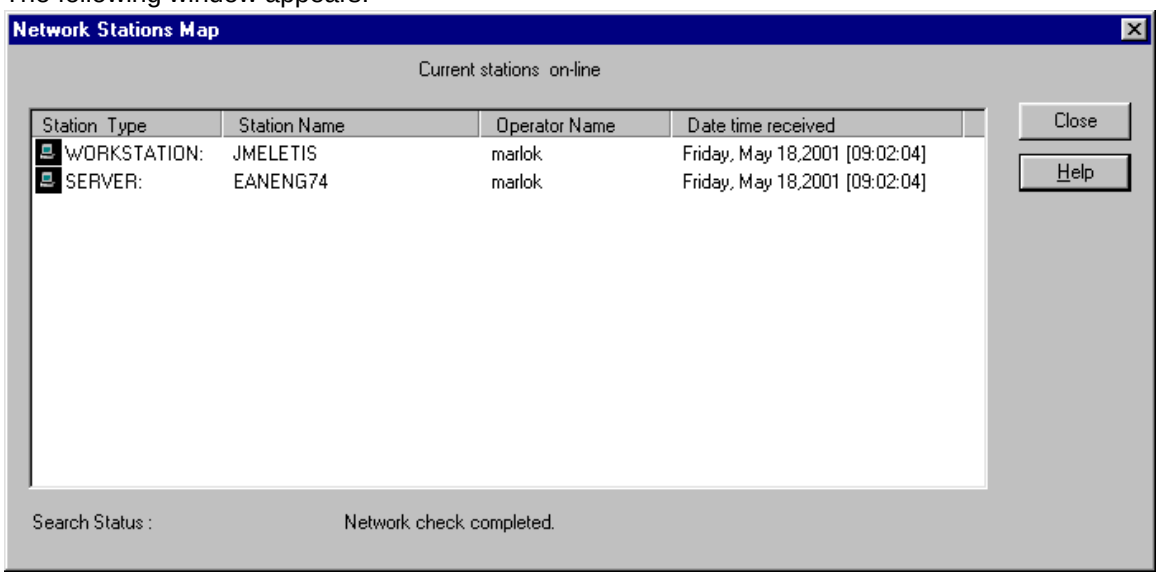
Network Messaging

Millenium Enterprise Network features the capability of network messaging. This allows you to send messages, which will appear instantly on the screen of the workstation or workstations you, select. You can send an instant message to all the workstations on the network if you choose the Broadcasting Option. This feature is obviously very useful in emergency situations.

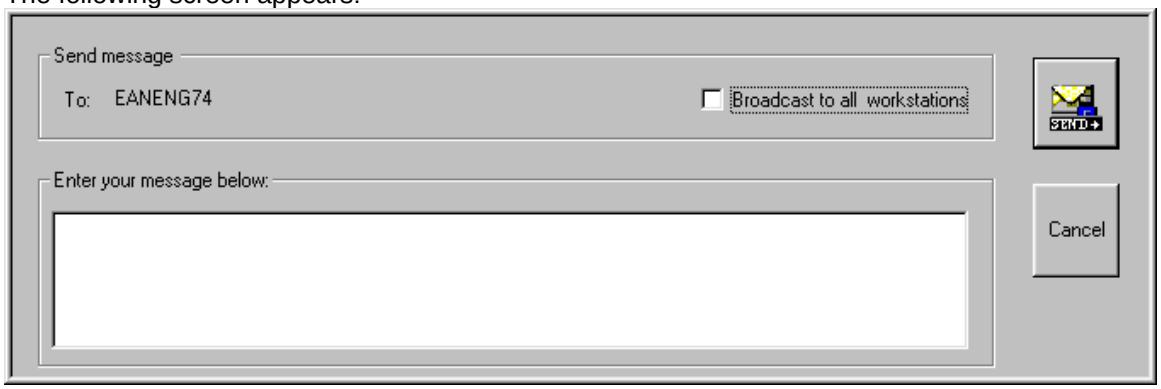
Sending a message over the network

1. From the main menu, select Map, then Network Map.

The following window appears:



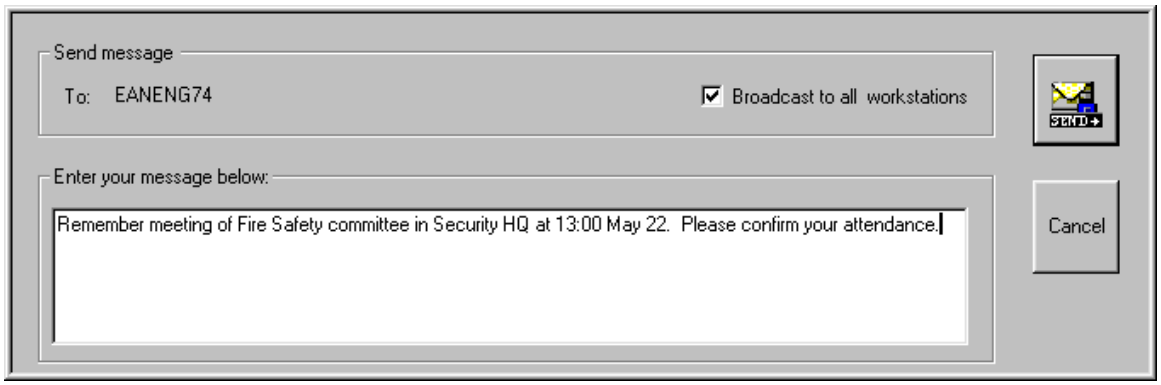
2. (This example has only one workstation on the network but most networks would have several workstations and one server.)
3. Right-click on the workstation(s) that you want to send a message to.
4. The following screen appears:



5. Select Broadcast to all workstations if you want everyone to receive the message.

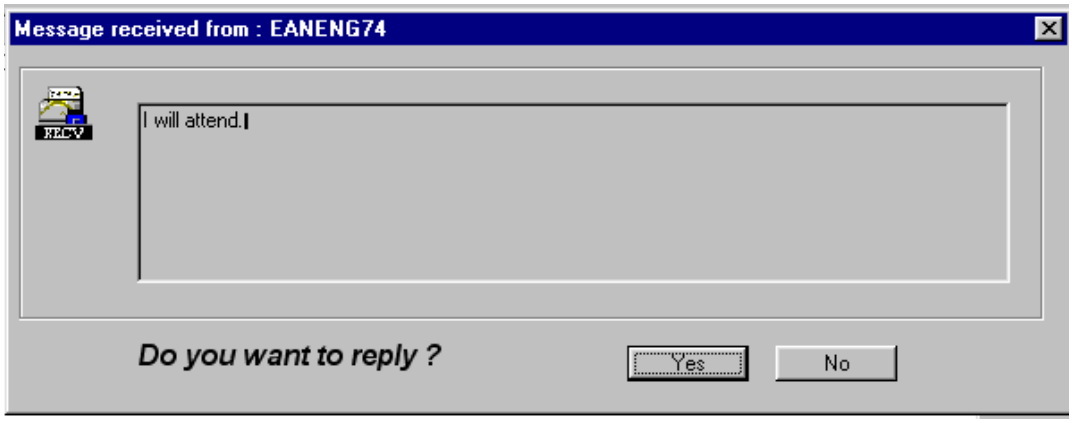
6. Enter your message and click on  .

7. The message pops up instantly on the screens of all the stations you have chosen.

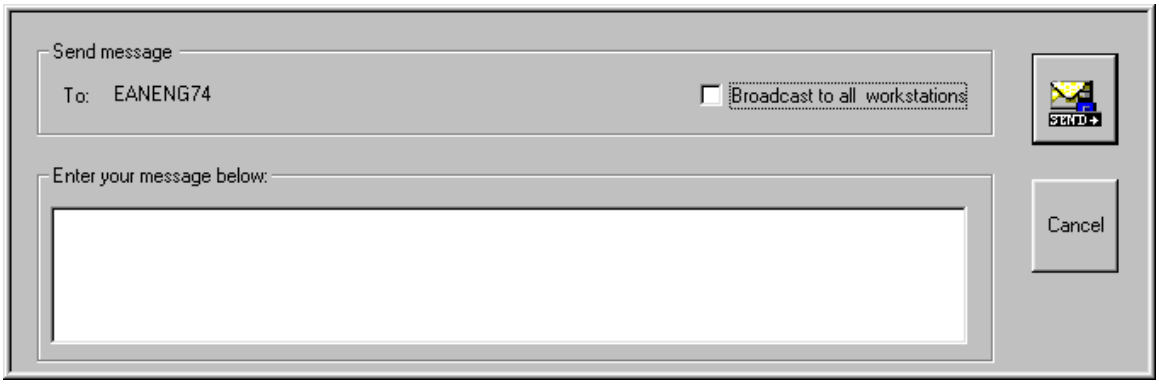


Replying to a message

1. When you receive a message, it will appear in the following format:



2. Click on Yes and a new message form appears.



3. Enter your message and Send.

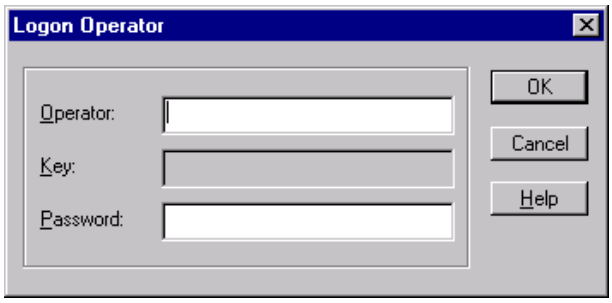
Chapter 19: Database Utilities

How to back up your Millenium Enterprise System

Millenium Enterprise uses Microsoft SQL Server as its database server. This database server can typically run many different databases simultaneously; its functions do not need to be dedicated to Millenium Enterprise. As such, backup and restore functions are a part of general maintenance normally performed by a qualified Database Administrator (DBA).
As with all software systems that accumulate database information, there should be up a regular routine to back up the Millenium Enterprise system, and a backup should preferably be performed before installing an update. Work with your database administrator to establish a schedule.
How to Archive your Access Management history **(MpwDB.exe)**
History files may be archived using a special SQL Query program. Ask your Database Manager for complete information.

Login to DB Utilities

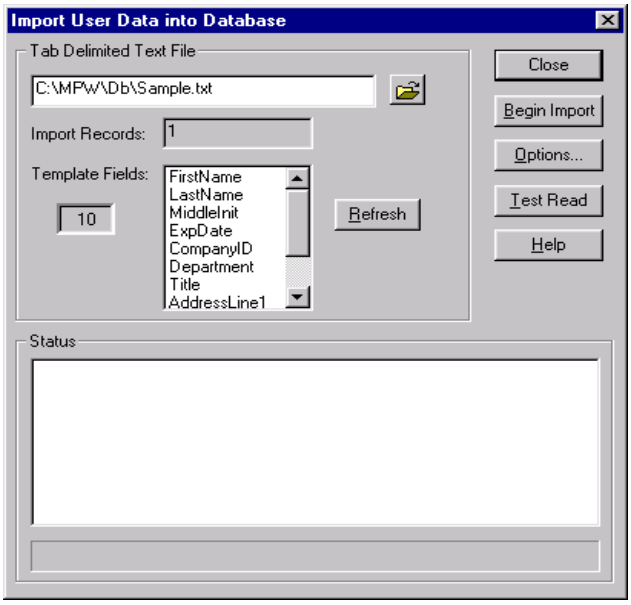
- Select DB Utilities from the Start Menu  and the following dialog box will appear:



- If you have not yet created an Administrator in your Millenium application, use **marlok** as the Operator and **stcharles** as the password.
- If you have an operator, use his/her name and password.
  - The DB Utilities Module can be closed without logging off.

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 Enterprise database. Therefore, the utility offers an option to create a TEMPLATE import file with point-and-click heading selection.



Step-by-Step: Importing User Data Using Database Utility

1. 

Click the database import icon from the Millenium Enterprise DB Utility toolbar.
2. 

Use the import Options..., as applicable.

NOTES:
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.
Check the settings on the miscellaneous tab. 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.

3.  Click the file folder icon to select the import file to be used.
4. 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.
5. 

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.

1. Begin Import 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 Enterprise database.

2. (Stop Import) 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.

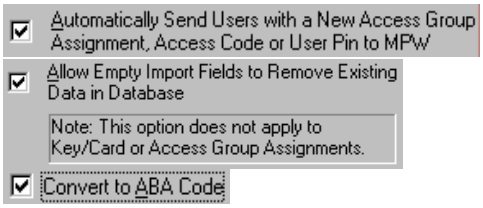
Important! If you import blank fields, the import replaces existing fields in the Millenium Enterprise database with blank fields. Import action always produces an **Import.log** file entry. Any critical errors from the import action append at the end of an **MpwDbErr.log** file.

Comments

NOTE: 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.

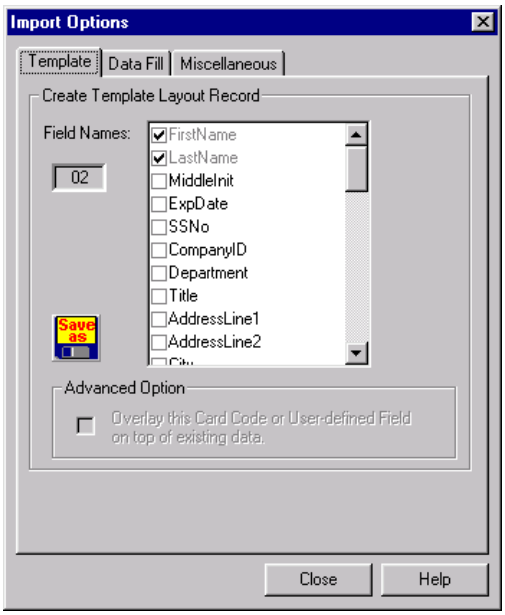
Importing selected user data

Importing a User Access Code, Access Group and/or User PIN



Import Options Dialog

Return to main Import Users dialog.



The Import Options dialog includes three "tabs" of information:

Template tab—

The template option creates a sample text import file with column headings that have the exact syntax of the Millenium database fields.

When you press the  button, you name the sample import file. The utility then creates a file with the column headings you selected.

Data Fill tab

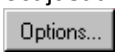
- Offers option to have the Database Utility generate random data patterns to fill **one** selected field.
- Offers option to generate a unique 9-digit ABA code in **one** selected field.

Miscellaneous tab—offers additional options for specific data import utility features

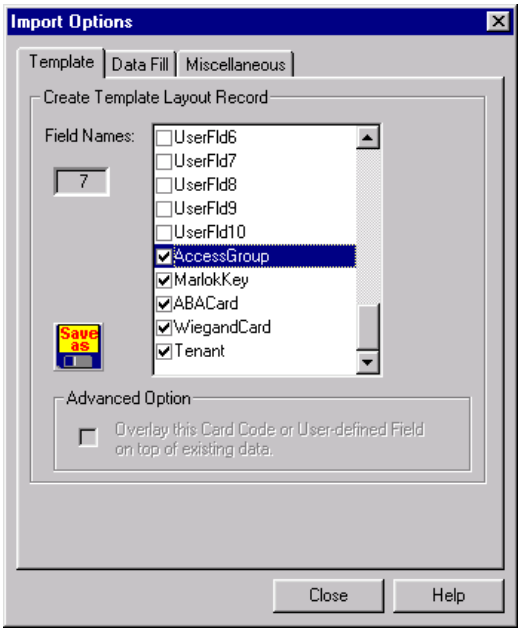
- Return to step-by-step instructions on **main** Import Users dialog.
- See how to automatically send changed user data to Millenium Enterprise
- The User Import feature can accept **Marlok Key** and **Wiegand** and **ABA** card access codes as part of the ASCII import utility. The import can also include 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.

Step-by-Step: Importing Access Code, Access Group, or PIN

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 *Marlok Key*, *ABA Card*, or *Wiegand Card*, as appropriate. Include any other database fields to be part of the import process.
5. To add *Access Group* and or *User PIN* as column headings in the import file, select them from the Field Names listbox. (*User PIN* 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: *Marlok Key*, *ABA Card*, *Wiegand Card*, *Access Group*, and/or *User PIN*, 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.

Example:	First Name	Last Name	Middle Init	**Marlok Key**	**Wiegand Card**
	Randy	Myers	A	3AD4C2	125-49231

9. 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.

NOTES:

Remember these import files are <TAB> delimited, so follow conventions outlined in the Template tab topic in this help file.

If you leave the **Marlok Key** or **Wiegand Card** (or ABA Card 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.

Importing User Access Codes - Restrictions

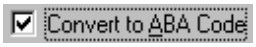
- To import Wiegand or ABA card codes, you must **first** define the DISPLAY FORMAT in Millenium Enterprise Setup (setupmpw.) The import utility rejects any access code that does not match the setup format.
- The utility will not import any access code that is **currently in use** by another user OR that is **reported LOST** in the Millenium database.
- By default, key and card access codes are **not** automatically communicated to doors or elevator floors as part of the import.

  Two options exist:

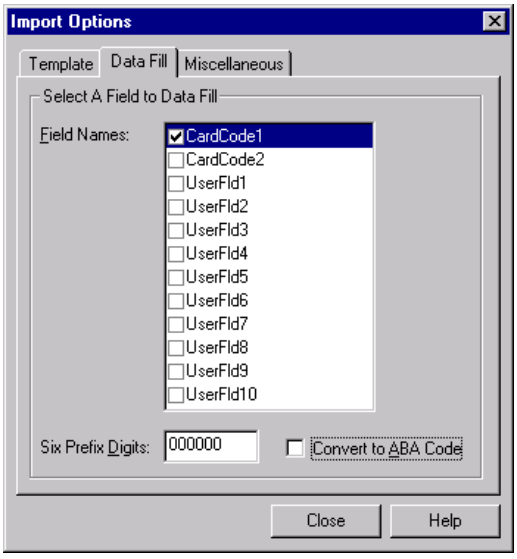
  - An operator must perform an **UPDATE** in Millenium Enterprise software to send this data to Millenium access control devices, or
  - Import Options-Miscellaneous tab 

option must be checked. This will enable MPW to update sites with new key data as it is imported.

Generate 9-Digit ABA Code

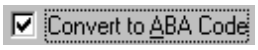
After you select the **one** field to be filled with a random data code, the 

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 Enterprise Systems Setup (setupmpw.) Display Format must be nine data digits (DDDDDDDDD.)
- ABA Card field must be selected in the Import Options Template tab (to create a template for the import file), or you must add *ABA Card* as one of the column headings in the import file.

If you try to click the 

option without the correct ABA Display Format in setupmpw, the above message displays.

The import **ignores** the ABA Conversion in the following situations:

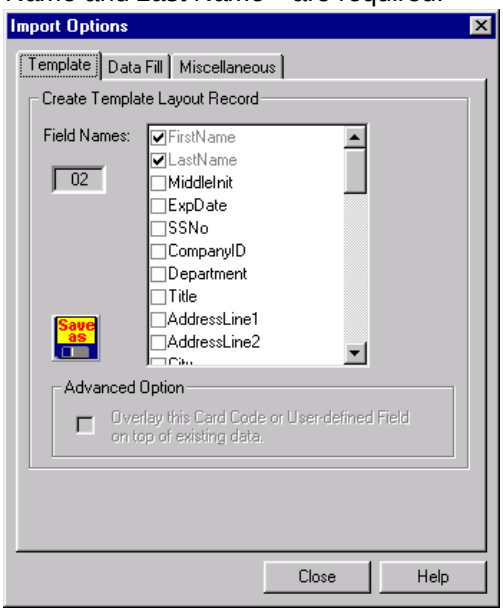
- Correct ABA Display Format has not been recorded in Millenium Enterprise Setup (setupmpw.)
- Regular Data Fill feature did not generate a random digit sequence (as described under Data Fill topic – ignores section.)
- ABA Card field was not specified in the header record of the import file.
- ABA Card field in the import file contained valid data.
- User already has an ABA card assigned.

Import Options

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 Enterprise database tables. Two fields—User's *First*

Name and *Last Name*—are required.

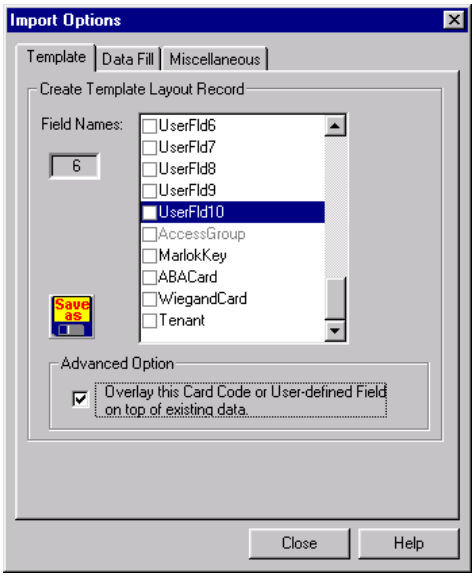


- Click to select any additional fields to be included as header columns in the sample import template. (Click again to de-select.)

Checked fields become the header columns for the sample import file.

Press the button to name the template header file.

Advanced Option: Selected fields (*CardCode1* & *CardCode2* and custom user fields– *User Flds 1-10*) enable an Advanced Option that makes imported data overlay existing data.



To have the data being imported overlay existing data for the selected fields(s), click the

advanced option checkbox.
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.
In other words;
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.

Once checked, the Advanced Option will remain in effect from now on.

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 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 Enterprise database names.

Header	First Name	<tab>	Last Name	<tab>	Middle Init	<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 files heading that you plan to use.

Headings must exactly match field names in the Millenium Enterprise database.

Therefore, the 

button on the IMPORT dialog takes you to a Template tab where you

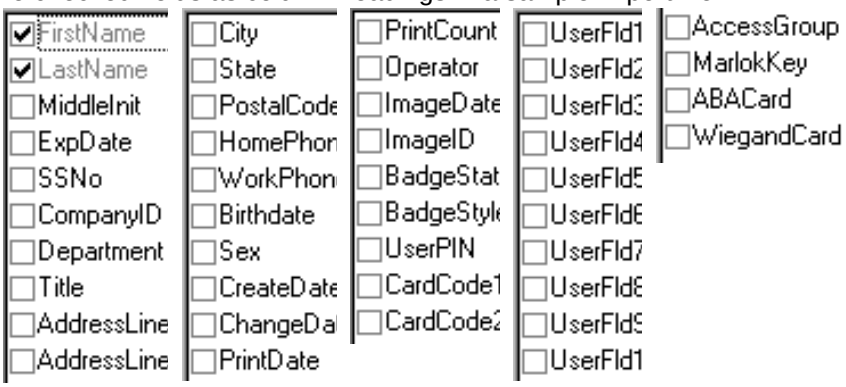
select the exact field names to be used as the import file headings. You can then save the template and use it as the import file—with Header column names already in place.

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.

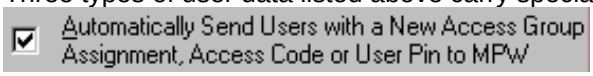
Importing Selected User Data

Step-by-Step: Importing Marlok Key, ABA card or Wiegand

Millenium Enterprise 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 Options... 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.



Three types of user data listed above carry special import features:

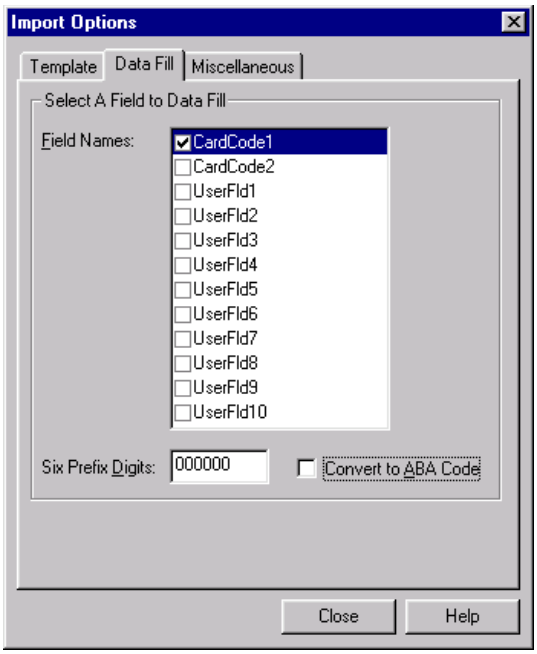


Even if you keep the import option to Allow Empty Import Fields to Remove Existing Data, the replacing option does NOT apply to importing Access Group assignments or Key/card access codes.

Data Fill Tab

Return to the main Import Users dialog.

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 Enterprise 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 Card Code 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.

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 ABA Card field selected in the Template Header Record.

Imports where you want to provide code data for some individual users;

- Type the data in the appropriate column in the IMPORT TEXT FILE. As you run the import, a "Using Card Code/User field from Import File" message displays. The database utility will not generate random code for records that contain data in the import file.

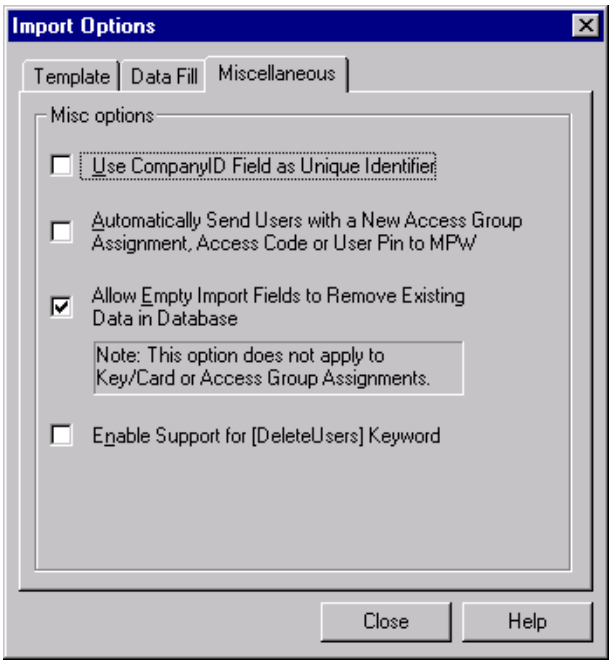
Imports for users that already exist in the Millenium Enterprise database

- If you choose to provide data in the template record for an individual user, the database utility will **not** generate random code for those records in Millenium Enterprise USER database that already contain data. Instead, a "Keeping Card Code / User field Data in DB" message displays. Existing data will **not** be replaced.
- If you want to use the utility to re-generate data in the selected field for certain users, you must first remove data from the selected field in the individual user's record (Millenium USERS dialog.) A "Using Card Code/User field from Import File" message displays.

Miscellaneous tab

Return to the main Import Users dialog.

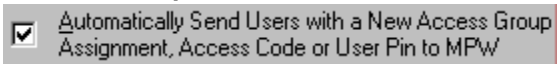
The Miscellaneous tab on the Import Options dialog offers settings to perform specialized data import utility functions.



Unique Identifier:

Millenium Enterprise uses a combination of the Last Name + First Name + Middle Initial 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 Company ID 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 "to-be-imported" users to existing ACCESS GROUPS in Millenium 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 Enterprise 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 Enterprise 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:

This option lets you remove users from the Millenium Enterprise 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 [**Delete Users**] in the import record header. Once the [Delete Users] 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 Enterprise uses a combination of the *Last Name* + *First Name* + *Middle Initial* 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 

option lets you make the import program look at the *Company ID* as the unique identifier instead of the user name combination. The Company ID 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 Company ID Field as Unique Identifier*" option, the utility checks for a unique *Company ID*. If the *Company ID* is unique, the program slightly modifies the user name by appending a digit to the *Last Name*.

Example: If three identical names come up in the import process, (and you have checked the Use Company ID option and assigned unique Company IDs in the import file,) the duplicates come into the Millenium Enterprise database as follows:

	Name Combination	**Company ID**
Existing record	Lane, Penny A	1025
Imported record	Lane**0**, Penny A	1026
Imported record	Lane**1**, Penny A	1027

If the import runs into a duplicate Company ID, the import would UPDATE the existing name and record with the record being imported.

	Name Combination	**Company ID**	
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	**Company ID**
Existing record	Lane, Penny A	1025
(Importing record	Harvey, Penny A	1025)
Existing record	Harvey, Penny A	903
Imported record	Harvey**0**, Penny A	1025

Delete Users with Import Utility

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: Using Company ID field as Unique Identifier

Enable the option on the Miscellaneous tab of the Import Options dialog.

1. 

2. Include the keyword [Delete Users] in the Import Template file's Header Record that contains the Name(s) or Company ID(s) of the **users you want to delete**. 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.

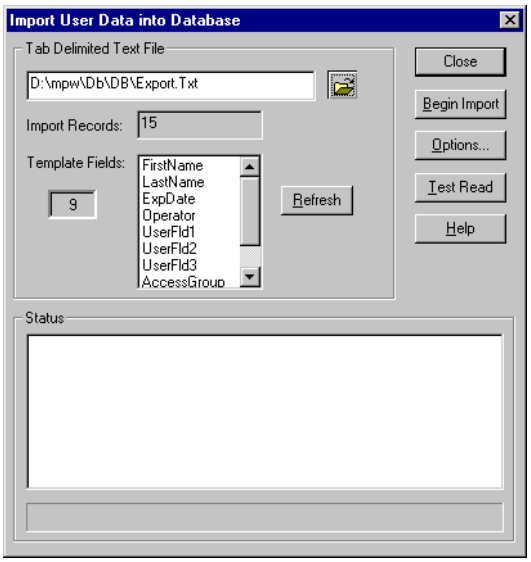
<tab>

Example:	**[Delete Users]**	**First Name**	**Last Name**	**Middle Init**	**Marlok Key**	**Wiegand Card**
	Randy	Myers	A	2. AD 4C 2	125-49231	

Example:	**First Name**	**Last Name**	**Middle Init**	**Marlok Key**	**Wiegand Card**	**[Delete Users]**
	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 [Delete Users] keyword appears in the main Import dialog Template Fields listbox.

NOTE: Press the Refresh button to make sure the template header file reflects the latest changes. Template Fields display in the order by which they exist.



The process looks for the User Name field first. If you want the user record deleted based on Company ID, do not include any user names.

The process allows you to use any existing import file and just add the [Delete Users] 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 Company ID 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 [Delete Users] keyword.
- Press the Refresh 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 Delete Users 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 [Delete Users] 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 [Delete Users], **the import continues as a normal import, and therefore could affect your database according to existing import settings.**

  Example: If the default : 

is checked, any empty fields in the import file will remove data in their corresponding fields in the Millenium Enterprise database.

Updating:

- If Millenium Enterprise software is running, DELETED users are automatically broadcast to Millenium devices (doors, elevator floors.)
- If Millenium Enterprise 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 Enterprise devices.
- To delete based on Company ID:

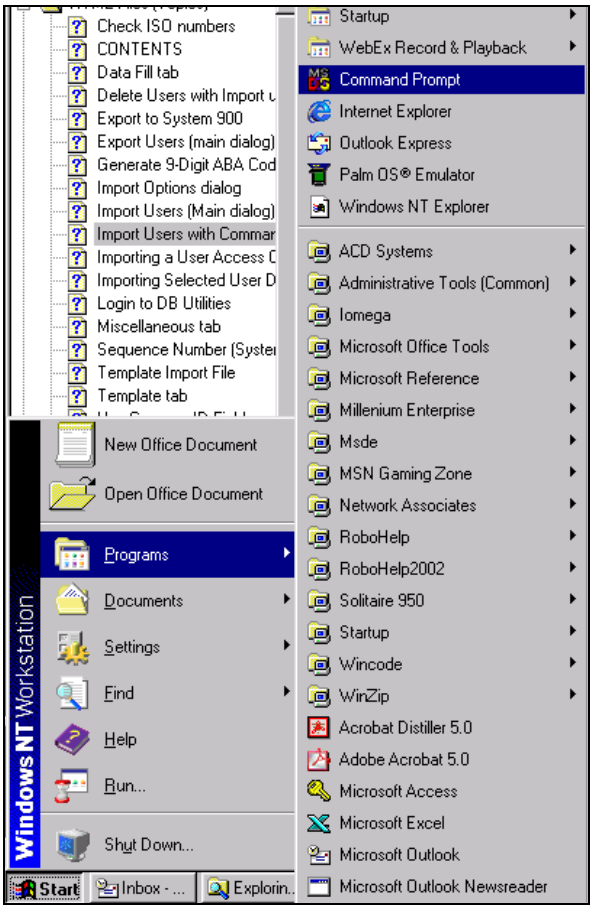
  Do **not** include the User Name.
- Realize that the delete option removes the first occurrence of the Company ID. (The Company ID can exist multiple times in the database.)
- If you delete based on User Name, the utility option searches for the unique combination of Last Name, First Name and Middle Initial.

Import Users with Command Line Prompt

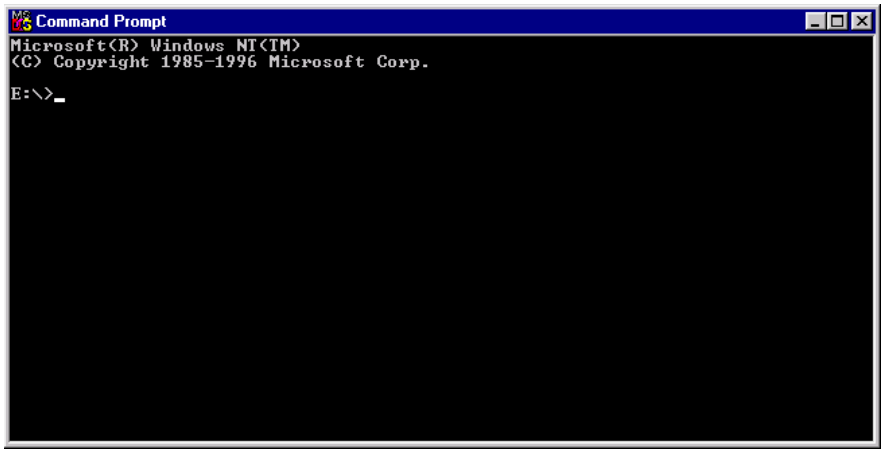
If your Millenium Database Utility is on any of the eligible operating systems, Windows"98, NT, 2000, or XP, you can import Users in a .TXT file by using a Command line prompt.

Step-by-Step: Importing Users Using Command Line

1. From the Start menu of your PC, find the Command Prompt item and click on it.



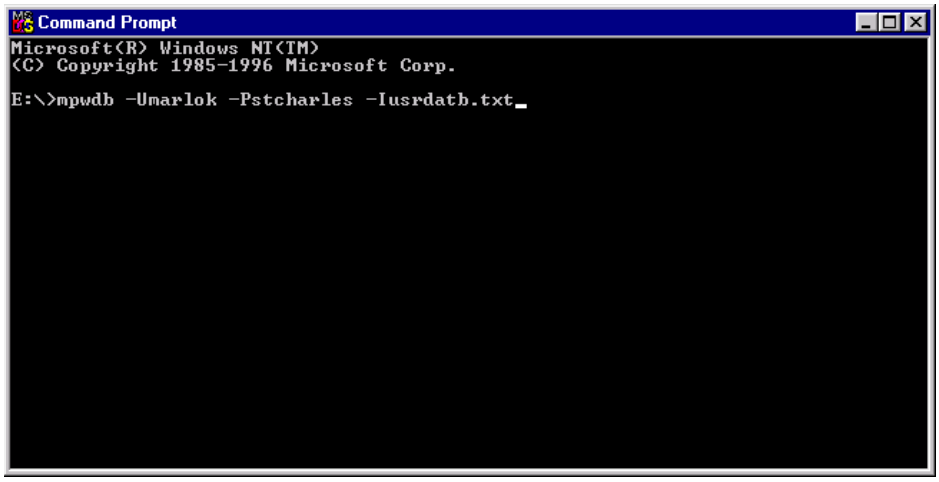
The following screen appears



2. Enter the following command (use either upper or lower case, but not a mix):
mpwdb <space>-U{username}<space>-P {password} <space>-I {import file name}

3. Click on Enter

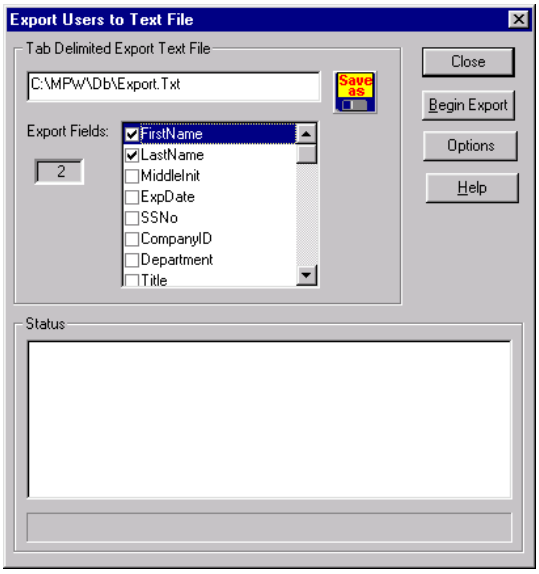
Example:



4. The text file should be imported into the directory you selected in Import Users (Main dialog).

Export Users

The export database utility lets you extract user data from Millenium ' 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.

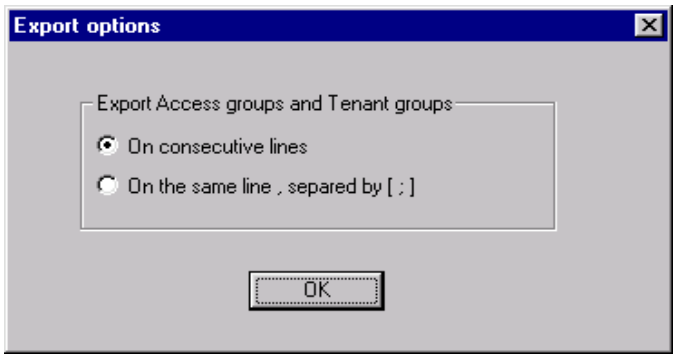


The exported file automatically includes identification information at the beginning of the file as indicated by the semi-colon (**;**) in front of each comment line. The comments describe the contents of the export file and the date the export was generated.

Step-by-Step: Exporting User Data from the Database

1. 

Click the database export icon from the Millenium DB Utility toolbar.
2. Give the export file a name.
3. The .txt extension will be added automatically.
4.  If you want to browse to place the export file in a specific location, press the Save As button.



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 Enterprise directory. This file summarizes what took place during the export process.

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.
Date of birth data does not contain the time component.

Check International Standards Organization (ISO) numbers

What is ISO?

In the ISO 9000 context, **the standardized definition of quality refers to all those features of a product (or service) which are required by the customer**.

In the case of database management, the following ISO standard is applicable:

"Standardization of quality control and integrity maintenance in the field of document management. Documents may be managed in micrographic or electronic form.

This includes:

- processes involving capture, indexing, storage, retrieval, distribution and communication, presentation, **migration**, exchange, preservation and disposal;"

What are ISO numbers?

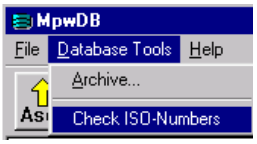
When you generate a list of users to export and then view a log of the export (see Export Users (main dialog) you will see a long (19-digit) number for each user. This is internal to the database and is contained in the Card ID. A new ISO number is generated each time you create a new user although you do not see the number at that time.

The current Millenium Enterprise does not permit you to create two users with the same ISO number, but if you have an old database imported into your system, there may be users with duplicate numbers.

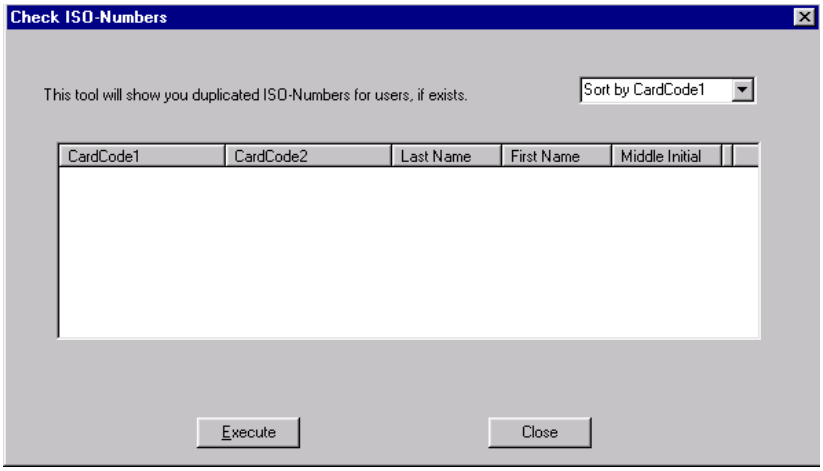
It's important to get rid of any duplicate numbers, so this database function was set up to enable you to do that.

How do I check for duplicate ISO Numbers?

1. Click on the Database Tools menu and select Check ISO Numbers

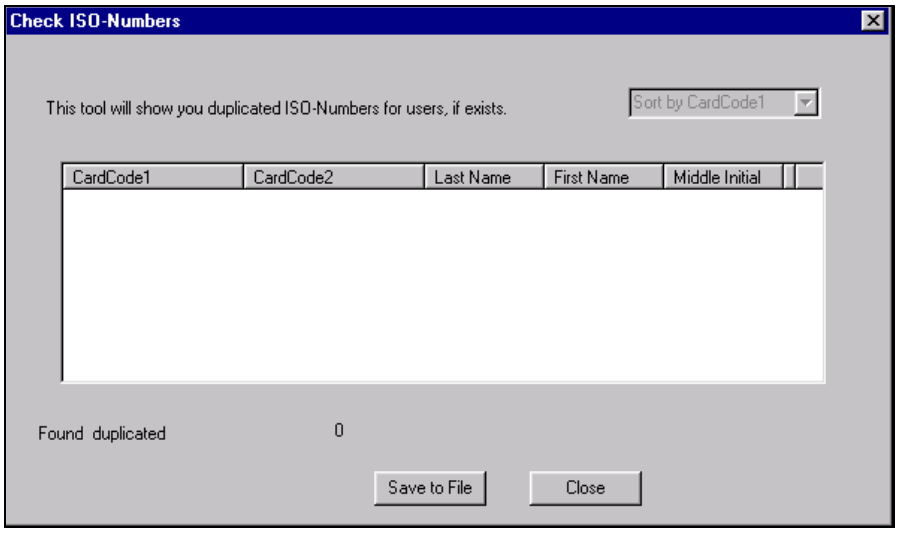


The following dialog box appears:



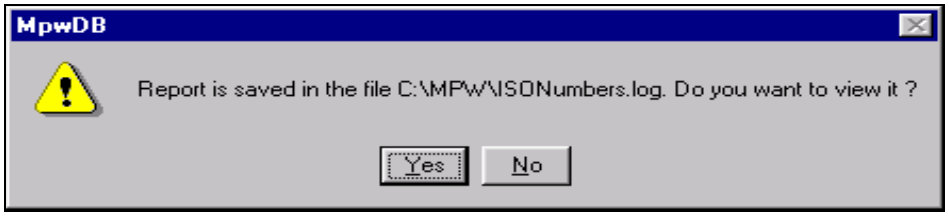
2. Select Card Code 1 or 2 from the dropdown listbox at the top left.
3. Click on Execute, wait while the database is searched - the bigger the database, the longer it will take - and you will see the result.

In the example below, no duplicates were found.



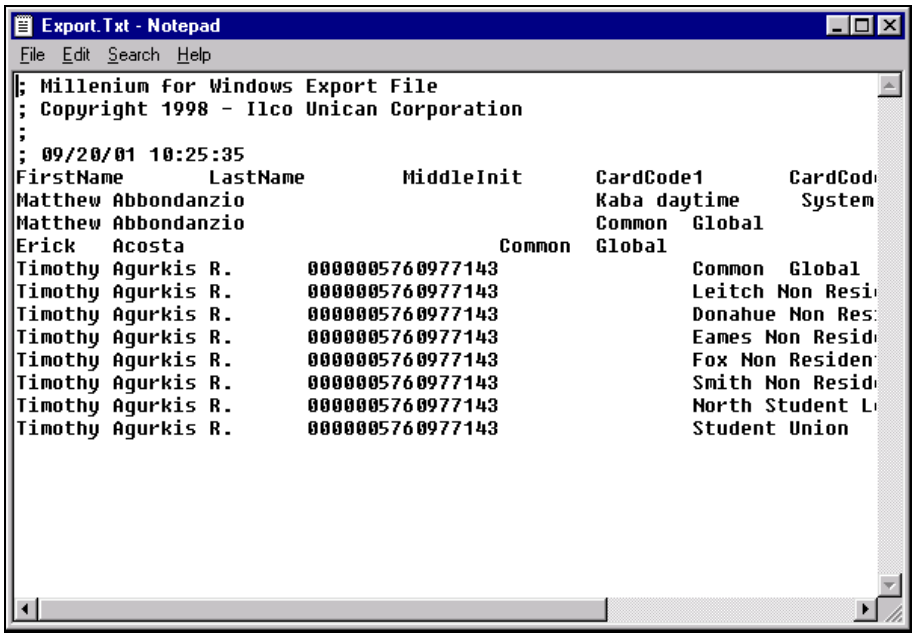
4. Click on  if there were duplicates found and you want to keep a list so you can eliminate them later.

   The following prompt appears:



Click yes to view the file.

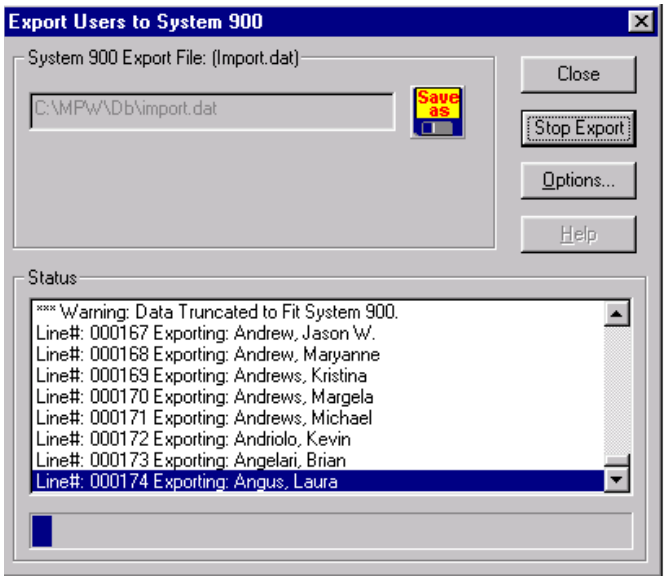
The only other places where ISO numbers are visible is in the Badge profile in the Badging module and the Export Users .txt file, as in the example below:



Export User Data for System 900

The export database utility lets you extract user data from Millenium and create an **Import.dat** file to export users into System 900 software. The illustration below shows an import in progress.

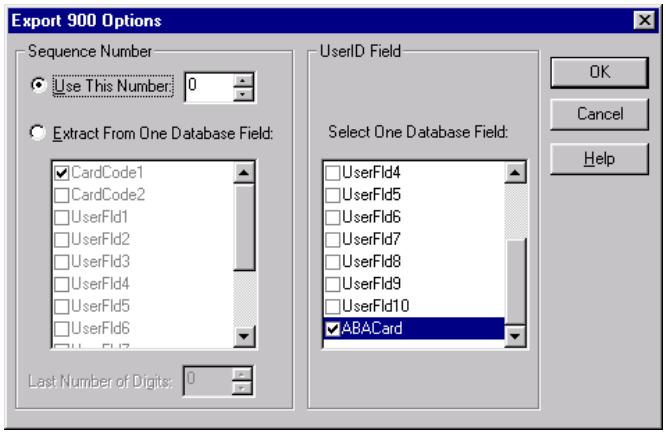
When it is in progress the button changes from Begin Export to Stop Export.



Step-by-Step: Exporting User Data from Millenium 900

1. Click the database 900 export icon 900 from the Millenium Database Utility toolbar.
2. Give the export file a name.
3. The utility automatically assumes the .dat file type extension required in System 900 software.
4. If you want to browse to place the export file in a specific location, press the **Save as** button.
5. Click Options... to select what will become the Sequence Number in the System 900 .dat file you are about to create.
   Selection options are:

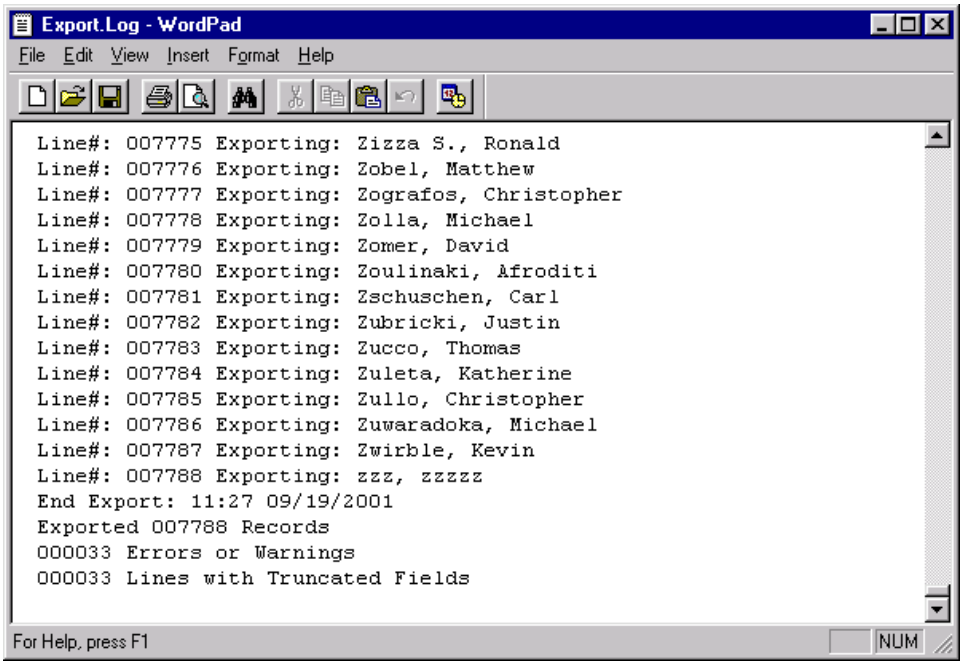
- a uniform sequence number (same for all users,) or
- the Millenium field from which the sequence number will be extracted for each individual user. Options include Card Code 1 or 2, one of the ten user-defined fields, or the ABA access code field.



6. Click the Begin Export button  to generate the export file.
7. 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
User ID		9
Last Name	10	15
First Name	25	14
Middle Init	39	
Sequence #	40	4
CLRF	44	

One example you may run in to is the middle initial field. If you have a period following the letter in the Millenium database, the period truncates out of the export file. A message displays and is documented in the **Export.log** file, as shown below.



The exported .dat file is ready to be imported through Kaba System 900 software, according to System 900 requirements.

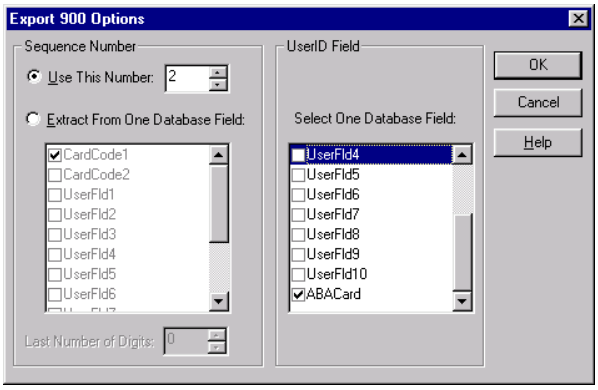
Sequence Number

Millenium Enterprise Database Utility offers two options for the Sequence Number that will be produced for Kaba 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.)

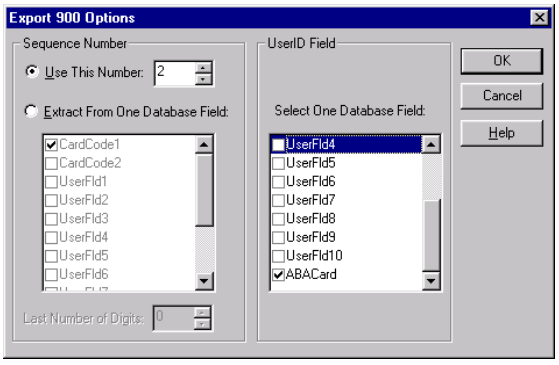
Example:

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.

User ID

Millenium Database Utility offers an option for the User ID field that will be produced for 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.

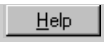


The utility produces a User ID field as follows:

DB Field	Actual User ID #
Card Code 1 **Card Code 2** **UserFlds 1-10**	**First 9** text characters from Display Format
ABA Card	**Last 9** characters from Display Format.

Chapter 20: How To Get Help

Millenium Enterprise help comes in many forms:

Millenium Enterprise HELP	Source	How To Get There
Written documentation	User Guide	You're there.
	Setup Millenium Enterprise Full MPW system	 Click the Help icon on the main toolbar for overall online help (or open the Help file menu.)
		Choose the Print option to produce a written copy of the currently displayed on-line help topic.
	-OR-	 Press Help button in the dialog box where you are currently working for help about the currently displayed dialog.
Technical Support	Your local dealer	Record your local dealer's name, address and phone number here for easy reference. Dealer name:_____ Phone #: (_____)-(_____) Fax#: (_____)-(_____)
(SALES) Order Access Management components such as readers, keys, Door Control devices, Site Control Devices, etc.	Your local dealer	
Return Access Management component for repair or warranty replacement (RMA)	Your local dealer	