



## Access Control Users Guide

# Users Guide

## Table of Contents

Access Control Users Guide.....	1-0
Users Guide Conventions.....	2-0
Windows Conventions.....	3-0
Online Help.....	4-0
Introduction to the Access Control Software.....	5-0
The Symetrix Access Control software can handle.....	5-1
Network Computer System Requirements.....	6-0
Set the Network Computer Date and Time.....	7-0
Software Installation.....	8-0
Installing the Symetrix Access Control Software.....	8-1
Installation Maintenance.....	9-0
Removing a Previous Installation of Symetrix Access Control.....	9-1
Product Documentation.....	10-0
Installing the Acrobat Reader Program.....	10-1
Accessing Documentation.....	10-2
Using the Auto Run Menu and Windows Explorer.....	10-2.1
Using the Acrobat Reader Program.....	10-2.2
Starting the Symetrix Access Control Software.....	11-0
Starting the Program.....	11-1
From the Windows Start Menu.....	11-1.1
From the Windows Desktop Shortcut.....	11-1.2
System Login.....	11-2
To Log On to the Symetrix Access Control Software.....	11-2.1
Logging Off the Symetrix Access Control Software.....	11-2.2
Introducing the Symetrix Access Control Desktop.....	12-0
The Simplified Side Menu Bar.....	12-1
The Standard Side Menu Bar.....	12-2
Online Help.....	12-3
Exiting the Symetrix Access Control menu Window.....	12-4
Window Management.....	13-0
Cascading Windows.....	13-1
Tiling Windows Vertically.....	13-2
Tiling Windows Horizontally.....	13-3
Exiting the Symetrix Access Control Software.....	14-0
Adding and Editing System Managers.....	15-0
Editing a System Managers Access Level.....	15-1
Editing a System Managers Password.....	15-2
Adding a new System Manager.....	15-3
Associating a System Manager with a Department.....	15-4
Associating a System Manager with Doors.....	15-5
Configuring Access Control Users.....	16-0
Search Access Control User Form.....	16-1
Edit Access Control Users Form.....	16-2
Edit Access Control User Fields.....	16-2.1
Adding a New Access Control Card using a Reader.....	16-3
Edit Access Control User Privileges.....	17-0
View User Privileges Form.....	17-1
Edit Access Control Schedules.....	18-0
View Access Control Schedule Form.....	18-1
Edit an Access Control Schedule.....	18-1.1
Symetrix Access Control System Log Report.....	19-0
Downloading Records from the Access Control Panels.....	19-1
Creating a User Based Access Control Report.....	19-2
Creating a Date / Time Based Access Control Report.....	19-3
System Maintenance.....	20-0
Secure Storage of Program CD-ROM.....	20-1
Periodic Database Backup.....	20-1
Glossary.....	21-0

© 2011 Symetrix Data and Security – ALL RIGHTS RESERVED  
Document Number ACCCONTRLEU, Revision 1.0 – May, 2011 *Symetrix Data and Security*  
Acrobat® Reader © 1987-2001 Adobe Systems Incorporated. All rights reserved.  
Adobe and Acrobat are trademarks of Adobe Systems, Incorporated.  
Windows is a trademark of Microsoft Corporation.  
This software is based, in part, on the work of the Independent JPEG Group. © 1991-1996.

The trademarks used in this Users Guide are the property of the trademark holders. The use of these trademarks in this Users Guide should not be regarded as infringing upon or affecting the validity of these trademarks. Symetrix Data and Security reserves the right to change, without notice, product offerings or specifications. No part of this publication may be reproduced in any form without written permission from Symetrix Data and Security.

# 1.0 *Symetrix Access Control* Users Guide

The *Symetrix Access Control* Software is designed to make the access control system configuration and operation as simple as possible. This is achieved by breaking the configuration and operation processes into logical sections. Each section is responsible for a specific operation; whether it is entering information regarding how some aspect of the system is to be used or physically performing some operation. This Users Guide is written for the novice user, learning how to navigate the *Access Control* software menus and how to use the commands within the menus. The Users Guide presents the configuration and operation process in a recommended order of implementation. An operator can configure the system in almost any order, but the order described in the Users Guide provides the most sequential and complete path for the first time installer and for a new installation. Generally speaking, each section of the Users Guide builds upon what has been completed in the previous section.

## 2.0 User Guide Conventions

To present this information, the Users Guide is written in simple step-by-step instructions. There are certain conventions the Users Guide follows for presenting information and for indicating when an operator needs to perform an action on the computer.

- **Items that require special attention or that can dramatically affect the access control network are prefaced by a caution sign and may be in bold face for extra emphasis.**
- Folder or directory names are identified in the text as “folder/subfolder.”
- Information to be typed by an operator is identified in **Boldface**.
- If a button is clicked to perform an operation, the button icon is displayed or the button name is shown in **Boldface**.
- Locating an item under a pull-down menu is identified as Menu Option -> Sub-Menu Option.
- Program names are identified in all UPPER CASE letters.
- Operation notes are shown in *italics*.

These are things of which to be aware while using the *Symetrix Access Control* software.

## 3.0 Windows Conventions

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

## 4.0 Online Help

To assist the user the Users Guide is available as an online help file in the *Symetrix Access Control* software. To access the help file when in the *Symetrix Access Control* program, click on the Help/Contents pull-down menu or click on the button on the *Symetrix Access Control* tool bar to open the help file.

## 5.0 Introduction to the *Access Control Software*

The *Symetrix Access Control* software for *Windows* is a software program that configures and manages an access control system using *Symetrix Access Control Panels*. The *Symetrix Access Control Software* is a fully functional *Windows* program, making full use of all popular *Windows* features such as resizing and relocating windows, drag-and-drop functions, multiple windows open simultaneously, background operation, and real-time operation. *Symetrix Access Control* operates under *Windows Vista*, *Windows XP*, *Windows 98*, *Windows 2000*, *Windows ME*, or *Windows 7*. The *Symetrix Access Control Software* provides the operator with a user-friendly interface for defining system parameters, managing cards/User IDs, setting event timer functions, and preparing reports. An extensive online help file displays information with a click of the mouse. A dedicated PC is not needed to run an access control network. The PC with the *Symetrix Access Control* program is only needed for entering and uploading information to the controllers, downloading information from the controllers, real-time network monitoring, and event data storage. The *Symetrix Access Control Software* uses a proprietary communications protocol to automatically check all controllers on the network and then configures itself according to the connected hardware, greatly simplifying the system set-up procedure. The *Symetrix Access Control Software* is capable of managing a single site via TCP/IP (UTP / LAN Cable), as well as RS-232/RS-485.

### 5.1 The *Symetrix Access Control* software can handle:

- A single master system operator.
- Up to 4 normal / holiday user schedules
- Up to 40 user defined holiday dates
- Up to 255 controllers per site.
- Up to 1024 doors (four per controller)
- Up to 9214 cards/users.
- Virtually unlimited system event history, including date, time, and user stamping.
- Each controller can store up to 18724 events. These events can be transferred to the *Access Control* software for storage on the host computer's hard disk and for event reporting.

## 6.0 Network Computer System Requirements

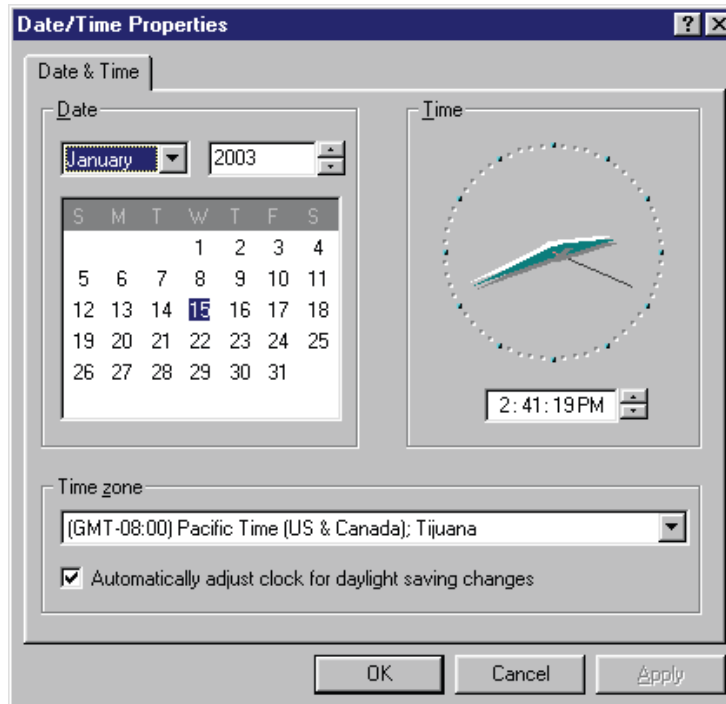
For proper operation of the access control system, the host computer running the *Symetrix Access Control* software must meet the following requirements.

- PC compatible computer using a Pentium-III or faster microprocessor
- minimum of 128 MB of system RAM
- SVGA colour monitor with SVGA graphics card (1024 x 768 minimum resolution )
- CD-ROM, keyboard, and mouse or other pointing device
- 50 MB of hard disk space
- UTP Ethernet card for TCP/IP connection
- RS-232 Serial Port for RS-232 / RS485 connection
- one of the following operating systems: - *Windows 98* - *Windows ME* - *Windows Vista* - *Windows XP* - *Windows 2000* - *Windows 7*

## 7.0 Set the Network Computer Date and Time

To ensure that the date and time assigned to events on the access control system are correct, the date and time kept by the host computer should be checked for accuracy. Part of the controller configuration process is to set the time and date of the controllers to match that of the host computer. *NOTE: If the Symetrix Access Control program is running, please close the program before setting the host computer's date and time. Closing the program ensures that when the Access Control program is started, all timing functions are based on a correctly set host computer clock.*

1. Double-click on the field on the *Windows Task Bar*. A clock/calendar window appears (see Figure 1).



**Figure 1 : Host Computer Clock/Calendar Window**

2. To set the time, double-click on the hours field of the digital clock display. Click on to advance the clock to the correct hour. Repeat this process for the minutes, seconds, and A.M./P.M. setting.
3. In the Time zone field, click on and a list of time zones appears. Scan through the list and click on the time zone corresponding to where the computer is located. If you live in an area that uses Daylight Savings Time, click in the box beside the “Automatically adjust clock for daylight savings changes” check box. A check mark in the box enables the automatic adjustment feature.
4. To set the month, click on the in the month field and a list of months appears. Scan through the list and click on the month.
5. To set the year, click on to advance to the correct year.
6. To set the day, click on the day in the calendar.
7. Click the button and the time and date are set in the host computer.

*NOTE: International date and time formats are supported by the Symterix Access Control software. The program displays and reports dates and times in the format selected when setting the host computer's date and time.*

## 8.0 Software Installation

This section covers the following types of installations.

- a new installation of the *Symterix Access Control* software
- upgrading an existing *Symterix Access Control* software installation to a new revision
- performing certain installation maintenance tasks

### 8.1 Installing the Symterix Access Control Software

The Windows Installer handles the software installation/upgrade process. Installing software is basically a question and answer process. To accommodate the installation process and install the *Symterix Access Control* software the host computer must meet the system requirements detailed in “Host Computer System Requirements” of this section.

## 9.0 Installation Maintenance

The following section provides information on verifying host computer system resources for optimum program operation, for running a previous *Symetrix Access Control* installation, and for deleting a previous *Symetrix Access Control* installation.

### 9.1 Removing a Previous Installation of *Symetrix Access Control*

If installing a new version of *Symetrix Access Control*, the previous installation should be removed.

1. Click on the [START] button on the Task Bar. The Start menu will appear.
2. Click on Settings -> Control Panel.
3. When the Control Panel window appears, double-click on the **Add/Remove Programs** icon.
4. The Add/Remove Programs Properties window appears. The bottom half of this window will display a list of installed programs. Scroll through this list of programs, locate and click on the *Symetrix Access Control* software you wish to remove from the host computer.
5. Click on the [Add / Remove] button.
6. The *Symetrix Access Control* Removal Confirmation window will appear.
7. Un-install the *Symetrix Access Control* Software to continue.

## 10.0 Product Documentation

The *Symetrix Access Control* installation software is available in CD-ROM format. The CD-ROM format includes copies of product documentation in Adobe Acrobat PDF format, and it includes a copy of the Adobe Acrobat Reader installation program. The Adobe Acrobat PDF – portable document format – allows an end user to easily view and print copies of documents encoded in the PDF format.

*NOTE: The documents on the CD-ROM are the current revisions at the time of CD-ROM release. However, these documents are subject to change at any time. If necessary, please visit Technical Support at the Symetrix Website to download the current revision of any document.*

### 10.1 Installing the Acrobat Reader Program

If the Acrobat Reader is not already installed on your host computer, follow these instructions to run the Reader installation program.

1. Insert the *Symetrix Access Control* installation CD-ROM in to the host computer's CD-ROM drive.
2. From the Auto Run Menu, click on the **Install the Acrobat Reader** link. The installation program will begin.
3. The Acrobat Set-up Wizard will take you through the installation process.
4. When the installation process is complete, an Acrobat Reader shortcut will be placed on the host computer's desktop.

### 10.2 Accessing Documentation

Once the Acrobat Reader program has been installed on the host computer, there are two ways to access product documentation on the *Symetrix Access Control* CD-ROM – using the Acrobat Reader program directly or using Windows Explorer.

#### 10.2.1 Using the Auto Run Menu and Windows Explorer

1. Insert the *Symetrix Access Control* installation CD-ROM in to the host computer's CD-ROM drive.
2. From the Auto Run Menu, click on the desired link (End User Documentation). If you chose the End User Documentation links, a sub-menu appears. Once you have made another selection (or if you select Explore the CD-ROM), the Windows Explorer is automatically opened to the desired location with a list of the available PDF documents.
3. Scan through the list of PDF files and double-click on the desired file. The Reader program will open displaying the selected file and its contents.

### **10.2.2 Using the Acrobat Reader Program**

1. Double-click on the Acrobat Reader shortcut icon. The Reader program should open.
2. Click on the File -> Open pull-down menu option. A standard Windows open file window will appear.
3. Use the navigation tools to display the contents of the desired folder on the *Symetrix Access Control* CD-ROM (in either User Documentation or Technical Documentation). A list of PDF documents will be displayed.
4. Scan through the list of PDF files and either double-click on the desired file, or click on the file and then click on the button. The selected file will appear in the Reader window.



## 11.0 Starting the *Symetrix Access Control Software*

The first step to start the *Symetrix Access Control* program is to log onto the system. In normal operation, the login process identifies to the software which operator is entering the program. With this identification, the program is able to limit the operator's actions to those that the operator has been approved to perform.

### 11.1 Starting the Program

There are several ways to start the *Symetrix Access Control* program. The easiest, most common methods are described below.

#### 11.1.1 From the *Windows Start Menu*

1. Click the [START] button. The windows start menu will be displayed.
2. Select the [Programs] Menu option.
3. Double click on the Access Control Icon
4. The Symetrix Access Control software will now open.

#### 11.1.2 From the *Windows Desktop Shortcut*

A desktop shortcut should have been automatically created during the installation process. Simply double click on the icon to start the *Symetrix Access Control software*.

## 11.2 System Login

Once the program begins, it will prompt for a user to login (see Figure 1-11). This is an identifying name and password for the user or installer to operate the software. The first time the program is executed, the user name and password entered will be used for the System Installer. Until this login information is changed, the original user name and password will provide access to everything in the *Symetrix Access Control Software*. Later in the *Symetrix Access Control* configuration process, each authorised operator can be assigned identifying user names and passwords (see "Add System Operators" in section 2).

**The Default Login User name is abc**

**The Default Login Password is 123**

#### 11.2.1 Log on to the *Symetrix Access Control Software*

1. Click on the "User name" field, and type the name of the operator logging on (**abc**)
2. Click on the "Login Password" field, and type the password assigned to the operator listed in the User Name field. Asterisks will appear in the password field instead of letters to prevent someone looking over your shoulder and learning your password. (**123**)
3. Click on the [OK] button to continue.



Figure 11.2.1 - Symetrix Access Control Login Form

The program will now verify the operator name and password. If both are correct, the Login window disappears and the *Symetrix Access Control* main menu will be displayed. If either the user name and or password are incorrect, the system will prompt you to correct either one of these fields.

***NOTE: The user name and password are both case sensitive. That is, the program differentiates between UPPER CASE and lower case in both the operator name and password. Please keep this in mind when creating operator names and passwords, and when entering your operator name and password to log on the Symetrix Access Control software.***

### **11.2.2 Logging out of the *Symetrix Access Control* Software**

Whenever one operator replaces another operator, for instance during a shift change, the original operator should log off the system and allow the new operator to log on. This provides for correct tracking of operator initiated events during the operator shift.

1. Click on the File -> Exit pull-down menu option. The original operator is logged off the system and the *Symetrix Access Control* Software will close.
2. Re-open the *Symetrix Access Control* Software, and login using the required User name and Password.

## 12.0 Introducing the *Symetrix Access Control Desktop*

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

### 12.1 The Simplified Side Menu Bar

There are eight menu options on the *Symetrix Access Control* Simplified side Menu Bar.

*Note: The simplified side menu bar can be displayed at any time by clicking on the Doorstep tab located at the bottom of the side menu bar.*

1. **Add Controller** – Allows you to add further access control main panels to expand your existing system.  
**Note :** It is recommended that this menu option is disabled for all users except the System Installer, as incorrect settings can disable the access control system functionality.
2. **Test Controller** – Allows testing the connection between the access control software, and the door controller unit, as well as manually open doors.
3. **Auto Add Card** – Allows adding, new access control cards, tags and key fobs to the system.
4. **Update Privilege** – Allows changing user and card privileges for individual users, and individual doors..  
**Note :** It is recommended that this menu option is disabled for all users except the System Installer, as incorrect settings can disable the access control system functionality.
5. **Upload** – This menu option allows you to upload any changes made in the software, such as users, privileges, schedules, and door settings, to the configured access control panels.
6. **Monitor** – This menu option allows managers and installers to view live status information for all the access control panels added to the system, including communication, door open / close status, and live error messages.
7. **Download**– This function obtains the latest log information from panels connected to the access control software, allowing user and log reports to be generated.
8. **Query Records** – This function allows managers to view information such as user accessing the system at a particular date and time, log information for individual users, and logged error messages for the access control system.



### 12.2 The Standard Side Menu Bar

There are a number of menu and sub menu options on the *Symetrix Access Control* Simplified side Menu Bar.

*Note: The standard side menu bar can be displayed at any time by clicking on the Operation tab located at the bottom of the side menu bar.*

1. **Basic Configure** – This menu option includes the following sub menu options
  - a) **Controllers** – This sub menu allows you to configure the access control panel communication settings as well as panel specific settings.
  - b) **Departments** – This sub menu allows you to add and remove departments, which can be used to group similar users, allowing simplified user privilege management.
  - c) **Personnel** – This sub menu allows you to manage individual users / cards and tags. You can change user names, allocate users to departments, and add / remove users and tags.
2. **Personnel** – This menu option includes the following sub menu options.
  - d) **Lost Card Register** – This sub menu allows to mark tags and cards as lost, allowing you to re-allocate a new card to an existing user, as well as disable lost cards from gaining access to any doors configured within the system.
3. **Access Control** – This menu option includes the following sub menu options
  - a) **Access Privilege** – This sub menu allows you to grant or revoke access to one or more doors, for selected users.

4. **Basic Operate** – This menu option includes the following sub menu options

a) **Console** – This sub menu option allows a low level live view of the access control system.

b) **Check** – This sub menu option is used to check the system operation and function.

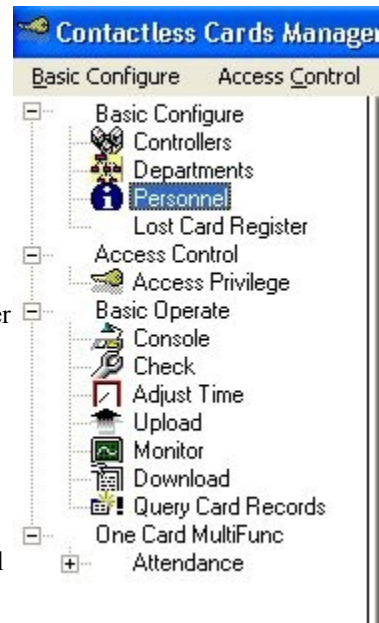
c) **Adjust Time** – This sub menu option allows you to upload the current date and time settings from your PC to your access control system. This function should be used at the beginning or end of daylight savings.

d) **Upload** – This sub menu option allows you to transfer the settings from the Symetrix access control software, to the connected access control panels. This operation should be performed whenever there have been changes made to users, privileges, schedules, and other parameters.

e) **Monitor** – This sub menu option allows you to view in real time, the door and panel status information, including if a door is open or closed, if an access control panel is communicating and is online, and if there are any errors with the system.

f) **Download** – This sub menu function allows you to download the latest log information from the access control panels connected to the system. This operation should be conducted before you generate any access control reports using the software.

g) **Query Card Records** – This sub menu option allows you to generate reports based on the access control system logs. These reports include users that have accessed the system during a particular date / time, user access logs, and other reporting functions.



## 12.3 Online Help

Online help is built into the *Symetrix Access Control* software. To view the online help, click on the help icon displayed on the tool bar or click on the “Help” menu option in the menu bar. A new window will appear displaying the relevant help information for the current section of the *Symetrix Access Control* software.

*NOTE: When using online help, you may consider resizing the Symetrix Access Control program window to take up half of the computer screen and then resizing the online help to take up the other half of the computer screen. This allows you to jump back and forth between the program and the online help, tracking down assistance for nested items.*

## 12.4 Exiting the Symetrix Access Control menu window

Whenever changes are made to information displayed in a window, the *Symetrix Access Control* software will prompt if the changes are to be saved if the window is closed, and the changes have not been saved. Changes can be saved by clicking on [SAVE] button located on the menu bar, at the top of the selected window. When system changes are saved, the software will connect to the configured access control panels, and will upload the new settings.

To exit any window in the program at any time, click on the [X] box in the upper-right corner of a window. *NOTE: If you click on the [x] box in the upper-right corner of the main Symetrix Access Control window you will close the Symetrix Access Control software immediately.*

If changes have been made to the system, and have not been saved, the window will display a “Save Changes” prompt, allowing you to save changes, quit *Symetrix Access Control* or cancel closing *Symetrix Access Control*

## 13.0 Window Management

At times an operator might find it necessary or advantageous to have several *Symetrix Access Control* menu item forms open at the same time. There are 5 tools to help in switching between open window forms.

- cascade windows
- tile windows vertically
- tile windows horizontally
- cycle windows

### 13.1 Cascading Windows

Cascading windows automatically takes all open windows and arranges them, one on top of another, with the title bars showing for each window.

To cascade all open windows, click on the Window -> Cascade pull-down menu option.

### 13.2 Tiling Windows Vertically

Tiling windows automatically takes all open window forms and arranges them, side-by-side, from left-to-right, filling the *Symetrix Access Control* window.

To tile all open windows, click on the Window -> Tile Vertically pull-down menu option.

The individual *Symetrix Access Control* forms will be organised in the *Symetrix Access Control* window side by side.

### 13.3 Tiling Windows Horizontally

Horizontally tiling windows automatically takes all open window forms and arranges them, side-by-side, from top-to-bottom, filling the *Symetrix Access Control* window.

To horizontally tile all open windows, click on the Window -> Tile Horizontally pull-down menu option.

The individual database windows will be organised in the *Symetrix Access Control* window one form on top of another.

## 14.0 Exiting the *Symetrix Access Control Software*

Perform the following step to exit the *Symetrix Access Control* software and return to the operating system. *NOTE: Exiting the Symetrix Access Control software does not halt operation of the access control network. The network operates based on all the information uploaded to the access control system hardware by the Symetrix Access Control software. The Symetrix Access Control software is only needed for making changes to the access control system, receiving access control events, and for real-time monitoring of network activity.*

1. Click on the File -> Exit pull-down menu. If any access control system changes have been made that have not been saved, the program will prompt the operator to either save changes, continue closing or cancel closing *Symetrix Access Control*. The *Symetrix Access Control* program will then shut down.

## 15.0 Adding and Editing System Managers

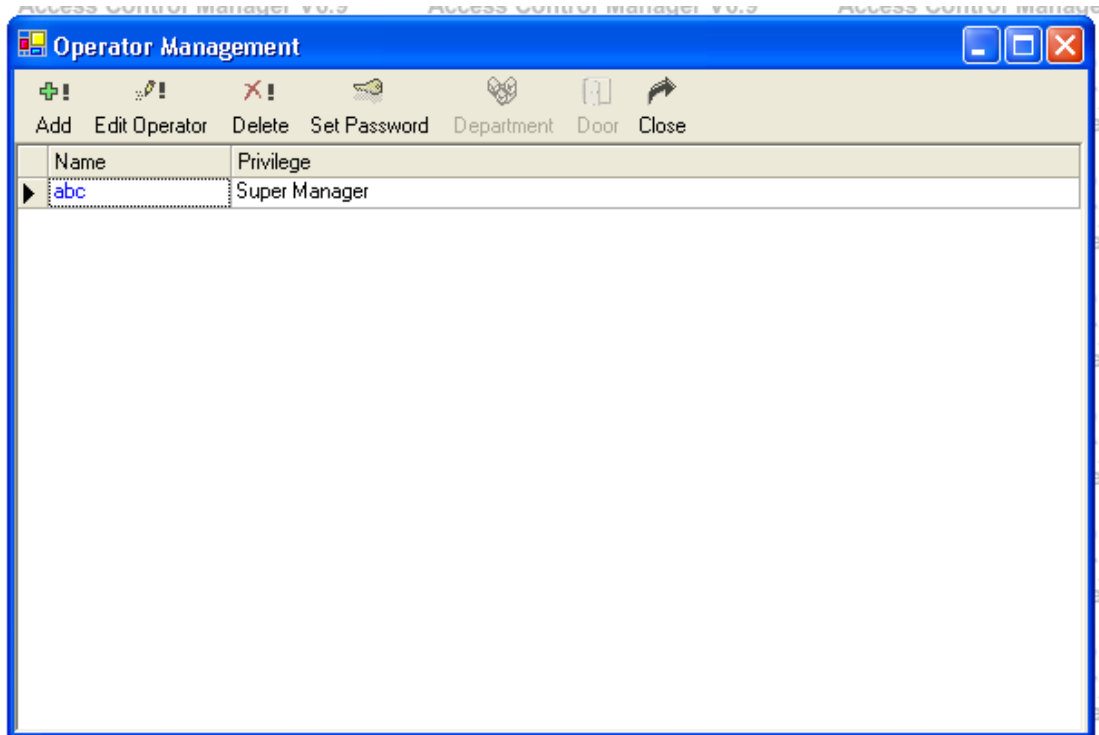
This section describes the process for creating system managers and assigning *Symetrix Access Control* privileges for system managers. System managers are the people who will be performing the work – creating and modifying users required by the *Symetrix Access Control* software to do its job and monitoring the access control system. Every operation performed by a system manager is logged in the system. This allows you to track changes performed by system managers throughout the life of the system.

The default System Manager is the system installer. The system installer is the initial user name and password entered when creating the access control database, and configuring the system.

**Since the default system installer account has access rights to every operation, anyone who knows the default system installer name and password will have complete programming access.**

**It is recommended that only the installation technician uses the system installer account to configure the access control system, and that System Manager accounts are created by the installer to allow restricted access to the system.**

Click on the Tools menu option, located on the top menu bar, and select the Operator Management sub menu item. The Operator Management window will appear. (see Figure 8).



**Figure 15 – Operator Management Window**

The Operator Management window will display a list of access control users that have been added that can administer the access control system.

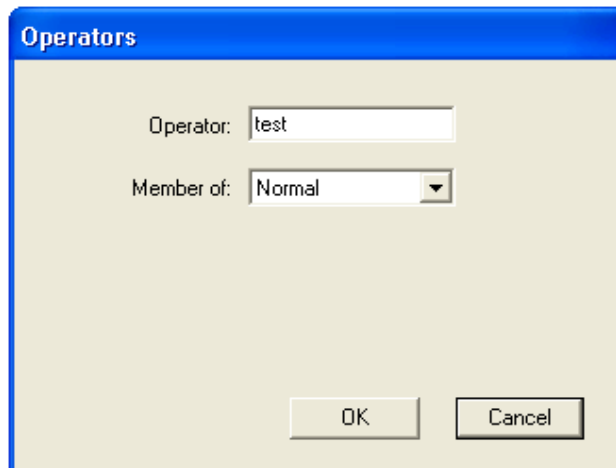
Do a little planning before assigning operator operation rights.

- Determine how many operators are needed to cover operation of the access control system
- Consider any time of day and day of the week requirements
- Determine the requirements and responsibilities of these operators.

## 15.1 Editing a System Managers Access Level

To edit a system manager, select an existing access control user by clicking the user entry in the search results panel, and then click on the Edit Operator button located at the top of the window.

Once completed, the Edit System Managers window will appear. (see Figure 9).



**Figure 15.1 - Edit System Managers Window**

The Edit Operator window allows you to change the login name, as well as the access level for the selected operator.

The following Access Levels (Member of) are available,

1. Normal – A normal operator can access and program only the doors allocated to them, as well as add, edit and delete users that are associated with the department allocated to them.

Normal users cannot upload changes to the connected access control panels, and normal users cannot add or edit further system managers.

2. Manager - A manager can access and program only the doors allocated to them, as well as add, edit and delete users that are associated with the department allocated to them.

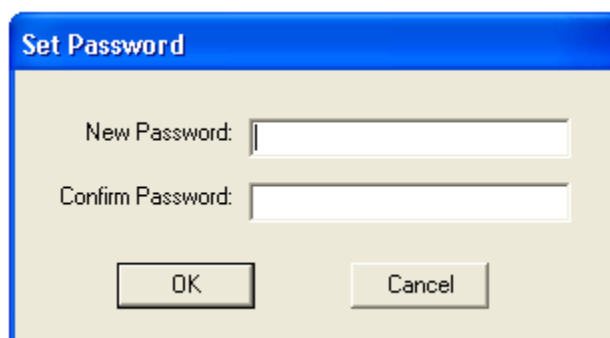
Managers can upload changes to connected access control panels, however cannot add or edit further system managers.

3. Super Manager – A super manager can access the system in its entirety. There are no limitations for Super Managers.

## 15.2 Editing a System Managers Password

To edit a system manager, select an existing access control user by clicking the user entry in the search results panel, and then click on the Set Password button located at the top of the window.

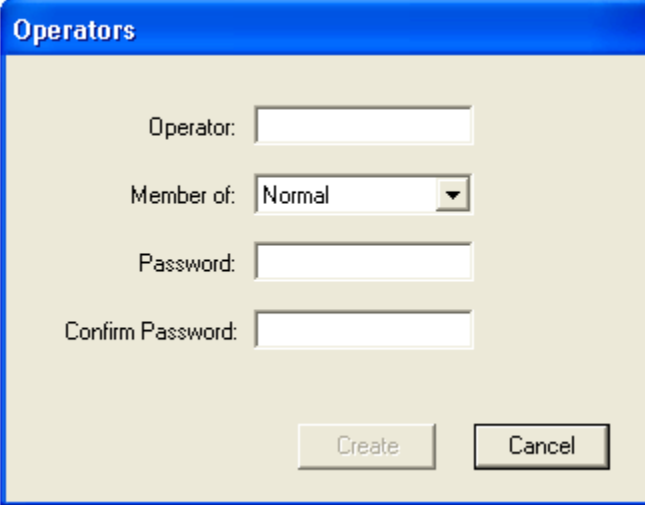
Once completed, the Edit Password window will appear. (see Figure 10).



**Figure 15.2 - Edit System Managers Password Window**

## 15.3 Adding a new System Manager

To add a new system manager, click on the Add button located at the top of the window. Once completed, the Add Manager window will appear. (see Figure 11).



The screenshot shows a window titled "Operators" with a blue header. It contains four input fields: "Operator:" (text box), "Member of:" (dropdown menu with "Normal" selected), "Password:" (text box), and "Confirm Password:" (text box). At the bottom, there are two buttons: "Create" and "Cancel".

**Figure 15.3 – Add new System Manager Window**

Enter the new System Managers Login name in the Operator field.  
Enter the new System Managers Password in both the Password and Confirm Password fields.  
Finally, select the required access level for the new System Manager by choosing one of the following options in the Member Of: field,

1. Normal – A normal operator can access and program only the doors allocated to them, as well as add, edit and delete users that are associated with the department allocated to them.

Normal users cannot upload changes to the connected access control panels, and normal users cannot add or edit further system managers.

2. Manager - A manager can access and program only the doors allocated to them, as well as add, edit and delete users that are associated with the department allocated to them.

Managers can upload changes to connected access control panels, however cannot add or edit further system managers.

3. Super Manager – A super manager can access the system in its entirety. There are no limitations for Super Managers.

## 15.4 Associating a System Manager with a Department

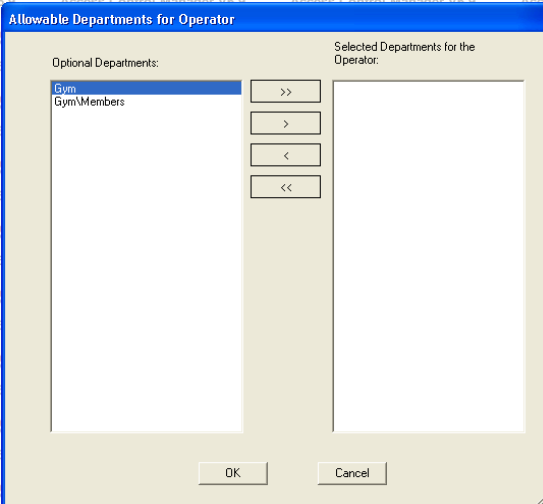
To allow a non Super Manager to access one or more departments (and associated users), the system manager must first be associated to the required department.

To add or edit the departments a system manager is allocated to, click on the Department button located at the top of the window.

Once completed, the Allowable Departments for Operator window will appear. (see Figure 12).

Select the required departments by clicking on the required department, and pressing the Right Arrow Button located in the middle of the form.

Finally, click the [OK] button to save any changes made.



The screenshot shows a window titled "Allowable Departments for Operator" with a blue header. It features two columns: "Optional Departments:" on the left and "Selected Departments for the Operator:" on the right. The left column contains a list with "Gym" and "Gym\Members". Between the columns are four arrow buttons: ">>", ">", "<", and "<<". At the bottom, there are "OK" and "Cancel" buttons.



## 15.5 Associating a System Manager with Doors

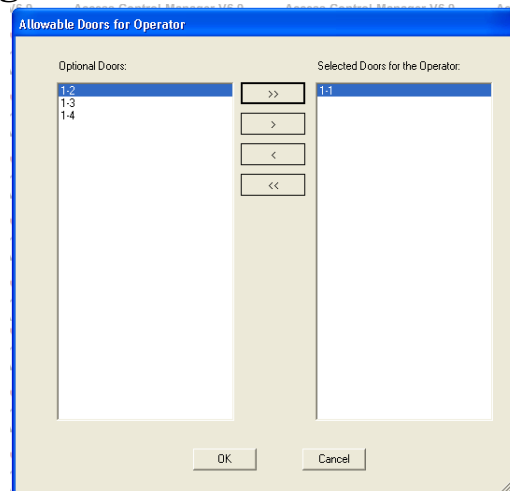
To allow a non Super Manager to access one or more doors, the system manager must first be associated to the required doors.

To add or edit the doors a system manager is allocated to, click on the Door button located at the top of the window.

Once completed, the Allowable Doors for Operator window will appear. (see Figure 12).

Select the required doors by clicking on the required door, and pressing the Right Arrow Button located in the middle of the form.

Finally, click the [OK] button to save any changes made.



## 16.0 Configuring Access Control Users

Each person to be granted access to secured areas will have assigned to them a proximity card, allowing the person to be identified by the access control system.

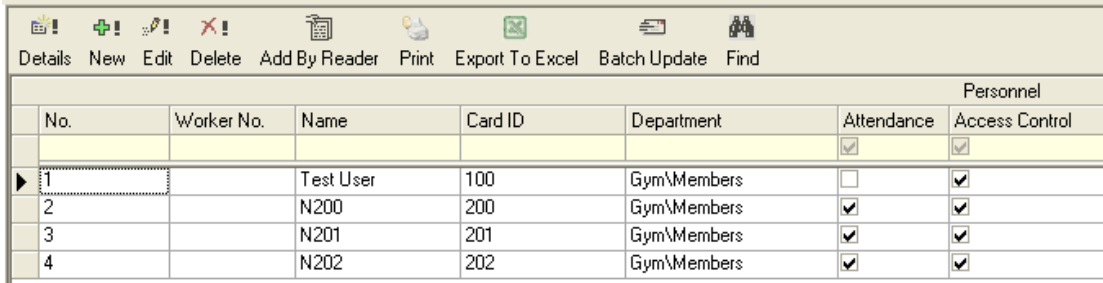
The “Personnel” form allows an operator to enrol (Add), void (Remove), and change proximity cards / Tags; assign proximity cards / Tags to users; and enter and edit user information, including personal information; and apply an access control schedule to users.

Consider the variety of access points for employees and customers, and consider special requirements such as janitorial, service/repair personnel (may require special access), supervisory/management staff (may require access to all areas), and shift personnel.

*NOTE: The program will not allow proximity cards with identical numbers to be enrolled. If you attempt to enrol a proximity card that has an identical internal number with a proximity card already enrolled, it will be rejected.*

### 16.1 Search Access Control Users Form

To open the “Personnel” access control users form, click on the “Personnel” Menu item located on the side menu bar of the main Symetrix Access Control Window. The “Personnel Access Control Users” form will be displayed, showing the current access control users configured. (see Figure 19-1).



The screenshot shows a software interface for managing access control users. At the top, there is a toolbar with icons for Details, New, Edit, Delete, Add By Reader, Print, Export To Excel, Batch Update, and Find. Below the toolbar is a table titled "Personnel" with the following columns: No., Worker No., Name, Card ID, Department, Attendance, and Access Control. The table contains four rows of data.

No.	Worker No.	Name	Card ID	Department	Attendance	Access Control
					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1		Test User	100	Gym\Members	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2		N200	200	Gym\Members	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3		N201	201	Gym\Members	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4		N202	202	Gym\Members	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 16-1 - Search Access Control Users

Select the User you wish to edit, or alternatively click on the [New] button located on the tool bar to open the “Edit Access Control User” form, allowing you to add a new access control user to the system. (see Figure 16-2).

## 16.2 Edit Access Control Users Form

The screenshot shows a 'User' dialog box with a blue title bar. It has two tabs: 'Main' (selected) and 'Others'. The 'Main' tab contains several input fields and checkboxes. The fields are: '\*User No.' with the value '1', 'Card ID' with the value '100', '\* Name' with the value 'Test User', 'Department' with a dropdown menu showing 'Gym\Members', '\* Required' (checkbox), 'Worker No.' (empty), 'Attendance' (checkbox), 'Access Control' (checked), and 'Deactivate' with a dropdown menu showing '2020-12-31'. There is a 'Photo' button next to the 'Card ID' field. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 16.2 - Edit Access Control Users

### 16.2.1 Edit Access Control User Fields

**User No:** The memory slot in the access control panel this user is currently occupying.

**Name:** The name that is displayed for reports. This usually does not include middle names, and suffix names.

**Card ID:** Displays the proximity card serial number for the proximity card issued to this access control user.

**Department:** Displays the department, division, or business group that the selected access control user belongs to, within the above company.

**Worker No :** An optional identification field or number that can be used to identify an access control user.

**Attendance Check box :** If checked, the Start and Finish times for the selected access control user will be logged for time attendance reporting.

**Access Control Check Box :** If checked, the access control functions for the selected user will be enabled.

**Deactivate:** Displays the date when this access control user will no longer have access to the system. This field is useful for issuing proximity cards to temporary staff such as casual workers, and contractual workers.

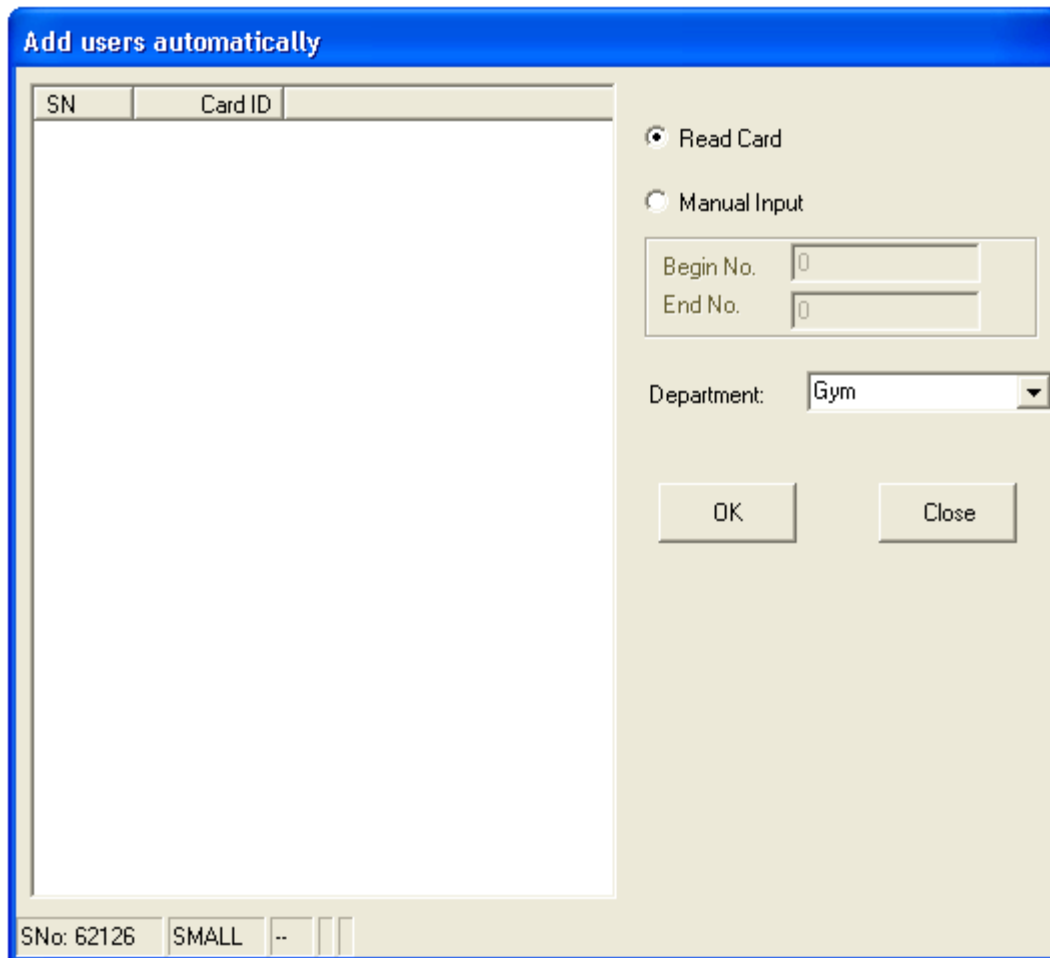
## 16.3 Adding a new Access Control Card using the Reader

When adding a new access control user, the easiest method to obtain the unique card id is to use the Add By Reader Function.

This feature allows you to swipe the card at one of the configured access control card readers, and add the user name, department, and other required information for the card to be added.

To add a new access control user card to the system,

- 1) Click on the [Add By Reader] button located on the top tool bar.
- 2) The software will prompt you for the access control reader to use.
- 3) Click on the [OK] button to use the default access control reader.
- 4) The Add Users Automatically form will be displayed.



**Figure 16.3 – Add Users Automatically Window**

- 5) Select the required Department you wish to allocate the new card / user to.
- 6) Ensure the Read Card option is selected
- 7) Swipe the required cards at the selected door card reader. The cards should be added automatically to the card list.
- 8) Once completed, click the [OK] button to continue.
- 9) The New cards will now be displayed in the Access Control Users Window.
- 10) Further information for the newly added access control users can be added by clicking on the selected user, and clicking on the [EDIT] tool bar button.

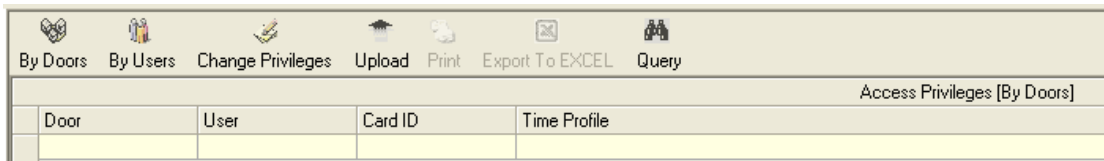
## 17.0 Edit Access Control User Privileges

Once you have added access control users to the system, you will need to grant or deny access to the doors configured in the system.

Without completing this step, the newly created access control user(s) will not be able to access any of the doors configured within the system.

### 17.1 View User Privileges Form

To open the “Access Privilege” access control users privileges form, click on the “Access Privilege” Menu item located on the side menu bar of the main Symetrix Access Control Window. The “User Privileges” form will be displayed, showing the current access control users and their privileges. (see Figure 20-1).



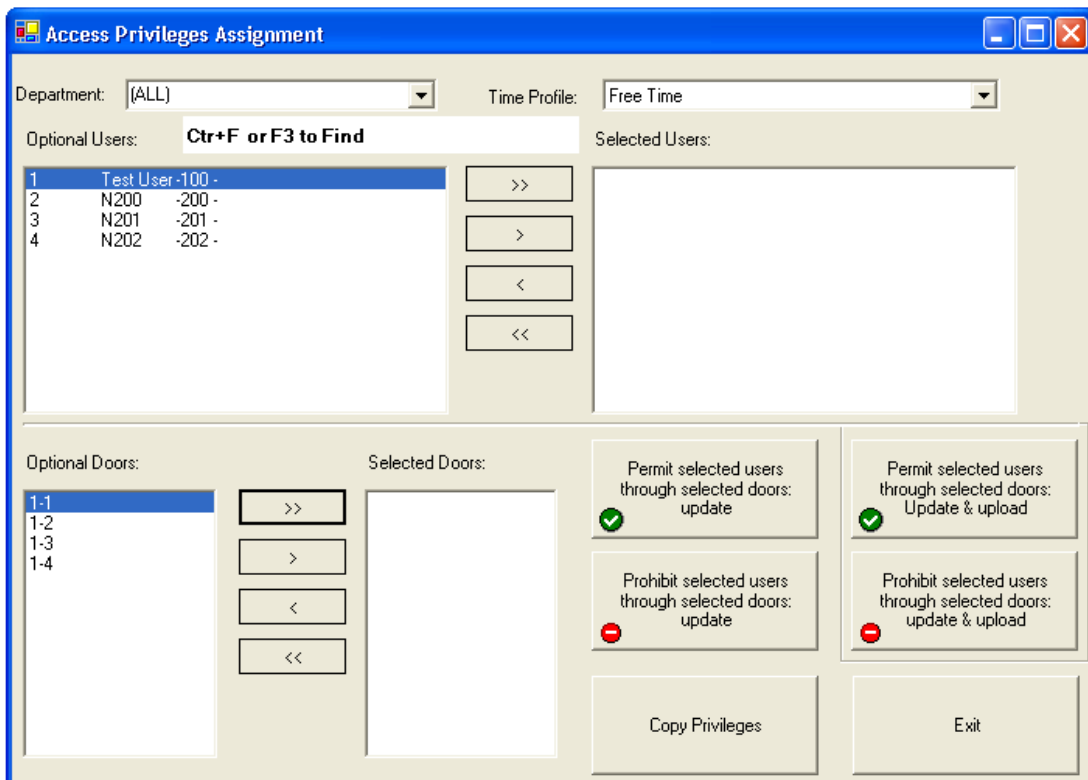
Door	User	Card ID	Time Profile

Figure 17-1 – User Privileges Window

To view what doors have users assigned to them (Door Based Report), click on the [By Doors] button located on the top window tool bar.

To View what users are allocated to what doors (User based report), click on the [By Users] button located on the window tool bar.

To edit User privileges, click on the [Change Privileges] button to open the edit privileges form. (see Figure 17-2).



Department: [ALL] Time Profile: Free Time

Optional Users: **Ctrl+F or F3 to Find**

1	Test User -100 -	>>
2	N200 -200 -	>
3	N201 -201 -	<
4	N202 -202 -	<<

Selected Users:

Optional Doors:

1-1	>>
1-2	>
1-3	<
1-4	<<

Selected Doors:

Permit selected users through selected doors: update

Permit selected users through selected doors: Update & upload

Prohibit selected users through selected doors: update

Prohibit selected users through selected doors: update & upload

Copy Privileges Exit

Figure 17.2 - Edit Access Control Privileges Window

To grant one or more users access to one or more doors,

- 1) Click on the user you wish to change access privileges for on the left hand side of the window.
- 2) Click on the [RIGHT] arrow button to move the selected user to the right hand side of the screen, (Selected Users)
- 3) Continue with Steps 1) and 2) until all the required users that you wish to change access privileges for have been moved to the right hand side of the screen. (Selected Users)
- 4) Click on the Door you wish to Grant or Deny Access to, on the left hand side of the screen,
- 5) Click on the [RIGHT] arrow button to move the selected door to the Right hand side of the screen (Selected Doors).
- 6) Continue with steps 4) and 5) until all the required doors that you wish to Grant or Deny access to have been selected.
- 7) If you wish to limit user access through the selected doors via an access schedule, select the required schedule from the Time Profile: drop down list at the top of the window.
- 8) Finally, if you wish to grant the selected users access to the selected doors, click on the [Permit selected users through selected doors: Update and Upload] button.
- 9) If you wish to deny the selected users access to the selected doors, click on the [Prohibit selected users through selected doors: Update and Upload] button.

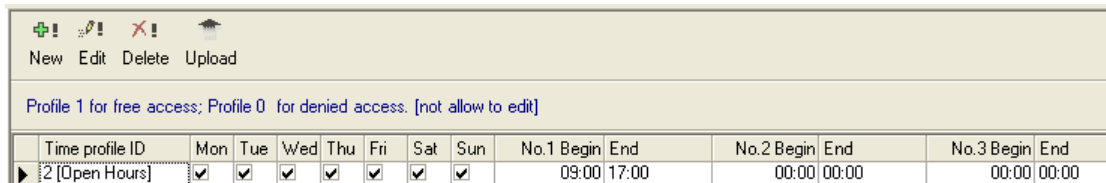
The access control software will now upload the user privileges for the selected user, to the access control panels connected to the system.

## 18.0 Edit Access Control Schedules

The edit access control schedules form allows defining the normal operation days and holiday / weekend access time periods to be applied to access control users. An access control schedule is defined as the hours-of-the-day when a user group is granted access to a secure area. Multiple access control user group schedules can be defined, with each schedule consisting of a separate start/stop period for normal operation days, as well as weekends / holidays. This provides an incredible amount of flexibility in setting time zone work schedules for the users using the access control system. Before defining access control schedules, take some time and map out all the schedule usage possibilities for the site. Consider the variety of access hours for employees and customers, and consider special requirements such as janitorial personnel (may require night access), service/repair personnel (may require all hours access), supervisory/management staff (may require extended hours access), and shift personnel (first/day, second/swing, third/grave, flex). *NOTE: All time values used and stored by the Symetrix Access Control software are in 24-hour format. For example: midnight is stored as 00:00 hours, 8 A.M. is stored as 08:00 hours, noon is stored as 12:00 hours, 6 P.M. is stored as 18:00 hours, and 11:30 P.M. is stored as 23:30 hours.*

### 18.1 View Access Control Schedule Form

To open the access control schedule form, click on “Access Control → Time Profile” Menu item located on the side menu bar. The “Edit Access Control Schedule” form, will be displayed, allowing you to create and change the various access control schedules entered in the system. (see Figure 18.1).



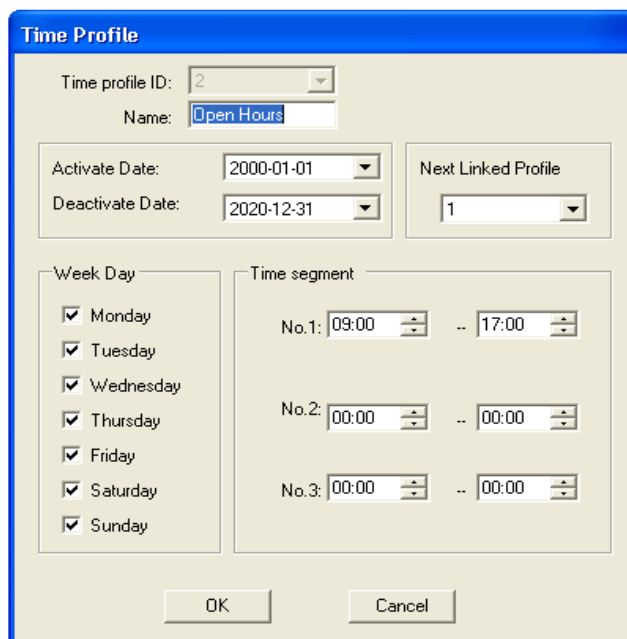
Time profile ID	Mon	Tue	Wed	Thu	Fri	Sat	Sun	No.1 Begin	End	No.2 Begin	End	No.3 Begin	End
2 [Open Hours]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	09:00	17:00	00:00	00:00	00:00	00:00

Figure 18.1 - View Access Control Schedules

Select the Schedule you wish to edit, or alternatively click on the [New] button located on the tool bar to open the “Edit Access Control Schedule” form, allowing you to add a new access control schedule to the system.

#### 18.1.1 Edit an Access Control Schedule

The Edit Access Control Schedule form contains a number of configurable fields for defining an access control schedule.



**Time Profile**

Time profile ID: 2  
 Name: Open Hours

Activate Date: 2000-01-01  
 Deactivate Date: 2020-12-31  
 Next Linked Profile: 1

Week Day

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

Time segment

No.1: 09:00 .. 17:00  
 No.2: 00:00 .. 00:00  
 No.3: 00:00 .. 00:00

OK Cancel

**Time Profile ID :** This is the unique number associated with the access control schedule.

**Name :** This is the name for the access control schedule. It is recommended that you choose a name that is easy to understand, for example business hour for typical 9am to 5pm Monday to Friday Schedules.

**Activate Date :** This section of the form allows you to determine from what date the access control schedule will become active. Setting this date in the past will automatically make the schedule active.

**Deactivate Date :** This section of the form allows you to determine at what date the access control schedule will no longer function. If this schedule will never expire, it is recommended that this date be set in the distant future.

**Linked Profile :** Set this Number to 1 to enable access to the system during the selected schedule time, otherwise set this value to 0 if you wish to disable access to the system during the selected schedule time.

**Week Day :** Check the Days of the Week you wish this schedule to be active.

**Time Segment – No1 :** Enter the schedule start and end times for when the schedule will commence and cease for the selected Week Days.



## 19.0 Symetrix Access Control System Log Report

The Symetrix Access Control System Log Report Form allows system managers and installers to search for and view in detail, access control events, and log information that have occurred either during a selected period, or for a particular department / user.

Once a report has been generated, it can then be printed, or exported as a Microsoft Excel worksheet.

To open the access control event report form, click on “Query Card Records” Menu item located on the side menu bar of the main Symetrix Access Control Window. The “Access Control System Log Report” form will be displayed. (see Figure 19).

ID	Card ID	Worker No.	Users	Department	Date/Time	Address	Allowable	Description
21	22235878				15/11/2010 12:13:08 P	1-2[n]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
20	22235878				15/11/2010 12:13:00 P	1-3[n]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
19	22235878				15/11/2010 12:12:58 P	1-3[n]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
18	22235878				15/11/2010 12:11:48 P	1-3[n]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
17	22235878				15/11/2010 12:11:46 P	1-3[n]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
16	22235878				15/11/2010 12:11:04 P	1-3[n]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
15	3106993				15/11/2010 11:30:40 A	1-3[n]	<input checked="" type="checkbox"/>	Allowable Access
14	3106993				15/11/2010 11:30:36 A	1-3[n]	<input checked="" type="checkbox"/>	Allowable Access
13	3106993				15/11/2010 11:21:56 A	1-3[n]	<input checked="" type="checkbox"/>	Allowable Access
12	3106993				15/11/2010 11:21:48 A	1-3[n]	<input checked="" type="checkbox"/>	Allowable Access
11	3106993				15/11/2010 11:14:42 A	1-3[n]	<input checked="" type="checkbox"/>	Allowable Access
10	10222864				27/10/2010 5:45:12 P	1-1600001[Exit]	<input checked="" type="checkbox"/>	Allowable Access
9	10222864				27/10/2010 5:42:58 P	1-1600001[Exit]	<input checked="" type="checkbox"/>	Allowable Access
8	10222864				27/10/2010 5:42:48 P	1-1600001[Exit]	<input checked="" type="checkbox"/>	Allowable Access
7	10222864				27/10/2010 5:42:20 P	1-1600001[Exit]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
6	10222864				27/10/2010 5:42:06 P	1-1600001[Exit]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
5	5142172		N200	Gym\Members	27/10/2010 5:31:08 P	1-1600001[Innie]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
4	22235878		Test User	Gym\Members	27/10/2010 5:29:38 P	1-2600001[In]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
3	10222864				27/10/2010 5:27:12 P	1-1600001[Exit]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
2	5142172		N200	Gym\Members	27/10/2010 5:21:42 P	1-1600001[Innie]	<input type="checkbox"/>	Denied Access-No PRIVILEGE
1	5142172		N200	Gym\Members	27/10/2010 5:21:24 P	1-1600001[Innie]	<input type="checkbox"/>	Denied Access-No PRIVILEGE

**Figure 19 - Access Control Log Report**

Select the start date for the report that you wish to generate. The start date is the first day of access control events that you wish to include in your report.

Next, select the report end date for the report you wish to generate. The end date is the last day of access control events that you wish to include in your report.

Finally, click on the [REFRESH] button to generate your report.

The Symetrix Access Control software will connect to all the configured access control panels, and will check for any new information that may be available, since the last time an event report had been generated.

This may take some time, so it is important to be patient. A progress bar will be displayed at the top of the report, indicating an estimated time of completion for this process.

Once any new information has been obtained from the access control panels, the system will then generate your report, using the criteria entered.

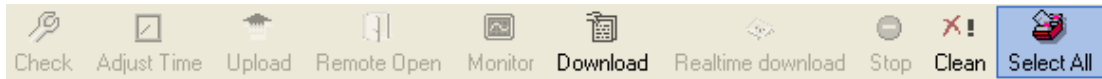
Once completed, Symetrix Access Control will then display the report, in a printable report format.

## 19.1 Downloading Records from the Access Control Panels

Before attempting to generate an access control report, it is highly recommended that you first download the latest access control log information from the access control panels.

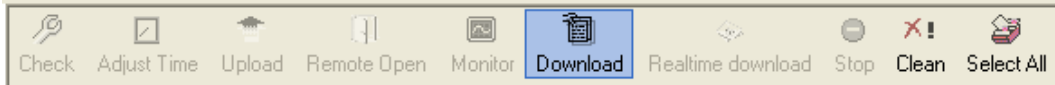
To do this,

- 1) Click on the “Download” menu item located on the side menu bar of the main Symetrix Access Control Window.
- 2) The Download panel log screen will be displayed.
- 3) Click on the Select All button on the tool bar



This will highlight all the available access control panels for your system.

- 4) Click on the Download button on the toolbar.



- 5) The software will now prompt you if you wish to proceed with the download.
- 6) Click on the [YES] button to begin downloading the latest event information from the access control panel.
- 7) Once the download has completed, you can continue on to the next step of creating your access control

## 19.2 Creating a User Based Access Control Report

A user based report is suitable when you wish to ascertain when, and how many times a person or a department has accessed one or more doors.

Typically, this style of report does not require a date range to be specified, but rather it requires access to all the records available in the system.

To create a User / Department style report.

- 1) Select "First Event" in the FROM field.
- 2) Select "Last Event" in the TO field.
- 3) If required, select the desired department for the report by clicking on the department drop down, and selecting a department.
- 4) Select the desired Person / User that you wish to view the report for, by clicking on the User field, and selecting the required user / card.
- 5) Click on the Query button to begin executing the query, and view the results.

## 19.3 Creating a Date / Time Based Access Control Report

A date / time based report is suitable when you wish to who has accessed the system during a selected date and time range.

This style of report requires a date range to be specified, and optionally can be further filtered by specifying a particular department or even user if required.

To create a Date / Time style report.

- 1) Select "Event Time" in the FROM field.
- 2) Select "Event Time" in the TO field.
- 3) Select the required start date for the report by clicking on the FROM Date field. Once you have clicked this field, a calendar date selection box will be displayed.
- 4) Select the required start date for the report by clicking on the FROM Date field. Once you have clicked this field, a calendar date selection box will be displayed.
- 5) If required, select the desired department for the report by clicking on the department drop down, and selecting a department, otherwise leave this field as ALL.
- 6) If required, select the desired user that you wish to limit this report to.  
If you do not wish to limit this report to a single user, leave this field as ALL.
- 7) Click on the Query button to begin executing the query, and view the results.

The screenshot shows a software interface with a toolbar at the top containing icons for Query, Print, Export To Excel, Save Layout, and Restore Default Layout. Below the toolbar, there are several filter fields: FROM: Event Time (dropdown), 2011-05-04 (calendar), 12:00:00 AM (time); To: Event Time (dropdown), 2011-07-26 (calendar), 11:59:59 PM (time); Department: (ALL) (dropdown); and User: (ALL) (dropdown). To the right of these fields is an 'Addr:' section with a list of checkboxes:  (ALL),  1-1[In],  1-2[In], and  1-3[In].

Set the FROM field to You can change the displayed format by changing the “View Report As” option located on the side panel. Options include “Printable report” and “Sortable Item Table”.

You can also print your newly created report by clicking the [PRINT] button located on the tool bar. Clicking this button will open the Windows “Print” Dialogue box, allowing you to specify which printer you wish to use, as well as configure other printer options for your report.

## 20.0 System Maintenance

To provide the best long-term operating conditions for the *Symetrix Access Control* software, there are two system maintenance steps that should be performed.

- Secure storage of the *Symetrix Access Control* program CD-ROM.
- Periodic backup of the *Symetrix Access Control* database.

### 20.1 Secure Storage of Program CD-ROM

The original *Symetrix Access Control* installation CD-ROM should be stored in a safe, secure place away from environmental extremes. Safe, secure storage is not just for the sake of software reinstallation should there be a host computer system crash, but to keep the software out of the hands of unauthorised personnel. Using the installation CD-ROM, it is possible for an unauthorised person to reinstall the *Symetrix Access Control* software on a non-secure machine.

### 20.2 Periodic Database Backup

The *Symetrix Access Control* access control database should be backed-up periodically. The more often the system is backed-up, the less data reconstruction will need to be done in the event of a host computer system crash. Unless otherwise specified, the default database is located in the following directory.

C:/Program Files/iCCard/iCCard.mdb

# Glossary

**Access Control** – Access control is a general term describing the management of the entrance and exit of people through secure areas.

**Access Control Network** – An access control network is an interconnected set of access control panels, door controllers, card readers and keypads that manage the entrance and exit of people through secure areas.

**Access Control Panel** – An access control panel is a microprocessor based circuit board and panel that manages access to a secure area. The access control panel receives information from door controllers that it uses to determine through which doors and at what times users are granted access to that secure area. Based on that information, the access control panel can lock/ unlock doors, sound alarms, and communicate status to a networked computer.

**Address** – Each controller must be assigned a unique address, identifying that controller in the network. A controller address is similar to a home address. By addressing an envelope, mail is sent to a specific individual at a specific home. By assigning unique controller addresses, operating information can be sent directly to specific controllers.

**Amnesty** – Amnesty allows a card/user to violate anti pass back rules and re-enter a secure area that a controller has tracked as having already been entered by that card/user. (See **anti pass back**.)

**Anti pass back** – Anti pass back (APB) provides one-card one-way access into and out of a secure area. It prevents someone from using a card to enter a secure area and then passing that card back to someone else to use to enter that same secure area. APB – See **anti pass back**.

**Aspect ratio** – The aspect ratio is a scaling number based on the height versus width of a graphic. When resizing graphics, as the height changes, the width changes a corresponding amount maintaining the aspect ratio. This ensures the graphic appears correct regardless of the new size of the graphic.

**Auto-collection** – Auto-collection allows the host computer to automatically receive event information from the controller's event buffer, when the controller's buffer becomes full.

**Card** – A card is an access control identification device assigned to an individual to give that individual access rights to an access control network. It typically is the size of a credit card. Each card has a unique identification code. That identification code is then associated with an access control user to determine through which doors and at what times a card holder is granted access.

**Card PIN** – The Card PIN (Personal Identification Number) is a special number automatically generated and assigned to a card during enrolment when the card + PIN feature has been enabled. This feature is only available when used in conjunction with an SIS Keypad and Card Reader Module. This PIN allows a secondary verification of a user by requiring a PIN be entered after presenting a valid access card. The Card PIN cannot be changed or edited and must be given to the user with the card.

**Card number** – The card number is the 26 Bit Wiegand ID for the access control card or tag.

**Card holder** – A card holder is an individual who has been assigned an access control card or tag. (See **user**.)

**Check Box** – Check Boxes are used whenever a program command has a can be enabled or disabled. As a system manager clicks on the check box a tick is displayed if the option has been enabled, or the box is empty if the option has been disabled.

**Collecting events** – Collecting events from all controllers clears the controller buffers and stores the events in the *Symetrix Access Control Database*. Event data can then be processed and exported as a report in many different formats. Collection of events can take place while exporting a system log report, or by using the access control monitor software.

**Database** – A database is an organised set of information.

**Department group** – A department group is an operator assigned field in the user database. It is not actively used by the *Symetrix Access Control* software, but is provided to allow an operator to sort the users within the database based on the department for which they work.

**Desktop** – The desktop is the primary window in the Windows operating system, from which programs are started.

**Dialogue box** – A dialogue box is a text window that the *Symetrix Access Control* software displays on screen when the software needs information from a system manager or installer. The system manager enters the information by reading the instructions in the window and then filling-in-the-blanks in designated fields in the window.

**Door name** – An operator can assign a descriptive name to a door on the access control system.

**Download** – Downloading is the process by which the host computer receives information from the access control network; information is downloaded to the host computer. (See **upload**.)

**Dual verification** – The use of two credentials to gain access into a secure area.

**Egress** – Egress is a term for exiting a secured area. (See **ingress**.)

**Enrol** – Enrolling is the process of activating a card for use by a user in the access control network. A card must be entered into the access control network and then assigned to a user.

**Event** – An event is an occurrence at a controller (such as unlocking a door, requesting to exit, forcing a door open) that generates a message stored by the controller.

**Export file type** – The selection of the archive file type determines how event files will be saved, archived or exported.

**Firmware** – Firmware is a set of operating instructions for a controller, stored on a ROM on the controller.

**General protection fault** – A general protection fault (GPF) occurs whenever a program executes a command that the operating system considers dangerous to the operating system. When a GPF is generated, the program that generated the GPF is closed and control is returned to the operating system.

**Global secure** – Global secure allows an operator to set a time of day at which all doors that are not under automatic control (i.e. controlled by an unlock/lock time zone) are locked.

**Global unlock** – Global unlock is a feature that designates a specific input on the access control panel that is used to automatically unlock all doors in the access control network.

**Ingress** – Ingress is a term for entering a secured area. (See **egress**.)

**Input** – An input is a set of points on a controller that is able to receive a signal indicating when an external device changes state. For example, the door switch input on the controller is attached to a switch on the door. Using the switch, the input is able to keep track of when the door is opened or closed; when the switch is open, the door is open and when the switch is closed, the door is closed.

**Log on** – Log on is the process by which an operator enters a name and a password that identifies that system manager to the *Symetrix Access Control* program. This identification is used by *Symetrix Access Control* to limit menu options a system manager is authorised to access, as well as tracking operations performed by the system manager.

**Manager** – See **System Manager**

**Menu bar** – A menu bar is a horizontal field near the top of a program window of a program operating in a Windows operating system that allows a program operator to select program commands and options.

**Monitor** – A monitor is a window within the *Symetrix Access Control* software that tracks events that are occurring on the access control system as they happen.

**Multiple sites** – See **site**.

**Network computer** – The host computer is the computer running the *Symetrix Access Control* software and communicating with the access control network.

**Off-line** – The access control network is off-line when it is not actively communicating with the host computer.

**Online** – The access control network is online when it is actively communicating with a network computer.

**Online help** – Online help is a mini-program within the *Symetrix Access Control* software that provides basic descriptions and instructions for the *Symetrix Access Control* software. Online help can be run at the same time as the *Symetrix Access Control* program, side-by-side, making it easier for an operator to receive basic information regarding a program command or operation.

**Output** – An output is a relay on a controller that is toggled, to open or close an external circuit based on either commands programmed into the access control panel or based on the state of an input. For example, if a door is forced open, an output relay is programmed to sound an alarm.

**Personal identification number** – A personal identification number is a means of providing an extra level of security. Pins may be assigned to a user by a system manager, allowing some users to access a secured area using either / or a card and or PIN.

**PIN** – An acronym for personal identification number (see **personal identification number**).

**Proximity card** – See **card**.

**Proximity tag** – See **tag**.

**Pull-down menu** –When an operator clicks on an option on the menu bar, a pull-down menu appears listing all the available options for that menu selection. An operator then selects the desired operation.

**Push to exit** – Push to Exit (PTE) is an input on the door controller that accepts a signal from a normally open input device. The signal indicates a request has been made by someone to exit a secured door.

**Radio button** – Radio buttons are used whenever a program command has a set of options that require the selection of one and only one option. As an operator clicks on the radio buttons within an option set, the old selection is disabled and the new selection is enabled.

**Reader** – A reader is a device that "reads" an identification number from a card or tag presented to the reader by a user. It then sends that identification number to the controller for processing.

**Report** – A report is a summary of event information generated from the event log collected from all controllers on the access control network. A report may be displayed on the computer system screen, printed at a local printer, or exported using various formats for processing by another program.

**Request to exit** – see **push to exit**

**RFID card** – See **card**.

**RFID tag** – See **tag**.

**ROM** – A ROM is a memory device on the access control panel that permanently stores instructions and information. ROM stands for Read Only Memory, referring to the fact that information can only be read from the device. Information cannot be changed unless the device itself is replaced.

**RTE** – See **push to exit**.

**Schedule** – A Schedule is a definition of the time-of-day and the days-of-the-week when a user may be granted access to a secure area.

**Shortcut** – A shortcut is a command that directs a program to begin. Typically shortcuts are associated with icons placed on the Windows desktop, i.e. clicking on the *Symetrix Access Control* icon starts the *Symetrix Access Control* program.

**Site** – A site is another term for an access control network. Site is generally used when there is more than one access control network that is managed from one network computer. The *Symetrix Access Control* software installed on the network computer keeps track of the different access control networks by assigning each one a site.

**Spreadsheet** – A spreadsheet is an organised collection of information managed in a matrix format.

**System Manager** – A system manager is an individual who has been granted the authority to perform certain *Symetrix Access Control* program managerial operations.

**Tag** – A tag is an access control identification device assigned to an individual to give that individual access rights to an access control network. A tag is designed to be attached to a key ring. Each tag has a unique identification code. That identification code is then associated with an access group to determine through which doors and at what times users are granted access.

**Temp users** – The temp users feature allows an operator to set a future date and time for activation and expiration of an access control user.

**Timer event** – The timer events are usually used to automatically unlock and then lock selected doors based on when the time-of-day when the timer event begins and ends. When the time event begins, the selected doors are unlocked; when the timer event ends, the selected doors are locked.

**Tool bar** – The tool bar is a set of buttons in a horizontal field beneath the menu bar, made up of shortcuts to the commonly used *Symetrix Access Control* program features.

**Upload** – Uploading is the process by which the access control network receives information from the host computer; information is uploaded to the access control network. (See download).

**User data file export** –The user data file export feature allows a systems integration expert to export then import selected and limited user data to/from an external application (such as Excel™ or some similar spreadsheet or database program).