AMADEUS 5

ACCESS CONTROL AND ALARM MANAGEMENT

SECURITY AND SOPHISTICATION OF ON-LINE NETWORKS

USER MANUAL

Amadeus 5 – User Manual – Rev E - Doc. 10UE400
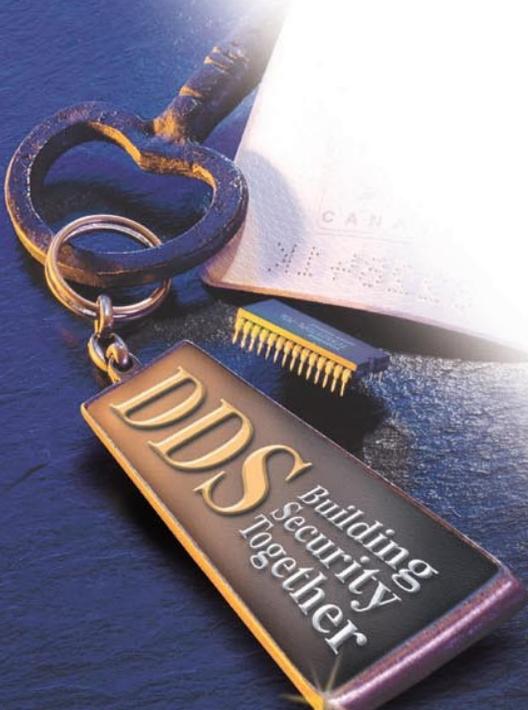
Table of Content

1. WELCOME

1.1. About Amadeus 5

Amadeus 5, the sophisticated yet user-friendly access control and alarm management software, centralizes security requirements within all types of installation irrespective of their complexity.

Amadeus 5 offers intelligent and flexible access control that manages time zones, access levels, data layout and relays activation. Controllers and groups of badge holders are automatically created with a click of a mouse. The set-up process is therefore reduced to minutes instead of hours. The crisis level function allows modifying access authorizations to all doors for a specific group of employees with a single command.

Amadeus 5 alarm management module monitors all alarm events and movements in real time. All the information needed to react immediately with full knowledge of the facts is provided on the screen. Security is reinforced as alarm conditions and events automatically trigger predefined reactions: flashing icons on relevant displayed maps, written and vocal instructions, alarms, CCTV or any programmed relay activation, zone on/off alarm, card invalidation, etc.

Amadeus 5 transforms your facility into a smart building. The passage of a badge at the exit automatically switches off the lights and heating in any designated area, thus allowing for energy savings. Alarms can be automatically activated when the counter of the employees in the building reaches a certain value.

1.2. Monitoring Tool

1.2.1. Access Control

Your organization can prevent material or information robbery, by limiting / supervising the access to all or part of your facility (lab, computer room, or storage areas) to authorized persons, during specific time periods.

Smart multi-technology controllers, linked to advance identification systems, are programmed to control "who is going where and when". Each person is equipped with a personalised card or another ID that controls access.

When a badge holder needs permission to access a particular area, the information is relayed from the reader to the controller. The controller either grants or refuses access according to the parameters defined (access authorization, time zones, etc.) The operations are then sent to the PC and listed in the backlog and the journal.

Access control parameters are mainly defined in the " Parameter" section of the application.

1.2.2. Alarm Management

Your organization can prevent catastrophes or limit damage by being informed of abnormal events and reacting to them in real time. Alarm Monitoring usually functions in coordination with Access Control.

Alarm management consists in supervising alarm inputs. Different sensors, such as magnetic contacts, motion detectors, broken window sensors and temperature indicators are connected to intelligent controllers that centralize the information. As soon as an alarm is activated the system reacts: CCTV cameras, alarms, heating switched on or off, display of appropriate maps and instructions on the screen, etc.

Alarm management parameters are mainly defined in the "Parameter" and "Event Handling" sections of the application.

1.2.3. Lift Management

DDS provides a solution for supervising access in lifts. The user runs his/her badge to the reader installed inside the cabin and pushes the floor button as usual. If access is granted within the time zone, the lift will move towards the requested floor. The lift will stay still if access is denied.

In case of buildings shared by several firms, each person will only be able to select the floor(s) attributed to the company he/she belongs.

Lift management parameters are mainly defined in the "Lift Program" menus in the "Modules" section of the application.

1.2.4. Parking Management

Amadeus 5 enables to monitor access to designate parking spaces. The software monitors the filling up of parking zones with respect to groups of users and allows establishing attendance sheets.

The necessary parameters are mainly defined in the "Parking" menus of the "Modules" section of the software.

1.2.5. Time & Attendance Management

Time & attendance management facilitates the computation of employee attendance, overtime, absences and lateness. It allows calculating pay slips more efficiently.

1.3. Types of Installations

Amadeus 5 centralizes security within any type of on-line installation:
  ➢ Big or small installation
  ➢ TCP/IP, RS485 or modem networks
  ➢ Single or remote sites
  ➢ Single or multiple company sites

1.4. Modules

1.4.1. Database

The database module allows creating and modifying databases (reader, systems, badge holders, time zones, etc.)

As soon as a data is created or modified, it is recorded in an exchange file. The file is then sent to the controller via the communication module.

Database parameters are defined in the "Create", "Save" and "Restore Database" screens in the "Tools" section of the application. Similar options exist for the journal.

1.4.2. Communication

The communication module coordinates the data transfer between the main computer and the controllers that detect the events. The information collected is recorded in the journal and displayed in the log.

1.4.3. Operation

The operational module interprets information collected by the communication module. Its role is to activate predefined tasks such as alarms, reflexes, etc.

The events to consider, and the resulting actions, are specified in the different screens of the "Event Handling" section.

1.5. Basic Configuration

1.5.1. Operating System and Computer
Operating system:
Windows 2000 Pro
Windows XPRO

The manufacturer recommends these two operating systems and is not responsible for errors occurring while using other operating systems.

Computer:
Pentium III 450 MHZ
128 MB RAM
500 MB free hard disk space
CDROM Drive
1 free serial COM port
1 parallel port or USB port

Recommended enhancement
Sound Card
Speakers
SVGA definition (800*600)

1.5.2. Controllers

All our controllers for on-line networks are compatible with Amadeus 5.

1.5.3. Readers

The vast majority of readers available on the market are compatible with the Amadeus 5 system: magnetic, proximity, bar code, smart card, biometry, Wiegand, contact, infrared, Watermark, keypad, etc.

Consult with your Amadeus reseller for further information.

1.5.4. Other Materials

In order to successfully install and run the Amadeus 5 system, other materials are required. These vary according to each installation: computer network, devices to open doors, alarm detectors, etc.

Consult with your Amadeus provider for further details.

1.6. General Use of Amadeus 5

1.6.1. Installation

In order to install the Amadeus 5 application, insert the CD ROM and follow the instructions on the screen.

1.6.2. Setting Up

To start the Amadeus 5 application, select the Amadeus 5 application in the Windows scrolling menu "Start" and click on the corresponding icon on the desktop.

In the start menu that appears on the screen:
- ➢ Type the user name
- ➢ Press "Tab" - if you hit the "enter" key this will result in an error message
- ➢ Type the user's name
- ➢ To confirm, click on the OK button

The application's main menu appears on the screen

Tips & Notes

User name and password

By default, the name required is "dds" and so is the password.

Significance of lower case and capital letters

The "name" and "password" fields notice the difference between lower case and capital letters. For ex: the computer will interpret AFI, afi, and aFi differently.

Introduction delay

If the name and password are not entered within the predefined delay, the start window will disappear from the screen.

Using the software for the first time

It is recommended to change the name and password at the first use.

1.6.3. Exiting the Application

In order to terminate a work session and exit the application, choose one of the following steps and confirm your desire to exit the application:
- ➢ Click on the icon represented by a door, at the far right of the navigation bar
- ➢ Click on the icon represented by a magical wand, in the upper left corner of the screen
- ➢ Click on the "X", in the upper right corner of the screen
- ➢ Click on the function key ''F4''

The system offers the possibility to log off unauthorised users.

1.6.4. New Data Entry

To create a new data entry:
 - ➢ Select the required screen
 - ➢ Click on the icon "New" from the navigation bar, to create a new data entry
 - ➢ Give a name to the new data entry in the field entitled "Name"
 - ➢ Define the new data entry in the field entitled "Description"
 - ➢ Fill in the other fields
 - ➢ Click on the icon "Save" from the navigation bar to confirm the creation of the data or press the function key ''F3''
 - ➢ Click on the icon "Close" to terminate entry operations and to come back to the general screen or press the function key ''F12''

Tips & Notes

Emptying fields

By clicking on the icon "New" all the fields are cleared away or set to their default value to allow for new data entry.

Chose self-explanatory names

1.6.5. Modifying Data Entry

To modify an existing entry:
 - ➢ Select the desired screen
 - ➢ Modify the fields
 - ➢ Click on the icon "Save" from the navigation bar to confirm the creation of the data captures
 - ➢ Click on the icon "Close" to terminate the data entry operations and to return to the general screen

Chose self-explanatory names

1.6.6. Demonstration Version

A demo version of the Amadeus 5 software is available. It includes all functions referring to alarms, graphics, lift management and time management. Nevertheless the capability of the demo version is restricted to two controllers, four readers and ten employees. In order to exceed these capabilities and to use the software in real situation, a plug is requested.

1.6.7. Plug

Different plugs are available. The combination of plugs purchased defines the system capability.

 - ➢ C   controllers
 - ➢ R   readers
 - ➢ B   badge holders
 - ➢ A   alarm module
 - ➢ G   graphic module
 - ➢ P   parking module
 - ➢ L   lift module
 - ➢ T   time & attendance
 - ➢ M   multi-company
 - ➢ U   guard patrol
 - ➢ W   workstations

2. GENERAL SCREENS

2.1. Main Screen

The main screen of Amadeus 5 allows access to all system options through the use of
- ➢ Scrolling menus, leading to all capture screens, information tables and system options
- ➢ Toolbar, providing shortcuts towards some important screens
- ➢ Log display, presenting the list of events in real time
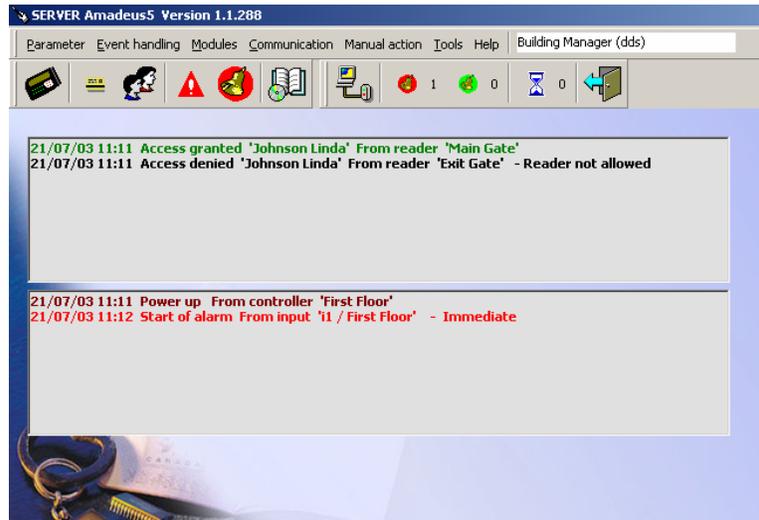
Tips & Notes

The options displayed depend on the authorization level of the user. Certain options are not suitable for certain users and therefore do not appear on the screen.

The fields of the scrolling menus in the main screen appear in **black** before use. However after consultation, they appear in **blue**.

The help screen is available from any screen by pressing the F1 key.

Several windows can be opened simultaneously.

It is possible to dissociate the alarm log from the access log, in the "Options – Tools – Journal & Log" screen. The software needs to be restarted to implement this option. By default, a single log shows access, alarms and system messages.

2.2. Tool Bar

The icons of the toolbar provide shortcuts to some important screens: controller, badge, all card holders, event-handling program, active alarms, report wizard, polling, number of active alarms, number of acknowledge alarms, number of pending commands to be sent, exit.

2.3. Scrolling Menus

Capture screens and menus are organized as follow:
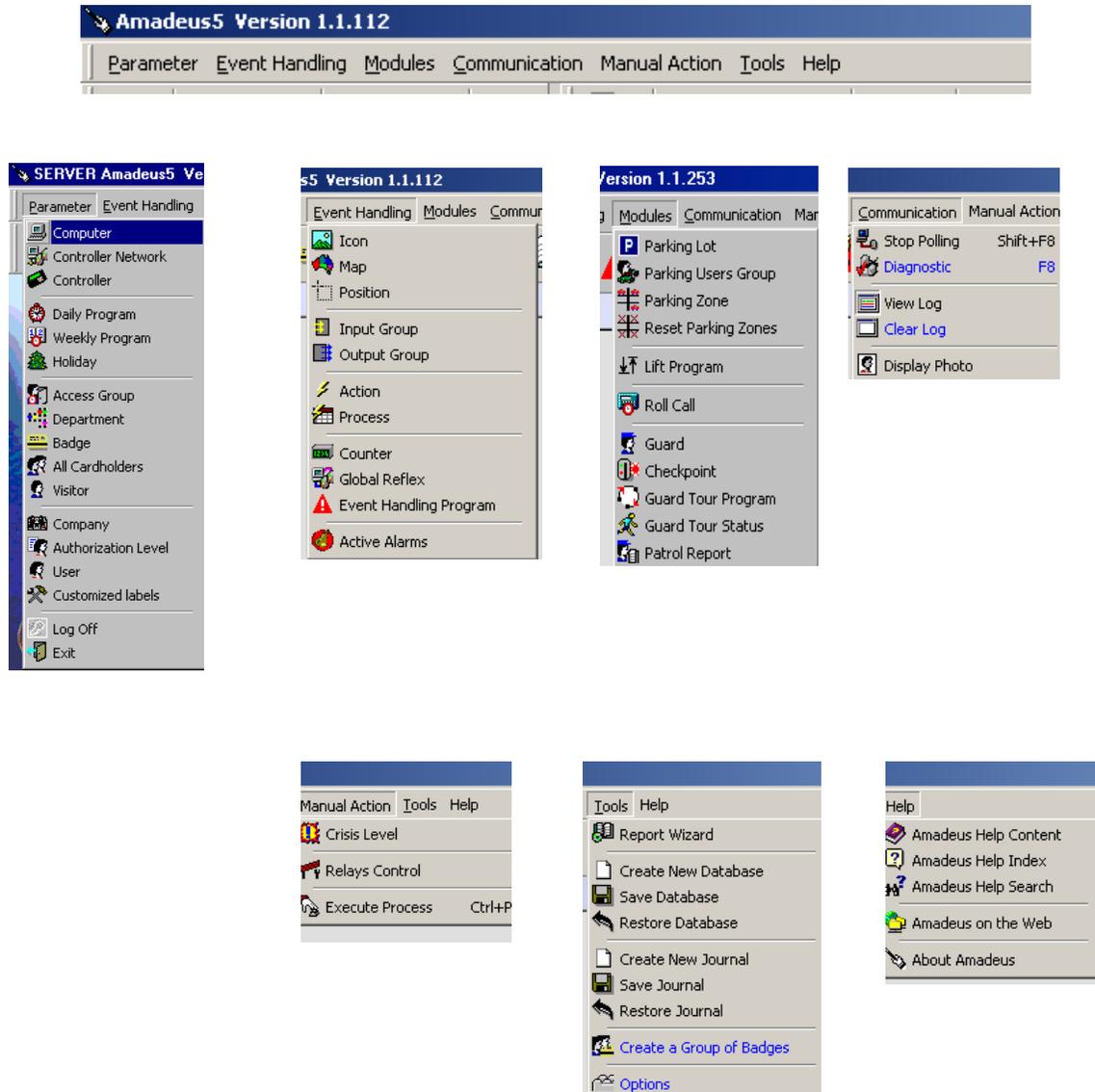
2.4. Navigation Bar

The 12 function keys correspond to the icons on the navigation bar. They are available from each capture screen.

F1   Help   Display the help of a selected screen

F2   New   Define a new data entry

F3   Save   Save the information from the entry created

F4   Delete   Delete the data selected

F5   Previous   Select the previous data entry

F6   Next   Select the next data entry

F7   First   Select the first data entry of the list

F8   Last   Select the last data entry of the list

F9   Download   Transfer all the parameters to the corresponding controllers even if the information has not been modified

F10   Search   Look for the desired information in the database

F11   Print   Print data in a "table" format on your default printer

F12   Close   Close the screen and go back to main screen

Tips & Notes

F2   New   The fields of the newly created item are empty to allow for entry of new data. If existing information has not yet been saved, a message appears requesting the user to save or cancel the changes.

F3   Save   Automatically transfers modified parameters to corresponding controllers

2.5. Personalized Navigation Bar

A personalized tool bar gives added flexibility to the system.

If, following software development, new screens appear, the application cancels the personalised navigation bar.

Creating a personalized tool bar
- ➢ Place the mouse on the original tool bar
- ➢ Click on the mouse right button
- ➢ Select " personalize" in the menu that appears on the screen
- ➢ Give a name to the new tool bar
- ➢ Select the desired option
- ➢ Select the tool bar and position the arrow on the desired area

Saving a personalized tool bar

To save the tool bar, select this option in the "Tools - Option - General" menu. If this option is not selected the tool bar will be lost after closing the work session.

Toolbar initialisation

This option sits in the screen ''Tool - Options - General''.

3. MENU: PARAMETER

3.1. Computer

This screen is used to define the computer parameters (PC name and IP address) of the server and the workstations.
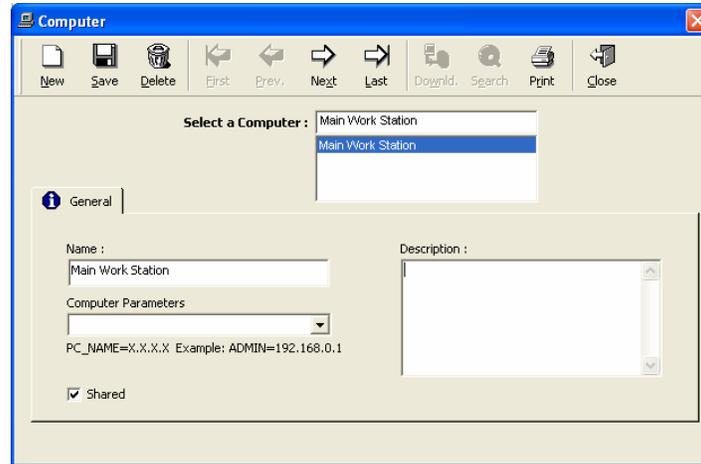
Fields

Name: name the computer

Description: define the new item

Computer Parameters: enter the parameters using the format
    PC_name=x.x.x.x
For example   ADMIN=192.168.0.1
Consult your system administrator to get the IP address.

Server and workstation(s) set up

Example
LAN beholding two computers, a server and a workstation
  ➢ Server   DEV   IP address 192.168.0.1
  ➢ Workstation   PROD   IP address 192.168.0.2

Step 1. Install Amadeus 5 software on the server

Choose "Application Type: Server" in the "Select Additional" screen

Step 2. Define the server and workstations from the server application, in the "Parameter - Computer" screen (See above)

Record 1:

Name: Main workstation (or any other suitable name)
Computer Parameters: DEV=192.168.0.1

Record 2:

Name: Sub workstation (or any other suitable name)
Computer Parameters: PROD=192.168.0.2

Step 3. Restart the computer or kill the spread at the server

Upon exiting the "Parameter – Computer" screen wherein a workstation has been defined, the user is prompted to either:
- ➢ Restart the PC or
- ➢ Exit the application, kill the "spread.exe" process (via Windows Task Manager) and restart AM5

The software Amadeus 5 is ready to run on the server after restarting the computer or killing the spread.

Step 4. Install the Amadeus 5 software on the workstation

Choose "Application Type: Workstation" in the "Select Additional" screen

Step 5. Modify the "amadeus5.ini" file at the server

Modify the line "DbsFolder =   " and specify the full network path of the database folder
Example: DbsFolder = \\Dev\c\Program Files\Amadeus5\

Note: The workstation can only run after the server has been started and its "amadeus.ini" file has been set to the server database

Note: after each addition of workstation or modification of their parameters, in the screen "Parameter – Computer", the server as well as all workstations must be restarted.

3.2. Controller Network

A network is an electrical physical support - or bus - to which controllers are connected. The different networks, to which groups of controllers are connected, are defined in this screen. The network can be either COM, TCP or modem.

Each network is associated to a communication port PC series or to a Wan network.

The controller network parameters are divided into two tabs:
- ➢ General, for name and description
- ➢ Definition, for selection of the different parameters

3.2.1. Controller Network – General
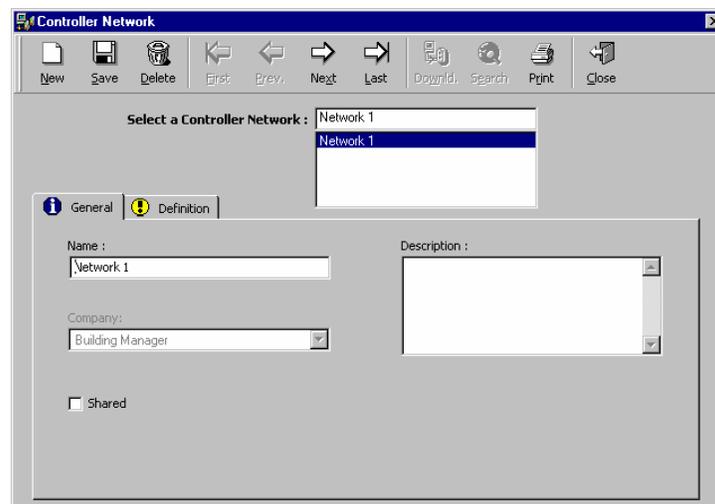
Name: name the new network

Description: describe the new data entry

Company: mentions the company the item refers to; field used mainly in multi-company applications

Shared: share the information between different companies; for use in multi-company application

3.2.2. Controller Network – Definition

Three network types are recognised by the system: COM, modem and TCP.

3.2.2.1. COM Network
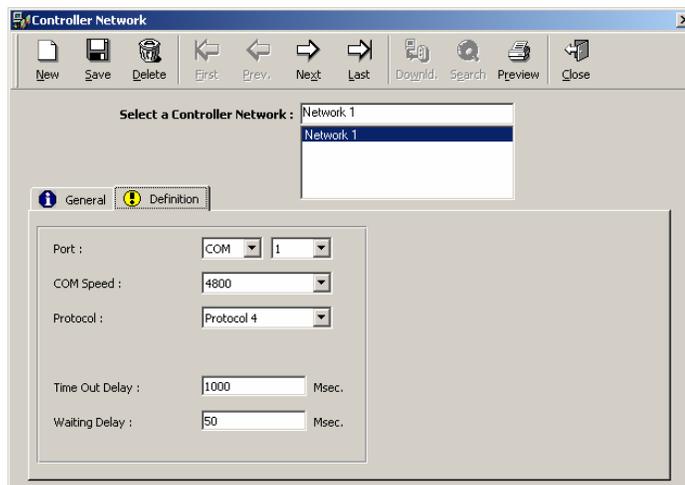
Fields

Port: choose "COM" and specify the port address (1 to 9); by default the serial port COM1 is created

COM Speed: choose the communication speed between
  ➢ 4.800 bauds (default value)
  ➢ 9.600 bauds
  ➢ 19.200 bauds
  ➢ 38.400 bauds

Protocol: choose the protocol between
  ➢ Protocol 4, (proprietary, default value)
  ➢ Modbus, open protocol

Time out delay: specify a delay beyond which the computer will signal a communication problem; in which case an error message will appear after three time the specified delay - measured in milliseconds.
The default value is 1000 msec. (keep this value unless specified otherwise)

Waiting delay: specify the delay between two communication operations between the computer and the controllers (polling or commands) - measured in milliseconds. This function will help slow down the system so as to free up the PC.
The default value is 50 msec. (keep this value unless specified otherwise)

3.2.2.2. TCP Network

Fields

Port: select "TCP" to establish a link to remote controllers via TCP/IP

Phone No. or TCP address: specify the TCP address requested in the format <Address>:<Port>, for example: 10.0.0.1:10001

COM Speed: choose the communication speed between
- ➢ 4.800 bauds (default value)
- ➢ 9.600 bauds
- ➢ 19.200 bauds
- ➢ 38.400 bauds

Protocol: choose the protocol between
- ➢ Protocol 4, (proprietary, default value)
- ➢ Modbus, open protocol

Time out delay: specify a delay beyond which the computer will signal a communication problem; in which case an error message will appear after three time the specified delay - measured in milliseconds.
The default value is 1000 msec. (keep this value unless specified otherwise)

Waiting delay: specify the delay between two communication operations between the computer and the controllers (polling or commands) - measured in milliseconds. This function will help slow down the system so as to free up the PC.
The default value is 50 msec. (keep this value unless specified otherwise)

3.2.2.3. Modem Network
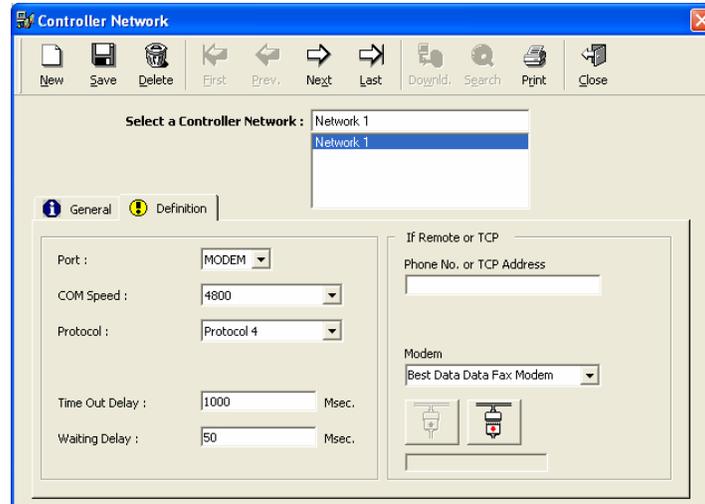
Fields

Port: select "Modem" to establish a link to remote controllers via modem

Phone No.: specify the phone number of the modem requested

Modem: select the required modem among the drop-down list showing the current Windows pre-defined connections

Note
- ➢ Set the remote modem in auto answer mode
- ➢ Fit the specific wiring and settings to installation instructions
- ➢ Establish modem selection at the server

Connect: click on the connect button to start the connection procedure. The server application will show messages such as "Proceeding", "Line Busy" or "Connected".

The connect button is available on any workstation of the system, nevertheless the status messages are only sent to the server computer.

Disconnect: select to stop the connection procedure; this button is only enabled while the controller network is connected

Note: In case of off-line network, all the controllers are considered as inactive by the system. Database modifications are saved and automatically transferred during the next successful connection.

COM Speed: choose the communication speed between
- ➢ 4.800 bauds (default value), 9.600 bauds,19.200 bauds38.400 bauds

Protocol: choose the protocol between
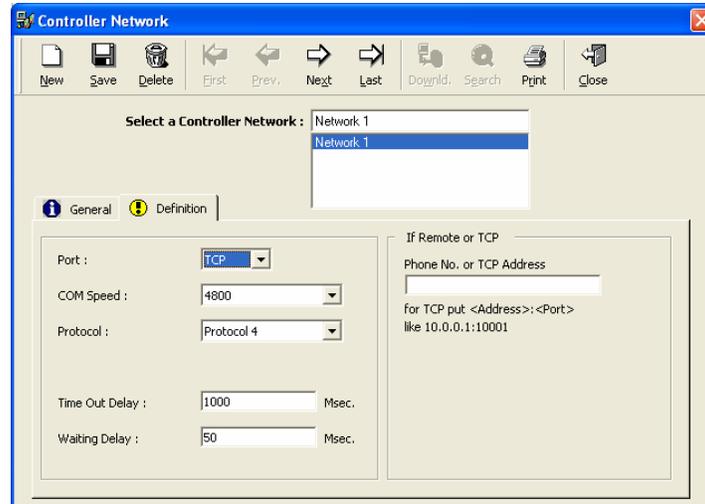- ➢ Protocol 4, (proprietary, default value)
- ➢ Modbus, open protocol

Time out delay: specify a delay beyond which the computer will signal a communication problem; in which case an error message will appear after three time the specified delay - measured in milliseconds. The default value is 1000 msec. (keep this value unless specified otherwise)

Waiting delay: specify the delay between two communication operations between the computer and the controllers (polling or commands) - measured in milliseconds. This function will help slow down the system so as to free up the PC.
The default value is 50 msec. (keep this value unless specified otherwise)

3.3. Controller

A controller is an electronic card that has a huge memory capacity for storing the parameters monitored, such as users, time zones, reflexes, etc. It supervises the following components of the security system:
  - ➢ Readers, and consequently the corresponding doors
  - ➢ Alarm inputs
  - ➢ Relay outputs

Information regarding controllers is organized into 5 tabs:
  - ➢ General tab
  - ➢ Reader tab
  - ➢ Input tab
  - ➢ Output tab
  - ➢ Local reflex tab

3.3.1. Controller - General

The "Parameter - Controller - General" menu allows to define the controller's parameters in the system.
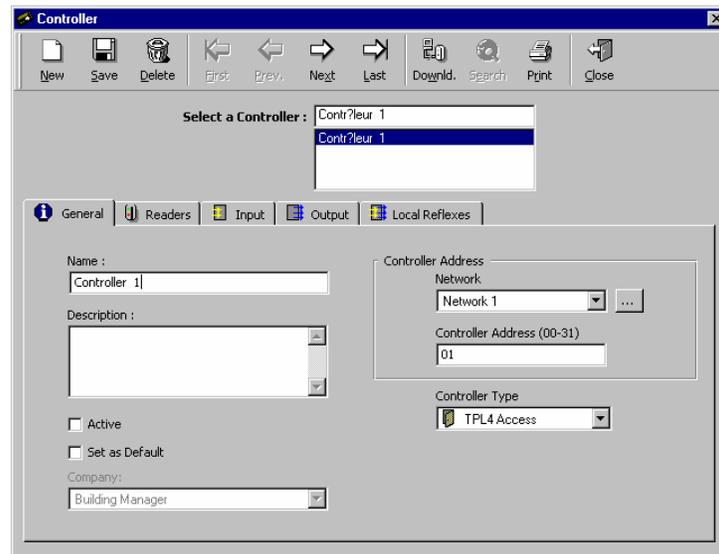
Fields

Name: the following names appear by default: Controller 1, Controller 2, etc.
Modify the default name by a name linked to the geographical position of the controller or to the department it monitors. In the event where the controller monitors many readers at a time, the name chosen must be coherent.
Examples: main entrance, stairs –1, parking 2, R&D

Description: describe the new data entry

Active:

     V: to activate communication between the PC and the controller. Polling is completed within the specified time intervals in the "polling" menu.

     ☐: to disengage communication between the PC and the controller. Polling does not exist in this case; the controller is not polled and is not downloaded by the system.

Set as default: select this option if the current controller should serve as a reference. Its parameters are automatically copied as default parameters for newly created controllers, thus preventing to have to parameter newly created future controllers.

Company: mentions the company the item refers to; field used mainly in multi-company applications

Controller address:

      Network - or communication port: select an existing network from a list of previously defined networks or create a new network by clicking on the […] button

      Controller address: mention the physical address of the controller in the selected network. The address is contained between 00 and 31; it is defined by the position of the dip switches (internal jumpers) JP4/1 to JP5/6

Controller type: enable to parameterise controllers by default (readers, inputs and outputs). Choose the type of controller from the list:
- ➢ TPL4 & TPL4D4: access, alarm, alarm 15/16, parking, parking with 16 relays, lift
- ➢ NSL
- ➢ DS216

Tips & Notes

Types of controllers and associated readers, inputs and outputs

Type of controller	Doors	Readers	Inputs	Outputs	Notes
TPL4	2	2	8	4	Access control
TPL4 alarm	-	-	15	4	Alarm control only
TPL4 alarm 15/16	-	-	15	16	Alarm control only
TPL4 parking	2	2	8	4	Access control in parking
TPL4 parking 16 relays	2	2	8	16	Access control in parking
TPL4 lift	2	2	8 to 15	64	Lift monitoring
TPL4D4	4	2	16	8	Access control
TPL4D4 alarm	-	-	15	4	Alarm control only
TPL4D4 alarm 16/8	-	-	16	8	Alarm control only
TPL4D4 parking	4	2	16	8	Access control in parking
TPL4D4 parking 16 relays	4	2	8	16	Access control in parking
TPL4D4 lift	4	2	8 to 15	64	Lift monitoring
NSL4	2	2	4	3	Access control only
DS216	-	-	16 anal.	4	Alarm control for analogical inputs

Saving and downloading

Saving the data entered will automatically result in downloading initialisation data, updating date and hour and transferring group parameters, daily and weekly programs for access, reader parameters, card format and access authorizations.

Parameters by default

When entering information with respect to name, network, address and controller type, the system defines controller's parameters (readers, inputs and outputs) by default.

TPL4 parking controllers

In the case of TPL4(D4) or TPL4(D4) 16-relay parking controllers (2 and 4-door), select the requested parking in the field that appears at the bottom of the screen.

TPL4 lift & TPL4 D4 64 relays

A single controller can pilot several lifts independently.

3.3.2. Controller - Reader

The informative table synthesizes reader parameters that are associated to a controller. Default parameters are defined according to the type of controller. To obtain full information and modify the reader data, click on the […] button situated to the right of the table of the corresponding tab.
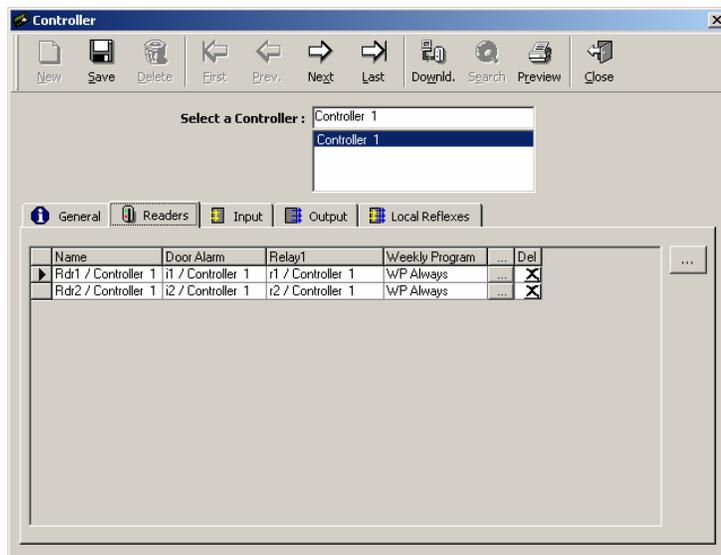
Table explanation

Nom: reader name

Door alarm: name of the input signalling the closure of a door

Relay 1: name of the first output in the system

Weekly program: weekly program that automatically flip-flops the way the reader operates between the two security levels

Button […] (on the line of the reader): click on the button to display the "Reader" screen to consult information or to modify data

Delete: click on the X sign to remove a reader from the list displayed

Button […] (outside the table): click on the button to display the "Reader" screen even if no record is selected

3.3.3. Reader

The "Parameter - Controller - Reader" screen enables the reader's parameters specification. It is accessible from the corresponding tab in the "Parameter - Controller" screen, by pressing on the […] button situated to the right of the table.

Reader parameters are divided into four categories:
- ➢ General
- ➢ Door control
- ➢ Access mode
- ➢ Miscellaneous / Badge format

Tips & Notes

Default Parameters

When entering information linked to the name, network, address and type of controller, the system defines default readers, inputs and outputs.

Modifying default parameters

Suppress readers that automatically appear in the table and are not physically connected. If the default parameters of a reader are not suitable, eliminate the reader from the list and manually create a new data entry. In case of an empty list, click on the […] button to create a reader.

Saving current information

As soon as a new tab is selected all the current information is saved.

Table of default connections for inputs, relays and RTX

	Reader 1	Reader 2	Reader 3	Reader 4
Door alarm	E1	E2	E5	E6
Door relay	R1	R2	R3	R4
RTX	E3	E4	E7	E8

3.3.3.1. Controller - Reader - General

The capture screen about reader's general information can be accessed by clicking on the […] button situated to the right of the corresponding table summary in the "Parameter - Controller" screen.
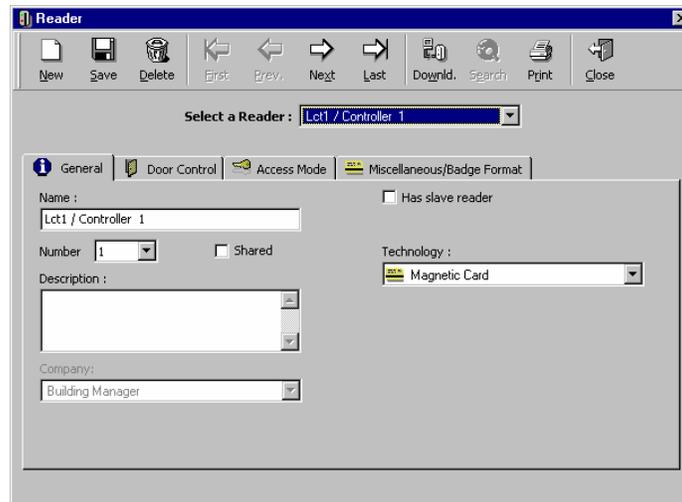
Fields

Name: name the reader

Number: indicate the connector that is hooked up to the reader, to be chosen between 1 and 2 for a 2-door controller and between 1 and 4 for a 4-door one

Shared: share the information between different companies, in a case of multi-company applications

Description: describe the new data entry

Company: mentions the company the item refers to; field used mainly in multi-company applications

Has a slave reader: if affirmative, specify the name of the slave reader

Technology: select the reader technology from the list:
  ➢ Magnetic
  ➢ Bar code
  ➢ Wiegand
  ➢ Smart card 1
  ➢ Smart card 2
  ➢ Smart card 3
  ➢ Touch
  ➢ Radio
  ➢ Motorised reader

The information downloaded to the readers is limited to the types of badges specified above. Please note that badge technology is specified in the "Type" option in the "Parameter - Badge" screen.

Note, when a reader is deleted in the "Parameter – Controller'' screen its slave reader is also deleted

3.3.3.2. Controller - Reader - Door Control

This screen defines the way the door is wired

Fields

Input: select the alarm to which the door opening control device is wired

Door alarm: select the alarm input from the list; an alarm is set off when a door is forced or stays open beyond a predefined delay

Feedback: select this option in order to verify the entry or exit of a badge holder that has been granted access

Operation mode: A badge holder swipes his badge through a reader. The controller authorizes access to the badge holder by ac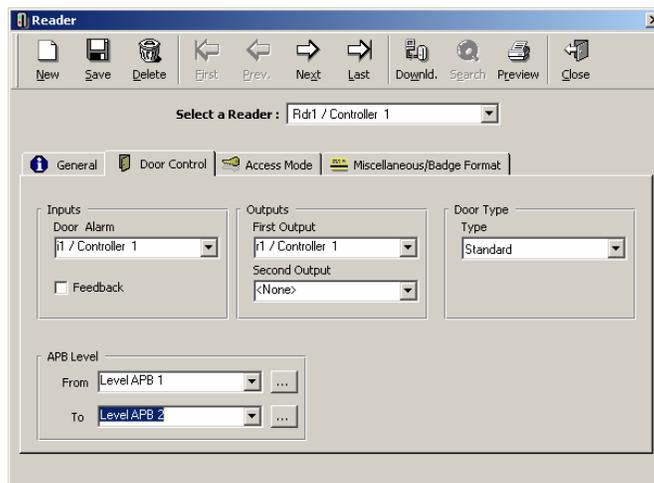tivating a door relay. During the predefined door alarm delay, at which time the door can be opened, the controller goes into a waiting mode. If the door has been opened and closed - as will attest the door contact activation - the badge holder is supposed to have passed and the controller records the access transaction in memory. If the door has not been opened, the door contact is not activated and the controller records the transaction "access refused" in memory

APB Level

 From: select the reader's APB level at the time access is requested from the list or click on the […] button to define a new APB level

 To: select the reader's APB level after access has been granted and after passage through the door from the list or click on the […] button to define a new APB level

Outputs 1 and 2: select the relays of the activated controller following access authorization; define separately for the two relays of the reader

Door type: select from the list:

      Standard door: access is granted if badge is authorized

      Door controlled by input: a door is controlled by a signal with respect to the status of the input. Specify the input in question. The door opens if the status of the door is active but remains closed if the status is inactive.

      Man trap 1, 3, 4: select this option if the doors operate in the man trap mode, which means that the passage through two consecutive doors is a requisite in order to access a site. Refer to the page "Man Trap" for more information on how to use this parameter.

      Manually controlled: access is manually regulated

3.3.3.3. Man Trap

The man trap mode supervises the activation process of an interlock entrance. The opening of a door and the possible activation of an input, condition the opening of a second door.

Amadeus 5 supervises three types of man traps:
- ➢ The first door will open only if the second door is closed (Man trap 1)
- ➢ The second door opens automatically following the opening and closure of the first door (Man trap 3)
- ➢ The second door automatically opens consecutively to the following two conditions (Man trap 4):
  - o Opening and closure of the first door and
  - o Receipt of a signal - activation of an input

In order to parameterise a man trap entrance, go to the option "Door Type" of the menu "Parameter - Controller - Reader - Door Control".

Three types of mantrap configurations are recognized:

Man trap 1: 2 doors / 2 readers

Principle: the first door opens only if the second door is closed.

Operation mode

Both readers of a same controller monitor two doors. The first reader is in a waiting state as long as the second door is opened and as a result the first door remains shut. The contact relay status attests to the opening or closure of doors.

The "Controlled by Input" field must not be selected.

Man trap 3: 2 doors / 2 readers

Principle: the second door opens automatically following the opening and closing of the first door.

Operation mode

Both readers of a same controller monitor two doors. When the first door opens and closes the second door automatically opens. The door contact relay status attests of the opening and closure of the doors.

The "Controlled by Input" field must not be selected.

Man trap 4: 2 doors / 2 readers

Principle: the second door opens automatically after the following two conditions have been met:
- ➢ Opening and closure of the first door AND
- ➢ Receipt of a signal - activation of an input

Operation mode

Both readers of the same controller supervise two doors. When the first door opens and closes, and a predefined input is activated, the second door opens automatically. The status of the door contact relay attests of the opening/closure of the doors.

Select the "Controlled by Input" field and specify the input activated.

3.3.3.4. Controller - Reader - Access Mode
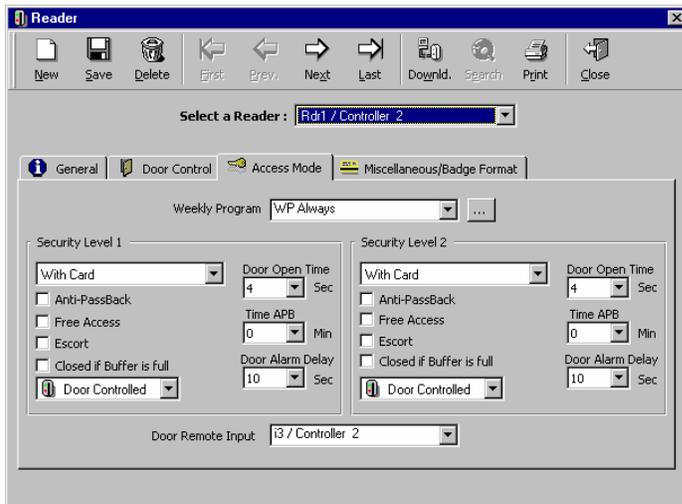
The reader can operate differently according to predetermined time zones. The parameters of these two operation modes - or security levels - are defined in the "Parameter - Controller - Reader - Access Mode" screen.

Example

During office hours, access is freely granted (no need to swipe a badge). After office hours, badges need to be swiped (controlled door).

Fields

Weekly program: choose the weekly program that automatically flip-flops the reader's functioning mode between the two security levels. The default weekly program is always associated with security level Number 1.

Security level 1 and 2: must be filled out separately for both access modes

Access authorization: define the manner in which the authorization access must be required:
  ➢ With card
  ➢ With keypad, for the entry of a PIN code (Personal identification number)
  ➢ With card OR keypad
  ➢ With card AND keypad

Anti-Passback: refer to "Anti-passback" chapter

Free access: select to grant unlimited access to all badge holders registered in the system without any limitation of time zones or access groups

Escort: select this function to require a double valid card reading - the employee who needs escort and his escort - to authorise access at certain readers. The escort has 10 sec. to present his badge.

If the escort needs to be performed by an authorised cardholder (supervisor), specify it in the "Parameter – All Cardholder" screen, by choosing the function "Need Escort".

A weekly program can be linked to the escort function, requesting the double badge reading only at certain time zones.

Close if buffer is full: select to authorize access only when the corresponding transaction can be registered in the system memory. If this option is not selected, access is granted even if the buffer is full and, as a consequence, transactions are not recorded.

Door mode
- ➢ **Door open**: access mode in which the door is permanently open
- ➢ **Door closed**: access mode in which the door is permanently closed; access is always refused even with valid badge
- ➢ **Door controlled**: standard access control mode, in which access depends on the badge and its authorizations

Door open time (from 0 to 120 seconds): delay during which the badge holder has to pass through the door after receiving authorization access; it corresponds to the time delay of the door activation relay

Note
Alternated mode (Door open time set to 122): the door relay opens after the first valid swipe and stays open; the door closes only after a second badge reading and stays closed, and so on

Time APB (from 0 to 15 minutes): waiting period between two successive access authorizations granted to the same badge through the same reader; the second access can only be granted after the predefined time delay has elapsed

Door alarm delay (from 0 to 75 seconds, by multiples of 5): delay during which the door must remain closed; if the door is still open beyond the closure delay an alarm is activated

Door remote output: define the controller input connected to the door remote output; by default the door remote output for readers 1 to 4 are connected respectively to input 3, 4, 7 and 8.

3.3.3.5. Controller - Reader - Badge Format

The "Parameter - Controller - Reader - Badge Format" screen defines the character codes to read on magnetic, bar code and Wiegand cards.

A badge, or card, is a physical medium that has a unique code enabling its identification. Most of the time, this code is randomly attributed and unknown to the user. Badge recognition required registration of their code in the system memory. When a badge is being read the system verifies if the badge is known and if yes, to whom it is attributed, in order to check the person's access authorization.

Numerous card technologies are available: magnetic, bar code, Wiegand, proximity, smart cards, etc. Amadeus 5, as well as our controllers, is compatible with the majority of reader technologies on the market today.

The technology used must be defined in the "Parameter - Controller - Reader" screen. Jumpers on the controller's electronic card help to select the technology.

There are various formats of magnetic, bar code and Wiegand technologies. By default the system reads the first 8 encoded numbers on the badge but this reading can be changed as described hereunder.

3.3.3.5.1. Card Format: Magnetic or Bar Code

In the "Parameter - Controller - Reader" screen, specify the technology "Magnetic" or "Bar Code".

The information about the card code and the customer code are entered in the "Parameter - Controller - Reader - Badge Format" screen.
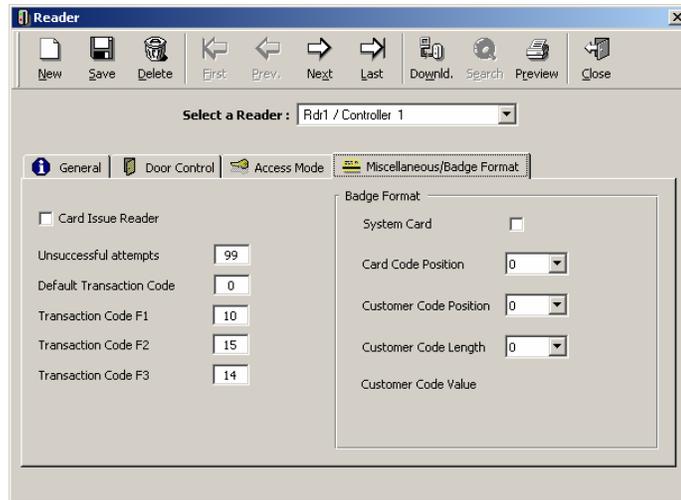
Fields

System card: card on which a four-digit number between 1 and 9999 has been inscribed; since the card number is already on the badge, it enables immediate recognition of the badge holder and therefore, a system badge need not be recorded up in the system.

Card code position: a bar code or magnetic code may contain many numbers or characters. The system only records the 8-digit code; by default, the first 8 characters of the badge code. It is possible however to read another 8-digit by specifying the position of the first one in the "Badge Code Position" field. (Value between 00 and 29, the default value "00" corresponds to the first encoded character)

Customer code: this unique code appears on all the cards of a same company, besides the badge code; the use of a customer code value is optional and strengthens system security by identifying the company

By the default this option is not used. To use it, fill out the following three fields:

Customer code position: specify the position of the first character of the code; choose a value between 0 and 29 (00 corresponds to the position of the first number encoded in the badge)

Customer code length: specify the size of the code to be read; choose a value between 0 and 8 (0 is the default value, which means that the customer code value is not verified)

Customer code value: enter the customer code value into the squares that appear on the screen

3.3.3.5.2. Wiegand Card Format

The use of Wiegand technology is specified in the "Parameter - Controller - Reader" screen. Amadeus 5 recognizes the hexadecimal and decimal Wiegand formats, among others.

General Format (Hexadecimal)
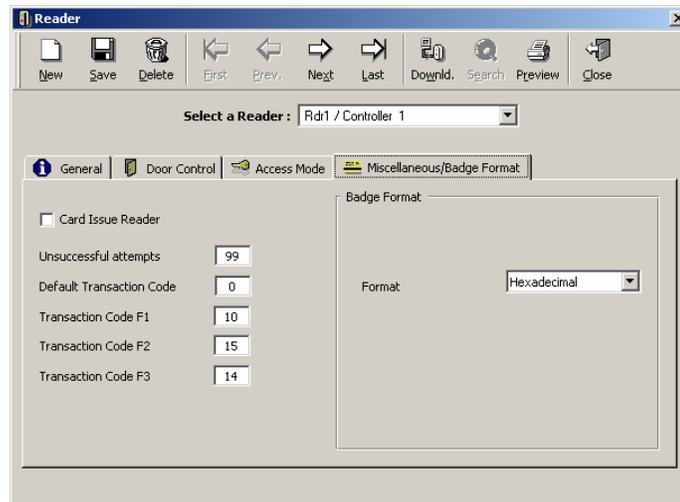
The "Hexadecimal Wiegand" format must be selected in the "Parameter - Controller - Reader - Badge Format" screen.

There are many standards on the market. Our controllers can read all Wiegand cards up to 50 bits, including 48 bits data (12 binary characters) and 2 parity bits. The system stores in its memory only the 8 least important characters, in other words the last 8 characters of the code.

Two parity bites are added to the card besides the badge code for confirmation of a proper reading. Most Wiegand standards use a similar algorithm to calculate these parity bites and this algorithm has been integrated into the controllers. It is thus preferable to use it by selecting the corresponding jumpers on the controllers' electronic card.

However, certain card standards have original algorithm for the calculation of bite parity. In order to enable these controllers to read these badges, the jumper position "no parity bites" must be selected. (See the controller installation manual for further details).

Wiegand decimal format

The card has a five decimal digit code (often clearly printed on the card) and sometimes a 3-digit decimal customer code value.

To specify the use of Wiegand decimal format:
> Select the decimal format in the "Parameter - Controller - Reader - Badge Format"
> If the customer code value does not need to be checked, enter "0" in the "Customer Code Length" field
> If the customer code value needs checking, enter the value 3 in the "Customer Code length" field and type the 3-digit code in the 'customer code value' field

3.3.3.6. Controller - Reader - Miscellaneous
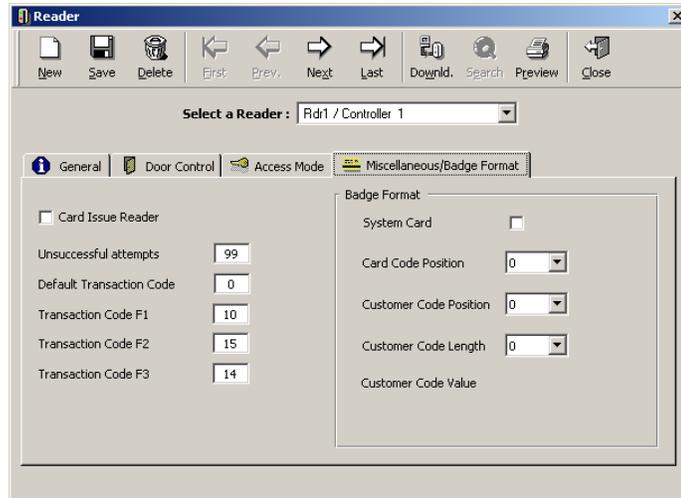
<ins>Fields</ins>

Card issue reader: select this option to create new badges using a reader. If the reader is in the card issue reader mode, it cannot be used for access control purposes.

The card issue reader is generally situated close to the computer.

Swiping a badge through a reader will generate different reactions according to the type of reader:
  - ➤ Standard reader: the system checks in the database if the card code exists and what the access authorizations are
  - ➤ Card issue reader: the card code is sent to the computer and a new badge is created; this prevents the two seconds waiting time after each reading of cards

Unsuccessful attempts: specify the number of unsuccessful attempts tolerated by the system before an alarm is raised; choose a number from 00 to 99

Transaction code F1, F2, F3: specify the code sent by the controller to the PC during the process of an access request; the user via the reader keypad can modify this code

3.3.4. Controller - Input

The informative table summarizes the input parameters connected to the controllers. Default parameters are defined according to the controller type. To obtain more detailed information and modify input data click on the […] button situated to the right of the table of the corresponding tab.

Inputs are used for access control or for alarm monitoring purposes. A digital input is either normally open or normally closed. In access control, this corresponds to the opening and closure of a door. In alarm monitoring, this corresponds to the normal or abnormal status of the input.

Each input can be used for:
➢ **Door control**: a door contact device is connected to the input; an alarm is activated in case a door is forced or left open beyond the specified delay period
➢ **Exit request**: a RTX button is connected to the input, this will lead to the activation of the corresponding door relay
➢ **General alarm input**: the activation of a sensor/detector connected to an armed alarm input triggers:
    o An alarm
    o Predefined relays or local reflexes
    o Automatic processes or predefined global reflexes
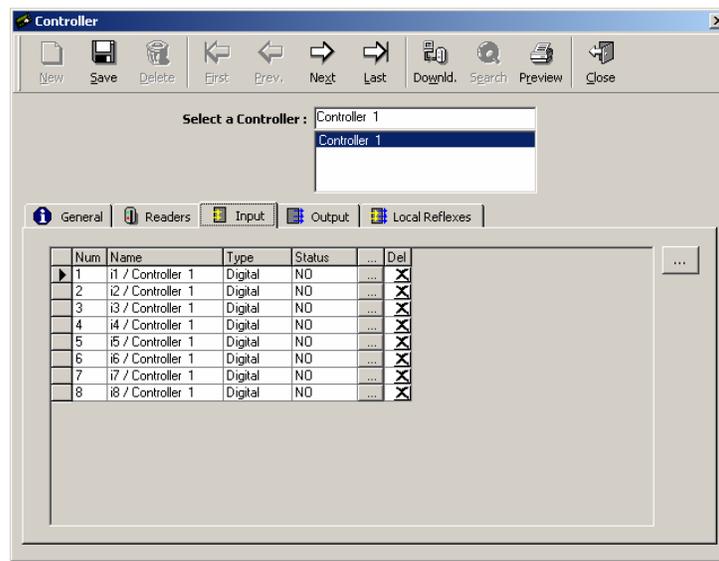
Table analysis

Number: number of the selected input

Name: name of the input

Type: digital

Status: NO - normally open or NF - normally closed

Button […] (on the input line): click on this button to display the "Input" screen for consultation or modification purposes

Delete: click on the X sign to remove one input from the list displayed

Button […] (outside the table): click on this button to display the "Input" screen even if no input is selected

3.3.5. Input

3.3.5.1. Input – General

The "Input" screen enables the input parameter definition. It can be reached from to the corresponding tab of the "Parameter - Controller" screen, by clicking on the […] button situated to the right of the table.
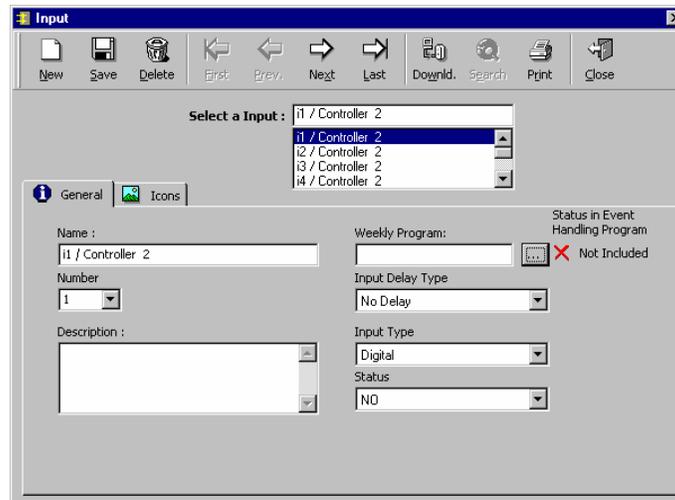

Fields

Name: name the input

Number: choose the input number, between 1 and 16; the maximum input number connectable depends on the type of controller used

Description: describe the new data entry

Icon: select the icon that graphically represents the input in the "Active alarms" screen; the icons must then be positioned on maps in the "Position" screen
Form the list, choose a graphic icon, which will appear on the maps or select the […] button to create a new icon.

Weekly program: assign a program to the input to define alarm activation and non-activation periods; to modify the program click on the […] button

Input delay type:
- ➢ No delay: an alarm is raised as soon as the input is activated
- ➢ After … (if still on alarm): specify the number of seconds, in multiple of 25, beyond which an alarm is raised if the input is still activated
- ➢ After…(even if no more on alarm): specify the number of seconds beyond which an alarm is raised, without further check of the activation state

Input type: the input reacts to digital signals (magnetic contacts, movement detectors, etc.)

Status: standard status of a digital input, **NO**, normally open or **NC**, normally closed
Note that the inputs defined in the "Parameter - Controller - Input" screen are not compatible with the MINILOCK.

3.3.5.2. Input – Icons

Choose the icons representing the input when it physical status is ON and OFF.
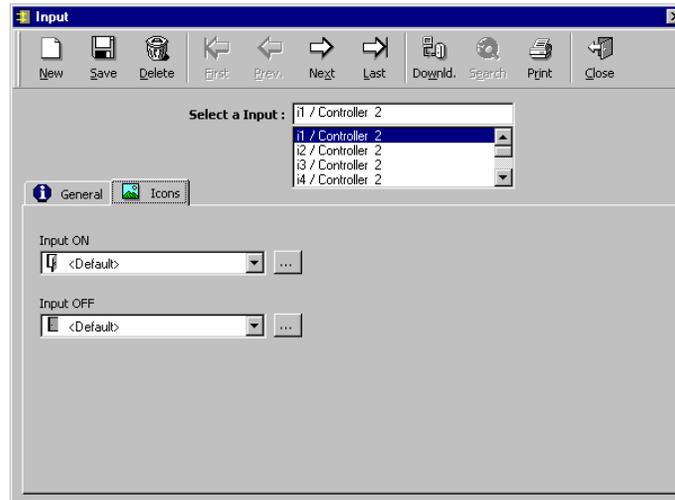
Fields

Input ON: in the list, choose the icon associated to the input which physical status is ON, or select the […] button to create a new one

Input OFF: in the list, choose the icon associated to the input which physical status is OFF, or select the […] button to create a new one

The icons associated by default are as follow

> ➢ For the first two inputs, door open for ON, door close for OFF
> ➢ For all other inputs, red circle for ON, white circle for OFF

The icons are dragged and dropped on maps in the "Event-handling – Position" screen. The icons can be automatically be updated in the "Event-handling – Active Alarms" screen according to the input physical status, if the initialisation parameter "NO IO = 1"

3.3.6. Controller - Output

The informative table summarizes the parameters of the outputs connected to the controllers. Default relays are defined according to controller definition. To obtain more detailed information and modify input data, click on the […] button situated to the right of the table of the corresponding tab.
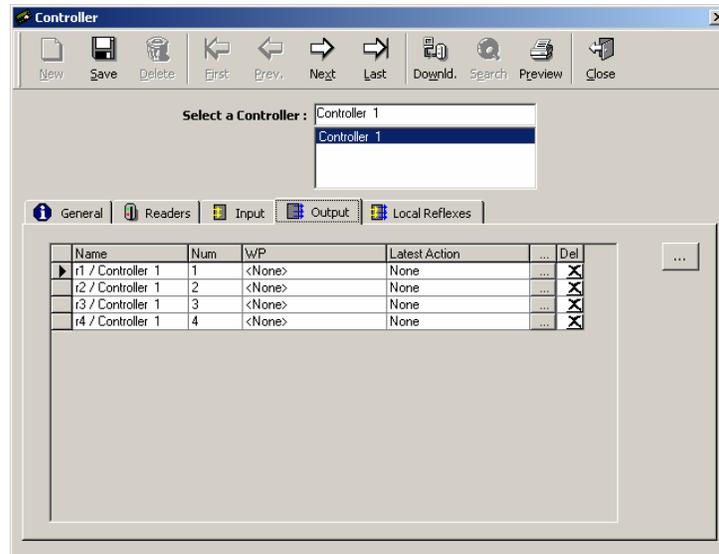

Table analysis

Name: name of the output

Number: number of the output selected

Weekly program: name of the weekly program associated with the output, defining the activation and non-activation periods

Last action: mention of the last action that could have affected the output; for instance, the action that closed a "normally open" output by a global reflex

Button […] (on the relay line): click on this button to display the "Output" screen in order to consult or modify data

Del (Delete): click on the X sign to delete an output from the list displayed

Button […] (outside the table): click on this button to display the "Output" screen even if no item is selected

3.3.7. Output

3.3.7.1. Output - General

The "Parameter - Controller - Output" screen allows output parameter definition. It is accessible by going to the corresponding tab of the "Parameter - Controller" screen and clicking on the […] button located to the right of the table.
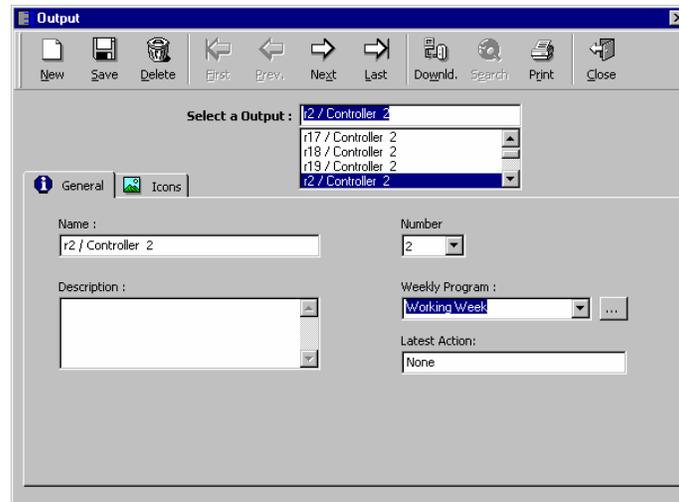
Fields

Name: name the output

Description: describe the new data entry

Number: choose the output number, between 1 and 16; the maximum number depends on the type of controller used

Weekly program: select from the list the program defining the output's activation and non-activation periods or click on the […] button to create a new weekly program
Note that the weekly program cannot be modified from this field.

Latest action: mention the last action that could have affected the output; for instance, the action that closed a "normally open" output by a global reflex

3.3.7.2. Output - Icons

Choose the icons representing the input when it physical status is ON and OFF.
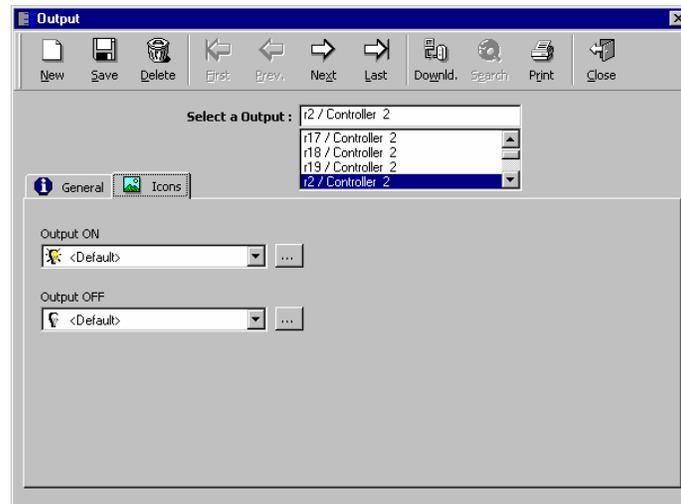
Fields

Output ON: in the list, choose the icon associated to the output when its physical status switches to ON, or select the […] button to create a new one; default icon: a yellow lit bulb

Output OFF: in the list, choose the icon associated to the output when its physical status switches to OFF, or select the […] button to create a new one; default icon: a white bulb

3.3.8. Controller - Local Reflex

A local reflex defines the outputs' activation following the trigger of an input of this same controller. The reflex occurs even if communication with the controller is interrupted. The "Local reflex" screen defines the connection of inputs and outputs.

The informative table summarizes the parameters of the local reflexes associated with the controller. To obtain more detailed information and modify the data, click on the […] button situated to the right of the table of the corresponding tab.
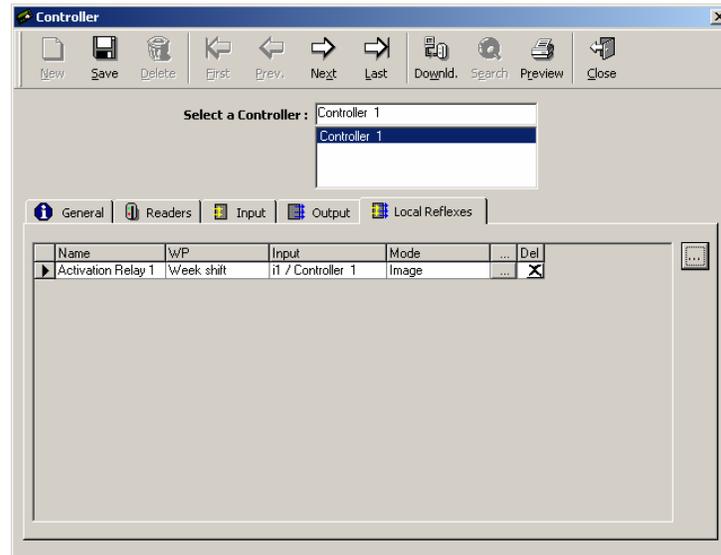

Table analysis

Name: name of the reflex

Weekly program: the local reflex' weekly program defines the reflex activation and non-activation periods

Input: name of the input that sets off the local reflex

Mode: type of action set off by the local reflex (image, constant on, during)

Button […] (on the line of the reflex): click on this button to display the "Parameter - Controller - Local Reflex" screen, in order to consult or modify data

**Del** (delete): click on the X to delete a reflex from the list displayed

Button […] (outside the table): click on this button to display the "Parameter - Controller - Local Reflex" screen, even if no item is selected

3.3.9. Local Reflex

A local reflex defines the outputs' activation following the trigger of an input of this same controller.

The "Parameter - Controller - Local reflex" screen allows the definition of the reflex parameters. It is accessible by going to the corresponding tab of the "Parameter - Controller" screen and clicking on the […] button located to the right of the table.
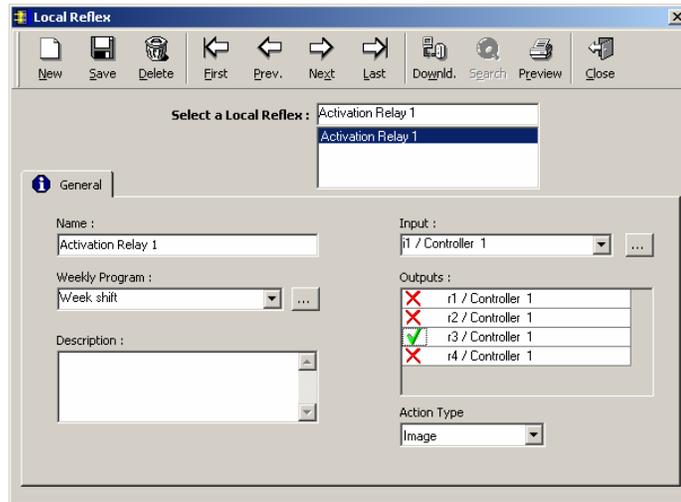
<u>Fields</u>

Name: name the reflex

Weekly program: choose from the list the weekly program which defines the reflex's activation and non-activation periods or click on the […] button to create a new weekly program
Note that the weekly program cannot be modified from this field.

Description: describe the new data entry

Input: from the list, choose the input setting off the local reflex or click on the […] button to create a new input

Output: click on the X or V to activate or deactivate the output

Action type: choose the type of action set off by the local reflex (image, constant on, during (multiples of 2 seconds))

3.4. Time Zone

3.4.1. Basic Concepts

Time zones consist of calendar divisions into daily, weekly and holiday time segments associated with predetermined system functions.

The system recognizes:
> * **Daily program**: division of a 24-hour day into access and non-access zones
> * **Weekly program**: made up of a daily program for each day of the week and a supplementary daily program for holidays
> * **Holiday**: dates specified as holidays

These programs are used during periods of time during which:
> * **Employees** access different areas of a site according to their access group
> * **Readers** operate in predefined access modes
> * **Alarms** are armed
> * **Relays** are automatically activated

Time zone application table

	Within the limits of the program	Beyond the limits of the program
Access control	Access granted according to access group	Access refused
Readers	Access mode 1	Access mode 2
Alarm zones	Armed	Not armed
Relays	Activated	Non activated

Tips & Notes

Arming alarms

Refer to the "Event Handling - Active Alarm" paragraph for more information regarding how to arm an alarm.

Importance of a proper definition

Properly defining time zones is essential for the system to work optimally.
It is highly recommended to successively specify the daily, weekly and holiday programs prior to defining the other parameters of the system.

Maximum number of usable programs

Many daily, weekly and holiday programs can be created by the system but the type of controller employed restricts the number of usable programs. An error message appears if the limit of usable programs has been exceeded

Number of usable time zones according to the type of controller

Controller	Daily programs	Weekly programs	Holiday programs
TPL4 & TPL4D4	99	32	20
NSL4	7	4	20
DS216	99	32	20

3.4.2. Daily Program

The division of days (24H) into time zones, to which are associated the system's predetermined functions, is defined in this screen. A maximum of 4 access zones and 5 non-access zones are usable. Refer to the chapter "Time Zones" for the basic concepts.
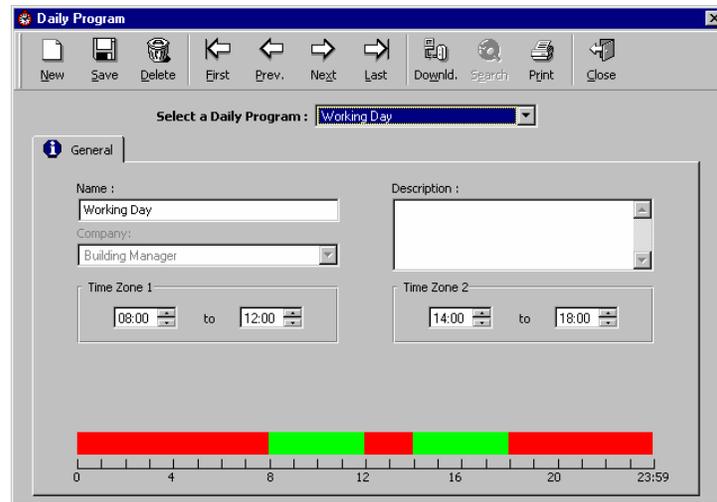
Fields

Name: name the new daily program; examples: part-time AM, night team

Company: mentions the company the item refers to; used mainly in multi-company applications

Description: describe the new data entry

Time zones 1- 4: define the limits of the 4 time zones using the format XX:YY, where X = hour and Y = minute

The ruler at the bottom of the screen gives the time frames in a visual manner.
  ➢ The **green** frames represent the access time zones (4 maximum)
  ➢ The **red** frames represent the restricted time zones (5 maximum)

Tips & Notes

Controllers that can recognize 2 or 4 zones in the daily programs

Controllers equipped with an EPROM dating from 1/1/2000 are compatible with 4 zones.

Controllers equipped with an EPROM dating before the year 2000 recognize only 2 time zones. If only 2 time zones appear on the screen, the first thing to do is to check the date of the EPROM.

The number of time zones by default can be modified in the "Communication" tab in the "Options" menu in the "Tools" section. The firmware date is available in the "Communication - Diagnostic" screen.

Number of time zones according to the date of the EPROM

Number of time zones posted	EPROM date	Comment
4	<1/1/2000	Communication error
4	>1/1/2000	OK
2	<1/1/2000	OK
2	> 1/1/2000	Modify the number of zones from 2 to 4

Maximum usable programs

A big number of daily, weekly and holiday programs can be created. However the type of controller restricts the number of programs that can be used at a time. By default, TPL4 controllers recognize a maximum of 99 daily programs.

Programs by default

The two daily programs "All the time" and "Never" are defined by default. Their denomination can be modified but the two programs can neither be erased or their contents modified. The "Always" program is selected by default.

New daily program

The time frames for a new daily program are from 8 AM to12 AM and from 2 PM to 6 PM.

3.4.3. Weekly Program

A weekly program is made up of 8 daily programs, one for each day of the week and an extra program for holidays. Refer to the "Time Zones" chapter for the basic concepts.
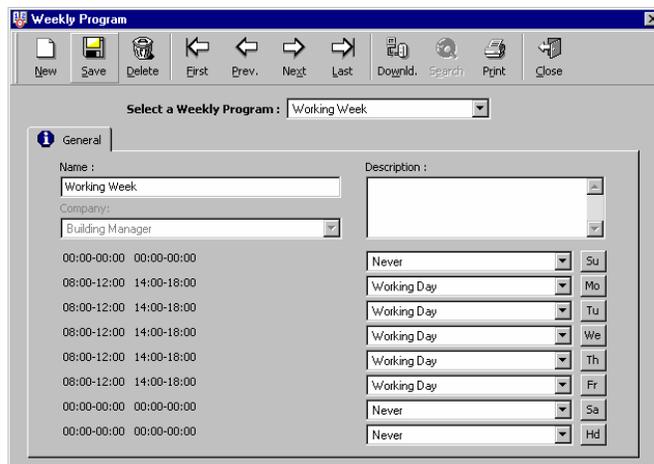
Fields

Name: name the new weekly program

Company: mentions the company the item refers to; used mainly in multi-company applications

Description: describe the new data entry

Daily programs: one for each day of the week (Sunday - Saturday) and one for holidays (Hd); select the adequate program from the list or create a new daily program by clicking on the [...] button associated with the day

Time frames corresponding to the program selected are displayed on a grey background.

Tips & Notes

Maximum number of usable programs

The system can create many daily, weekly, and holiday programs. However the type of controller being used limits the number of usable programs. By default, TPL4 controllers recognize a maximum of 32 weekly programs.

Programs by default

The two weekly programs "All the time" and "Never" are defined by default. Their denomination can be modified but both programs can neither be deleted nor modified. The "Always" program is selected by default.

3.4.4. Holiday

Days considered holidays by the system are defined in this screen. During holydays access is refused for everybody. Nevertheless individual authorizations can be granted in the "Parameter - All Cardholders" screen. The TPL4 controllers recognize a maximum of 20 holidays. Refer to the chapter "Time Zone" for basic concepts.

<u>**Fields**</u>

Name: name the new program

Description: describe the new data entry

Date: the current date is listed by default. In the calendar, it will appear circled in red. To call up the calendar, click on the arrow situated to the right of the current date. Select the day, month and year in the calendar that appears on the screen. By clicking on "Today" the calendar of the current month appears on the screen. The date can also be entered directly on the screen.

To select a given month
 ➢ Produce the list of months by pressing on the name of the month displayed
 ➢ Skip from one month to the next by pressing on one of the double arrow keys' ends (next to the month)
 ➢ Scroll the calendar from month to month by pressing and maintaining depressed on one of the double arrow keys' ends (next to the month)

To select the desired year
 ➢ Produce the list of years by pressing on the name of the year displayed
 ➢ Skip from one year to the next by pressing on one of the double arrow keys' ends (next to the year)
 ➢ Scroll the calendar from year to year by pressing and maintaining depressed on one of the double arrow keys' ends (next to the year)

Each year: select to repeat the definition of a holiday for coming years; for example, Christmas always falls on the 25 of December.

Company: mentions the company the item refers to; used mainly in multi-company applications

<u>**Tips & Notes**</u>

Maximum number of usable programs

Many daily, weekly and holiday programs can be created by the system. However the type of controller restricts the number of usable programs. By default, TPL4 controllers recognize up to 20 holidays.

Holidays in red

A date, which is defined as a holiday, appears in red on the calendar.

3.5. Access Group

This function determines "who can go where and when". The access group attributed to employees determines the doors accessible, the weekly programs associated with the doors and the door crisis level.

To use this function:
- ➢ Select the authorized doors for the individuals of a group
- ➢ Associate the corresponding weekly programs
- ➢ Attribute a crisis level to each group
- ➢ Attribute an access group to each employee, in the "Parameter - All Cardholders - General" screen

The system does not limit the number of access groups. However if a large number of access groups are required due to the variability of the badge holders' work hours, it is recommended:
- ➢ To create an access group that guarantee permanent free access and, at the same time
- ➢ To restrict access by using personal weekly programs and individual crisis levels, in the personalised data of the badge holder

When a new data is created, status for all doors is checked. By default, minimal authorization is granted.
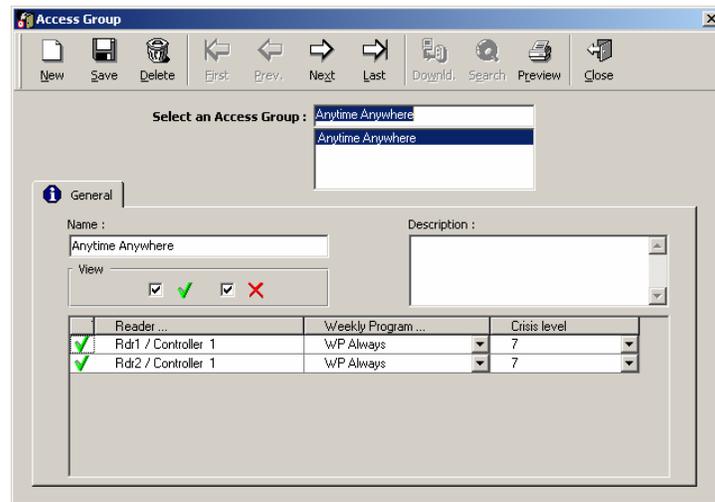
Fields

Name: enter a name for the access group

Description: describe the new data entry

View: display the list
- ➢ V: readers for which access is granted
- ➢ X: readers for which access is refused
- ➢ X & V: all readers
- ➢ --: no reader

First column of the table: **V or X**
Select V to include the reader in the access group
Select X to exclude the reader from the access group

Please note the difference in the error message associated with an access refusal in the following two cases:

Reader	Weekly Program	Error message
V	Never	Time zone forbidden to access
X	-	Reader forbidden to access

Reader: list of readers and doors associated

Weekly program: select the weekly programs associated with the reader from the list or create a new program by clicking on the […] button; the personal weekly program suggested in the list is defined in the "Personal" tab of the screen "Parameter - All Cardholders"

Crisis level: enter the individual crisis level; the personal crisis level suggested in the list is defined in the "Personal" tab of the screen "Parameter - All Cardholders"
Refer to the " Manual Action - Crisis Level" chapter for more information.

3.6. Department

A department is a functional notion, which allows site division into various work areas. This function is mostly informative. A department can be chosen as a selection criterion to display and print reports.

Examples

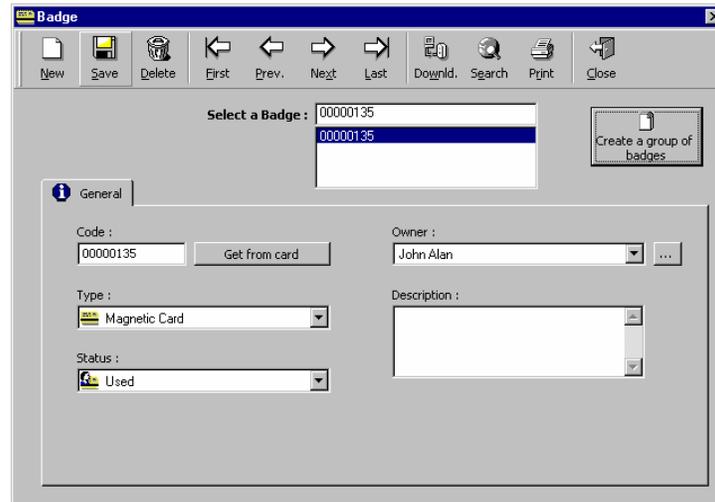Administration, R&D, Top Management
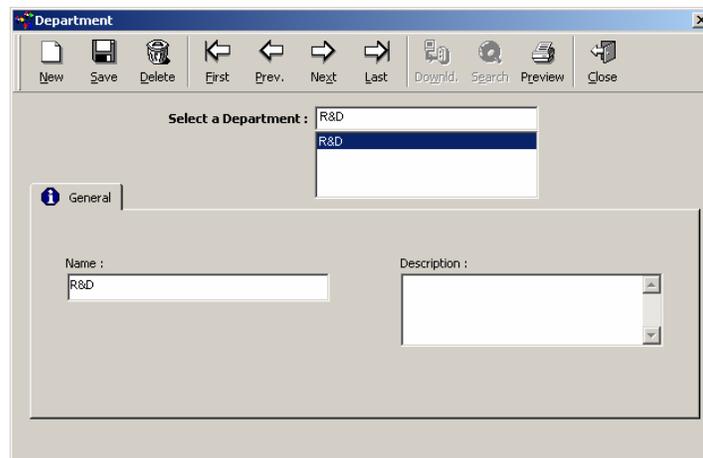
Fields

Name: name the new department

Description: describe the new data entry

3.7. Badge

This screen defines the badges used and who is allowed to use them.

Fields

Code: sequence of 8 characters using numbers from "0" to "9" and letters from "A" to "F"; if the length of the code is smaller than 8 characters the system will complete it by adding zeros at the beginning of the code

Get from card: press on the button to get the code from by reading the card

Type: choose the badge technology from the following list:
- ➤ Magnetic
- ➤ Bar code
- ➤ Wiegand
- ➤ Smart card 1
- ➤ Smart card 2
- ➤ Smart card 3
- ➤ Touch
- ➤ Radio

Please note that badge technology is defined in the "Technology" option in the "Parameter - Controller - Reader - General" screen. Information about badges is only downloaded to readers of compatible technology.

Status: specify the status of the badge
- ➤ Used
- ➤ Cancelled
- ➤ Free (default)
- ➤ Lost
- ➤ Stolen

A badge cancelled, lost or stolen is automatically invalidated in the system.

Owner: assign a badge to an individual; when an attributed code is selected, the name and surname of the badge holder appear in this field. The field remains empty if the code entered is not attributed. From the list, select the employee who is going to receive a new badge. Click on the [...] button to display the employee's screen.

Description: describe the new data entry

Create a group of badges: create a series of badges by clicking just on this option. In which case, a new window opens.

3.7.1. Badge Search

It is possible to check if a badge exists according to the code.

Displaying the list of all the attributed badges

Double click on the "Search" icon of the icon bar.

Performing a search according to the code
- ➢ Enter the code
- ➢ Click on the "Search" icon of the icon bar
- ➢ If the badge is attributed, details of the badge will be displayed on the screen
- ➢ If the code is not in use, the fields remain empty and the screen has a grey tint
- ➢ Click on the "Search" icon a second time to exit the screen

Performing a search using the first characters of the code

If the first characters of the code have been entered, the system will display all the badges that start with the desired sequence.

Examples:

In the "Code" field type	The system displays all the card codes attributed
"32*"	Beginning with "32"
"32%45"	Beginning with "32", which last two characters are "45"

3.7.2. Group of Badges

This menu allows the creation a group of cards in a single command.

It is accessible via the menu "Parameter - Badge" or "Options - Create a group of badges".

Fields

First card code: type the 8-character code assigned to the first badge

Number: type the number of badges to define; the list has been provided for information. The maximum number of badges depends on the type of controller used.

Type: choose the badge technology from the following list:
- ➢ Magnetic
- ➢ Bar code
- ➢ Wiegand
- ➢ Smart card 1
- ➢ Smart card 2
- ➢ Smart card 3
- ➢ Touch
- ➢ Radio

The choice of reading technology will enable selective data transfer to the readers. Only data compatible with the selected technology will be transferred to the readers.

Position to increment (between 0 and 8): define the position of the character to increment in the 8-character sequence making up the code. This allows keeping a constant group of characters as code endings. To use this function, it is necessary that only numbers compose the beginning of the code, till the position to increment.

Example

Code	Position to increment	Next Code
12345ABC	5	12346ABC

Create also the cardholder: create simultaneously a group of badges and the same number of badge holder

　　　Basic parameters: create a valid employee to whom the access group "Everywhere - Always" is attributed

　　　Set parameters same as: specify the name of the badge holder whose parameters will serve as reference for new badges

3.8. Cardholders

3.8.1. Cardholders - Basic Concepts

Each badge holder, employee, visitor or guard, that requires access authorization to the site must be recorded beforehand in the database. To access or modified information related only to visitor or guard, consult the screens "Parameters - Visitor" or " Modules " Guard".

The "Parameter - Cardholders" screen defines the details of all the users, employee and visitor alike. The menu is divided into four tabs:
- ➢ General information
- ➢ Personal information
- ➢ Location data
- ➢ Customized fields

Tips & Notes

Quick definition

The family name is the only obligatory field for creating a new badge. Nevertheless, in order to grant access, the field "Badge" is necessary. The access group granting minimal access is associated by default to the new cardholder.

3.8.2. Cardholders - General

This screen records general information about the badge holder.

<u>**Fields**</u>

Delete (in the tool bar): delete the badge holder from the database. Deleted badge holders are not erased from the database but saved under the type "Deleted record". They are not displayed by default.

Actions following the badge holder deletion:
- The badge holder is classified as "Deleted"
- The corresponding badge allocation is removed
- The badge is added to the non-allocated badges list
- The validation case is unchecked
- The record disappear from the badge holder screen, unless the "Show Deleted" box is selected

Note that only allocated cards are taken into account into the computation of the plug limitation.

<u>**General**</u>

Last name and first name of the cardholder

Number: enter an identification number

Type: choose between "employee", "visitor" or "guard"; the "Type" field does not appear in the "Visitor" or "Guard" screens

Company: mention the name of the company the badge holder works for

Display photo: click on the icon of the file to select the name of the file beholding the employee's picture (jpeg or bmp)

Show deleted: select to display the deleted badge holders; by default, this box is unchecked

<u>**Location**</u>

Department: select the department the employee works for from the list provided or create a new department by clicking on the […] button

Office phone: mention the office phone number, the cell phone number, etc.

<u>**Badge**</u>

An employee cannot have several badges of the same technology. It is possible to:
- **Create new**: create a new badge and associate it to an employee
- **Allocate**: allocate an existing badge
- **Edit**: display details of existing badges
- **Remove**: remove the badge information

<u>**Access**</u>

Access group: select an access group from the list or click on the […] button

Personal weekly program: select the personal weekly program from the list or create a new program by clicking on the […] button; this program is only used if its value matches the access group one

PIN code: mention the badge holder personal identification code to enter on the reader's keypad; this code is common to all the reading technologies used

Personal crisis level: select the individual crisis level, between 0 and 7

<u>**Validated**</u>

From date: specify the beginning date of the validation period of the badge holder

To use the validation date
- Uncheck (clear) the "Validation" box
- Check the "From Date" box
- Set a future validation in date in the "From Date" field
- Save

Note: if the validation date chosen belongs to the past, the "Validation" box will be checked automatically.

Every 30 minutes, at xx:15 and xx:45, the program verifies if new cardholders need validating (if their "From date" is due), in which case the corresponding cardholders modified definitions are sent to the controllers.

To date: use this function to limit badge validity; click on the white square to activate this option. Specify the date and hour when the badge validity will end. Type data in directly or select a date by using the direction arrows. Beyond the specified validity date, the badge will automatically become invalid.

Validated: select this function to validate badge use; a non-validated badge exists in the database but its used will be forbidden

Set as default: the badge holder selected serves as a reference. His parameters are automatically copied as default parameters for newly created badge holders. This function saves the trouble of having to define parameters for all the employees, visitors and guards that will be created in the future.

3.8.3. Cardholders - Personal

This screen records personal information about the badge holder.

Fields

Address: enter the badge holder's address, including street, city, district, zip, phone and fax numbers

Description: describe the new data entry

Car number: enter the employee's car license number; the parking lot module of the application will use this data

ID: give the employee an identification number such as a social security number, employee number, etc.

Privileges: certain privileges can be granted or restricted to badge holders
- Keep the cards in case of motorized reader
- No APB, no timed anti-passback
- No access during holidays
- Reset APB level when information is downloaded, selected by default
- Supervisor
- Need escort

Supervisor: select to attribute the quality of supervisor to the cardholder

The supervisor is a particular employee that can

- Escort other cardholders and/or

- Initiate automatically a global reflex, which send the code 99 to the PC, by presenting his card twice consecutively – within 15 second - to a single reader

Need escort: select to request an escort for this cardholder

The escort function requires a double valid card reading within a 10 seconds delay - the employee who needs escort and his escort - to authorise access at certain readers. The escort is requested in the "Parameter – Controller – Reader – Access Mode" screen.

Simple escort (neither "Supervisor", nor "Need Escort" functions have been selected)
A double badge reading is required from two unspecified cardholders. Any cardholder can escort any cardholder.

Escort with supervisor (the "Need Escort" function has been selected)
A double badge reading is required, one from an unspecified cardholder – the employee who needs escort – and a second one, from a supervisor escorting him.

Note: a supervisor can cancel the need of escort for himself, by selecting both functions "Need Escort" and "Supervisor"

Parking users group: select a parking users group from the list or create a new group by clicking on the […] button; this information is for application in the parking module

Lift program: select the lift authorization group from the list; this information is for application in the lift module

3.8.4. Cardholders - Location

Locating employees enables to check attendance and to evacuate designated areas in case of emergency. The information regarding the were-about of a badge holder is supplied by his last passage through a reader.

Fields

Data of the last badge swipe through a reader is automatically updated by the system.
- ➤ Date of the last swipe
- ➤ Last reader pass
- ➤ Anti-passback level before and after passage

Reset button: click on this button to reset the global APB level for this badge holder

Reset all button: click on this button to reset the global APB level for all badge holders

3.8.5. Cardholders - Customised

Define the labels of the four personalised fields in the screen "Parameter - Customised labels" prior to their use in the present screen.

3.9. Visitor

The system distinguishes occasional visitors from employees. The "Parameter - Visitor" screen allows consulting and modifying information with respect to visitors only. This enables the secretary at the entrance of the building, or the guard, to create a temporary badge for visitors without having the need to access the main employees database.

Note: this screen is identical to the "Parameter - All Cardholders" screen except that the "Type" field is set to visitor and does not appear on the screen

When a cardholder is defined as "Visitor", the new tab "Visitor" is added, to specify visit information.
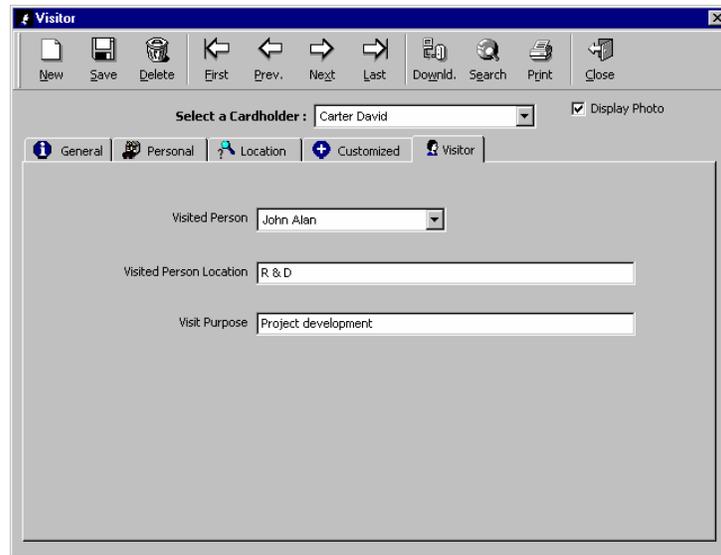
Fields

Visited person: select in the list of cardholders

Visited person location: specify the requested information

Visit purpose: specify the requested information

3.10. Multi Company Application

3.10.1. Multi Company Application – Basic Concepts

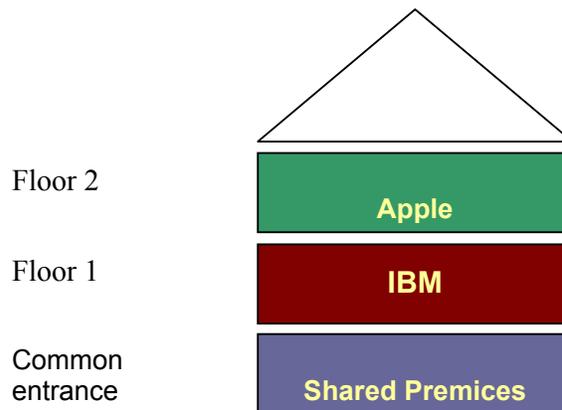The "Company" screen is used in multi-company applications, in which several independent entities are sharing the Amadeus 5 software. In practice, each company works virtually independently from the others.

When a user logs into the system, he will only be able to consult the portion of the database (cardholder, controller, etc.) related to his company. A single user can not consult records from all the different companies unless he gets a username and a password for each entity and logs in and off accordingly.

All the controllers are linked to the main worstation. The actual polling job for the all system is executed by a single PC, the main worstation.

Usually, the installer will enter as the default user (dds - Building Manager) and has the capacity of a super-user. One entity will be created for each company. An extra-entity will be create to manage shared premises (readers).

For example, a building beholding two companies, IBM and Apple. Each company occupies its own floor and is totally independent from the other. The shared entrance is managed by a separate entity created for this purpose.

To launch the multi-company application,
  - ➢ A user should create the different companies sharing the application ("Parameter - Company" screen)
  - ➢ A user within each company should be allocated, who will be responsible for system set up definitions for his own company ("Parameter - User" screen)
  - ➢ The default name, password and companies of the default user should be modified - and remembered ("Parameter - User" and "Parameter - Company" screens)
  - ➢ Each user sets up the system parameters for his own company

Example
  - ➢ The installer enters in the system as the default user
  - ➢ He modifies the default user, password and company
  - ➢ He creates the following companies: IBM, Aplle and "Shared Premices"
  - ➢ He creates the following users: Irvin, Alan and Patrick
  - ➢ Irvin enters in the system and sets all IBM parameters, such as controllers, cardholders...
  - ➢ Alan enters in the system and sets all Apple parameters
  - ➢ Patrick enters in the system and sets all "Shared Premices parameters

Default User

By default, the system defines a user (name: dds, password: dds) for the company "Building Management".

Displaying the current user name

The name and the company of the current user are always displayed in a white box at the far right of the tool bar.

Multi-site application

The multi-company application can be used for multi-site installations. The central database encompasses the information about all the companies. The multi-site manager will receive a user name and password for each site. He will be able to enter the different sites and control the events within each entity.

3.10.2. Company Screen

The "Company" screen is used to create new companies in a multi-company application.
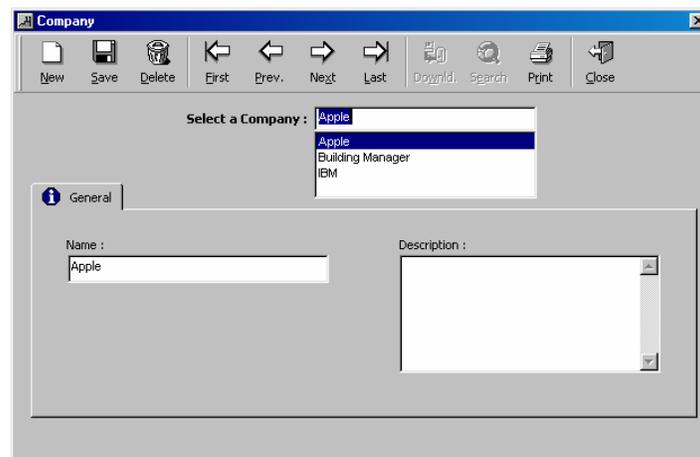
Fields

Name: name the new company

Description: describe the new item

3.10.3. Super-User

The super-user is a special user whose functions are:
  ➢ Creation of new companies sharing the application
  ➢ Allocation of a first user for each new each entity
  ➢ Decision on who the other super-user(s) will be
  ➢ Creation and removal of database and journal

One super-user is required for the default company and optional for the other entities. The default user is defined as default super-user by the system. The default super-user cannot be erased; nevertheless his name can be modified. All further super-users created can be modified and erased.

Only a super-user can delete companies, all entities but his company or the default one. The possibility to create and delete a company database will not even appear on the screen of a user.

A user is defined as a super-user by selecting the option in the "Parameter - User" screen.

3.10.4. Shared Information

3.10.4.1. Ownership of records: General Rule

Each company creates its own records and can only display, modify or erase their own data. Log and displays are related to a specific company. Two companies cannot choose the same record name.

3.10.4.2. Exceptions

Cross companies

If an employee from company A presents his badge to a reader from company B. The access denial message will be notified to both companies.

Shared Items

A. Shared controller networks

The shared controller network and its definition are available to all in a read only mode. Only the company that owns the network can modify it.

By default, the default network (Network 1 on COM 1) is shared. The sharing possibility can be manually removed.

B. Shared readers

Example: IBM owns the main entrance reader. It lets Apple use that reader.

A company that owns a reader can share it, by checking the corresponding box in the "Parameter- Reader - General" screen. By doing so, the ground is set to allow all employees all companies to use the reader. The system will automatically insert this reader into the "Anytime - Anywhere" default access group of all companies and update the controllers correspondingly. From now on, all companies will be able to select the shared reader for any access group manually created.

The weekly program associated should either be:

"Always", or whatever modified name it has, in which case the company it originates from is of no significance - recomanded to keep full control of the access

Any other weekly program of the company that has shared the reader

C. Shared computer

A computer can be shared between different companies. The "Log Off" function can be useful in this case.

d. Shared icons

Icons created by a company can be seen and used by all companies. Only the company that has created the icons can modify them. This means that the icons are always shared by default.

3.11. Authorization Levels

The different authorization levels corresponding to the access groups, as well as options and screens that can be viewed and modified by each group, are defined in this screen.

For example,
- ➢ The site's manager has access to all the information
- ➢ The parking lot attendant can only modify information regarding parking and view user details
- ➢ The secretary at the entrance of the building can only create visitor' badges
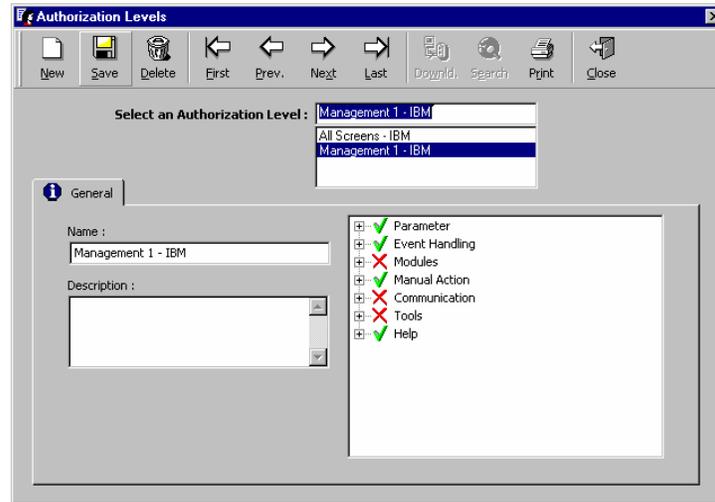
Fields

Name: name the new authorization level

Description: describe the new data entry

View: determine the authorization level for each option and menu

Tips & Notes

Screen status

Consultation and modification status of options and menu is as follows:
- ➢ V   read, write and delete
- ➢ X   no access granted
- ➢ R   read only, without modification

Modification of the screen status from V to X to R

Viewing status can be modified by clicking successively on the sign to the left of the screen definition.

Access level by default

The access level for all menus is X by default, which correspond to a minimal access (enter and quit).

Super users

By default the system will define a group of super users that has maximum accessibility. Super users can read, write and erase any screen of the application.

The + symbol indicates a head of chapter.

In order to produce the sub-menus click on the symbol + located to the left of the name of the menu. The application allows differentiating within a head chapter, the screens that are accessible, restricted and forbidden.

The status of the head chapter applies to all sub-menus that it contains except if it is manually modified. If access to a head chapter is refused to a group of users, access to all sub-menus will automatically be refused.

3.12. User

New users added to the system and authorizations level granted are defined in this screen.

In order to follow their movements within the system, it is advised:
  ➢ To define the authorization levels prior to entering user data
  ➢ To save individual employee data
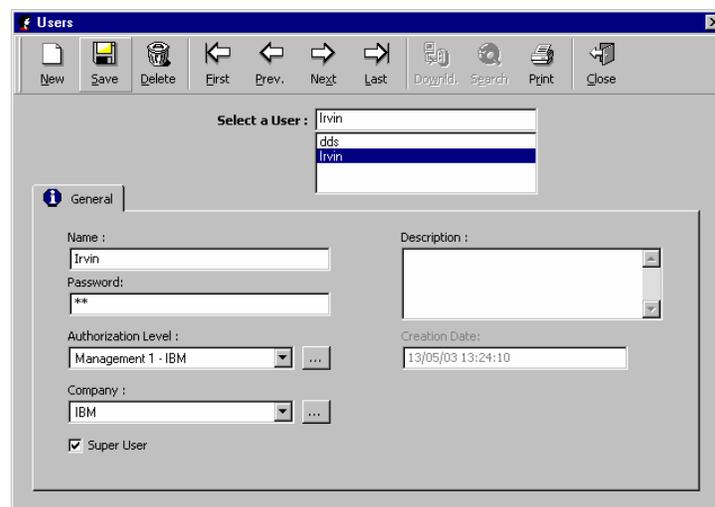
Fields

Name: name the new user

Password: type the password that the user will use to enter the system

Description: describe the new data entry

Authorization level: select an authorization level from the existing list or click on the […] button to create another authorization level

Company: mentions the company the item refers to; field used mainly in multi-company applications

Super-user: special user whose functions are the creation of new companies, the allocation of first users within each entities and the decision of who the other super-users will be; used in multi-company applications

**Creation date**: displayed automatically by the system without possibility of modification

Tips & Notes

See the password

Double click on the password to make it appear on the screen.

3.13. Customised Labels

Four additional free fields are available that can be parameterised according to the needs. The titles of these four fields are defined in this screen. The contents of these fields are encoded within the information relative to each user in the "Parameter - All Cardholders - Customized" screen. (Examples: code given by a company, social security number)
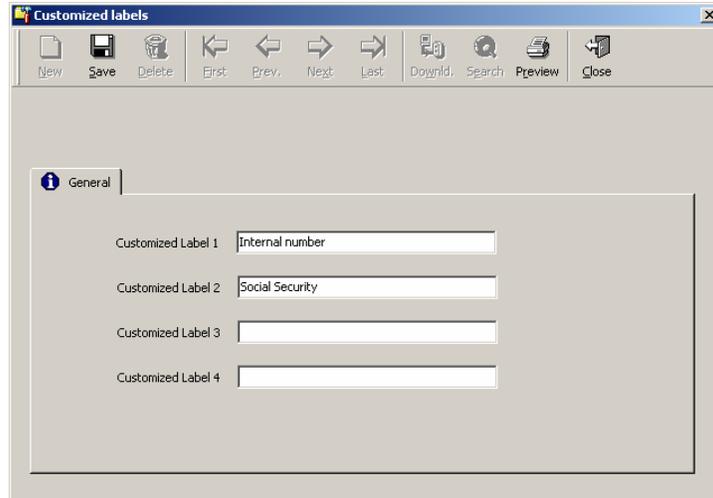
Fields

For each field to customize enter the new field name.

3.14. Anti-passback

3.14.1. Basic Concepts

Three types of anti-passback can be activated.

Local anti-passback: prevent the use of successive entries without a valid exit.

Temporal anti-passback: prevents two successive access authorizations on the same reader within a specified delay.

Global anti-passback: define a path - series of readers - the cardholder must follow in order to access specific areas.

3.14.2. Local Anti-passback

Two successive entries with the same badge without a valid exit are not authorized. Two readers of the same controllers can supervise the entry / exit of the same door. To operate the local anti-passback select the APB function in the "Parameter - Controller - Reader - Access Mode" screen. Note that the "Anti-passback" field in the "Parameter - Controller - Reader - Door Control" screen is not selected.

Access authorization sequence

With APBL	Without APBL
ENTER	ENTER
EXIT	ENTER or EXIT
ENTER	ENTER or EXIT
Exit requested before re-entering	Exit not requested before re-entering

3.14.3. Temporal Anti-Passback

Waiting period between two successive access authorizations for a same badge swiped through a specific reader. The second access will only be authorized after the predefined time delay has elapsed. To operate the temporal anti-passback specify the number of minutes for the delay to be in effect in the "Temporal Anti-passback" field, found in the "Parameter - Controller - Reader - Access Mode" screen. Note that the "APB" field in the "Parameter - Controller - Reader - Door Access" screen is not selected.

3.14.4. Global Anti-Passback

Compulsory path that must be followed in order to access specified areas. The badge holder will only be granted access between compatible anti-passback zones.

Examples
  ➢ Enforce discipline by having employees clock in before they go to their respective offices.
  ➢ Prevent a second car from entering the parking lot if its' identity is unknown. It will be stopped at the next checkpoint.

Operating mode
  ➢ Define or select the two anti-passback levels in the "Parameter - Controller - Reader - Door Control" screen
      o Define the reader's anti-passback level at the time access is asked for
      o Define the reader's anti-passback level after access has been granted and the user has passed through the door
  ➢ Activate the anti-passback function in the "Parameter - Controller - Reader - Access Mode" screen

Tips & Notes

Cancelling the anti-passback option for certain individuals

Select the "No Anti-passback" and "no Temporal APB" options in the "Personal" tab of the "Parameter - Badge" screen in order to cancel the APB function for specific badge holders.

Real time communication

Real time communication with a computer is necessary after each badge swipe in order to automatically locate employees and download the information to the controllers.

3.14.5. Anti-Passback Levels

This screen allows the creation of the different anti-passback levels. It is accessible through the screen "Parameter - Controller - Reader - Door control".
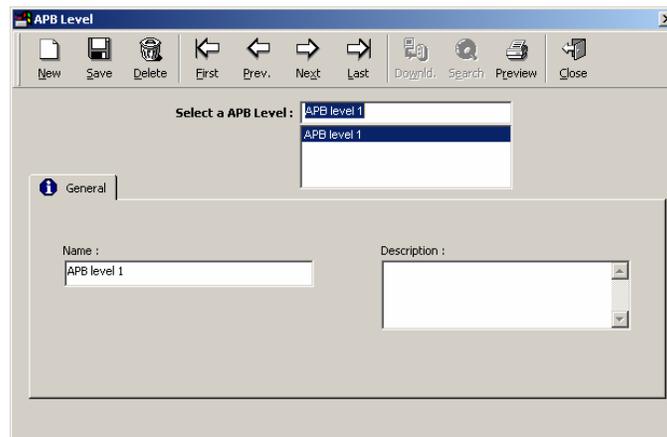
<u>**Fields**</u>

Two anti-passback levels must be defined in the "Parameter - Anti-passback Level" screen.
- ➢ From (previous level): badge holder anti-passback level prior to the entry request
- ➢ To (next level): badge holder anti-passback level after access authorization

3.15. Log Off

The "Log Off" function allows different users to log in and off the system. After log off, the "Log In" screen is displayed. Only authorised user, with adequate user name and password, can access the Amadeus 5 system. This can be used to prevent system access to unauthorized users, while the program is running.
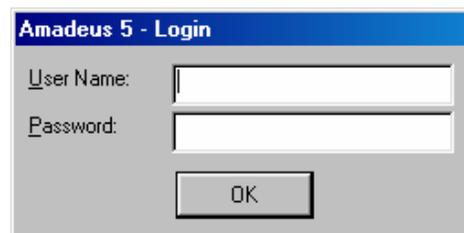
3.16. Exiting the Application

In order to quit a work session and exit the application, follow one of the three procedures:
- ➢ Click on the "door" icon situated to the far right of the navigation bar
- ➢ Click on the "magic wand" icon situated in the upper left corner of the screen
- ➢ Click on the "X" situated in the upper right corner of the screen
- ➢ Click on the function key "F4"
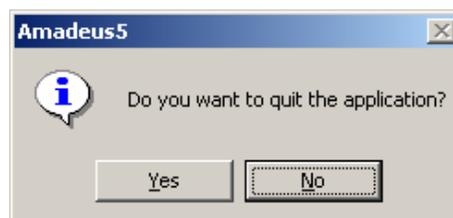
4. MENU: EVENT HANDLING

The "Event Handling" section of the application manages alarms, presents them graphically on maps, creates actions and processes and combines them in global reflexes following certain events.

Icons, maps and position

The graphical functions of the Amadeus 5 software integrate the dynamic display of inputs on installation maps.

- ➢ Define icons ("Event-Handling - Icon" screen), certain icons are defined by default
- ➢ Link the icons to the inputs ("Parameter - Controller - Input" screen, "Icon" function)
- ➢ Define site maps ("Event-Handling - Maps" screen)
- ➢ Position the inputs on the maps ("Event-Handling - Position" screen)
- ➢ Display the final status

Operating mode of the "Event Handling" menu

- ➢ Define the inputs
- ➢ Gather the inputs into an input group (if necessary)
- ➢ Define the outputs
- ➢ Gather the outputs in an output group (if necessary)
- ➢ Define the action to set off, following an input or group of inputs activation
- ➢ Define the process, in other words, the sequence of actions
- ➢ Define the global reflex, in other words, the events that generates the reflex and the actions to trigger

4.1. Icon

Icons are graphical symbols, attributed to input, output, map, process or action. They will positioned on maps and will be used dynamically in the "Event-handling – Active Alarms" screen.

Icons of controllers' inputs and outputs are created by default.

Basic graphical symbols are supplied in the directory:

"C:\Program Files\Amadeus5\Media\Icons"

Other icons can be added by specifying their name, description and location on the disc. They are automatically stored with all the icons in the directory mentioned above.
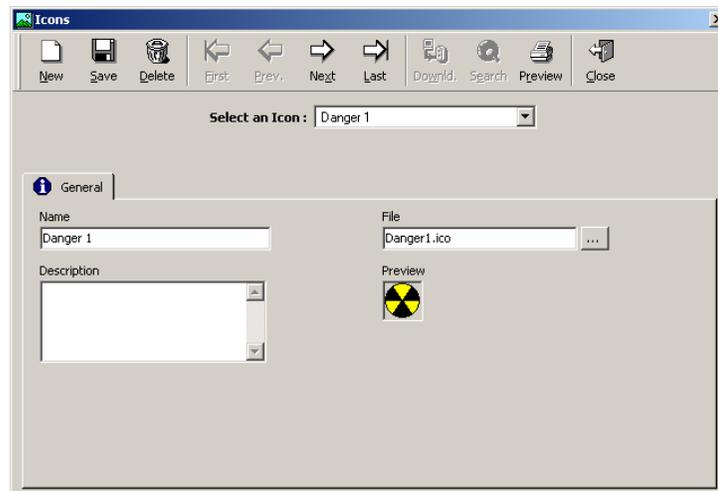
Name: type the icon name

Description: describe the new data entry

File: display the name of the file beholding the graphical symbol associated with the icon selected; click on the […] button to chose another file and specify its address

Preview: display the image of the selected icon

4.2. Map

The "Maps" screen allows the integration of maps into the software. In order to use the "Active Alarms" function, inputs must be positioned on maps.

It is advised to store all maps in the following directory:

 "C:\Program Files\Amadeus5\Media\Maps"

4.2.1. Map - General

A cascade of maps can be defined. For instance, the maps representing the different floors can be linked to the map of a multi-floor building.
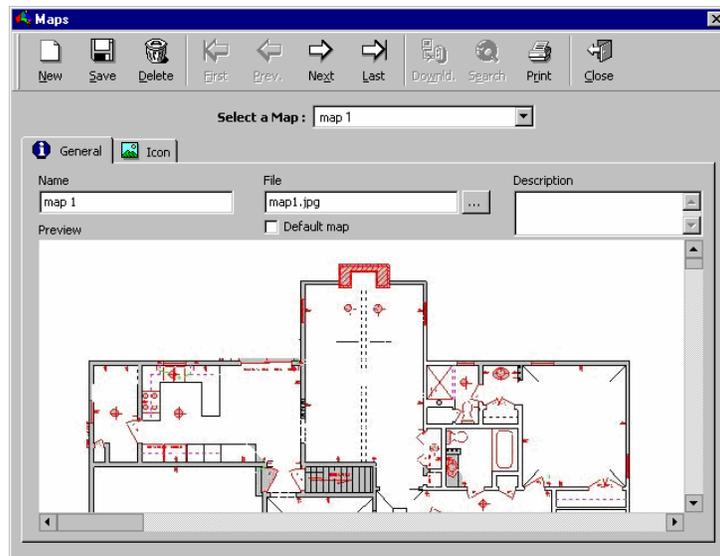
Fields

Name: type the name of the map

File: display the name of the file beholding the map; click on the […] button to choose another file and to specify its address

Description: describe the new data entry

Preview: display the map selected

Default map: the map selected serves as default map

4.2.2. Map - Icon

This screen enables the association of icons to maps.

Field

Icon: select the icon to associate to the map from the list, or select the […] button to create a new one

4.3. Position

The "Position" option allows the positioning of inputs, outputs, maps, processes and actions on the maps.

In the left window are listed active controllers, inputs, outputs, maps, process and actions, under a Microsoft Explorer format.

Drag the icon form the left column and drop it into the map, then save the positioning. Fine-tune the placing with the arrows. Onc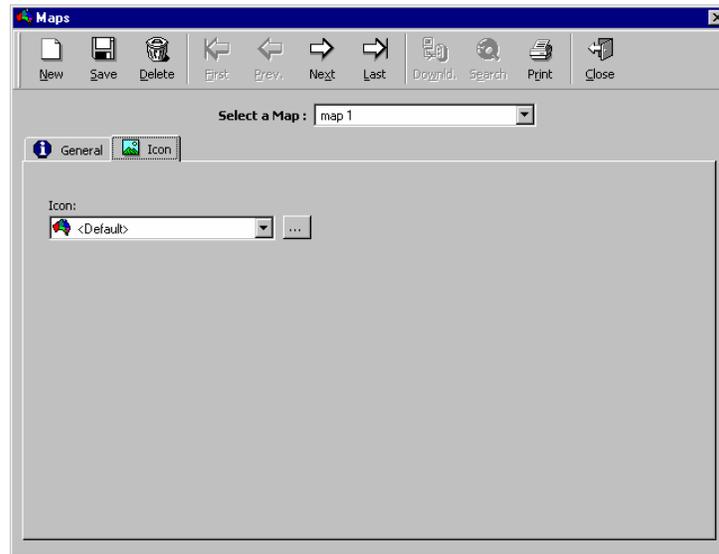e positioned, the item will disappear from the list, indeed each icon can only be positioned once on one map. The icons will be used in the "Event-Handling – Alarm Active" screen.
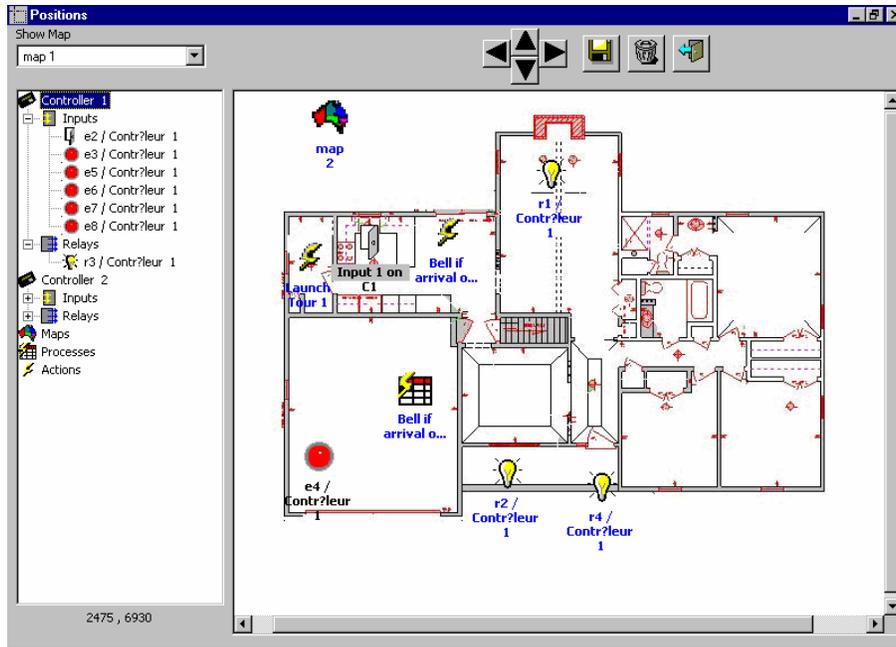
Fields

Show map: choose the map to be displayed from the list

Left column:
> ➢ Controllers: inputs and relays
> ➢ Maps
> ➢ Processes
> ➢ Actions

Direction arrows: four direction arrows refine the input positioning on the map; drag the icon to the map, then use the arrows

Tips & Notes

Positioning

Modifying the input position on the map can be done using a mouse: select the object, maintain the left mouse button depressed and move the mouse towards the new position.

Unique position

Each icon can only positioned once on a map.

4.4. Input Group

Inputs can be logically associated into group of inputs. The inputs can belong to one controller or to a series of controllers. The group is activated or deactivated in a single command. If a group of inputs has been activated, then activation of all the components of that group is set off.

This screen enables the definition of the group and its components. A group of inputs is used to define global reflexes.

Example

Grouping all the inputs of a room, such as movement detectors or windows and doors opening devices. A single control button will render the group active by night, for an exceptional meeting at night, for instance.

Fields

Name: name the input group

Description: describe the new data entry

View:
- ➢ V   display all inputs included in the input group
- ➢ X   display all the inputs excluded from the input group
- ➢ VX   display all inputs
- ➢ --   display no input

Change the **input inclusion status** by clicking on X or V in the left column
- ➢ The inputs preceded by V are included in the input group
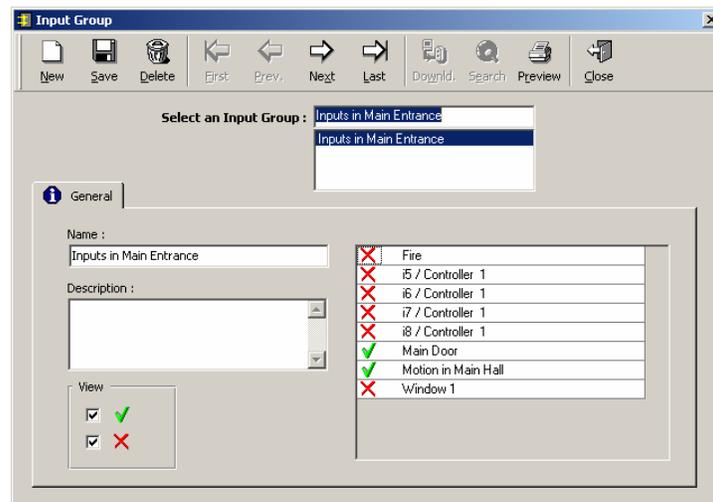- ➢ The inputs preceded by X are excluded from the input group

4.5. Output Group

Outputs can be logically associated into group of outputs. The outputs can belong to one controller or to several controllers. The group is activated or deactivated in a single command. If a group of outputs has been activated then activation of all the components of that group is set off.

This screen enables the definition of the group and its components. A group of outputs is used to define global reflexes.

Example

Activation of an output group engaging all night alarms when the last employee leaves the building

Fields

Name: name the output group

Description: describe the new data entry

View:
  ➢ V   display all outputs included in the output group
  ➢ X   display all the outputs excluded from the output group
  ➢ VX   display all outputs
  ➢ --   display no output

Change the **output inclusion status** by clicking on X or V in the left column
  ➢ The outputs preceded by V are included in the output group
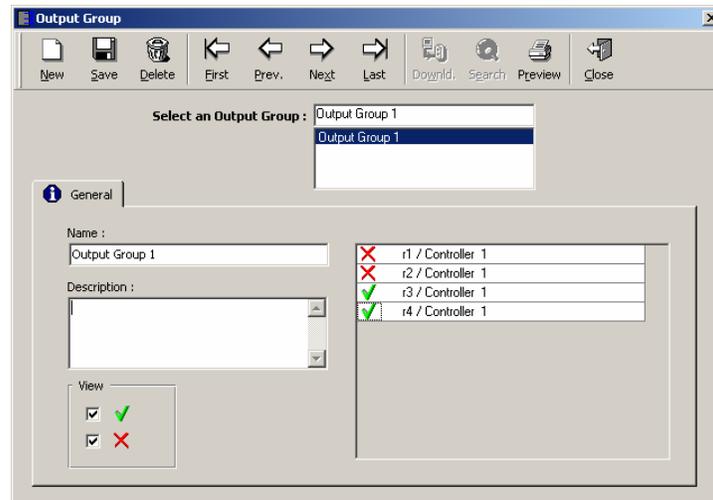 ➢ The outputs preceded by X are excluded from the output group

4.6. Action

Different types of actions can be defined, sequenced within a process and incorporated into global reflexes. The actions are created and described in this screen; their activation depends on the activation of the global reflexes they are part of.

Actions types and parameters

Action type	First parameter	Second parameter
Relay activation	Choose a relay from the list or create relay	Choose between: - Return to automatic mode - normal - Activated during (*) - Always activated - constant on - Never activated - constant off
Relay group activation	Choose a relay group from the list or create a new relay group	Choose between: - Return to automatic mode - normal - Activated during (*) - Always activated - constant on - Never activated - constant off
Display message on the PC	Enter the message to be displayed	
Print message	Enter the message to be printed	
Play sound	Mention the location of the sound file or create a new file	
Increment counter	Choose a counter from the list or create a new counter	
Decrement counter	Choose a counter from the list or create a new counter	
Display message on a controller	Choose a controller from the list or create a new controller	Enter the message to be displayed
Input group deactivation	Choose the input group from the list or create a new group	
Input group return to normal mode	Choose an input group from the list or create a new group	
Insert comment in journal	Enter the message to be inserted	
Execute external application	Specify the file (any .exe file)	
Invalidate cardholder	Choose the badge holder	
Validate cardholder	Choose the badge holder	
Print existing report (**)	Specify the report (.rpx)	
Start a guard tour	Choose the tour name	Select the guard

(*) Specify the number of second (third parameter)
(**) Print existing report (extension .rpx) saved in the directory "Amadeus5/Reports", gathering all system reports. In new installation, no report is predefined. The default name of the first report is "Last Report.rpx". This name can be modified in the last screen of the report wizard and is valid as long as the extension ".rpx" is preserved.
A possible use of this action is the automatic printing of a muster report in case of fire. Such report can be built using the "Last Reader Passed" field in the cardholder report.
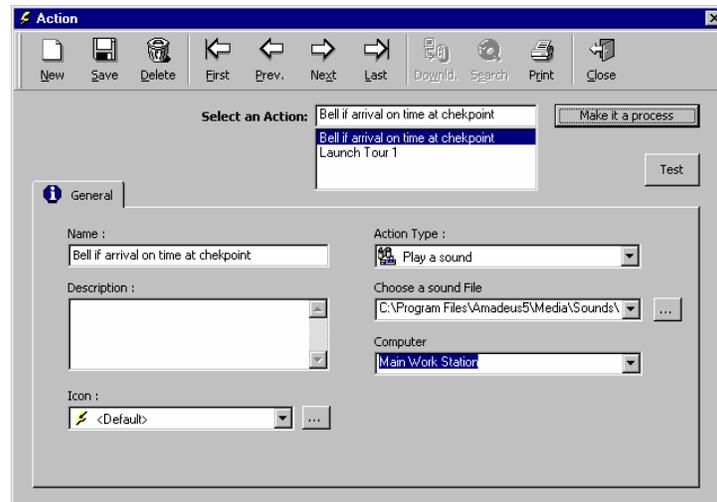
Fields

Make a process: click on this box to directly create a process beholding this single action
Note the action needs to be created and saved prior to process creation.

Name: name the new action

Description: describe the new data entry

Icon: choose the icon representing the action in the list, or click on the […] button to create a new one

Action type: select from the list

Parameter 1, 2, 3: select from the list (see actions and parameters table); the type and number of parameters vary according to the type of action selected. The third parameter is only accessible when defining the activation delay of a relay or group of relays.

4.7. Process

A process is a set of actions used to define global reflexes. In this screen the different actions are selected and organized; their activation depends on the activation of the global reflexes they are part of.
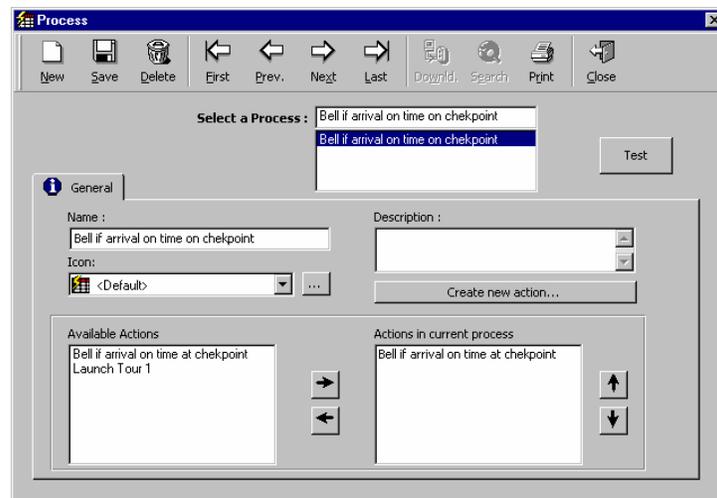
Name: name the new process

Description: describe the new data entry

Icon: select the icon associated to the process in the list or create a new icon by clicking on the […] button

Create a new action: click on the button to create a new action

Test: click on the button to test the new process

Available actions: using the horizontal arrows, insert the predefined actions into the current process, an action can be repeated several times in the process

Actions in current process: using the vertical arrows, organize the different actions into the current process

4.8. Counter

A counter is a tool that measures things and activate a process according to the value of the counter.

The "Event Handling - Counter" screen defines a particular global reflex type, whose main object is the increment of a counter.

Examples

> ➢ Count the number of persons in a room (so as not to leave a room empty, to signal excess of maximum capacity, to switch office lights off when all the occupants have left, to activate an alarm system when all the employees have left the building, etc.)
> ➢ Decrement the number of entries of a membership club card after each passage and refuse access if credit is null
> ➢ Check the filling up of a parking zone or cinema and refuse access to a full zone

Operating mode

> ➢ Create an action incrementing the counter
> ➢ Create an action decrementing the counter
> ➢ Create a process incrementing the counter
> ➢ Create a process decrementing the counter
> ➢ Create a global reflex determining which event increments the counter
> ➢ Create a global reflex determining which event decrements the counter
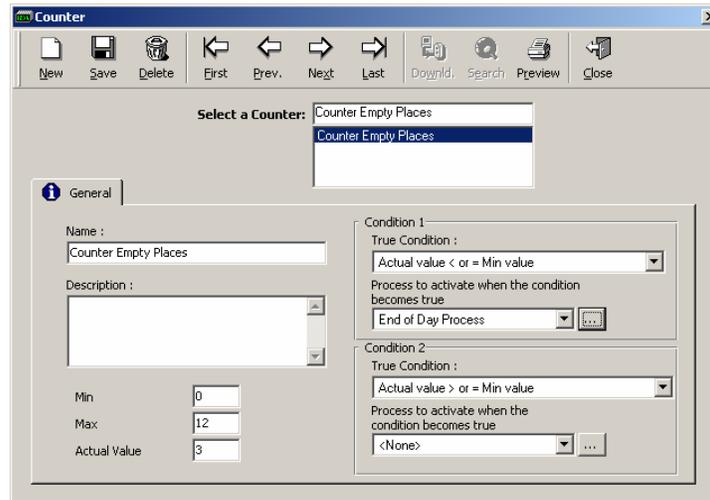
Fields

Name: name the new counter

Description: describe the new data entry

Min: enter the minimum value of the counter

Max: enter the maximum value of the counter

Actual value: enter the actual value of the counter; the value is automatically modified by the system

Condition 1

True condition: select the condition to apply from the list:
      Actual value < minimum value
      Actual value > minimum value
      Actual value not equal to minimum value
      Actual value = minimum value
      Minimum value < actual value < maximum value
      Actual value not equal to maximum value
      Actual value = maximum value
      Actual value > maximum value
      Actual value < maximum value
      Actual value = minimum value + 1
      Actual value = maximum value - 1

Process to activate when the condition becomes true: choose a process from the list or create a new process using the […] button

Condition 2

Proceed as above. Note that both conditions are independent.

Tips & Notes

Multiple condition counters

If more than two incrementation conditions are required, create a second counter, named as the first one, using two further conditions. Repeat this procedure as many times as necessary.

4.9. Global Reflex

4.9.1. Global Reflex - Basic Concepts

A global reflex defines the events to take into consideration and the process to activate.

The "Event Handling - Global Reflex" screen is made up of two tabs:
- ➢ General tab, used to define global reflexes
- ➢ Properties tab, used to define the event and process making up the global reflex

In order for a global reflex to be activated following an associated event, it must be activated in the " Event-Handling - Global Reflex" screen.

Examples

- ➢ Print instructions
- ➢ Sound a vocal file
- ➢ Display the activation of a camera in the area concerned
- ➢ Being informed of the arrival of a specific person
- ➢ Send a message to an employee when he badges
- ➢ Activation or deactivation of alarms
- ➢ Switching on the air conditioning in the office of the employee that badges at the entrance
- ➢ Light a red light if a parking is full

4.9.2. Global Reflex - General

The name, description and activation status of the global reflex are defined in this screen.

Fields

Name: name the new reflex

Description: describe the new data entry

Status in event-handling program: the current global reflex is either included or excluded from the event-handling program; by default the global reflex is included

In order to be activated, the reflex must be included in the event-handling program.
A global reflex, which is not included, will not be activated by the system when the defined events of the program arise. Modify the status by selecting the […] button, which will lead to the display of the "Event-Handling - Global Reflex" screen.

Active when

- ➢ **Always**: select if the global reflex is constantly activated

➢ **During weekly program**: select if the activation of the global reflex is dependent of a weekly program (activation will occur only during the green zones of the program). This enable to plan the execution of a reflex at pre-defined times, by specifying the month, day, hour and min, in the scheduler (event type "Scheduler" in the "Event-handling - Global Reflex - Properties" screen). Example: activation of a specific process everyday at midnight or on Monday 10AM – 11 AM and Friday 4PM – 6PM

4.9.3. Global Reflex - Properties

This screen defines the specific events that are going to set off the actions and their parameters.

Fields

Event: the screen is modified according to the type of event selected, displaying the appropriate number of parameters in each case. The table hereafter sums up the characteristics of the global reflexes.

Event type: choose the suitable event from the list:
➢ Access granted or refused at specific reader
➢ Start and end of alarm for digital inputs
➢ Status of analogue inputs
➢ Table errors
➢ Low battery or power down / up at a specific controller
➢ Unknown or non-allocated badge
➢ Scheduler

From: choose the suitable parameter from the list

Parameters 1, 2, 3: the parameters required appear automatically on the screen according to the type of event selected; in general one or two; three if access has been denied

For each parameter, select the reader, controller, input, code or person, or choose the mention "any" when the parameter applies to all the elements of a group.

Process: from the list, select the process - or series of actions - to activate following the occurrence of an event, or create a new process using the […] button

Time out: maximum delay, between the recording of an operation (date and hour) and the time of the PC, beyond which the process is not carried out and the global reflex associated will not be set off. (Expressed in second, maximum of 9 hours, default value = 3600 sec)

A global reflex is set off if the delay between the recording of an event by the controller and the processing of data by the PC is inferior or equal to the time out delay.
If the delay is greater than the time out delay, the event is recorded in the journal but the global reflex is not activated.

In general, the input activation sets off the associated global reflex. However, it could happen that the event that activates the process is only detected after a certain delay.

Example

10:00 AM: input activation of non-connected controller
12:00 AM: communication check between PC and controllers, followed by the controller connection
Should the global reflex be set off two hours after the event has occurred?

Events types and parameters

Event type	From	1ʳˢᵗ parameter	2ⁿᵈ parameter
Access granted	Choose the suitable reader	Choose the transaction code (+)	Choose the person
Access granted + duress code	Choose the suitable reader	Choose the transaction code (+)	Choose the person
Access denied (*)	Choose the suitable reader	Choose the transaction code (+)	Choose the person
Access denied + unsuccessful trials	Choose the suitable reader	Choose the person	
Start of alarm	Choose the digital input		
End of alarm	Choose the digital input		
Status 1 to 4	Choose the analogue input		
Table error	Choose the controller		
Low battery	Choose the controller		
Power down	Choose the controller		
Power up	Choose the controller		
Communication OK	Choose the controller		
Communication error	Choose the controller		
User acknowledgement	Choose the user	Choose the input	
User confirmation	Choose the user	Choose the input	
Unknown card	Choose the reader		
Non allocated badge	Choose the reader		

Application log in	Choose the user		
Application log out	Choose the user		
Arrival	Select the tour	Select the checkpoint	Select the guard
Early arrival	Select the tour	Select the checkpoint	Select the guard
Not arrival	Select the tour	Select the checkpoint	Select the guard
Late arrival	Select the tour	Select the checkpoint	Select the guard
Scheduler	Specify the day	Specify the month	Specify the hour & min (Parameter 3)

(+) Transaction and coercion code

When a transaction code is selected, the event is only set off if the badge holder types the transaction code on the reader's keypad prior to swiping his badge. The transaction and coercion codes are a sequence of two numbers between "00" and "99".

(*) Reasons why access can be denied

The reason of an event "Access denied" must be selected in the third parameter field that appears on the screen. They will be signalled as error by the system.

List of reasons of access denial

- ➢ Any denied reasons
- ➢ Wrong keypad code
- ➢ Full / Lock / No answer from door
- ➢ Time not OK

- ➢ Anti-passback not OK
- ➢ Reader not allocated
- ➢ Site code not OK
- ➢ Inhibited cardholder
- ➢ Access group

4.10. Event-Handling Program

4.10.1. Event-Handling Program - Basic Concepts

The "Event-Handling Program" allows the attribution of activation time zones to alarm input and the inhibition of global reflexes.

The "Event-Handling Program" is divided into three tabs:
  - ➢ General tab: define the event program
  - ➢ Alarm tab: define the alarms to consider
  - ➢ Global reflexes tab: inhibit existing reflexes and, eventually, modify or create new reflexes

4.10.2. Event-Handling Program - General

This screen allows the visualization of the active event-handling program; thus establishing a link between raised alarms and global reflexes that have occurred.

This screen does not allow the creation of a new event-handling program.
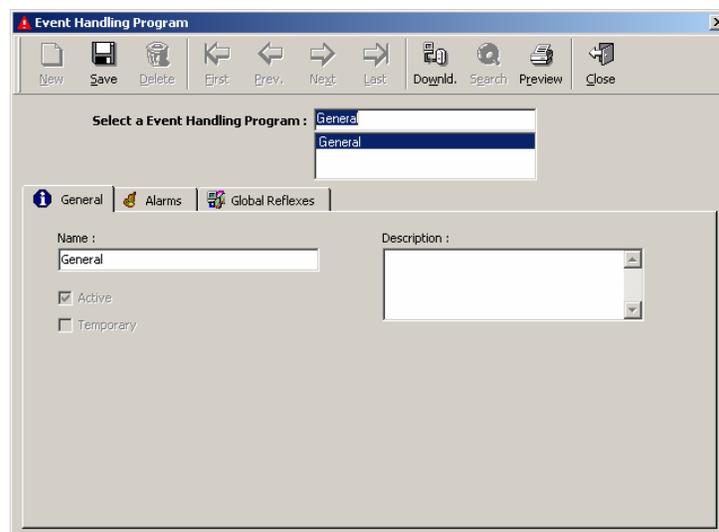
Fields

**Name**: name the new event-handling program

Description: describe the new data entry

Active: activate the selected event-handling program (within the activation conditions as quoted above); if a program is not "active", it will not be taken into consideration by the system

Temporary: select if appropriate

4.10.3. Event-Handling Program - Alarm

This screen defines the event-handling programs associated to the inputs.
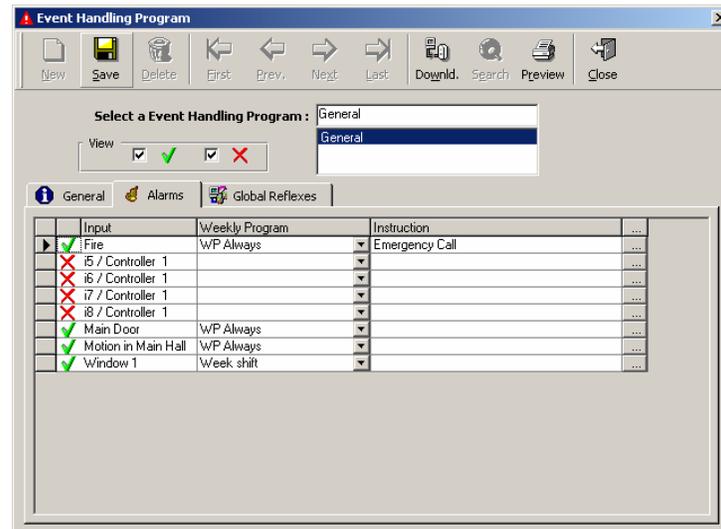
<u>**Fields**</u>

View:
  ➢ V   display all inputs included in the event-handling program
  ➢ X   display all the inputs excluded from the event-handling program
  ➢ VX   display all inputs
  ➢ --   display no input

Select the input(s) that belong to the event-handling program by modifying the symbol that appears in the first column.

Change the **input inclusion status** by clicking on X or V in the first left column
  ➢ The inputs preceded by V are included in the event-handling program
  ➢ The inputs preceded by X are excluded from the event-handling program

By default, all the inputs from the list are excluded from the event-handling program. Clicking on the desired inputs modifies its status.

Input: complete list of all the system's inputs

Weekly program: display of the weekly program associated with the input. Modify the selection by clicking on the triangle to the right of the field.

Note that the alarm input is only activated in allowed time zones of the weekly program.

Instructions: enter the instruction to display in the active alarm screen when the alarm is raised

Button […]: link to the properties screen of the selected alarm

4.10.4. Alarm Properties

The screen summarizing the alarm's properties is accessible by clicking on the […] button on the line of the alarm in the "Event-Handling - Alarm" screen.
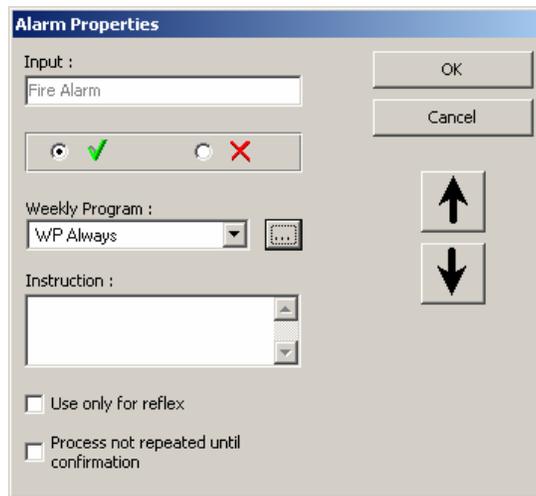
Fields

Input: input name

Inclusion status in event-handling program: select
  ➢ V to display only the inputs included in the event-handling program
  ➢ X to display only the inputs excluded from the event-handling program
  ➢ V and X to display all the inputs
  ➢ -- to display no input

Weekly program: select the weekly program from the list or click on the […] button to create a new program

**Instruction**: enter the comment that appears in the "Active Alarm" screen at the time of input activation

Use only for reflexes: without recording the information in the journal history

No process until confirmation: the primal automatic activation is not repeated, as it is the case of a movement detector, for instance

Direction buttons: review the different alarm property screens

4.10.5. Event-Handling Program - Global Reflex

This screen defines the actions to trigger when alarms are activated.
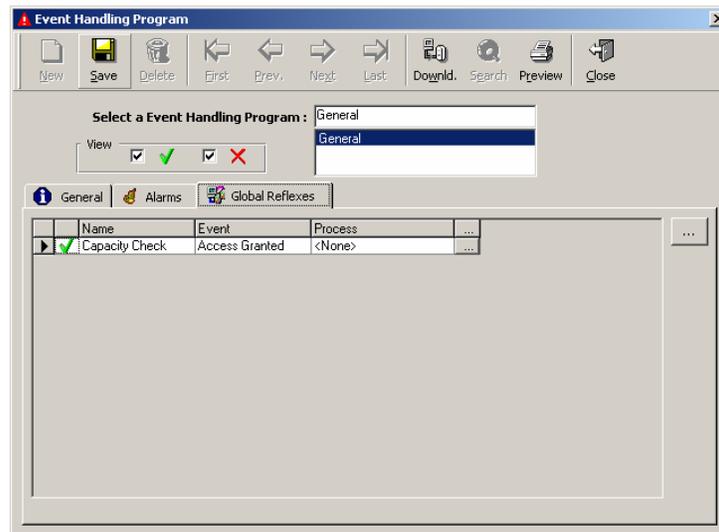
Fields

View:
- ➢ V   display all global reflexes included in the event-handling program
- ➢ X   display all the global reflexes excluded from the event-handling program
- ➢ VX   display all global reflexes
- ➢ --   display no global reflex

Select the global reflexes included in the event-handling program by modifying the symbol that appears in the first column.

Change the **global reflex inclusion status** by clicking on X or V in the first left column
- ➢ The global reflexes preceded by V are included in the event-handling program
- ➢ The global reflexes preceded by X are excluded from the event-handling program

Name: name of the global reflex

Event: events associated with the reflex

Process: series of events associated with the reflex

Button […] (on the line of the reflex): link to the selected "Event Handling - Global Reflexes - General" screen

Button […] (outside the table): link to "Event Handling - Global Reflexes - General" screen, even if no item is selected

4.11. Active Alarms

4.11.1. Active Alarms – Basic Concepts

The "Event Handling - Active Alarms" screen provides a dynamic status of the system's inputs, relays, actions, processes, maps

Two icons are assigned to each input and output, corresponding to the ON and OFF status. The dynamic swap of icons (if the initialisation parameter "NO IO = 1") allows for visual follow-up of input and output status: activation or deactivation of alarm points, door open or close and relays supervision. When an alarm point is activated, the corresponding new icon will automatically be displayed and the text describing the icon will appear in red. The text will turn black after alarm acknowledgement. It is possible to visualise only the active alarms or all the alarms and/or all the relays.

By default open and close door icons are associated to the first two relays and red and white circles to all other inputs.

Four cases of input activation coupled with alarm

	On alarm	Not on alarm
Input normally ON	Icon input OFF - Red text	Icon input ON - Black text
Input normally OFF	Icon input ON - Red text	Icon input OFF - Black text

Example: If a door alarm is detected, an icon will show a door open accompanied with red writing. If the door is closed, the icon will be updated to a closed door but the red writing signalling the alarm will remain till the alarm acknowledgement. After that, the text will return to black.

	On alarm	Not on alarm
Door open	Door forced open - Red text	Door normally open - Black text
Door close	Door closed after being forced- Red text	Door close - Black text

When an alarm is raised the system reacts:
- ➢ Log display: alarm displayed in red
- ➢ Journal: event is recorded
- ➢ Navigation bar: increase in the number of alarms raised
- ➢ "Active Alarms" screen: the icon connected to the alarm appears on the installation map displayed
- ➢ "Active Alarms" screen: mention of the name of the input activated and the date of the event in the top table
- ➢ "Active Alarms" screen: instructions related to the alarm are displayed in the "Alarm Properties" screen which is accessible from the "Event-Handling Program - Active Alarms" screen

4.11.2. Active Alarms - Map

The physical status of inputs and outputs is graphically displayed with icons. Those can be automatically updated automatically if the option "NO IO = 1" in the "amadeus5.ini" file.

The activation of inputs resulting in alarm is signalled in red in this screen.

When several alarms are detected, the last alarm is displayed in the table at the top of the "Active Alarms" screen. By clicking on the related alarm icon, the cursor automatically moves towards the corresponding row. The instructions displayed correspond to the alarm selected.

Actions and process can be directly executed by right clicking on their icons.

Swap from map to map by selecting the appropriate icons.

The last parameter selection is applied when reopening the screen.
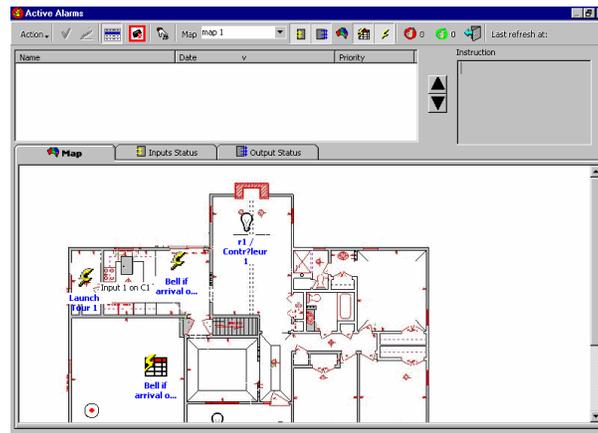
Toolbar

The functions available from the toolbar are as follow:

Action
  ➢ Acknowledge the alarm: select an alarm from the table and confirm the acknowledgement; this allows the differentiation between new and already acknowledged alarms. It is advisable to use this function to facilitate alarm management. When an alarm is acknowledged, the following events take place in the table of the "Event Handling - Active Alarms" screen as well as on the navigation bar:
    o The alarm icon goes from red to green
    o The numbers of acknowledged and non-acknowledged alarms are modified
  ➢ Confirm the alarm: confirm a specific alarm, already acknowledged; a new screen appears displaying the following information:
    o Name and date
    o Event date and hour
    o Alarm type: start or end of alarm
    o Comment: type in an optional comment, such as importance, user name, etc., that will appear in the journal "data" column
  ➢ Show all inputs / only active alarms (depending on current selection)
  ➢ Show / hide relays (depending on current selection)
  ➢ Show / hide maps (depending on current selection)
  ➢ Show / hide processes (depending on current selection)
  ➢ Show / hide actions (depending on current selection)
  ➢ Execute process
  ➢ Confirm all: confirm all alarms triggered using a single command. This option is useful in case of prolonged communication break. The computer will ask for confirmation. Individual alarm acknowledgement is not required.
  ➢ Exit
Acknowledge the alarm

Confirm the alarm
Remain on selected alarm
No polling
Refresh: appears only if no polling or if NO IO = 1 in the initialisation parameters
Open the "Execute Process" screen
Map: choose the map to display in the list
Show all inputs / only active alarms (depending on current selection)
Show / hide relays (depending on current selection)
Show / hide maps (depending on current selection)
Show / hide processes (depending on current selection)
Show / hide actions (depending on current selection)
Number of active alarms
Number of acknowledged alarms
Exit

Table

Active alarms: icons signal the alarm status in this table as well as in the tool bar of the main screen
- ➤ Active (red icon)
- ➤ Acknowledged (green icon)
- ➤ Confirmed (the alarm disappear)

Name: name of the alarm

Date: date and time of the alarm

Instruction: instruction to appear when the alarm is raised

Arrows: use the arrows to selct the requested alarm

Tabs

Input status: full detail on inputs, see hereafter

Output status: full detail on outputs, see hereafter

Right click

Point the mouse on an item, right click on the right button and choose among the following functions:

Input
- ➤ Acknowledge (when under alarm)
- ➤ Confirm (when under alarm)
- ➤ Open input properties
- ➤ Return to normal mode
- ➤ Input deactivation

Relays
- ➤ Open relays properties
- ➤ Return to normal mode
- ➤ Deactivate relay continuously (constant off)
- ➤ Activate relay continuously (constant on)
- ➤ Activate relay during, specify the number of seconds

Process
- ➤ Execute process
- ➤ Open process properties

Actions

➢ Execute action
➢ Open action properties

<u>Tips & Notes</u>
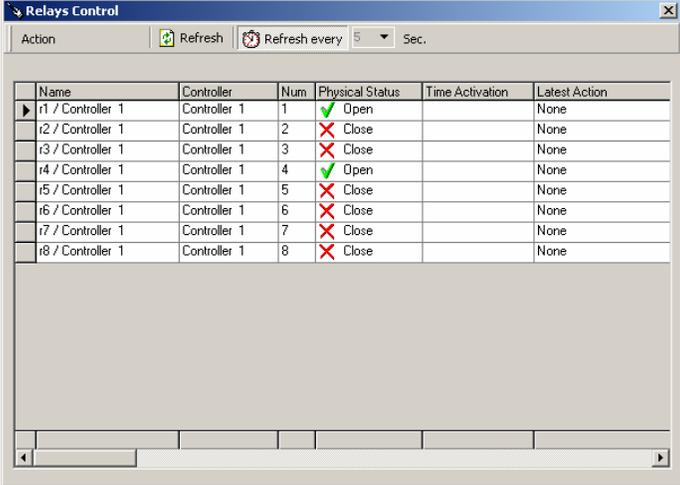
Dynamic map management

The map displayed is the one encompassing the activated input. If no alarm is signalled, the default map is displayed. If several alarms are activated, the map containing the most recent alarm raised will be displayed. If the "Event Handling - Active Alarms" screen is open and a new alarm is triggered, the map displayed is dynamically updated.

Active controllers

Inputs and relays are shown only for active controllers.

4.11.3. Active Alarms - Relays Control

This screen displays the dynamic status of relay activation in real time. It is accessible from the "Manual Intervention" menu or via the "Event Handling - Active Alarms" screen.

Icons

Action

> **Refresh**: select to update the diagnostic of the system on a manual manner

> **Return to normal mode**: select to cancel the actions described hereafter

> **Relay always on**: constant activation of a relay, allows for the permanent opening of a door, for instance

> **Relay always off**: constant non-activation of a relay allows for the permanent closure of a door, for instance

> **Activate the relay during**: the relay activation during a specific period allows the temporary opening of a door, the switching on and off of a red light, for instance

> **Number of seconds**: specify the activation length of time, between 1 and 60 sec.

Refresh: select to manually update system diagnosis status

Refresh every: select to automatically update system diagnosis status

Refresh delay (1 to 60 sec.): to modify the refresh delay, specify the number of seconds desired; the new delay will take effect only if the "Refresh Every" key is selected; by default there is an automatic refresh every 5 seconds

Table

Name: relay name

Controller: controller connected to the relay

Number on the controller: technical information on the physical connection of the relay

Physical status: open or close

Time activation:
- ➢ Armed (red icon): relay activation if the present time falls between the green zones of the selected weekly program
- ➢ Not armed (does not appear): when no weekly program is defined
- ➢ Not now (black icon): the present time does not fall between the green zones of the selected weekly program; there is no relay activation currently but the activation is defined in the system

Note that the weekly program "Always" trigger permanently the system while the program "Never" ensues in a constant deactivation

Latest action: enable to check if the normal situation has not temporarily been affected by the activation of a global reflex. As the reflex activation is a normal behaviour of the system, no error message appears in the log display. Nevertheless, the situation seems incorrect in the table.
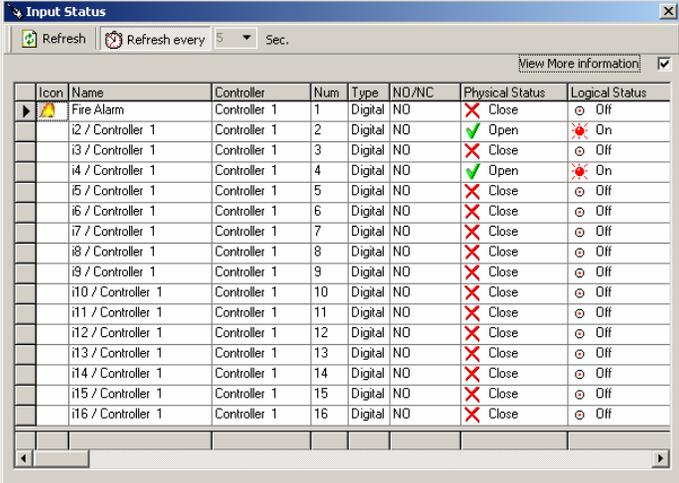
Tips & Notes

Sorting out information

The information that appears in the table can be sorted out. Each column can serve as a sorting criterion. To organize information in an increasing order, select the button containing the name of the column. To select the information in a decreasing order, select the empty button at the bottom of the column.

4.11.4. Active Alarms - Input Status

This screen displays a dynamic activation status of the input. Grant the system an approximate 15-second delay to check inputs status before the results are displayed.

Icons

Refresh: select to manually update system diagnosis status

Refresh every: select to automatically update system diagnosis status

Refresh delay (1 to 60 sec.): to modify the refresh delay, specify the number of seconds desired; the new delay will take effect only if the "Refresh Every" key is selected; by default there is an automatic refresh every 5 seconds

<u>**Table**</u>

Icon: icon associated with the input

Name: input name

Alarm physical status: open or close

Time activation: the input status switches between:
  ➢ Armed (in red): the arming process has been followed and the current time falls within the activation boundaries of the weekly arming program
  ➢ Not now (in black): the arming process has been followed and the current time falls outside the activation boundaries of the weekly arming program
  ➢ Disarmed: the process was not followed

The system automatically goes from "Not now" to "Armed", and vice versa, according to time zones.

Active alarms: coloured icons signal the alarm status (active, acknowledge and confirmed) in the table as well as in the tool bar
  ➢ Red icon: armed alarm
  ➢ Green icon: acknowledge alarm
  ➢ No icon: confirmed alarm

View more information: select this option to display the complete input information table

<u>**Extensive table**</u>

Icon: icon associated with the input

Name: input name

Controller: controller connected to the input

Input number on the controller: technical data about the input's physical connection

Type: digital

NO/NC: input normal status, normally open or normally closed

Alarm physical status: open or close

Alarm status: the logical status results from the combination of the normal status and the physical status

Normal, physical and logical status of an input

Input	Normal status	Physical status	Logical status
I1	NC	Closed	Off
I1	NC	Open	On
I2	NO	Open	Off
I2	NO	Closed	On

Time activation: see above

Active alarms: see above

Latest action: enable to check if the normal situation has not temporarily been affected by the activation of a global reflex. As the reflex activation is a normal behaviour of the system, no error message appears in the log display. Nevertheless, the situation seems incorrect in the table.

Example

The opening of a window will engage an alarm during the night (arming period) but not during the day (disarming period)

Arming process
  ➢ Define the input that checks the window opening, in the "Parameter - Controller - Input" screen
  ➢ Define the arming period, in other words, the daily and weekly programs, which are activated at night and inactivated during the day, in our example (in the "Parameter - Daily Program" and "Parameter - Weekly Program" screen)
  ➢ Activate the input in the "Event-Handling - Alarms" screen

Armed/disarmed input behaviour

	Arming program Night only	Arming program Always
During the night	Alarm	Alarm
During the day	No alarm	Alarm

During the night, both inputs will be activated if the window is opened. During the day, however, since the input has an inhibited time program, it is disarmed and will not raise an alarm.

Note that the weekly program "Always" corresponds to an activated non-armed input.

Alarm prevention

To prevent the alarm apparition, resulting from input activation, choose one of the following methods:
  ➢ Delete the input from the input list
  ➢ Deactivate the input, by going to the "Event Handling - Active Alarms" screen
  ➢ Link the "Never" weekly program to the input, by going to the "Parameter - Controller - Input" screen
  ➢ Deactivate the input conditionally for a specific person

Sorting out information

The information in the table can be sorted out. Each column can serve as a sorting criterion. To organize information in an increasing order, select the button containing the name of the column. To sort the information in a decreasing order, select the empty button at the bottom of the column.

5. MENU: MODULES

5.1. Parking

5.1.1. Parking - Basic Concepts

The parking module allows for access control to parking lots and for management of parking zone fill-up, according to user groups.

The system's ability to manage the parking activity is based on three concepts:
  ➢ **Parking lot**: physical area where cars are parked
  ➢ **Parking users group**: any company or entity that rents or owns parking spaces
  ➢ **Parking zone**: a certain number of spaces is allocated to each user group; a specific zone is accessible only to members of a corresponding user group

Two types of information are available for each parking lot:
  ➢ A counter displaying the amount of space available at any time
  ➢ A list of access points used to enter the parking lot. For each access point, the counter status determines if the counter should increment (+1), decrement (-1) or remain unchanged after the badge has been swiped.

Multiple parking lots

Several parking lots can be supervised simultaneously by the application.

Example: the company Alcaton has two buildings; one in Washington and one in New York, each site have its parking lot. Amadeus 5 controls the access to these two parking lots. The CBD company employs 6 people and rents three parking spaces in the Washington building and five in New York. In general, three employees work together in Washington. In New York, up to five people can work on a project at the same time.

In this example, it is necessary to create
  ➢ 2 parking lots: Washington and New York
  ➢ 1 user group: CBD company
  ➢ 2 zones:
    o Zone 1: CBD company in Washington (3 spaces)
    o Zone 2: CBD Company in New York (5 spaces)

All the employees of a user group are interdependent. Access to members of a user group is contingent to the space available in the zone allocated to the group. If six of CBD's employees arrive at the same time in Washington, access will be granted to the first three cars and denied to the other cars of the group.

Access permissions to a parking lot are independent of authorizations to other parking lots. An access denial in Washington does not anticipate on access in New York.

If al the allocated parking spaces of a company are occupies, other cars of this company will be denied access. Nevertheless other cars from other companies could still reach their respective zones according to their own occupancy rate.

Operating Mode

Define a controller of parking type, in the screen "Parameter - Controller"
  ➢ Define parking lots, in the "Modules - Parking Lot" screen
  ➢ Define user groups, in the "Modules - Parking Users Group" screen
  ➢ Allocate a user group to each member of the group, function "Parking Users Group" in the "Parameter - All Cardholders - Personal" screen
  ➢ Define parking zones, in the "Modules - Parking Zone" screen

Managing space availability

A free space counter is linked to each parking lot and zone. The movement of vehicles affects the counter level. For each car that enters, the amount of space is reduced. Each time a car goes out, the counter is incremented by one unit.

The number of space available can be computed at any time with respect to maximal parking capacity and counter status. A zone is full when the free spaces counter indicates zero.

5.1.2. Parking Lot

The parking lot is an area where cars are parked. Many parking lots can be supervised simultaneously.

This menu is divided into two tabs:
- ➢ General: define parking lots
- ➢ Presence list: follow up on all vehicle movements, within each parking lot, according to user groups

5.1.2.1. Parking Lot - General

This tab defines the different parking lots supervised by the system.
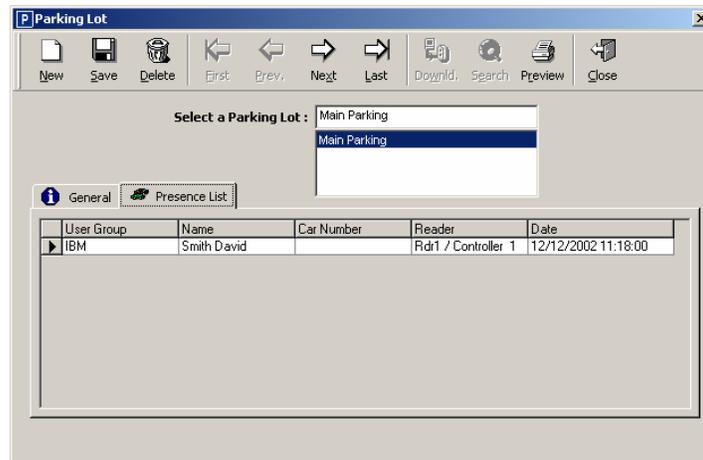

Fields

Name: name the different lots that make up the parking lot

Description: describe the new date entry

5.1.2.2. Parking Lot - Presence List

The "Presence List" tab allows the monitoring of vehicle movements within each parking lot. This information, which is displayed automatically, can be manually modified in the "Modules - Parking Zone - Presence Update" screen.

Fields displayed

User group: company or group to whom the vehicle belongs

Name: name of the badge holder requesting access

Car number: car license number

Reader: reader recording access to parking

Date: transaction date

5.1.3. Parking Users Group

A parking user groups is any company, or other body, leasing or owning parking spaces. Each group is allocated a specific parking zone, which can be identified by an identity number.

All group members are interdependent. Each group member has access to all the lots allocated to his company. If the lot allocated to his group is full, access will be refused to all the members of that group.

This menu is divided into two tabs:
  ➢ General tab, define of user groups
  ➢ Presence list tab, monitor car movements within each parking lot

5.1.3.1. Parking Users Group - General

This tab allows the definition of the different user groups supervised by the system.
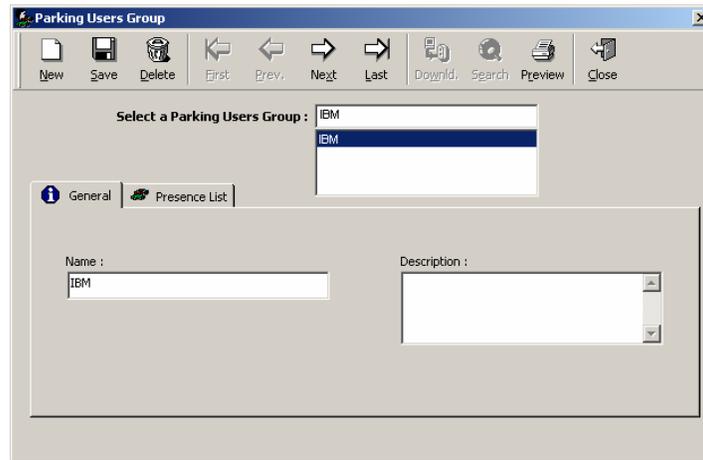
Fields

Name: name the different user groups

Description: describe the new data entry

5.1.3.2. Parking Users Group - Presence List

The "Presence List" tab displays details about the cars parked and their movements, according to user groups. This information can be manually modified in the "Modules - Parking Users Group - Presence Update" screen.
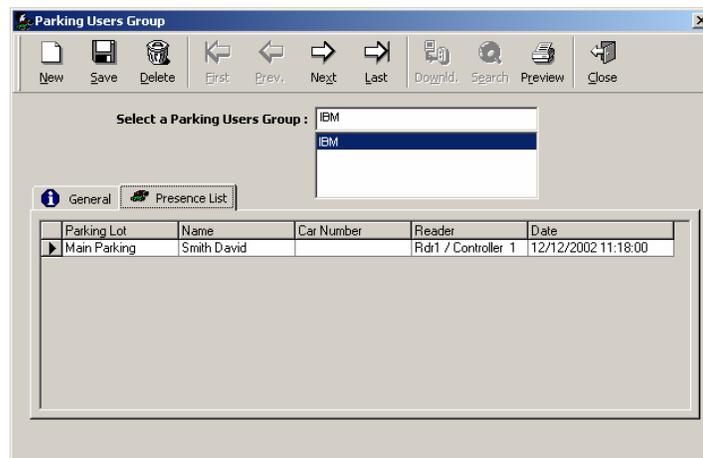
Fields displayed

Parking lot: portion of the parking allocated to a group of users

Name: name of badge holder that has passed through an access point

Car number: license plate number

Reader: reader that recorded the access to the parking lot

Date: transaction date

5.1.4. Parking Zone

The members of a user group can only access the parking spaces allocated to their group. Access to the parking lot is granted insofar as there are spaces available in the zone allocated to a group of users to which the driver belongs.

This menu is divided into three tabs:
- ➢ General tab, for parking zone definition
- ➢ Access tab, for access management
- ➢ Presence update tab, for modification of database information

5.1.4.1. Parking Zone - General

Fields

Name: name the parking zone

Description: describe the new data entry

Zone identification

  Parking user group: select the group that rents or owns parking spaces or press on the […] button to create a new group

  Parking lot: select the parking lot for which a filling up list has been established, or press on the […] button to create a new parking lot

Parking lot full / not full

 **Maximum number of places**: enter the parking lot's maximal capacity

  Actual free spaces: automatically displayed

  Actual occupied spaces: automatically displayed

Process to activate when full: define the reflex to engage if the parking lot is full; choose from the list or press the […] button to create a new process (for example, lighting of a red light)

Process to activate when not full: define the reflex to engage if the parking lot is not full, choose from the list or press on the […] button to create a new process (for example, lighting of a green light and opening of a gate)

5.1.4.2. Parking Zone - Access
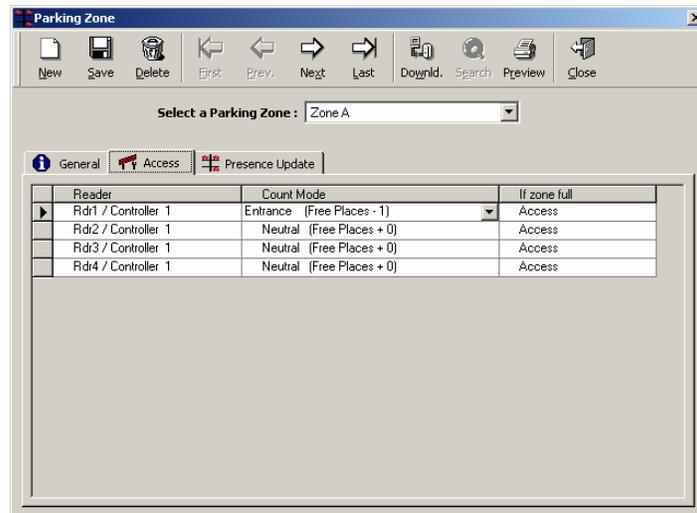
Fields displayed

Readers: activated access points

**Count mode**: number of spaces available
  ➢ In (available places –1)
  ➢ Neutral (available spaces +0)
  ➢ Out (available space –1)

If zone full: reader behaviour for the members of the user group (access granted or denied)

5.1.4.3. Parking Zone - Presence Update

This function is particularly useful when car movements occur without being recorded by the system, because of a power failure or communication breakdown between readers and controllers or when two cars enter simultaneously, for instance.

The system automatically displays driver names, car license numbers and user groups for those that have requested access. In this screen, it is possible to manually modify the presence list, which is automatically displayed in the "Presence List" tabs of the "Modules - Parking Lot" and "Modules - Parking Users Group" screens.
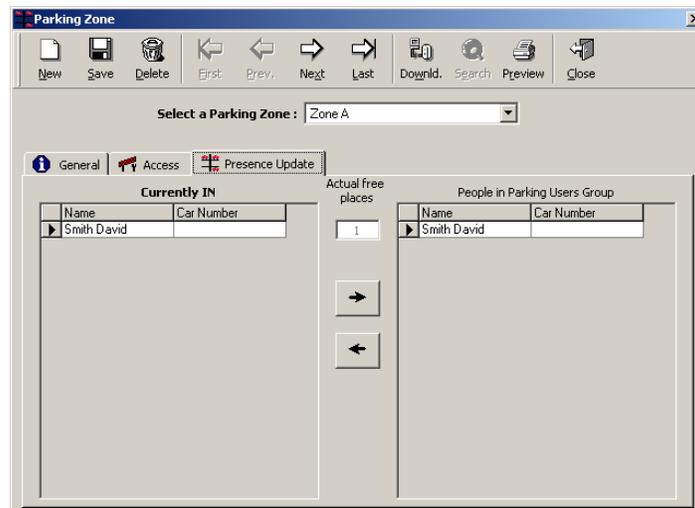
Fields

Using the arrow keys, data can be inserted or deleted.

Currently in: for cars in the parking lot, the system displays the following:

  Name of the badge holder that has requested access
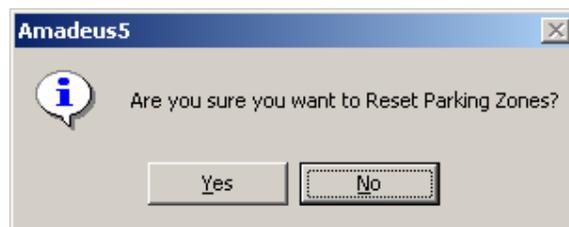
  License plate number of the car

Actual free spaces: the counter displays the unused capacity of the parking lot

People in parking users group:

  Name of the badge holder that has requested access

  License plate number of the car

5.1.5. Reset Parking Zone

The "Modules - Reset Parking Zones" menu deletes all the information from the parking lot database. The system asks for confirmation, by displaying the following message:
"Are you sure you want to reset parking zones?"

Confirm the wish to reset or cancel the operation. The following message confirms the reset:
"Reset parking zones has succeeded"

Note that a partial data modification is possible by going to the "Modules - Parking Zones - Update" screen.

5.2. Lift Program

A lift program defines the floor combination accessible by a group of users. Note that this function does not control access to the lifts, nor to the areas served by these lifts.

This function manages access to the floors served by one or several lifts. The badge holder swipes his card through the reader located inside the lift cabin and presses on one of the floor buttons that has been lit. If the badge holder is granted access, the lift will take him to the desired floor. If access is denied, the lift will stay put.

In a building shared by many companies, each person can select only the floors allocated to his company. If the badge holder has not selected which floor he wants to go to within a specified delay, access will be denied to all floors. This prevents unauthorized persons from using the lifts.

Information with respect to the lift program is divided into two tabs:
  ➢ General tab: to define lift programs
  ➢ Cardholders tab: to refer to the persons belonging to the lift groups

Operating mode

  ➢ Create a controller, which type is "Lift", in the " Parameter - Controller" screen
  ➢ Create lift program groups, connecting outputs to the lifts floor buttons, in the "Modules - Lift Program - General" screen
  ➢ Allocate lift programs to cardholders, using the "Lift Program" function of the "Parameter - All cardholders - General" screen

Series of lifts

A controller can supervise a series of lifts with identical floor authorizations. If access authorizations differ, several controllers will be required.

The basic controller has 4 relays; a 12-relay extension card can be plugged in. The sixteen available relays can be programmed to correspond to the floor buttons of the lift. If more than 16 floors are required, several controllers are required. A network, of maximum 32 controllers, can supervise different lifts in parallel. Several buses can coexist.

Example

Site with two buildings
  ➢ Building one is made up of three floors
  ➢ Building two is made up of six floors
 ➢ Each building has its own lift

Three user groups are defined:
  ➢ Top management can access all floors in both buildings
  ➢ Technical staff can access floors 1 and 2 of the first building and floors 1, 3, 4 and 5 of the second building
  ➢ Administrative personnel can access floors 1 and 3 of the first building and floors 1, 3 and 6 of the second building

To fill the needs of this site, three lift programs must be created with the following authorizations:

Lift program	User group	Accessible floors Building 1	Accessible floors Building 2
A: Top management	Top management	1, 2, 3	1, 2 , 3 , 4 , 5 , 6
B: Technical Division	Technical personnel	1 , 2	1 , 3 , 4 , 5
C: Administration	Administrative personnel	1 , 3	1 , 3 , 6

5.2.1. Lift Program - General
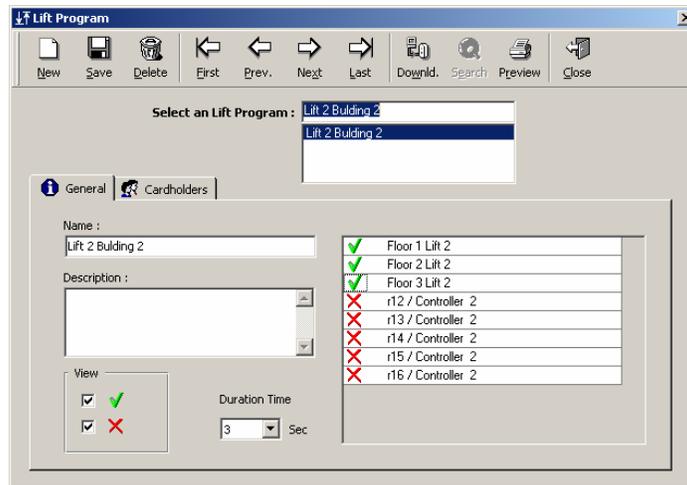
Fields

Name: name the new lift program

Description: describe the new data entry

View: select to display the list of relays of the lift controllers. By default, the relays - and thus the corresponding floors - are excluded from the program.
  - ➢ **V**: list of relays included in the lift program
  - ➢ **X**: list of relays excluded from the lift program; by default
  - ➢ **X and V**: list of all the relays in the lift program
 - ➢ -- : no relays displayed

Duration time: specify the relay activation delay engaging the selection of the floor button; the number of seconds of lift program activation must be included between 0 and 120 seconds; a delay of 3 seconds is set by default

Change the **relays inclusion status** by clicking on X or V in the left column of the relay table
  - ➢ The relays preceded by V are included in the lift program
  - ➢ The relays preceded by X are excluded from the lift program

5.2.2. Lift Program - Cardholders

The informative table displays the names and surnames of the member the user group to which the lift program is related. Note that this is not a presence list.
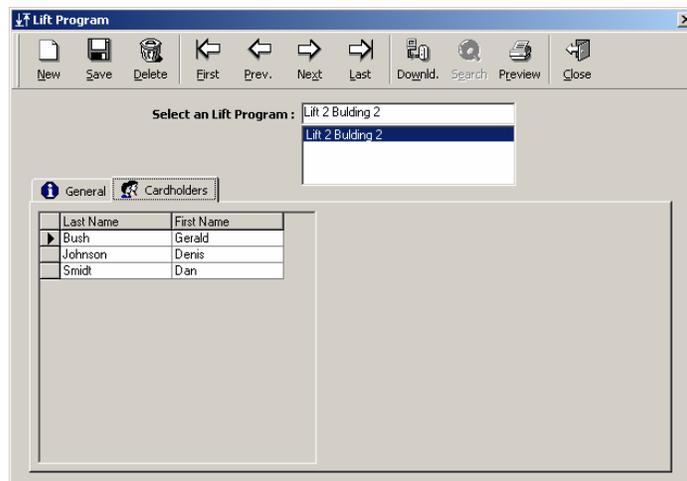
5.3. Time & Attendance Management

Time & attendance management facilitates the computation of employees' attendance, overtime, absences and lateness to provide the number of hours worked by employees. The calculation can be restricted to specific periods, readers or employees.
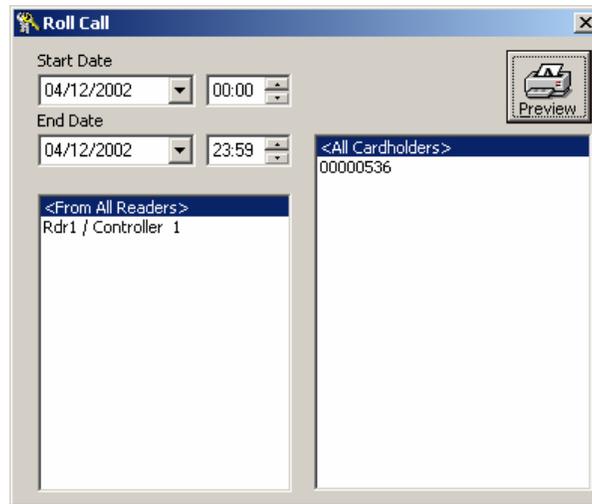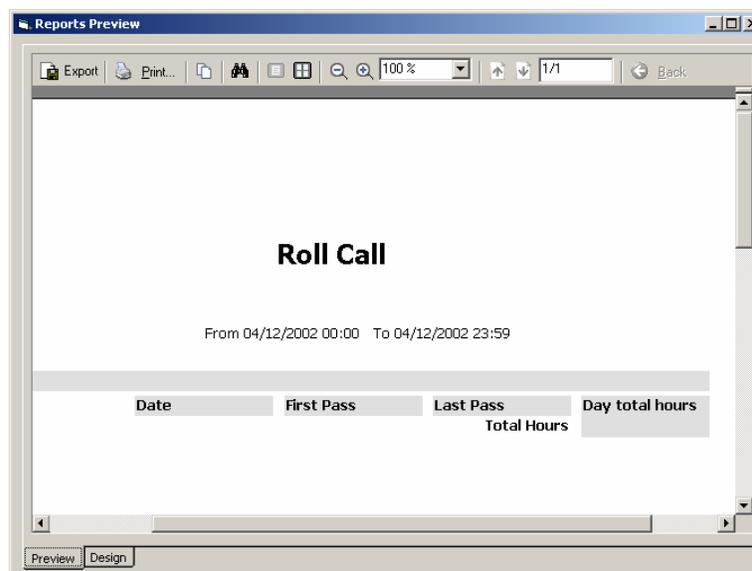

<u>**Fields**</u>

Start date: specify the date and hour of the beginning of the period

End date: specify the date and hour of the end of the period

Readers: select the reader(s) to take into account

Badge holders: select the badge holders(s) to take into account

Preview: preview the roll call report

5.4. Guard Tour Module

5.4.1. Guard Tour Module - Basic Concepts

A guard tour consists of a path of checkpoints reached by an authorised employee - the guard - within predefined deadlines. Arrival at a checkpoint is signalled via input activation or reading of a badge and results in a message sent to the PC. Each expected time allows for tolerance deadlines. Several tours can be defined and run in parallel. The log and the reports will show them.

Example

|	
8:00	Guard tour beginning
8:06 - 8:15	Predefined authorised arrival period at the first checkpoint, the guard should activate an input to signal his passage (expected time: 8:10, tolerance (-):04 min, (+): 05 min)
8:28 - 8:33	Predefined authorised arrival period at the second checkpoint, the guard should present his badge to the reader (expected time: 8:30, tolerance (-):02 min, (+): 03 min)

5.4.2. Guards

A guard is an employee habilitated to perform guard tours. An employee is defined as guard in the screen:
- ➢ "Parameter - All cardholders" screen, by manually setting his type to "Guard"
- ➢ "Modules - Guard", in which the type is automatically set to "Guard"

5.4.3. Checkpoint - General

Checkpoints, as well as the inputs or readers activated to confirm the arrival, are defined in the "Modules - Checkpoint - General" screen. The identity of the person changing the input status is not known by the system. If the security level requests the guard identity verification, readers should be installed at each checkpoint.
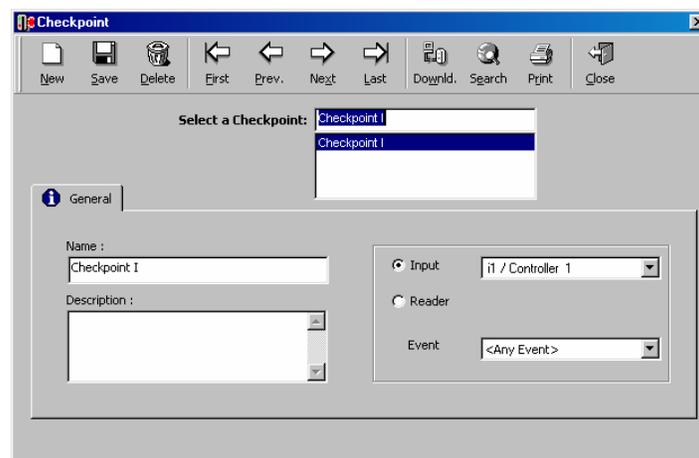
Fields

Name: name the checkpoint

Description: describe the new data entry

Input: select the input that signals the arrival of the guards among the list of system inputs; they must be activated before the start of the tour

Event (if input): choose between "Any event" and "Start of alarm

Reader: select the reader that will signal the arrival of the guard among the list of system readers

Event (if reader): choose between
  ➢ Access granted
  ➢ Access granted (duress code)
  ➢ Access denied
  ➢ Access denied (unsuccessful attempts)

Example of access denied: the guard must pass in front of the computer room but is not allow entering it.

5.4.4. Guard Tour Program
5.4.4.1. Guard Tour Program - General

Define a new tour, in the "Modules - Guard Tour Program - General". Select the processes to activate following the arrival of the guard at the checkpoint. The process on alarms can differ according to early or late arrival or the lack of it.
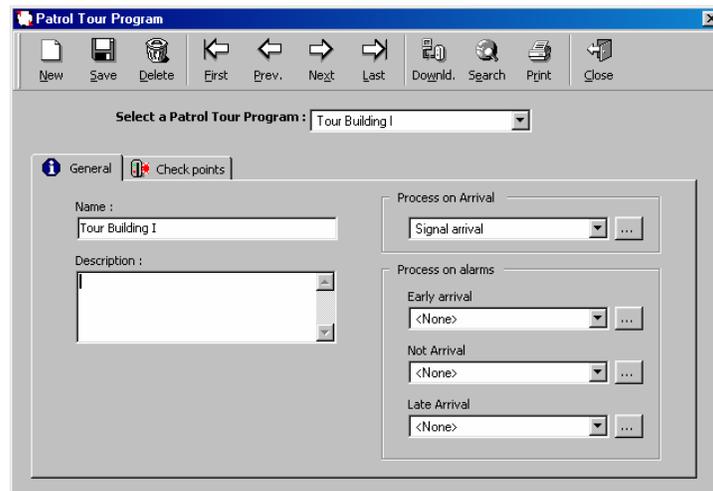
Fields

Name: name the new tour

Description: describe the new item

Process on arrival: select the process to trigger on arrival in the list or press on […] button to trigger a new one; examples: voice alarm on PC, relay activation triggering a buzzer

**Process on alarms**: in the list, select the process to trigger in case of
  ➢ Early arrival: arrival before the expected time minus its allowance
  ➢ Not arrival: automatic message displayed at the end of the expected arrival deadline (including the tolérance and a further 60 seconds) if arrival has not been signalled
  ➢ Late arrival: arrival after the expected arrival time (including the allowance and a further 60 seconds)

5.4.4.2. Guard Tour Program - Checkpoints

To complete the definition of the guard tour, select the checkpoints and attribute them an arrival time, including allowance for early (-) and late (+) arrival

The arrival times are computed from the beginning of the tour. They are independent of the actual time the tour begins - unknown at this state - and of previous checkpoints time.

Some computers will display the time as "0::00" instead of"00:00". This does not affect the operation.
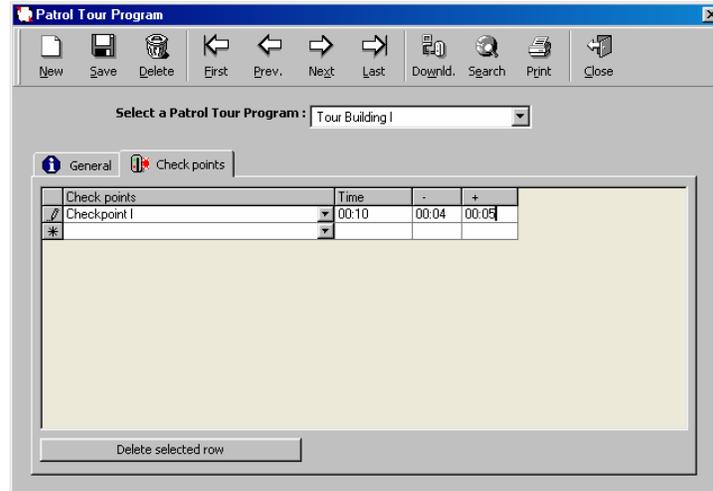
Fields

Checkpoints: choose the checkpoints of the tour path

Time: specify the arrival time, in relation to the beginning of the tour and expressed in a "hh : mm" format

(-): tolerance for early arrival

(+): tolerance for late arrival

Delete selected row: point on one of the checkpoint rows and hit this key to delete a specific row

5.4.4.3. Beginning the Guard Tour

The tour begins:
  ➢ **Manually**: execution of a launching process
    o Define a new action ("Event Handling - Action" screen) wherein the action type is set to "Start a guard tour", the first parameter corresponds to the tour name and the second parameter to the guard name
    o Define a new process ("Event Handling - Process" screen) including this action
    o Launch the process via the "Manuel Action - Execute Process" function
  ➢ **Automatically**: global reflex which will launch the tour as a result of a predefined event ("Event Handling - Global Reflex" screen); use any manual action (card pass, modification of input status, etc.) or the scheduler (set the global reflex event type to "Scheduler" and specify the date, time and hour the tour should begin)

Restarting a tour

Restarting a running tour will stop this tour and replace it by a new instance.

Scheduler weekly program

A weekly program is allocated to each global reflex. So even the scheduler can only activate the process at green times of a selected weekly program.
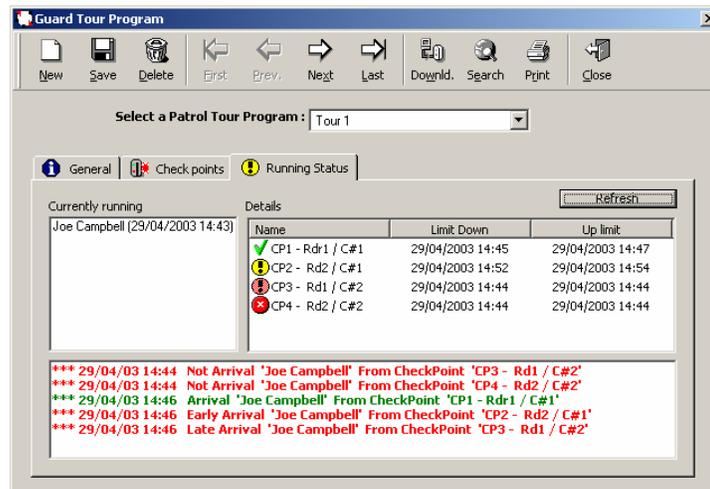
5.4.4.4. Ending the Guard Tour

The tour ends 15 minutes after the expected arrival time at the last checkpoint. After that, the tour status is set to "Not running". Refreshing the running status screen at this point will remove the tour information.

5.4.4.5. Guard Tour Program - Running Status

When a specific tour is running, tour description, checkpoints, expected times of arrival with tolerance limits and arrival status (on-time, early, late arrival or lack of it) are shown on this screen.

The details of a tour currently running will appear by clicking on the tour row. Press the "Refresh" button to update the status events.

Currently running: list of the tours presently running with mention of the guard that patrols, the date and time of the beginning of the tour

Details: include checkpoint name, upper and lower limit of arrival time

Four different icons are showing the type of arrival at each checkpoint (on time, early, late arrival or lack of it)

When an input is activated or a card presented to a checkpoint reader, two messages are displayed in the log:
  ➢ Message of input or reader events, according to the checkpoints definition
  ➢ Messages of guard tour events (arrival on time, late arrival, etc.)

In our example, the running status will show the following messages

12:00   Tour started: guard A starts the tour

12:00 -12:06   Early arrival: arrival before the lower limit of the expected arrival period

12:06 -12:15   Arrival on time: arrival within expected arrival period

At 12:16   No arrival on time: if the guard has not shown up at the checkpoint at the upper limit of the expected arrival period

12:16 – 12:31 Late arrival: arrival at the checkpoint after the expected time (plus 60 sec. for system synchronisation)

12:31   End of tour: 15 min after the last checkpoint expected time, plus the tolerance for late arrival (plus 60 sec. for system synchronisation)

5.4.5. Patrol Report

This function directly links to the guard patrol report of the report generator. Consult the report wizard for further information.
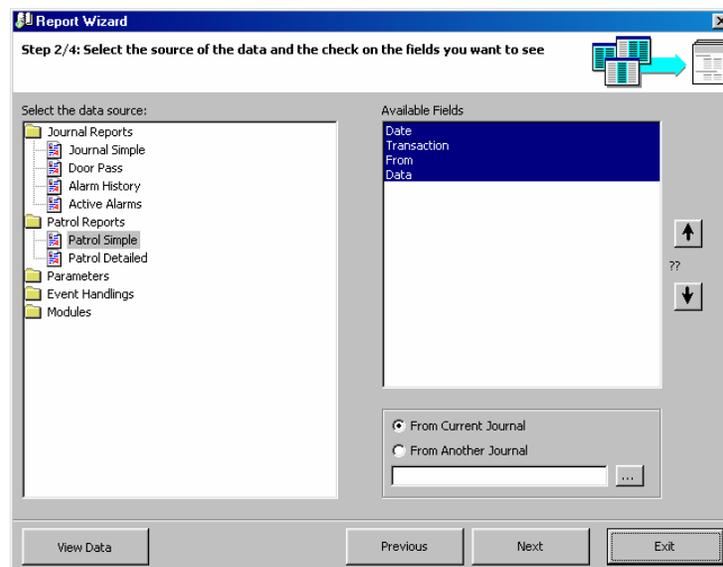
6. MENU: COMMUNICATION

6.1. Stop / Resume Polling

Polling allows the detection of events that brought about changes in the controllers. Polling consists in interrogating controllers at regular intervals. Detection of events in real time allows for rapid information update and decision making with full knowledge of the facts.

The time interval between two polling transactions is defined in the "Waiting Delay" function in the "Parameter - Controller Network - Definition" screen.

Fields

Resume polling (shift + F8): select this option to activate the polling

Stop polling (shift + F8): select this function to stop polling

Tips & Notes

Use the "shift F8" key at any time, from any screen, to modify polling status.

By default, the system carries out a polling activity at the start of the application. This option can be modified in the " Tools - Options - Communication" screen by changing the status of the " Do polling at start-up" function.

6.2. Diagnosis

This screen allows the visualization of the controllers' status. The F8 key displays the diagnosis of any screen.

This screen support the selection of multiple items with the keys Ctrl/Shift.

The diagnosis screen is made up of two windows:
  ➢ Left: system controllers list
  ➢ Right: information regarding the controller selected

The choice of a controller from the left window activates the right window where the details of the selected controller are displayed.
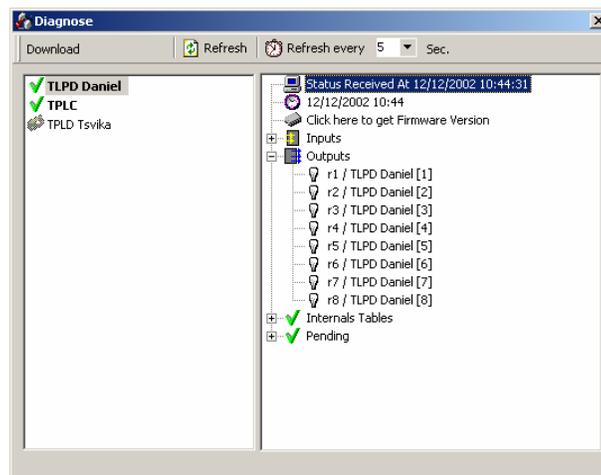
➢ Download: menu of the available downloads for the selected controller ; this function can be used only if the "Refresh Only" key is not selected
➢ Polling
➢ For all cardholders
➢ Reset controllers
➢ Send time & date
➢ Send daily & weekly programs
➢ Send all card holders (Quick)
➢ Send all card holders (Complete)
➢ Send pending
➢ Initialisation (Quick)
➢ Initialisation (Complete)

Refresh: select to manually update system diagnosis status

Refresh every: select to automatically update system diagnosis status

Refresh delay (1 to 60 sec.): to modify the refresh delay, specify the number of seconds desired; the new delay will take effect only if the "Refresh Every" key is selected; by default there is a refresh every five seconds

Data displayed

Controller status in the left window

Controller communication status is graphically represented as follow:
➢ **Grey**: if the controller is not active, communication is not monitored by the system
➢ **Bold**: if controller is active, communication is controlled by the system, in which case:
   o **V**: communication established
   o **X**: absence of communication

Information available in the right window

Request time: hour of event

Controller time when request was put in: can differ from time of request if internal controller clock is late

Click here to obtain firmware: the "checksum" date of the EPROM is displayed on the screen; this avoids physical check

Input status: name [input number from 1 to 8] [NO or NC status]
Icons specify input status in real time:
➢ Normal status
➢ Engaged input status
➢ Status undetermined

Output status: name [relay number]
Icons specify output status in real time:
➢ Normal status
➢ Engaged input status
➢ Status undetermined

Status of controller table: informative technical tables that refer to readers, card formats, weekly access programs, daily programs, holidays

Status of command pending: when downloading a non-connected controller, for instance, the information downloaded is signalled by the V symbol and the information pending by the X symbol

Retaining a diagnosis status

It is possible to retain a diagnosis status for later reference, by preventing further refresh. To do so, make sure the "Refresh Every" key is not selected.

Default parameters

By default, the "Refresh Every" key is selected and the "Refresh Delay" set for 5 seconds.

6.3. See / Clear Log Display

The log display is a temporary linear colour display that signalled events as they occur. The information is recorded in the journal for later reference and printing. Although they appear similar, the contents of the log display and those of the journal are not 100% identical.

Examples of differences between log display and journal:
  - ➢ User login: appears in the journal but not in the log display
  - ➢ Communication status at certain times: appears in the log display but not in the journal

Different colours indicate the type of information available.
  - ➢ **Burgundy**:
    - o Unknown badges (not recognized by the system)
    - o Non-allocated badge (recognized by the system but not allocated)
    - o System alarms, such as weak battery, power up after failure, memory deleted
  - ➢ **Red**: Start and end of input activation
  - ➢ **Green**: Access authorization and normal communication status (OK)
  - ➢ **Black**: Access denied and reason for denial
  - ➢ **Grey**: System commands, provided for informational purposes. They are not displayed by default. Use the "Show commands for information" option, in the "Tools - Option - Communication" screen, to modify the display status.

Example of information available

Green: **Number   Date   Hour   Type of event**
Number   Date   Hour   Badge holder   Reader   Transaction code

Identification number of the event in the journal: to estimate the size of the journal
Date and hour of event; type of event: access granted, COM OK, for instance; name of the badge holder requesting access; name of reader, and associated controller, where transaction has been requested; personal transaction code (a personal transaction code typed on a reader keypad engages an associated global reflex. It is independent of the personal identification code (PIN code). Different combinations can be recorded in the system.)

6.4. Display Picture

Compare the appearance of the person presenting his badge at a reader to the photograph associated to the badge and stored in the system. Select the reader(s) for which the identification check is requested. From this screen, it is possible to open the employee screen.
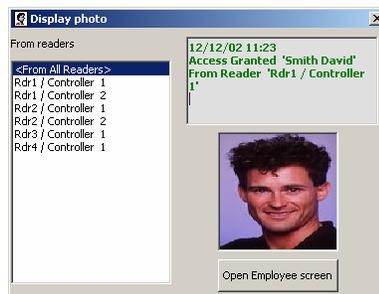
7. MENU: MANUAL ACTION

7.1. Crisis Level

The crisis level function enables simple and quick modification of access authorizations for a group of employees. Access denial for all doors could have been achieved through a specific action. However, since this action is connected to an individual, it would have been necessary to repeat this procedure for each employee separately. Downloading access authorization modifications, for a group of 1000 employees at 30 controllers, could have taken up to thirty minutes. The "Crisis Level" function solves this problem.

Personal crisis levels, which are defined prior to using this function, are compared to door crisis levels ("Manual Action - Send a Crisis Level" screen). According to their relative values, authorization will be granted or denied.

Example

- ➢ Three doors: R&D, offices and entrance/exit
- ➢ Three access groups: administration, top management and engineering

In a normal situation access authorizations are allocated in the following way:

Access authorizations according to access groups and doors in normal situation

	R&D door (door 1)	Office door (door 2)	Entrance/exit door (door 3)
Access group I Top management	Yes	Yes	Yes
Access group II Administration	No	Yes	Yes
Access group III Engineering	Yes	No	Yes

In a normal situation, all authorized employees (group II and III) can enter and exit the R&D department. In case of emergency, even the engineers are denied access to the R&D department. To do so, allocate a crisis level to the access group as follows:

Doors accessible	Access group	Access group crisis level
1 2 3	I Top management	6
2 3	II Administration	4
1 3	III Engineering	3

In order for a door to open, the following conditions must be met:
- ➢ Badge recognition
- ➢ Employee validity
- ➢ Access validation through the door
- ➢ Employee access time zone compatibility
- ➢ Door open time zone compatibility
- ➢ Absence of global reflex shutting the exit

When using the "Crisis level" function a further question need asking: What is the relative value of the persons' and doors' crisis level?

Relative crisis level value for persons and doors

CL = Crisis Level
If Person CL > or = Door CL   ➔ access granted
If Person CL < Door CL   ➔ access denied

<u>Personal and door crisis levels</u>

	Personal crisis level	Normal situation Door crisis level = 0	Emergency Door crisis level = 4
Access group I	6	Access granted	Access granted
Access group II	4	Access granted	Access granted
Access group III	3	Access granted	Access denied

By default, the crisis level for doors is equal to zero and the one for people depends on its access group, which means that everybody can go through any door.

When creating a new access group, the crisis level of the group members is null. The new crisis level must be entered manually.

<u>**Tips & Notes**</u>

The last crisis level specified to the system is shown in the "Manual Action - Send a Crisis Level" screen.

In order for the system to function optimally all the readers connected to a controller must have an identical crisis level.

Only the controllers equipped with an EPROM dated beyond the year 2000 support the crisis level function.

When the crisis is over, allocate a normal value (0 or 1) to the crisis level to regularize the situation.

7.2. Execute the process

Click on one of the icon of the screen "Execute the process" to launch it.
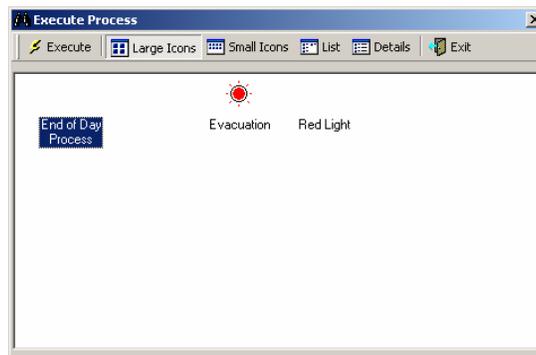
8. MENU: TOOLS

8.1. Report Wizard

8.1.1. Basic Concepts

Amadeus 5 incorporates a powerful tool for personalised report generation. The reports are compiled from the journal or from any other database (parameters, events or modules)

Amadeus 5 system incorporates a powerful report wizard for generation, modification and update of personalised reports. They are compiled from the journal or from any other database (parameters, events or modules). Reports are generated in the language of the application. They can be display, printed or exported. Four user-friendly screens lead the user to the widespread functions. They fit the need of the layman as well as those of the confirmed user.

8.1.2. First screen: Report Selection

The first screen of the report wizard allows for consultation of existing report and creation of new ones. It is accessible via the icon of the navigation bar or via the ''Tools'' menu. The last report is automatically saved.

The screens "Tools - Report Wizard" can also be reached via:
➢　　　"Patrol Report" of the menu "Modules" that branches to the "Simple Patrol Report"
➢　　　"F10" from any screen that leads to the report of the corresponding parameters
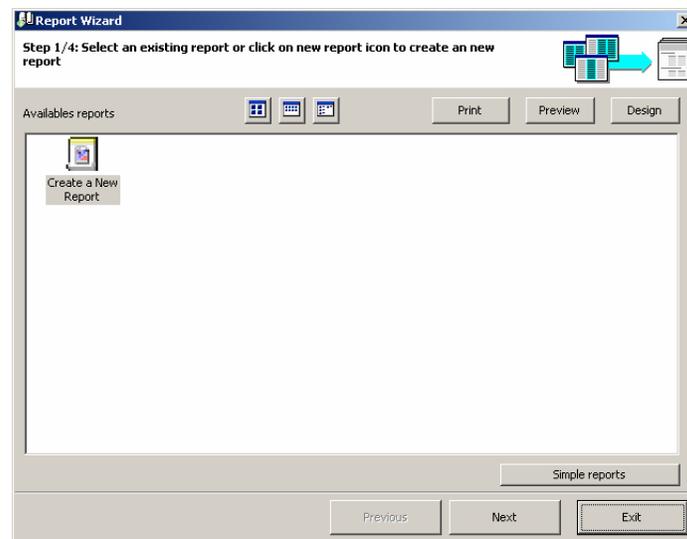
Fields

Big icons: preview the big icons of the available reports
Small icons: preview the small icons of the available reports
List: preview the list of available reports

Print: print the chosen report
Preview: preview the report on the screen
Modify: personalize the report

Simple reports: display the standard journal query report

Previous: return to the previous screen of the report wizard
Next: go to the next screen of the report wizard
Exit: quit the report wizard and go back to the main screen

8.1.3. Second screen: Data Selection

The second screen of the report wizard enables the selection of the data source and of the columns that appear in the report. Certain columns are automatically selected by the system. This choice and their order are easily modified.
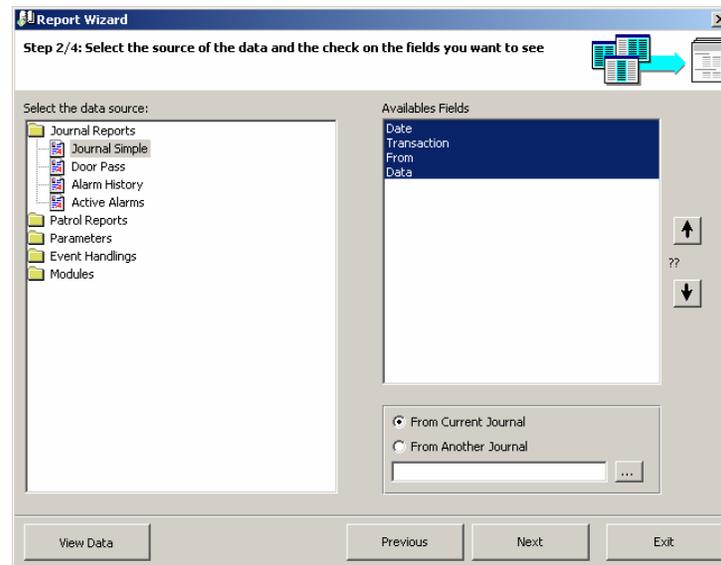
Fields

Select the data source: choose the type of the report among the following list:
  ➢ **journal report**: journal simple, door pass, alarm history, active alarm
  ➢ **patrol reports**: patrol simple, patrol detailed
  ➢ **parameters**: controller networks, controllers, daily programs, weekly programs, access groups, departments, badges, all cardholders, visitors, authorisations levels, users, customised labels
  ➢ **event handling**: icons, maps, input groups, output groups, actions, processes, counters, global reflexes, inputs in event handling programs
  ➢ **modules**: parking lots, parking users groups, parking zones, parking presence list, lift programs, guards

Available fields: display of the fields requested; the wordings on blue background appear by default in the report in the report; the others will not be displayed in further stages. Click on a field to include or exclude it from the selection.

Arrow: chose a field and move it with the arrow and the "Enter" key

Choice of journal: choose the journal (period) of the report. By default, the current journal is selected; all other journal of the system can be preferred, by indicating its position with the […] button
  ➢ From current journal
  ➢ From another journal: specify the name and directory of the journal to consider

View data: preview the content of the data; click again on the "See data" button to quit this mode
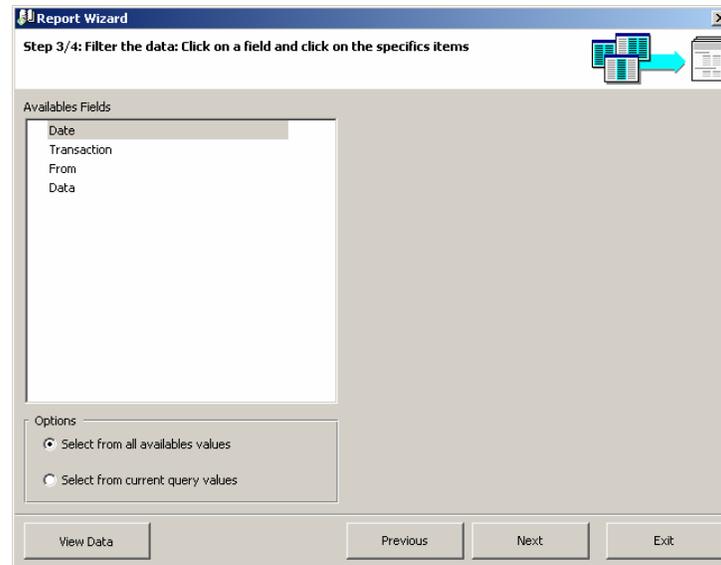
Previous: return to the previous screen of the report wizard

Next: go to the next screen of the report wizard

Exit: quit the report wizard and go back to the main screen

8.1.4. Third Screen: Data Filter

The third screen of the report wizard allows to fine tune the report by filtering the data. The fields selected in the previous screen are displayed at the top of the list. Fields non-withheld appear bellow the separation lines. When appropriate, fill the sorting criteria in the right window. It is possible to specify sorting criteria for fields not mentioned in the report.

Fields

Available fields: select the fields to display

Options: chose between
   ➢ Select from all available values
   ➢ Select from current query values: restrict the criteria to current request

View Data: preview the data content and scan the information

Previous: return to the previous screen of the report wizard

Next: go to the next screen of the report wizard

Exit: conclude the report creation and go back to the main screen

Tips and notes

Criteria: Date

Fill in as appropriate: since, till, during the last X months, during the last X days

The "During" alternative is useful to automatically update the period of the report.

Impact of the use of "Since" and "During"

	Date of creation of the report	
	February 1	March 1
Since January 1	Jan. 1 - Feb. 1	Jan. 1 - March 1
During last month	Jan. 1 - Feb. 1	Feb. 1 - March 1

8.1.5. Fourth Screen: Data Organisation

Data to be displayed, exported or printed is organized in this screen.
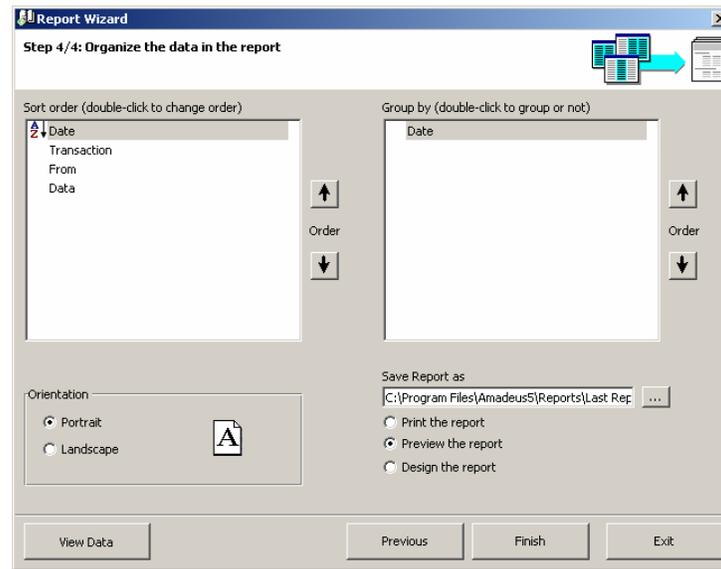
<u>**Fields**</u>

Sort order: double click on the requested field to sort the information in an alphabetic order (A to Z), in reverse order (Z to A) or to cancel the sorting on this column; by default the data is sorted alphabetically on the field on the top of the list

Group by: double click to group the information or ungroup it, by default no criteria is selected

Arrows: modify the order of the fields with the arrows

Orientation: choose between portrait and landscape

Save report as: specify the name and directory; by default the reports are save in
C:\PROGRAM FILES\AMADEUS5\Reports\Last Report.rpx
Accept the system choice or modify it with the […] button. It is advised to save the reports in the above directory for them to appear in the first screen of the report wizard.

What to do with the report: chose between
  ➢ Print report
  ➢ Preview report
  ➢ Design report

View Data: preview the data content

Previous: return to the previous screen of the report wizard

Finnish: finish designing the report

Exit: quit the report wizard and go back to the main screen

8.1.6. Screen "Report Preview"

Preview the report in this screen.

<u>Fields</u>

Select on the adequate options of the toolbar.

Export: select the appropriate export option
- ➢ RTF - Rich Text Format
- ➢ PDF - Portable Document Format
- ➢ HTML - Hyper Text Markup Language
- ➢ XLS - Microsoft Excel
- ➢ TIF - Tagged Image Format
- ➢ TEXT

Copy in: copy in the current page only

Search: search for a specific word in the report

Page: preview the report page by page

Several page: preview simultaneously several page on the screen

Shrink: shrink the preview size to fit more pages in the screen

Enhance: increase the preview size

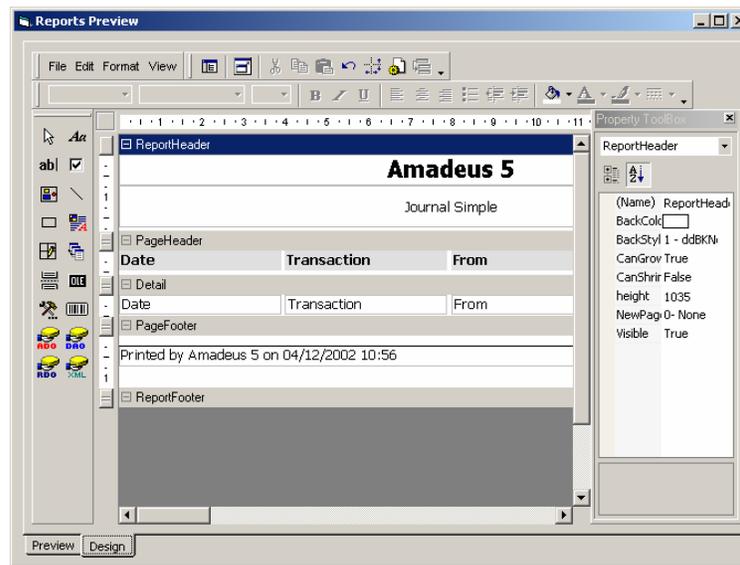**Page preview**: modify the zoom percentage

Previous: return to the previous screen of the report wizard

Next: go to the next screen of the report wizard

Go back: go back to the previous preview; this differs from "Previous page" if the preview order does not follow the pagination order

8.1.7. Modification screen

This screen is reserved for confirmed users only.

### Example of report modifications

Basic modifications
- ➤ Move a field
- ➤ Lengthen or shorten the space allocated to a field
- ➤ Suppress data
- ➤ Modify the police of characters and the font colour

Enhanced modifications
- ➤ Add a field
- ➤ Group information
- ➤ Go to the next page after each group
- ➤ Insert a picture
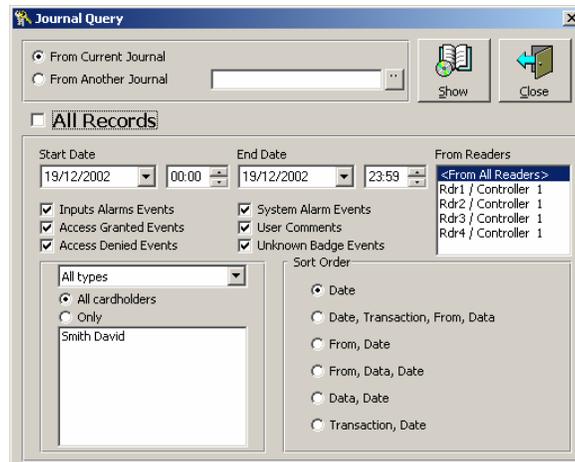
8.1.8. Screen "View Data"

Preview the content of the data. Click again on the icon "View Data" to exit the screen.
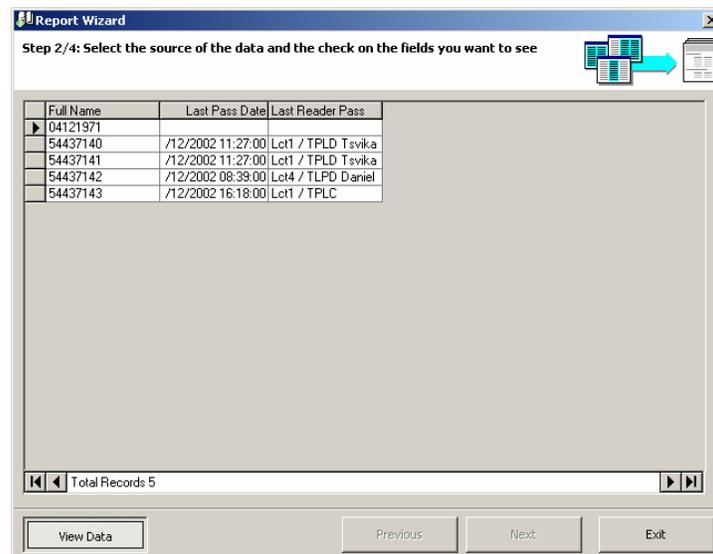
8.1.9. Journal Query

The journal allows the edition of activated records.

Once the databases have been defined, the screens "Journal" and "Event Handling - Active Alarm" are frequently used. Click on "Close" to leave this screen.

Fields

From current journal: the current journal is displayed

From another journal: select another journal using the […] button

Show: display the journal selected; it is possible to print the journal displayed

Close: close the screen and go to general menu

All records: display all the information available in the system; the bottom part of the screen is shaded grey

If this option is not checked, the bottom part of the screen is activated to allow the selection of criterion display.

Sorting out data: select the data criterion display from the journal

According to date: start and end date and hour

According to reader: select the reader

According to events: alarm input, access granted, access denied, system alarm, user comments, unknown badge

According to cardholders
> ➢ All cardholders
> ➢ Only: select specific cardholders from the list of persons

Sort order: define the order of the data selected; choose one of the following options:
> ➢ Date
> ➢ Date, transaction, from, data
> ➢ From, date
> ➢ From, data, date
> ➢ Data, date
> ➢ Transaction, date

8.2. Create New Database

The Amadeus 5 application allows the creation of simultaneous databases. The application installer has thus a constant access to all sites databases. The clean new database becomes the active database.

Information from the existing database is saved. The system displays the name of the file saved in the message:
"Your database has been saved as C:\ProgramFiles\Amadeus5\Backup\Amadeus5_xxxxx.mbd"
The extension of all the databases is "mbd".

By default, the files are saved in the directory: "C\ProgramFiles\Amadeus5\Backup". The default destination of the file saved can be modified in the "Tools - Options - Files Location" screen.
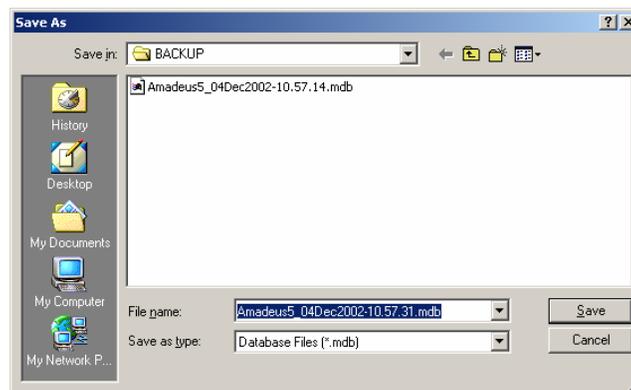
This option is only displayed for super-users. See the multi-company section for further reference.
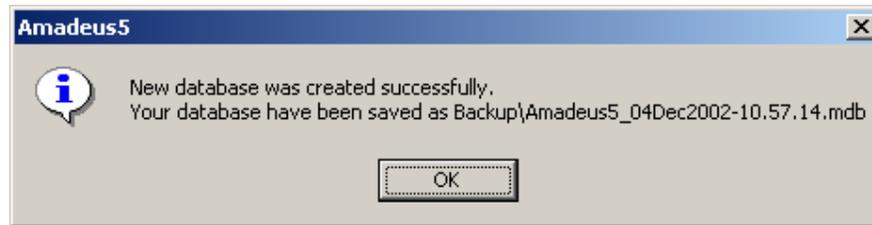
8.3. Save Database

The size of the Amadeus 5 database cannot exceed 70Mb for good operating condition. Once a month, it is therefore advisable to clean the system of unnecessary data.

Select the database from the list and confirm, or cancel, the operation.

Fields

Save in: type in the path where the file is saved

Name: enter the file name containing the database

 Save as type: select the file type
> ➢ *.mbd - database file - extension given by the system
> ➢ *.* - all files - database from other applications

Open as read only: select if the new database is provided for reference only

Destination by default

By default, the files are saved in the following directory: "C:\ProgramFiles\Amadeus5\Backup"

The default destination of the saved file can be modified in the "Tools - Options - Files Location" screen.

Windows Functions

Some Windows functions are available: Up One Level, View Desktop, Create New folder, List and Details.
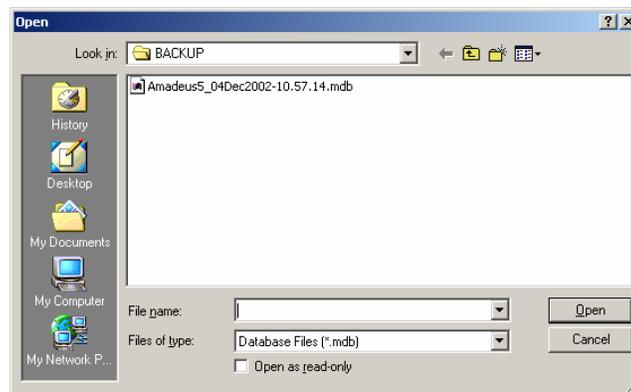
8.4. Restore Database

If necessary, the files saved can be restored.

This action checks if the restored files are valid databases.

To restore a database, select from the list displayed and confirm or cancel operation.

This option is only displayed for super-users. See the multi-company section for further reference.

Fields

File name: enter the file name containing the database

Save as type: select the file type
  ➢ *.mbd - database file - extension given by the system
  ➢ *.* - all files - database from other applications

Open as read only: select if the new database is provided for reference only

Tips & Notes

Destination by default

By default, the files are saved in the following directory: "C:\ProgramFiles\Amadeus5\Backup"

The default destination of the saved file can be modified in the "Tools - Options - Files Location" screen.

Windows Functions

Some Windows functions are available: Up One Level, View Desktop, Create New folder, List and Details.

8.5. Create New Journal

A journal is a database of all the events that have occurred in the system.

The Amadeus 5 application offers the possibility of using simultaneous journals. The application installer has thus a constant access to all site databases. The clean new database becomes the active database.

The information from the existing journal is saved. The system displays the name of the file saved in the message: "Your journal has been saved as backup\journal_xxxxx.mbd"
The extension of all the databases of the system is "mbd".

By default, the files are saved in the following directory: "C:\ProgramFiles\Amadeus5\Backup". The default destination of the file saved can be modified in the "Tools - Options - Files Location" screen.

This option is only displayed for super-users. See the multi-company section for further reference.
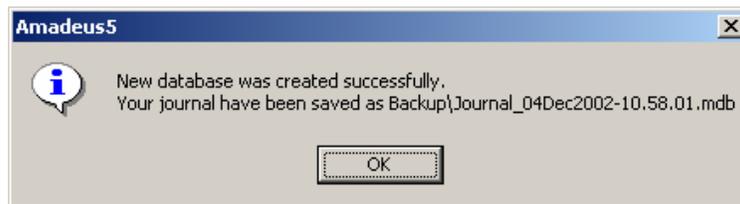
8.6. Save Journal
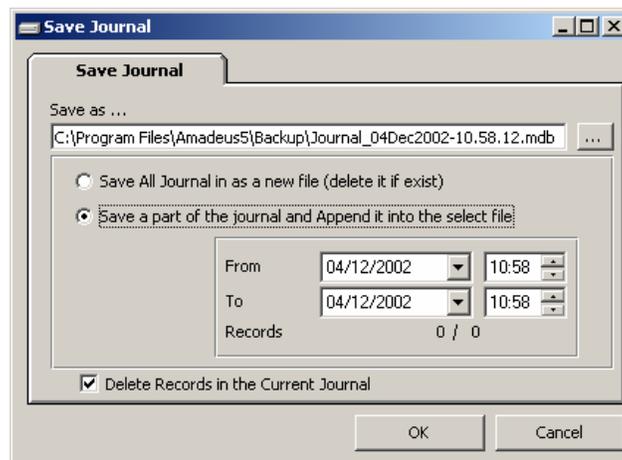
Fields

To save a journal, select from the list displayed and confirm or cancel the operation.

Save as: accept the name suggested or select another file name using the […] button

Choose one of the following options:
- ➢ Save the entire journal in a new file (delete if exists), default option
- ➢ Save part of the journal and append it into the file selected

From: specify start date and hour of journal

To: specify end date and hour of journal

Records: number of recorded records and total records number

Delete records in current journal: default option

Destination by default

By default, the files are saved in the following directory: "C:\ProgramFiles\Amadeus5\Backup".
The default destination of the saved file can be modified in the "Tools - Options - Files Location"
screen.

Windows Functions

Some Windows functions are available: Up One Level, View Desktop, Create New folder, List and
Details.

8.7. Restore Journal

If necessary, the files saved can be restored by select them from the list displayed.

This action checks if the restored files are valid journals.

To restore a journal, select it from the list and confirm the operation.

This option is only displayed for super-users. See the multi-company section for further reference.

Fields

File name: enter the name of the file containing journal information

Save as type: select the file type
  ➢ *.mbd - database file - extension given by the system
  ➢ *.* - all files - database from other applications

Open as read only: select if the new database is provided for reference only

Windows Functions

Some Windows functions are available: Up One Level, View Desktop, Create New folder, List and
Details.

8.8. Creation of a group of badges

This menu allows the creation a group of cards in a single command.

It is accessible via the screens "Parameter - Badge" or "Options - Create a group of badges".

Refer to the chapter "Parameter - Badge" for further information.

8.9. Options

8.9.1. Files Location

Modify the database files location and confirm or cancel your choice. The "Restore the default values" key allows cancelling the modifications.
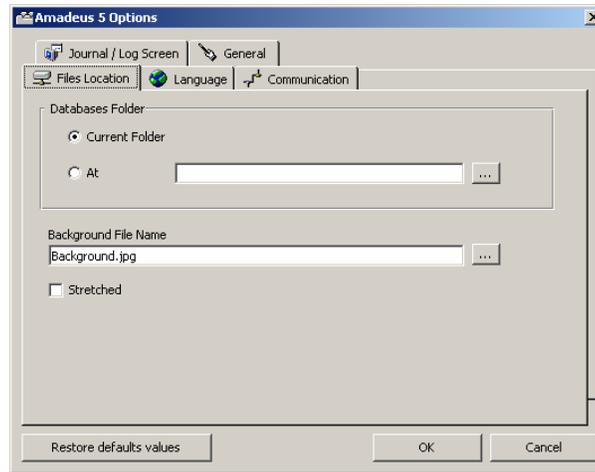
Fields

Database folder
  - ➤ **Current folder**: select current folder or
 - ➤ **At**: indicate the desired database directory

Background file name: select the desired file using the […] button

Stretched: select to stretch the image on the screen; this function is useful to display the background image

8.8.2. Languages

Amadeus 5 supports many languages. Screens and functions are translated instantaneously. Specify the requested language and confirm your choice.
The "Restore Default Values" key allows the modifications cancellation.
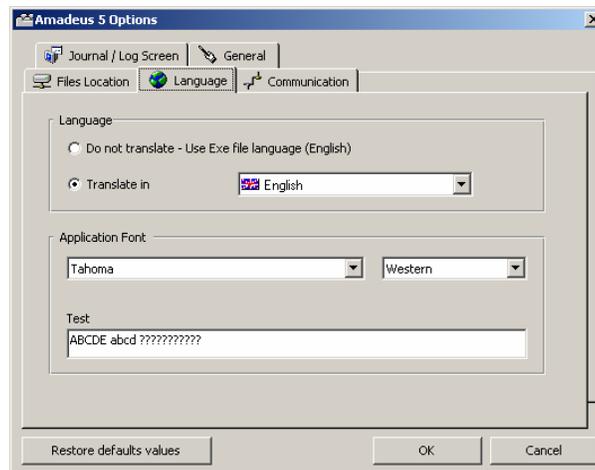
Fields

Do not translate - use Exe file language (English): select to display all the screens and keys in English

Translate in: select this option to modify screens and commands language

Choice of language: select the language desired

Application font: select the font desired

Font according to language: select the font type according to the alphabet used (Chinese, Western, etc.)

Test: display the font selected for visual verification

8.9.3. Communication

In this section, the polling status default values at the start of the application can be entered, as well as the number of time zones and the trial number of sending messages.

Specify parameters, then confirm or cancel your choice.

The "Restore default values" key allows the modifications cancellation.
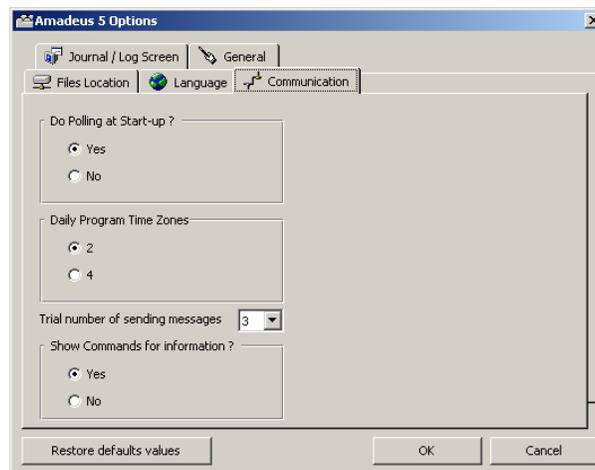
Fields

Do polling at start-up
  ➢ Yes: by default
  ➢ No

Consult also the chapter "Communication - Stop / Resume Polling"

Daily program time zones:
  ➢ 2: default value
  ➢ 4

Consult also the chapter "Parameter - Time Zones - Basic Concepts"

Trial number of sending messages: select the numbers of trials tolerated by the system before reacting; choose between 1 and 10, 3 being the default value

Show command for information: show commands in the log display
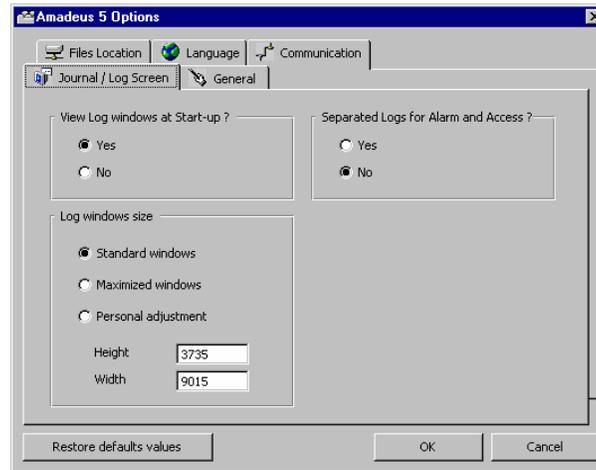 ➢ Yes: by default
  ➢ No

8.9.4. Journal / Log Screen

The Journal and log window give added flexibility to the system.

The log is a temporary linear colour display of events that have occurred in the system. The events are visualized as they take place.

Specify the parameters and confirm or cancel your choice.

The "Restore Default Values" key allows modifications cancellation.

Fields

View log windows at start-up: select "yes" or "no"

Log window size:

Standard window: height: 3735, width: 9015

Maximized window: depends on the screen definition

**Personal adjustment**: specify height and width

Separate logs for alarm and access: select "Yes" in order to dissociate the alarm log from the access log. The software needs to be restarted to implement this option. By default, a single log shows access, alarms and system messages

8.9.5. General

This screen allows the selection by default of the badge technology and the personal tool bar recording.

Specify the parameters and confirm or cancel your choice.

The "Restore Default Values" key allows modifications cancellation.
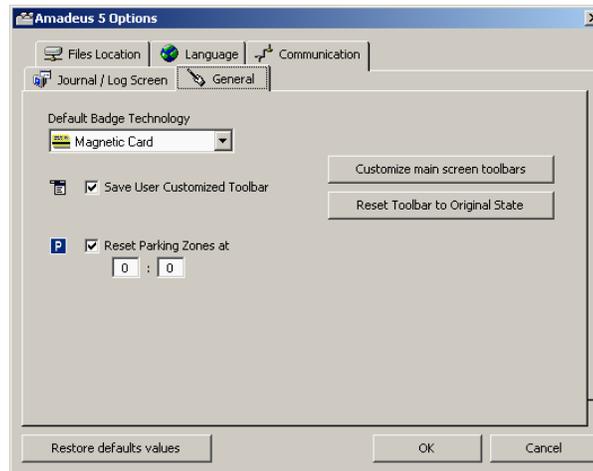
<u>Fields</u>

Default badge technology

Each site works with a main badge technology. The system creates new badges using the technology selected without having to specify the technology used each time.

Save user-customized toolbar

A customized toolbar gives added flexibility to the system.

Select this option to save a toolbar; if this option is not selected, the toolbar will be lost when closing the application.

Customized main screen toolbar
  - ➢ Position the mouse on the original toolbar
  - ➢ Click on the right mouse button
  - ➢ Select "Customized" from the menu displayed
  - ➢ Give the new toolbar a name
  - ➢ Select the appropriate option
  - ➢ Select the toolbar and position the pointer on the area desired

Reset toolbar to original state: delete the personalised toolbars

Reset parking zone

# 9. MENU: HELP

9.1. Amadeus Help Content

The explanation of each screen can be obtained by pressing "F1" at any time or via the "Help - Amadeus Help Content".

The list of topics available appears in the left window.
Click on a book or on any topic and then to "Open".
The right window is automatically updated when a chapter is selected.

The help content can be displayed on the screen or printed.
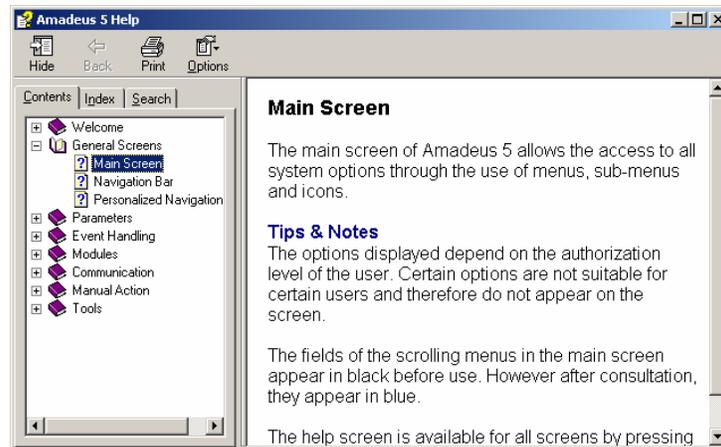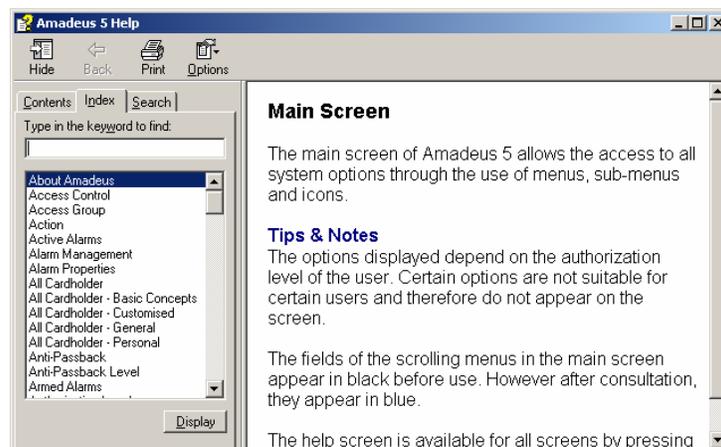
9.2. Amadeus Help Index

The index branches directly to the explanation of specific screens or concepts used in the Amadeus 5 software.
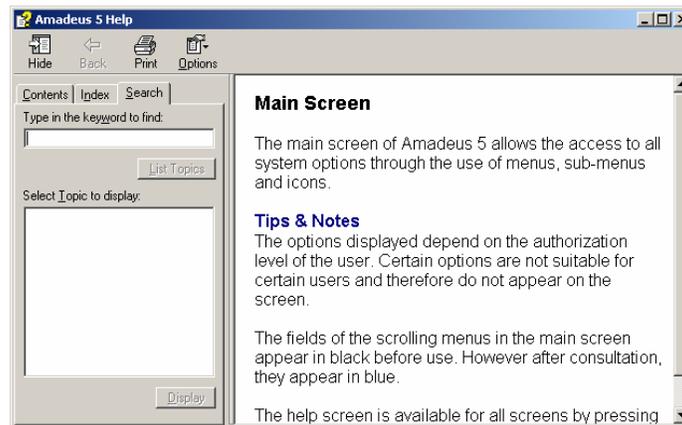
Two ways to use the index:
- ➢ Enter the first letters of the keyword looked at
- ➢ Click on the index data requested and then on the "Display" button

9.3. Amadeus Help Search

This screen enables the search of words or specific expressions in the help of the software; instead of looking for information by category

9.4. Amadeus on the web

Further information is available through the Amadeus 5 Web site.

9.5. About Amadeus

This screen provides the software version, plug and the system information.