

# ***Access Central Software***

Access Central is comprised of three programs. All programs and system parameter files must reside in the following subdirectory: "C:\tc85dir".

## **1. ACCESS CENTRAL.MDB**

This is a Microsoft Access Application called *Access Central*. All day-to-day programming and system maintenance is performed with this program. It resides in your TC85DIR subdirectory and loads when you click the Access Central.MDB shortcut icon on your Windows Desktop.

Note: The setup program places the Access Central.mdb icon on your Windows Desktop. If your Desktop is a personal Desktop and not the actual Windows Desktop (c:\windows\desktop), you must move the icon to the Desktop you are using.

## **2. LOG.MDB**

This is a Microsoft Access application called Report Manager, and you can run it any time you need activity reports. To insure that your reports contain the most up-to-date transaction data, always begin by pressing the Refresh Button. This brings all data from the large transaction log file into the Microsoft Access environment. The amount of time it takes to bring this data in depends on the size of your log file (tclog.dta), and the speed of your computer. *Note: If you get an error when refreshing data, it usually means that no new transactions have occurred since the last refresh.*

## **3. ACCESS-ONLINE**

This is the background communication utility that controls all the access control system field devices, and makes the actual decisions to grant or deny access. It runs in RAM memory so that it can respond instantly to all field events. Because it resides in RAM memory, it is fast and can unlock a door in less than 70 milliseconds when a card is presented. It responds to alarm events with the same speed. When you run this program from the Access Central Welcome Screen, it will load on your Windows Task Bar. You must keep this program running at all times, and you must be certain that you have only one ACCESS-ONLINE icon on your Task Bar.

It is highly recommended that you start ACCESS-ONLINE automatically when your computer boots up, this way if power should fail to your computer, the Access Control System will restart without human intervention. To do this, go to Explorer, and copy the PC.BAT shortcut in the c:\tc85dir folder to your Windows StartUp folder:

**C:\WINDOWS\START MENU\PROGRAMS\STARTUP**

# ***Access Central For Windows 95/98***

Microsoft Access version 97 or higher must be pre-installed on your computer. Access Central will not execute without it.

Access Central will continue to ship as a Microsoft Access 97 application for the foreseeable future. Customers wishing to run Access Central with Access 2000 must do the following:

1. Install the software according to the instructions so that Access Central.mdb, and Log.mdb are located in the subdirectory called: c:\tc85dir
2. Double click Access Central.mdb from Windows Explorer. You will be asked if you want to convert the file. Say yes, and accept the default name. Be sure the path of the new file is C:\tc85dir\??
3. Rename Access Central.mdb to: Access Central97.mdb
4. Rename the converted file to: Access Central.mdb

Follow the same procedure to convert Log.mdb (using appropriate file names)

## **Converting Existing Systems**

You can program a new version of Access Central from older Toye systems. Use the Programming

Utilities/Data Import Utilities features to do so.

## **Tool Bar Buttons**

ToolBar buttons are provided for quick access to the most frequently used functions. The function of each button will display when you place the cursor over the button.

## **Real Time Events Button**

When you click this button, a Dynamic Display of incoming card and alarm events will be displayed as they occur. You can click on an incoming cardholder's name to jump to that cardholder's database record (except Tenant Billing) . You can also filter all records to show just the transactions of one cardholder by highlighting the name, right mouse click, and select filter by selection. You can also change the display order to anything you want, and remove the filter with another right mouse click.

*Note: Only system transactions that occur while Real Time Events is open will be displayed. If you close this window using the exit button, and then reopen it, the transactions that occurred while it was closed will not be available for display. They will still be on the master log for reports. If you want to insure that the Real Time Events window reflects all transactions, just leave it minimized on your task bar.*

The following are special **Status Codes**status codes that indicate each type of transaction exception:

- A** Hard Anti-Pass-Back violation, no access granted
- a** Soft Anti-Pass-Back violation, access was granted
- s** Wrong system code, access was not granted
- Invalid card, access was not granted
- k** Keypad violation, access was not granted
- \*** **Alarm**
- N** Hard Nesting violation
- D** Debit card violation (out of uses)

Transactions without one of the above symbols are valid card transactions which do not involve exceptions.

## **Menu Button**

Displays the Main Switchboard Menu.

## **Cards Button**

Displays the Cardholder Database.

## **Binoculars Button**

When you click in any field (except cardholder memory number), you can search for any other record.

## **Manual Button**

Displays the entire contents of the Software Instruction Manual. You can use keyword search to locate the topics you want to find.

## **Unlock Button**

This function provides instantaneous release of any door or gate. A beep indicates that the unlock message was transmitted.

## **Locate Button**

Use this button to locate the owner of a vehicle

## **About Button**

Shows the configuration parameters of your system.

## **Report Manager Button**

This button takes you to another Microsoft Access Database named log.mdb. All system transactions are

stored in a large file named: tlog.dta. When you press the Refresh button, you are actually copying all the data from tlog.dta into the Microsoft Access environment.

### **Alarm Button**

Acknowledges Alarms that have been programmed for audible annunciation.

### **Background Print Button**

For line at a time Real Time Event printing on a dot matrix printer

## **MAIN MENU ITEMS**

Following is a description of all Menu Items. Most choices are self-explanatory, and when not, the Form for that function normally provides more detail.

### **Cardholder Records**

To program a card, you must minimally enter a name, a valid card memory number (which may differ from the number shown on the outside of the card), and a security level assignment. Once entered, you can program the card by clicking on the PROGRAM THIS CARD button. Only those levels displayed will be programmed. *Note: Do not use the apostrophe character when entering names. Use a space instead of an apostrophe, otherwise an error will occur while scrolling through transactions.*

If you make a mistake and generate error messages, just hit the Escape Key and start over.

You can change the TAB order of your form so that the cursor jumps only to the fields you wish to populate with data. To do this, select FORM DESIGN from the View Menu, and then select Tab Order.

To delete a record, you must first program that cardholder out of the system. Type VOID in the box provided, and Program This Card. Now the number is safely out of the system, and you can delete the record by using the "Record Selector Bar" that runs vertically along the left side of the record.

Note about searching records: The cardholder record form contains subforms for entering vehicles and security levels. These subforms reflect only the information about that particular record. So if you use the search utility in either subform, you will be seeking information pertaining only to that record. If you want to find a cardholder's record based on a license plate number, you must use the Locate Toolbar button.

You cannot search in the Memory Number field. If you need to locate a record using the Memory Number as the search criteria, you must press the *Open Report Of Search For Another Record* button provided on the Cardholder form.

### **Open Report Or Search For Another Record**

You can view the cardholder data in a columnar format. You can change the order of the displayed records, and you can filter records to be displayed by highlighting any value. If you want to display all cardholders currently programmed into level 5, just highlight the 5, and do a filter by selection (right click). *Microsoft Access* provides many tools for searching, filtering, and displaying data. Most of these capabilities can be explored without reading any manuals. Just click help, and enter a topic.

You can quickly locate a record by clicking in either the name or number field. Use the binoculars to enter the record you want. Once you've found the record, simply double click the record, and the cardholder's full record will be displayed.

### **Nine Digit Social Security Number Systems***Nine Digit Social Security Number Systems Only*

There is a special version of our **Access Central** Interface for nine digit systems. To enroll cardholders, you must begin by entering a nine digit number. The first record is a sample record, but you may type over the sample information to enroll your first cardholder. At the bottom of the record there is a field called: Internal Memory Location. You will notice that this number increases consecutively as you add new

records. Each system is specifically configured for a certain number of cardholders, and you can see what that capacity is by clicking on the ABOUT button. You must not attempt to enter records that exceed this capacity.

At any time, you may reuse a memory location previously occupied by a voided card. To void a cardholder, simply type the word VOID, and click the PROGRAM THIS CARD button. Now you may enter a new cardholder into this Internal Memory Location. Be sure to remove the word VOID, and be sure to reassign new levels to the new cardholder.

#### *Note to Johnson Controls Metasys Metasys Users With Nine Digit Systems*

The Internal Memory Location Number located at the bottom of each record is the decimal number that will be reported to Metasys. When you program this number into the PMI software, it will become available for Metasys-wide reports, Process Groups, and HVAC Interlocks.

#### **Make I.D. Badge**

Because *Microsoft Access* supports linked or embedded photos, the ability to include photographs in the database or to create a first quality photo I.D. card is virtually a free bonus of the system. You may use any low cost consumer digital camera such as the Casio QV-10A.

You may place a photo onto the cardholder form using any of three methods. You can create a link (BMP or PCX files only) to an existing photo, you may copy a photo image from your application into the Windows clipboard and paste it, or you may drag and drop a photo from your photo imaging application. To make the choice, simply right mouse click the photo area of the form.

Which ever method you use, the original size of the photo is not important since *Access* will re-size it to fit the I.D. badge form provided the proportions of the photo showing just head and shoulders is maintained for each image. If the photos you take are not confined to a portrait showing only head and shoulders, you can rotate and crop the image in your application, then copy and paste it into your cardholder database.

There are two ways to make a badge; print directly on the surface of a plastic I.D. card using a Fargo printer, or create a fully laminated I.D. card using the following process:

To make the badge, you will need the following equipment and supplies

1. Table top laminating machine and carriers
2. High resolution Inkjet printer (Epson 720 DPI)
3. Special Image Transfer Paper
4. Scissors

The complete process requires the following operations:

1. Load the Special Image Transfer Paper into the printer.
2. Print the desired employee record from the Access Print I.D. form.
3. Using your scissors, trim out the image to a width that will fit through your laminator.
4. Position the clear overlay over the image so that it frames the I.D. badge the way you want it.
5. Place the image and overlay into the laminating carrier pinching it together securely so it won't shift.
6. Tear the clear overlay away from the paper.
7. Place the clear overlay (now with I.D. image) onto the badge blank and run it back through the laminator.

This process permits a center core of any thickness, and back overlays with pressure sensitive adhesive for attachment to access cards. In addition, the badge blanks may be ordered with badge clip slot pre-punched.

#### **Cardholder Programming Utilities**

##### **Create a Sequence of New Card Records**

This utility makes it easy to initialize a system without having to enter each cardholder individually. Simply enter the beginning and ending number of your card deck range, and the records will be created automatically. You can personalize each record later by entering the actual cardholder's name in each record.

### **Assign a Level to a Sequence of Card Numbers**

If you have created new records using the utility above, you can assign one or more levels to these records.

### **Inactivate Random Card Numbers**

Inactivates a list of cards without deleting the records

### **Inactivate a Sequence of Card Numbers**

Inactivates a range of card numbers without deleting the records

### **Activate Random Card Numbers**

Activates random cards

### **Program All Cards at Once**

Use this utility to program every cardholder into your database at once. This utility would be useful for initializing a database where no cardholders had been programmed when the record was populated.

*Note: This process can take several minutes depending upon the speed of your computer and the number of cardholders to program. It can take as much as one second or so per record.*

## **Data Import Utilities**

Use these utilities to import data from previous versions of Toye Corporation software.

## **READER, MODULE, AND ALARM POINT DEFINITIONS**

### **Define Reader Modules**

In order to view transaction records and perform module programming, you must define each hardware device in the system. Use the two digit code you set on the Module, and the text description you want.

### **Alarm Point Descriptions**

An alarm will not report unless it is initialized by entering an alarm description.

Up to 32 characters of text may be entered for each alarm. This text will be displayed and logged each time the input changes state, and is not shunted. The actual display will also include either the text: ALARM OPEN, OR Alarm Secure.

Alarm inputs may originate from a Command Module, a Dual I/O Module, a Multi-Point I/O Module, or a 16 Input Alarm Module.

For monitoring alarms originating from a Command Module, or Dual I/O Module, simply enter the two digit Module code followed by 71 or 72 depending upon which input you are monitoring. See data sheet for programming a Multi-Point I/O Module.

To define text originating from a 16 Input Module, enter the two digit module code followed by the two digit input. When using both Command Modules, and Dual I/O Modules, you must not duplicate Module Codes since they are essentially the same type of device. You may however assign these same two digit module codes to 16 Input Modules without conflict.

### **Alarm Input Options**

#### **ALARM BATCh.FILE OUTPUTALARM BATCh.FILE OUTPUT**

This feature allows incoming alarms to cause the computer to execute predefined BATCh files. A BATCh file may be defined to load another program such as Procomm for example. Procomm would be configured to dial a pocket paging service to annunciate alarms.

Batch files can also be defined to display custom graphic or text screens that will appear automatically when there is an alarm. A commercial paint program can be used to create the graphics. For example,

to display a graphic saved in the PCX format (16 colors 640x480) named FRNTDOOR.PCX, simply copy the graphic file into the TC85DIR sub-directory, and create a Batch file with the following command line:

SHOWPCX FRNTDOOR.PCX

The program SHOWPCX has already been installed in this directory during installation of the access control program.

Batch files can be created using any text editor such as Word Pad. You can use different names for each Batch file such as ALARM1.BAT.

The Alarm Bat file feature can be applied to any alarm input, and that input can be automatically turned on and off in software using the shunt features described earlier. This restricts BAT.FILE responses only to specified times.

To cause a specific alarm to execute a BATch file, simply place an asterisk (\*) in the first character position of the alarm text. The next 8 characters should contain the path and name of the BATch.file. Do not use the extension .BAT. For example:

**\*ALARM1**

This assumes that you have placed ALARM1.BAT in the access control working sub-directory: TC85DIR.

You may add any additional text you wish to describe the actual alarm IE: **\*ALARM1 BUILDING 3 FRONT DOOR**

When adding additional text after the BAT file name, begin in position 10 or 11 to avoid any conflict regarding the name of the BAT file.

### **Transaction Activated Alarm Output**

Incoming alarms can be programmed to pulse one or more relays contained on the 16 Relay Output Module. This is accomplished by selecting an available system memory number, and entering it into the Alarm Text field preceded by a back slash. For example, if you want a certain alarm to pulse an output relay, you simply select an unused system memory number, and enter it anywhere in the alarm text field as follows: \1234. You must then create a Transaction Activated Output Level, and then program number 1234 to be valid in that level.

You may combine both an Alarm BATch file and Transaction Activated Alarm Output from the same alarm input if you want to both display an alarm graphic and create a relay output. For example:

**\*ALARM1 BUILDING 3 FRONT DOOR \1234**

**ALARM WARBLE** Audible Annunciation (Warble)

Any alarm can be programmed to warble by placing a caret symbol (^) in the first character of the alarm text:

**^ ALARM TEXT**

The caret symbol triggers the warble, and the text that follows defines the incoming alarm.

You may also want the incoming alarm to trigger a BATch file. If so, place the name of the BATch file next to the caret symbol beginning in the second text position. If you want to trigger the BATch file without setting off the warble, use an asterisk instead of a caret symbol.

## Define Input and Output Modules

You may enter text descriptions for each Module, and each relay on that Module. This will greatly facilitate final programming. For example, Module 01 Relay 1 might be defined as “First Floor Law Offices”.

## Define Levels and Holidays

### Cardholder Security Levels

To simplify the selection of appropriate levels for cardholder programming, Access Levels you define may be fully described in *Access Central*. The descriptions you make are displayed on each cardholder record form in the Level Library. When you assign a level to a cardholder, this description will automatically be displayed. For a level to be valid, it must have at least one reader, one day of the week, and one start and stop time (or 24 hours).

This function is the key to the system’s ability to manage access authorization conveniently. Access levels may be defined by simply entering the desired location(s), applicable week day(s), and time parameters. After LEVELS have been defined, individual cards, or all cards can be quickly programmed into one or more of these levels.

Each LEVEL is independent of all other LEVELS (there is no hierarchy between levels). The number of available levels is determined by the size of the memory.

### Reader Module Level Definitions

While Security Levels define the status of cardholders, Reader Module Levels define the status of Command Modules. Each Reader Module Level can be defined to perform one of the following commands:

- Timed Unlock
- Timed Alarm Shunt
- Timed Keypad activation

For entry points equipped with only a Keypad, a Command Level must be defined in order to activate it for use. If a Keypad Level is not currently active, the Keypad will not permit access. This insures against off-hour tampering.

### Keypad Operation

#### *Keypad Only*

For entry points with a Keypad and no card reader, it is necessary to both create a Command Level to activate the Keypad as described above, and a Security Level To authorize Keypad use just as you would for cardholders. You must then program the active Keypad numbers into this Security Level. When an individual enters a valid Keypad number into the Keypad, entry will be granted.

A Keypad transaction begins with the star key (\*), followed by the Keypad number, and ending with the pound key (#).

#### *Keypad Or Card Keypad Or Card*

If the Command Module firmware is set up to accept either the use of a Card or Keypad Code, the instructions above for *Keypad only* apply.

#### *Card Plus Keypad Card Plus Keypad*

When the Command Module firmware is set up for Card Plus Keypad you must first enter a valid Keypad number when a Keypad Command Level is active. If a Keypad Command Level is not active, access will be granted based only on a valid card.

A detailed explanation of the Keypad option is contained in the Component Installation Instruction Manual.

## CAUTION

Never disable a command level that is currently active by removing its module location code, unless that module is defined in another level. Doing so will prevent the module from receiving a command to secure. In other words, if a door is unlocked, it will not re-lock until commanded to do so. Removing a location code from an active level will terminate communication to that module unless it is also defined in another level.

To disable a level that is currently active (relay(s) pulled in), first replace the current day with any another day of the week. Wait two minutes to insure that the secure command has been transmitted to the module. After two minutes, modules codes may be removed.

To define or change a command, you must select a Command Level number, and then choose either “U” for UNLOCK, “A” for Alarm, or “K” for KEYPAD ENABLE. When choosing UNLOCK, the defined command will both UNLOCK, and shunt the ALARM during the programmed period.

If ALARM is chosen, only the alarm will shunt during the programmed time period.

Any command can be changed from one type of command to the other by simply hitting “A”, “U”, or “K”.

A command definition can include up to 127 entry points, one or more days of the week, and a specified time interval.

For increased security, the computer checks every programmed module once per minute to insure that its output relay is in compliance with the programmed parameters. When programmed commands are initiated, they will be transmitted to their respective modules on the minute.

## **Transaction Activated Levels (Elevator)**

Selective programming of individual cardholder access to authorized floors can be accomplished with the 16 Relay Output Module. The Output module may be used for either continuous time programmable output commands, or for momentary activation in response to authorized cards.

For elevator control applications, when a card is inserted into the car’s reader, all the relays applicable to that cardholder’s authorization LEVEL will activate for a period of time pre-selected at the Output Module. When that time period expires, the Module will assume the relay matrix that was set before the Transaction activated event.

The time selected should give the cardholder time to select a floor button. A separate timer adjustment screw is provided for each bank of 8 relays. If the button pressed matches an active relay, then the elevator control logic should provide the cardholder access to that floor. This system provides relay outputs only, and interfacing to actual elevator control circuitry should be coordinated with the manufacturer of the elevator equipment.

An output relay should be dedicated for each controlled floor per reader. For example: One elevator car with a reader serving 10 floors requires 10 relays. If two elevator cars access the same 10 floors, then 20 relays should be dedicated. If more than one elevator car has access to the same relay, a possible contention could exist when there are simultaneous card insertions in both cars. If this is not considered to be a problem, then up to 15 readers can be programmed to address the same relay.

You may combine Transaction activated Levels And Time Programmed Levels when certain floors are required to have free public access, and other floors require card activation.

Up to 63 Output Modules may be used providing 1008 relays each with a unique code. A relay output code is a four digit number consisting of the two digit Module code plus the specific two digit relay number indicated along the terminal strip. Any Module code may be selected from 00 to 3F except for the code 20 which cannot be used.



Transaction Activated Levels are used to define the various access categories of floor authorization in which cardholders will be programmed. There are typically 100 possible Transaction Activated Levels. The levels dedicated to elevator control must be numbered between 801-900 unless the system is custom, in which case the levels may begin at 601.

Programming these levels is similar to Access LEVEL Definitions used for entry control.

A Transaction Activated Levels is defined as follows:

- One Reader/Command Module Location Code (One elevator car except as noted)
- One or more days of the week.
- A time parameter.
- One to 78 Output Relay codes (Floors).
- A start and stop date if required.

As stated earlier, each car should have exclusive outputs, however there is no problem applying many different levels to the same Outputs. For example, a single output for a given floor may be included in a master level for top executives, and also included in a level intended for more restrictive cardholder use. Any cardholder may be assigned to one or more levels, or all the levels.

After at least one Elevator LEVEL is defined, individual cards may then be programmed.

#### Transaction Activated Levels Triggered by Alarm Inputs

As discussed earlier under Alarm Text, Transaction Activated Levels may be triggered by unused card numbers sent from incoming alarms. This feature is useful when specific alarm inputs must pulse specific relays for alarm panels, zoned alarm dialers or CCTV controllers. Setting up Transaction Activated Levels which are triggered by card numbers defined in alarm text is performed exactly as described above for elevator levels. Remember to choose memory numbers that are not assigned to cards, otherwise the use of those cards will trigger the output defined in the alarm text.

#### I/O Module Levels

I/O Modules levels include 16 Relay Output Modules, 16 Input Alarm Modules, and Multi-Point I/O Modules. These levels can be defined to determine the status of the modules by time and day. When relays should be pulled in, or alarms shunted.

Output LEVEL Definitions apply to the 16 relay Output Modules. These levels are handled exactly like the Remote Command Definitions used for Command Modules, except that a four digit number is used to define these levels instead of two. If both 16 Relay Output Modules, and Programmable 16 Input Alarm Modules are used on the same system, care should be taken not to duplicate module codes (See hardware installation instructions).

Output Levels defined for Relay Modules simply activate and deactivate the relays when programmed to do so. Output Levels defined for the Programmable 16 Input Alarm Modules deactivate or shunt the alarm inputs when programmed to do so. There are up to 100 available LEVELS numbered from 1-100.

An Output LEVEL consists of the following:

- One or more output address (Up to 78)
- One or more days of the week
- A time parameter
- A start and stop date if required

When each of these three parameters are entered, the command will be transmitted at the next one minute update. Every output in the system which is defined in at least one LEVEL, is automatically updated once per minute on the minute to insure maintenance of the programmed status in the event of

a remote power interruption. Only locations programmed into properly defined levels (active or inactive) will receive the update, so a location should not be removed from an active level (relay pulled in or alarm shunted) unless it is also programmed into an inactive level, otherwise it will not receive a command to change states.

#### **ALARM MODULE LEVELS: Programmable Shunting**

Alarm Module Levels apply to the 16 Zone Alarm Input Modules with codes ranging from 00-3F for a total of 1008 shuntable alarms. Module code 20 is not usable.

These levels simply deactivate (shunt) alarm inputs when programmed to do so. Alarm Module Levels are handled exactly like Output Module Levels. If both 16 Relay Output Modules, and Programmable 16 Input Alarm Modules are used on the same system, care should be taken not to duplicate module codes (See hardware installation instructions).

An Alarm Module Level consists of the following:

- One or more input addresses (Up to 78)
- One or more days of the week
- A time parameter
- A start and stop date if required

When each of these three parameters are entered, the command will be transmitted at the next one minute update. Every input in the system which is defined in at least one LEVEL, is automatically updated once per minute on the minute to insure maintenance of the programmed status in the event of a remote power interruption. Only locations programmed into properly defined levels (active or inactive) will receive the update, so a location should not be removed from an active level (alarm shunted) unless it is also programmed into an inactive level, otherwise it will not receive a command to change states.

If an Alarm Level expires when its input is open (in alarm), that alarm will be annunciated, and will display as an open alarm.

#### **Enter Holiday Exceptions**

You may define up to 32 holiday exceptions at one time. You may replace expired holiday dates with future dates.

#### **Anti-Pass-Back Controls**

Any reader in the system may be defined as an entry point or an exit point for the purposes of detecting multiple entries by a single card. If the Anti-Pass-Back feature is enabled, a card will be denied passage if an attempt is made to use it for a second entry if it has not first passed through an exit reader, and vice versa. For Anti-Pass-Back to be enabled, you must define at least one entrance reader, and one exit reader.

#### **Timed-Anti-Pass-Back**

Timed Anti-Pass-Back is designed to control entrance tailgating where there are no on-line exit readers. In addition, the Timed Anti-Pass-Back feature may be used for automatic once per day resynchronization with or without on-line exit readers.

When timed Anti-Pass-Back is enabled, all cards are resynchronized at the time interval specified. You may select a resynchronization interval from 1 minute to 2400. For resynchronization every 15 minutes, simply enter 15. For once per hour, enter 60. For automatic resynchronization once per day at 1 AM, simply enter 0100. To disable Timed Anti-Pass-Back, enter 0.

If Timed Anti-Pass-Back is to be used without an exit reader, you must select a bogus exit reader location in order to initiate Anti-Pass-Back.

The icon header will show T-APB for Timed Anti-Pass-Back, and D-APB for Daily resynchronization. The icon will also show whether APB is enabled on entrances, exits, or both.

### **Hard and Soft Anti-Pass-Back**

When any reader module code is entered as either an entrance or exit location, all cards using that reader automatically become subject to anti-pass-back detection. If anti-pass-back is disabled, “soft” anti-pass-back will be in effect which means that violations will be logged as exceptions, but passage will not be denied. If anti-pass-back is enabled, “hard” anti-pass-back will be in effect denying passage to violators. It is possible to invoke “hard” anti-pass-back at exits, and “soft” anti-pass-back at entrances, or any combination.

### **Valet and Special Anti-Pass-Back Exceptions**

Specific cardholders can be programmed to be exempt from anti-pass-back control. Simply define the highest available Transaction Activated level. Transaction Activated levels are not subject to Anti-Pass-Back control, so any cardholder programmed into these levels will be exempt. Transaction activated levels require an Output to be defined. Enter 2001 for the output code.

### **Hard Nesting**

Nesting is the term used to describe enforcement of special area parking. The nest is the special area into which designated vehicles are to park. Nesting software is designed to detect vehicles which fail to park in the special area, but instead remain in a premium area. The software permits the selection of a grace period (up to 255 minutes) within which nested vehicles must vacate the premium parking area.

Hard nesting actually denies use of the card for exiting the premium area if the nesting grace period has been exceeded. In order to avoid a hard nesting violation, the vehicle must enter the nest, or exit the parking facility within the grace period. If the grace period is exceeded, the card will not operate any nest entrance reader, and will not operate any premium area exit reader.

For the purpose of nesting enforcement, any reader that permits entry to the premium area is considered an ENTRANCE reader. Any reader that can be used to exit the premium area is considered an EXIT reader. Therefore, the entrance to the nest must be defined as an EXIT reader. The nest exit reader must be defined as an ENTRANCE reader.

For systems with hard nesting, the highest security level is used as a special nesting level. If the system has 100 Security Levels, Level 100 is used to define the nesting level. The use of a level to control nesting permits the operator to designate specific times and days when hard nesting will be active. There may be certain days, times, or holidays that may not be subject to hard nesting.

Any ENTRANCE READER, and any EXIT READER to be used in conjunction with nesting must be so defined using the Anti-Pass-Back Definitions. Hard, Soft, or Override Anti-Pass-Back may be invoked without affecting hard nesting. In either mode, hard nesting will prevail.

Any cardholder to be subject to hard nesting must be programmed into the nesting level. This makes it convenient to program any card in the system in or out of hard nesting.

#### *Reviewing the steps:*

1. Define any reader that places the vehicle into the premium area as an entrance reader. Define as an exit reader any reader that exits the premium area. A reader that provides access to the nest is an exit reader. Select the nesting grace period.
2. Define the highest Transaction Activated (Elevator) level. You can determine what the highest level is by clicking the **About** Toolbar Button. Under Location, ENTER ONLY EXIT READERS. Select the days and times hard nesting is to be invoked. In addition to this nesting level, you must also define at least one normal security level which contains both entrance and exit readers.
3. Program any cardholder to be subject to nesting as valid in the nesting level, and the normal security level.

To quickly override Hard Nesting, simply remove the current day from the Nesting Level.

### **Capacity/Limitations**

Hard Nesting is accomplished by calculating the time lapse between an exit request and an entrance transaction. The transaction data on which the calculations are made are contained in a memory buffer with a total capacity of 1,000 entrance transactions. For Hard Nesting to work properly, the total number of entrance transactions can not exceed 1,000 transactions per grace period. To calculate this capacity, divide 1,000 by the minutes in the grace period. A grace period of 10 minutes would provide a capacity of 100 entrance transactions per minute, or almost 2 per second. A 15 minute grace period would accommodate a capacity of about 67 entrance transactions per minute or more than one per second. Higher memory buffer capacities are available on special order, and are subject to the limitations of the host computer.

### **Unlock or Relock Doors**

This button loads the first Command Level record in case you want to use this record as a master Unlock Level. Set the time and day parameters, then simply select or unselect the entry points to be locked or unlocked respectively.

### **Enable Background Printing**

Use this utility to print real time events. It is best to use a dot matrix printer which will print a line at a time. Please observe the on screen instructions.

### **Start Up**

If for any reason ACCESS-ONLINE needs to be restarted, you can do so from here. Please make sure that one, and only one ACCESS-ONLINE icon is displayed on your Task Bar.

### **Access Central Database Properties**

All tables, queries, forms, reports, macros, and modules are contained in a single database. All definitions and properties are available for user modifications utilizing the full capabilities of Microsoft Access, however Toye Corporation is only able to provide support for those features it has included in the mdb file, and which have not been modified. Be sure to keep a back up of Access Central.mdb if you plan to make modifications so you can restore the original files if necessary.

Certain procedures assume that ACCESS CENTRAL.MDB, and LOG.MDB are located in your TC85DIR subdirectory even though you have a shortcut icon on your desktop.

You may explore the database structure at any time by hitting the F11 key. Never close this Database Window or you will shut down the database. When you are finished examining the Database Window, select Window from the File Menu Bar, and Hide the Database Window. If when you hit the F11 key, no tables are displayed, Hit the Tools/Options button and select "hidden objects".

Following is an overview of this structure:

### **Tables**

Tables are the basic raw building blocks of a database. The tables you find here are used in combination with other tables to create meaningful information. One of the tables (tclog.dta) has an arrow indicating that it is linked to an outside table. It assumes that the tclog.dta table is in a subdirectory named: c:\tc85dir. If this file is located elsewhere, the import definition must be modified in Linked Table Manager.

### **Queries**

Queries combine information from one or more tables or other queries to create relational data. For example, when you display transactions, the information comes from two different tables; tclog.dta, and entry points.

### **Forms**

Forms are created to display the information from tables, or from queries.

## Reports

Reports format data when they require formatting or calculations, such as the Time Management Report.

## Macros

Macros perform sequential tasks. For example, the macro name “autoexec” initializes the program so that the Access Central Main Switchboard Menu appears when you load the program. If you don't want the Opening Welcome screen to appear, open this macro in the design mode, and delete the last item in the macro.

## Modules

Modules contain the actual Visual Basic Code needed to link with ACCESS-ONLINE. The module named *Global* sets the directory paths, so if your software is not running in C:\tc85dir, you will need to change the path statement in this code module. It only appears once at the top.

## BACKING UP DATA

Data crucial to your specific system is contained in all files with the extensions: .BAS, .DTA, and .MDB. It is wise to maintain a backup of these files in the event of a computer failure. If you are backing up your transaction data on a regular basis, there is no need to maintain a separate backup of TCLOG.DTA which is the large file used for transaction storage. Should you experience a computer failure, or you wish to move your system to another computer, simply use the original installation program to start up the system, and then copy all the .BAS, .MDB and .DTA files (except tclog.dta) from your backups into the TC85DIR sub-directory. When you initialize the system, a new TCLOG.DTA file will be created.

## Access Central Password Options

Passwording an MS Access database can be taken to virtually any level from a simple password for the entire database to different passwords for virtually every object and function. MS Access includes extensive help screens together with Password Wizards to guide you through the process, so the following instructions are intended for you if you don't want to follow the MS Access instructions.

### 1. Password the entire database

To set a password, you must open the Access Central Database in the Exclusive mode. To do that, start up MS Access (the executable, not the MDB), and proceed to open the Access Central MDB. Select Exclusive from the dialog box. When the MDB opens, click on the Tools Menu Bar button, select Security, and set the password.

### 2. Set Up Multiple Passwords for Function Specific Access

IMPORTANT: Unless otherwise directed, the following procedures must be performed while NOT Running Microsoft Access97.

#### 1. Creating a NEW WORKGROUP Information File:

- a. Using Windows Explorer, open the WINDOWS\SYSTEM folder and then double-click Wrkgadm.exe.
- b. In the Workgroup Administrator dialog box, click CREATE, and then type your name and organization.
- c. In the Workgroup Owner Information dialog box, type any combination of 4 to 20 numbers and letters, and then click OK.

Caution: Be sure to write down your exact name, organization, and workgroup ID, including whether letters are uppercase or lowercase (for all three entries), and keep them in a secure place. If you have to re-create the workgroup information file, you must supply exactly the same name, organization, and workgroup ID. If you forget or lose these entries, you can't recover them and might lose access to your databases.

- d. Type a NEW NAME for the NEW Workgroup Information File, and then click OK.  
(By default, the workgroup information file is saved in the folder where you installed Microsoft Access. To save in a different location, type a new path or click BROWSE to specify the new path.)

## 2. Joining the NEW WORKGROUP:

- a. Using Windows Explorer, open the WINDOWS\SYSTEM folder and then double-click Wrkgadm.exe.
- b. In the Workgroup Administrator dialog box, click JOIN.
- c. Type the path and name of the NEW WORKGROUP information file that you created in Step 1, and then click OK.
- d. The next time you start Microsoft Access, it uses the USER and GROUP ACCOUNTS and Passwords stored in the NEW WORKGROUP information file for the workgroup you joined.

Important: If you are setting up user-level security and need to make sure that your workgroup and its permissions can't be duplicated, you should make sure the WORKGROUP information file that defines the workgroup you are joining has been created with a unique Workgroup ID (WID) in step 1, above.

Note: You can also specify a workgroup information file when starting Microsoft Access by using the /wrgrp command-line option. Refer to "Command-Line Options", described in Section 7, later.

## 3. Creating Security User Accounts:

To complete this procedure, you must be logged on as a member of the ADMINS GROUP.

- a. Start Microsoft Access using the WORKGROUP in which you want to use the account.
- b. On the TOOLS menu, point to SECURITY, and then click USER AND GROUP ACCOUNTS.
- c. On the USERS tab, click NEW.
- d. In the NEW USER/GROUP dialog box, type the name of the new account and a Personal ID (PID), and then click OK to create the new account. It is automatically added to the USERS GROUP.

USER names can be 1 to 20 characters long and can include alphabetic characters, accented characters, numbers, spaces, and symbols, with the following exceptions:

The characters " / \ [ ] : | < > + = ; , ? \*  
Leading spaces  
Control characters (ASCII 00 through ASCII 31)

Caution: Be sure to write down the exact account name and PID, including whether letters are uppercase or lowercase, and keep them in a secure place. If you ever have to re-create an account that has been deleted or created in a different workgroup, you must supply the same name and PID entries. If you forget or lose these entries, you can't recover them.

## 4. Creating or Changing a Security Account Password:

- a. Start Microsoft Access using the WORKGROUP the USER ACCOUNT is stored in, and log on using the name of the account for which you want to create or change the Password.

You can find out which workgroup is current or change workgroups by using the Workgroup Administrator.

- b. On the TOOLS menu, point to SECURITY, and then click USER AND GROUP ACCOUNTS.
- c. On the CHANGE LOGON PASSWORD tab, leave the OLD PASSWORD box blank if a Password hasn't been defined previously for this account. Otherwise, type the current Password in the OLD PASSWORD box.
- d. Type the new Password in the NEW PASSWORD box.

A Password can be 1 to 14 characters long and can include any characters except ASCII character 0 (null). Passwords are Case-Sensitive.

- e. Retype the Password in the VERIFY box, and then click OK.

Caution: You can't recover your Password if you forget it, so be sure to store it in a safe place. If you forget your Password, a USER logged on with an Administrator Account (a member of the ADMINS GROUP in the Workgroup in which the Account and Password were created) must clear the Password before you can log on.

#### 5. Requiring USERS to log on:

Until you activate the LOGON procedure for a workgroup, Microsoft Access automatically logs on all USERS at startup using the predefined ADMIN USER ACCOUNT. You require USERS in a Workgroup to log on by adding a Password to the ADMIN USER ACCOUNT.

- a. Join the WORKGROUP (see section 2, above) whose LOGON procedure you want to activate.
- b. Start Microsoft Access.
- c. On the TOOLS menu, point to SECURITY, and then click USER AND GROUP ACCOUNTS.
- d. Click the USERS tab, and make sure that the predefined ADMIN USER ACCOUNT is highlighted in the NAME box.
- e. Click the CHANGE LOGON PASSWORD tab, click the NEW PASSWORD box, and type the new Password. Don't type anything in the OLD PASSWORD box.

To maintain the security of your Password, Microsoft Access displays asterisks (\*) as you type. Passwords are case-sensitive.

- f. Verify the Password by typing it again in the VERIFY box, and then click OK.

The LOGON dialog box is displayed the next time any member of the WORKGROUP that you joined in step 5.a starts Microsoft Access. If no USER ACCOUNTS are currently defined for that workgroup, the ADMIN USER is the only valid ACCOUNT at this point.

Note: When you SECURE a database, you create USER ACCOUNTS in a WORKGROUP and then assign PERMISSIONS for the DATABASE and OBJECTS to those ACCOUNTS and to any GROUP ACCOUNTS to which they belong. When USERS log on to Microsoft Access using their ACCOUNTS, they have only the PERMISSIONS associated with those ACCOUNTS. USERS log on to Microsoft Access by typing a USER Name and PASSWORD in the LOGON box.

#### 6. Securing the ACCESS CENTRAL Database using the User-Level Security Wizard:

- a. Join the secure WORKGROUP (established in Step 1 above, using step 2).
- b. Start Microsoft Access. On the TOOLS menu, point to SECURITY, and then click USER AND GROUP ACCOUNTS.

- c. In the USER AND GROUP ACCOUNTS dialog box, create a New USER to be the new Owner and Administrator of the Database, and then add that USER to the ADMINS GROUP.
- d. In the NAME box on the USERS tab, select the ADMIN USER, and then click the CHANGE LOGON PASSWORD tab and assign a Password to the ADMIN USER. This causes the LOGON dialog box to appear the next time you start Microsoft Access.
- e. Click the USERS tab, and then REMOVE the ADMIN USER from the ADMINS GROUP.
- f. Exit Microsoft Access and restart it, logging on as the Administrator USER that you created in step 6.c above.
- g. Open the ACCESS CENTRAL[.mdb] Database.
- h. On the TOOLS menu, point to SECURITY, and then click USER-LEVEL SECURITY WIZARD.
- i. Select the check boxes for the OBJECT Types you want to secure, and then click OK.

The User-Level Security Wizard creates a new Database, exports copies of all of the Objects from the original Database, secures the Object Types you selected by revoking all permissions of the USERS GROUP for those Objects in the New Database, and then encrypts the New Database. The Original Database is not changed in any way. Table relationships and any Linked Tables are also re-created in the new Database.

If you chose to Secure ALL Object Types in the Database, the User-Level Security Wizard removes the USERS GROUP's Open/Run permission of the for the Database itself. This means that only members of the ADMINS GROUP of the WORKGROUP Information File in use in step 6.a can Open the New Secured Database. All other Users of Microsoft Access and Visual Basic can't Open the Database or Access the Secured Objects within it.

If you chose to secure only SOME Object Types in the Database, the User-Level Security Wizard doesn't remove the USERS GROUP's Open/Run permission for the Database itself. In this case, All Users of Microsoft Access and Visual Basic can Open the New Secured Database and access Unsecured Objects, but they can't access the Secured Objects within it.

- j. Create your own USERS and GROUPS. Assign appropriate permissions to the GROUP Accounts, and then add Individual Users to the appropriate GROUPS. Typical permissions may include Read Data and Update Data permissions for Tables and Queries, and Open/Run permission for Forms and Reports.

The new Database created in step 6.j is now secure. The USER that you logged on as, in step 6.f, is now the OWNER of ALL OBJECTS as well as the DATABASE itself. The only people who can use the Objects in your application are those you gave permission to in step 6.j, and Members of the ADMINS GROUP of the Workgroup Information File you created or specified in step 6.a.

## 7. Starting Microsoft Access with Command-Line Options, using a Shortcut:

At the END of the SHORTCUT TARGET Line, simply add any of the following Command-Line Options (preceded by a space).

OPTION	EFFECT
/ro	Opens the specified Database for READ-ONLY Access.
/user USER-NAME	Starts Access using the specified USER-NAME.
/pwd PASSWORD	Starts Access using the specified PASSWORD.



/nostartup	Starts Access without displaying the startup dialog box (the second dialog box you see when you start Microsoft Access).
/wrkgrp WORKGROUP INFORMATION FILE	Starts Access using the specified WORKGROUP INFORMATION FILE (WIF).

Note: To specify a forward slash (/) or semicolon (;) on the Command Line, type the character twice. For example, to specify the Password ;FDT/mD on the Command Line, type ;;FDT//mD following the /pwd Command-Line option.

## REPORT MANAGER

Transaction activity may be viewed and printed using Report Manager. To insure that your report is based on the most recent data, always begin by pressing the Refresh Data Button on the main menu.

### Custom Reports

You can use Microsoft's powerful built in Report Wizard to generate new report formats. To specify the data on which to base the report, select the **query** named: **LogRcdTblTransactions**. *Note: To create custom reports, you must familiarize yourself with Microsoft Access by taking the tutorial and reading your Microsoft Access Manual. No phone support is available for customizing your system.*

### Cardholder History Report

#### Cardholder History Report

This is a predefined report that lets you enter the search parameters. You can enter a start date and time, and an end date and time. The default is today's activity. All cardholder transactions are automatically included unless you specify a search string. This search string can be the name of a cardholder, or a code that is contained in the text field of a number of cardholders.

### Alarm History Report

This is the same report as above, but for alarms. Use the text string to filter alarm descriptions.

### Cardholder Database

You can review cardholder records from Report Manager.

### View Transaction Log

This is a quick way to search, sort, and print transaction activity without waiting for a full report to format.

### Time Management Report

This utility creates a report based on "IN" and "OUT" time calculations. You must designate which entry points are entrances, and which are exits for the purposes of this calculation. Select "Define Entry Points" to make these designations. The default report contains a column for Revenue Time which is the actual time rounded up to the next 30 minutes. For Time & Attendance applications, you can ignore this column, or delete it Report Design.

You can run the report by individual, or by groups. If you want the report to be grouped by department number, or by tenant group, simply place unique descriptors on each cardholder's text, such as Dept 123. When you run the report, simply enter this unique string.