



# InVision 32<sup>TM</sup>

*Integrated Alarm Monitoring  
and Access Control*

---

***USER MANUAL***

**new generation  
building security**

# Copyright Notice

---

Copyright © 1995 – 2003 by Camden Door Controls Inc.

All rights reserved Worldwide. Printed in Canada. This publication has been provided pursuant to an agreement containing restrictions on its use. No part of this book may be copied or distributed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written consent of Camden Door Controls Inc., Mississauga, Ontario, Canada.

## ***Trademark***

Invision32™ is the trademark of Camden Door Controls Inc. Windows is a trademark of Microsoft Corporation. All other product names mentioned herein are the property of their respective owners. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## ***Disclaimer***

This book is provided *as is*, without warranty of any kind, either express or implied, including but not limited to performance, merchantability, or fitness for any particular purpose. Neither Camden Door Controls Inc. nor its dealers or distributors shall be liable to any person or entity with respect to any liability, loss, or damage, caused or alleged to have been caused directly or indirectly by this information. Further Camden Door Controls Inc. reserves the right to revise this publication, and to make changes to the content hereof from time to time, without the obligation of Camden Door Controls Inc. to notify any person or organization of such revision or changes.

## **CAMDEN DOOR CONTROLS INC.**

5151 Everest Drive, Unit #6  
Mississauga, Ontario  
CANADA  
L4W 2Z3

Tel: (905) 366-3377  
Fax: (905) 366-3378  
Email: [support@Camden-access.com](mailto:support@Camden-access.com)  
Web: [www.camdencontrols.com](http://www.camdencontrols.com)

Printing Date September 30, 2004

Invision32 Revision 3.2

# Table of Contents

---

<b>ABOUT THIS GUIDE .....</b>	<b>1</b>
BEFORE READING THIS GUIDE.....	1
CONVENTIONS IN THIS GUIDE .....	1
<b>CHAPTER 1 INTRODUCING INVISON32™ .....</b>	<b>2</b>
INVISON32 SERVER CLIENT NETWORK SETUP .....	2
<b>CHAPTER 2 GETTING TO KNOW INVISON32™ .....</b>	<b>3</b>
COMMAND BAR.....	3
<i>Menu Options</i> .....	4
<i>Toolbar Buttons</i> .....	5
DATABASE SCREEN .....	6
MONITOR SCREEN .....	7
ALARM SCREEN.....	8
LOG SCREEN.....	8
<b>CHAPTER 3 MONITOR SCREEN.....</b>	<b>10</b>
SYSTEM STATUS.....	10
HOW TO EXECUTE A COMMAND.....	10
<i>Command Type</i> .....	11
ACCESS POINTS COMMANDS .....	11
<i>Commands</i> .....	12
INPUT POINTS COMMANDS .....	13
<i>Commands</i> .....	13
OUTPUT POINTS COMMANDS.....	13
<i>Commands</i> .....	14
PANELS COMMANDS.....	14
<i>Commands</i> .....	14
AREA AND CARDHOLDER COMMANDS .....	15
<i>Commands</i> .....	16
<b>CHAPTER 4 ALARM SCREEN .....</b>	<b>17</b>
ACKNOWLEDGE/UNACKNOWLEDGE/CLEAR.....	17
ALARM DETAILS .....	17
<b>CHAPTER 5 PROGRAMMING .....</b>	<b>19</b>
INVISON32 DATABASE .....	19
<i>Users</i> .....	19
<i>Holidays</i> .....	20
<i>Schedule</i> .....	20
<i>Areas</i> .....	21
<i>Messages</i> .....	22
<i>Networks</i> .....	22
<i>Panels</i> .....	24
<i>Access Points</i> .....	27
<i>Inputs</i> .....	35
<i>Outputs</i> .....	38
<i>Access Levels</i> .....	40
<b>CHAPTER 6 CARDHOLDERS.....</b>	<b>41</b>
FIELDS AND OPTIONS .....	41
TEMPLATES .....	43

CARDHOLDERS TABS.....	44
<i>Cards</i> .....	44
<i>Profile Tab</i> .....	45
<i>Photo Tab</i> .....	45
<i>Notes Tab</i> .....	46
<i>More Fields Tab</i> .....	46
<b>CHAPTER 7 REPORTS.....</b>	<b>48</b>
HISTORY REPORTS .....	48
<i>File</i> .....	48
<i>Reports</i> .....	49
<i>Preview</i> .....	49
<i>DVR</i> .....	50
DATABASE REPORT .....	51
<i>Options</i> .....	51
<b>CHAPTER 8 OPTIONS.....</b>	<b>53</b>
SYSTEM OPTIONS .....	53
<i>General</i> .....	53
<i>Badge</i> .....	54
SYSTEM MESSAGES .....	55
ACCESS POINT ACTIVITY .....	56
<i>More/Less</i> .....	56
<i>Hide</i> .....	56
<b>CHAPTER 9 LINKS .....</b>	<b>57</b>
GLOBAL LINKS .....	57
<b>CHAPTER 10 TOOLS.....</b>	<b>58</b>
BACKUP.....	58
RUN BACKUP NOW.....	58
CONFIGURE AUTO-BACKUP .....	59
RESTORE .....	60
<b>CHAPTER 11 PROGRAM GROUPS.....</b>	<b>61</b>
INVISION32™ SECURITY SYSTEM.....	61
<i>Invision32™ Security System</i> .....	61
<i>Invision32™ Data Restore</i> .....	61
<i>Invision32™ Database Maintenance</i> .....	61
<i>Invision32™ Firmware Upgrade</i> .....	62
<b>GLOSSARY .....</b>	<b>65</b>
<b>LICENSE &amp; WARRANTY .....</b>	<b>66</b>
<b>READER COMMENTS .....</b>	<b>67</b>

# About This Guide

---

This guide documents how to install and use the Invision32™ Security Management System as developed by Camden Door Controls Inc. The **Invision32™** system represents the latest in access control technology specifically designed for the smaller application. Its intuitive graphical interface allows users to take advantage of the power of the **Invision32™** with a minimal amount of training.

Read this guide if you are:

- ◆ An operator who monitors security and access using Invision32™.
- ◆ A system administrator who updates Invision32™'s database.
- ◆ The system technician that installs and configures the Invision32™ onsite.

## Before reading this guide

This guide assumes that you:

- ◆ Are familiar and comfortable with a personal computer.
- ◆ Know how to use a mouse.
- ◆ Are familiar with the Windows operating environment.

## Conventions in this guide

Menu options, window titles, fields, and buttons are indicated by *italic typeface*. For example, “choose *Access Point Activity* from the *Option* menu” or “click *Cancel* to cancel your changes”.

Keyboard actions and function keys are denoted by **bold typeface**. For example, “press **F1** to display online help”.

Keyboard control sequences (i.e., using two or more keyboard keys in combination), are denoted by keys in **bold typeface** separated by a plus sign (+). For example, “press **Ctrl + Alt + Delete** to reboot the system”.

# Chapter 1

## Introducing Invision32™

---

The Invision32™ system Integrated Access Control, Photo-badging, Digital Video Recording and Alarm Monitoring into an elegant building management and security system specifically designed for the smaller application

Invision32™'s 32-bit software architecture together with Windows 95<sup>1</sup>, 98<sup>2</sup>, 2000<sup>3</sup>, XP, NT 4.0<sup>4</sup>, or ME operating system ensures that security management needs are met easily and economically with a minimal amount of training.

The new IRC-2000-2 Intelligent Field Panels utilize flash firmware for easy upgrades. The panel uses fully distributed intelligence for off-line operations. In addition to supporting two card readers, each IRC-2000-2 Intelligent Field Panel also has eight fully supervised alarm inputs along with eight outputs.

## Invision32 Server Client Network Setup

Please see technical document TB23 for step-by-step guide of Invision32 Install.

1. When Installing the Server software on to your PC ensure that the Network User you are logged on as, has Administrator Rights to DCOM Configuration on this PC. If the rights to DCOM Configuration are restricted the auto install will be unable to configure the DCOM settings, which are required to allow client PC's to access this server.
2. Once the Server software has been installed successfully the C:\Program Files\RBH\Integra32 folder will have to be shared to allow client PC's to connect and register to the Server database. This folder must be shared to allow Full Access to either 'Everyone' or at least full access to all users, which will be using Invision32 client software from their PC's.

---

<sup>1</sup> Must have Internet Explorer 4.0 or greater installed.

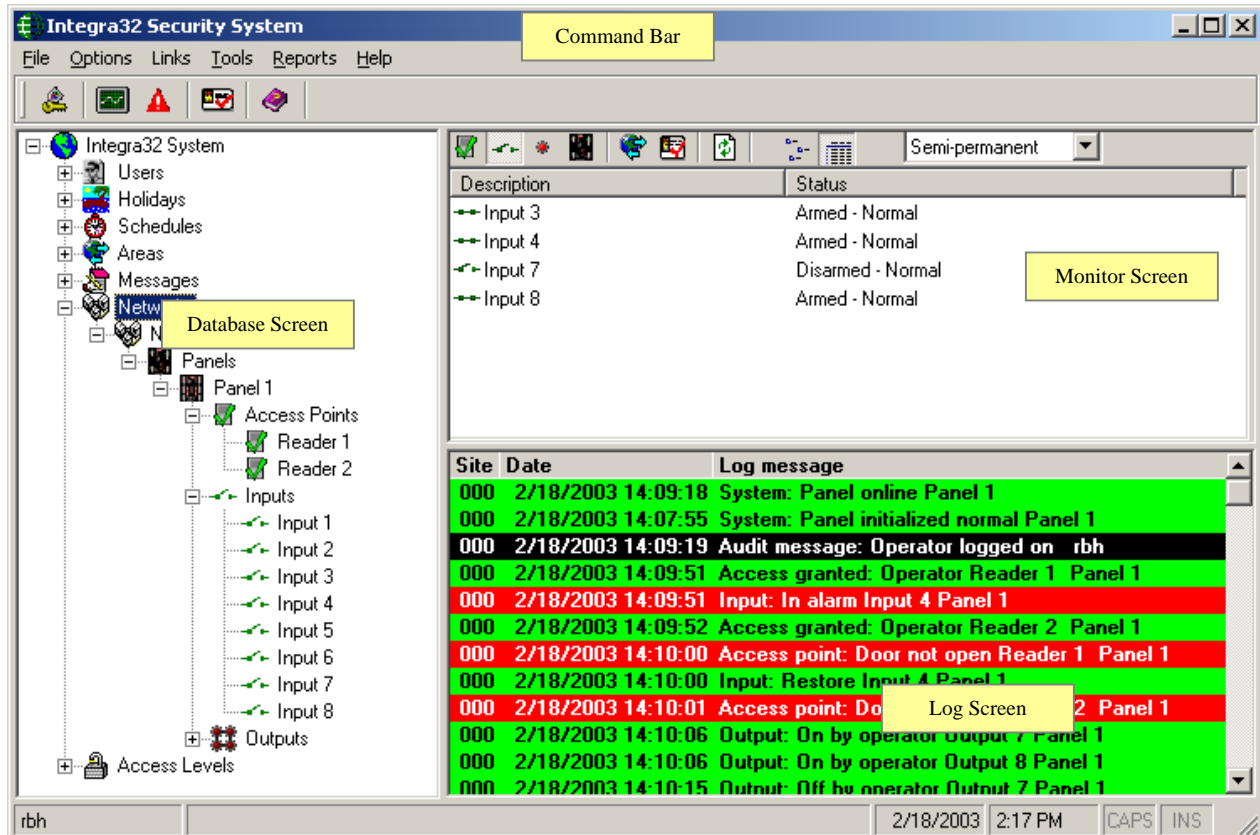
<sup>2</sup> Second Edition is recommended.

<sup>3</sup> Must have at least service pack 2 installed.

<sup>4</sup> Must have at least service pack 6 installed.

# Chapter 2 Getting to Know Invision32™

Invision32™ lets you manage and monitor all your security access needs using a standard PC. There are four separate parts to the Invision32™'s main screen:



## Command Bar

Menus and buttons to access other features of the system are available on the *Command Bar*. Invision32™ has the following menu options:



Each of these items has a drop down menu with further options that "launch" the functions contained in the drop down menu (e.g., *Log Out of the Invision32™ system*). In addition, Invision32™ provides Toolbar buttons as an optional means of launching either the same function contained in drop down menu or to launch new windows (e.g., *Cardholder window*).

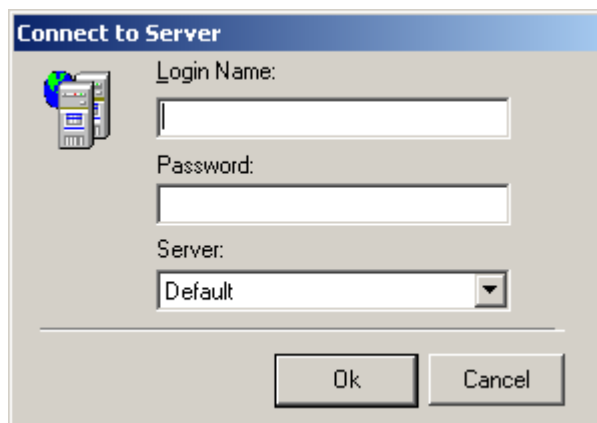
## Menu Options

### File

Use this menu to log in/log out or to exit the Invision32™ application.

#### ***Log In & Out (Ctrl+L)***

An operator must be logged in to operate the system. This ensures that all actions performed on the PC can be attributed to a particular operator.



To log in, enter your full login Name and password. The default login name is "RBH" and default password is "password". Both "Login Name" and "Password" are not case sensitive.

An operator should log out when leaving the computer unattended or when finished his/her shift. Logging out protects the system against unauthorized access.

#### ***Exit***

*Exit* will shutdown the Invision32™ System.

### Options

Use this menu option to customize user preference (*through system option window*) or customize system messages displayed on the *Monitor Screen* and in *History*. The Access Point Activity window is also enabled here. Details of this option will be discussed in Chapter 8.

### Links

This is where Global Links are setup; detail on this is done in Chapter 9.

### Tools

The *Tools* menu gives the option for *Backup*, which will be covered in more detail in Chapter 10.



## Reports

Use this menu option to customize and generate *History Reports* and *Database Reports*.

### ***History Reports (Ctrl+H)***

Reports are explained later in Chapter 7.

### ***Database Reports***

Reports are explained later in Chapter 7.

## Help

Use this menu option to display information regarding your Invision32™ software version.



## Toolbar Buttons



### ***Login/Logout***

Press this button to log in/ log out of Invision32™ system.



### ***System Status***

Press this button to change the *Command Screen*, displaying the status toolbars of access points, inputs, outputs and panels.



### ***Alarms***

Press this button to change the *Command Screen* displaying alarm messages, time and date of alarm and operator ID.



### ***Cardholders***

Press this button to launch Invision32™'s cardholder window to program new cards or edit existing cards.

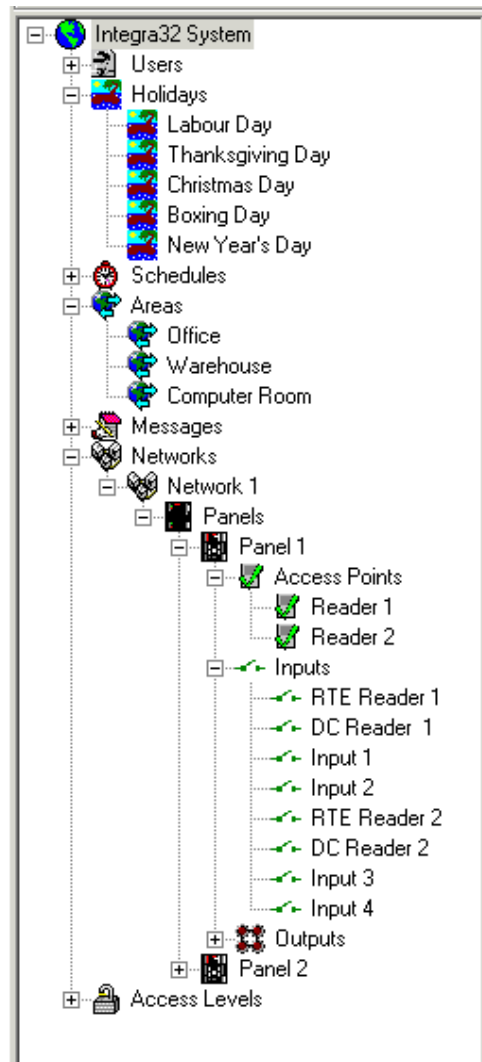


### ***Help***

Press this button to get online help.

## **Database Screen**

The system is configured for a particular installation from this screen. Setup and programming of hardware devices (*IRC-2000-2*), and programming of all records such as cardholder, access levels, schedules and holidays are done here.



Up to sixteen networks can be configured on each system, and up to sixteen panels can be configured for the Invision32™ system. These panels can all be configured for the same network or distributed across up to sixteen networks. A maximum of fourteen schedules, each with up to eight time zones, can be added to the existing schedules (*Never and Always*). The system is capable of handling up to forty holidays and one hundred messages.

## Monitor Screen

This screen gives the operator control of the system through *System Status (Access points, Input Points, Output points)*. It allows viewing of the *System Status* in List View or Report View.

Description	Status
Reader 1	Unlocked - Normal
Reader 2	Locked - Normal
Reader 3	Locked - DHO Warning
Reader 4	Locked - Normal
Reader 5	Locked - Normal
Reader 6	Locked - Normal

Status for items shown is in real time. Items are updated as events change keeping the operator up to date.

## Alarm Screen

This screen appears in the same pane in place of the *Monitor Screen*. From here alarms are acknowledged and cleared.

Site	Date	Alarm message	Operator
001	05/10/2001 09:18:44	Access Point: Forced entry alarm Employee Entrance	

Instruction messages can be obtained from the *Details* of the alarm, and actions taken can be noted there as well.

## Log Screen

This screen displays all system activity such as cardholder movement, inputs, and outputs. All system messages are also displayed here.

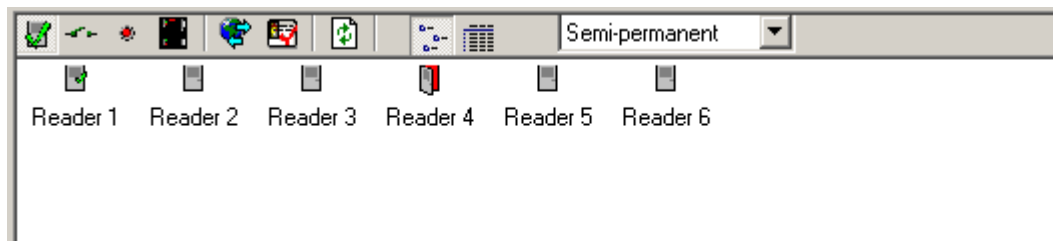
Site	Date	Log message
000	04/06/02 15:30:40	Access granted: Card Jim Turnbull (2497) Reader 3 Panel 2
000	04/06/02 15:30:49	Access granted: RTE Reader 1 Panel 1
000	04/06/02 15:30:58	Access granted: Card Jim Turnbull (2497) Reader 4 Panel 2
000	04/06/02 15:31:04	Access granted: Card David Mayes (2500) Reader 3 Panel 2
000	04/06/02 15:31:09	Access granted: Card David Mayes (2500) Reader 2 Panel 1
000	04/06/02 15:31:13	Access granted: RTE Reader 4 Panel 2
000	04/06/02 15:31:18	Access denied: APB violation Kanty Riarh (2698) Reader 4 Panel 2
000	04/06/02 15:31:25	Access granted: Card David Mayes (2500) Reader 3 Panel 2
000	04/06/02 15:32:07	Access granted: Card David Mayes (2500) Reader 2 Panel 1
000	04/06/02 15:32:14	Access granted: Card Jim Turnbull (2497) Reader 2 Panel 1
000	04/06/02 15:32:19	Access granted: Card Ken Mahoney (2498) Reader 2 Panel 1
000	04/06/02 15:32:22	Access granted: Card Kanty Riarh (2698) Reader 2 Panel 1
000	04/06/02 15:32:30	Access granted: RTE Reader 3 Panel 2
000	04/06/02 15:32:50	Access point: Door held open warning Reader 3 Panel 2

All the messages shown here are also saved to *History* and can be retrieved through *History Reports*.

## Chapter 3 Monitor Screen

---

From the *Monitor Screen* or the *System Status Window* the operator can issue commands to control various devices in the system, as well as view their status.



### System Status

Clicking on the *System Status* button on the toolbar of the main screen will change the *Alarm Screen* to the *Monitor Screen* or the *System Status Window*. From the *System Status Window* the operator can lock and unlock doors, arm and disarm inputs, and switch on and off outputs. The status is displayed in real time, but only for those devices that have reporting enabled. The operator can turn messages off for certain events and no history will be logged for those events, but the status of devices will not be affected.

The first six buttons will bring up Access Points, Inputs, Outputs, Panels, Areas, and Cardholders respectively. The status of the selected item can be shown either in *List View* or *Report View*. Button seven is used to update/verify the status of the items shown.

### How to Execute a Command

All operator commands are executed in the same manner.

1. Click on the appropriate button on the *System Status Window* toolbar to load the desired devices.
2. From the list of items (*Input, Output, or Access Point etc.*), select the item(s) you want to control. Clicking on the first item, then holding down the Shift key and clicking on the last item in the range can choose a group of items. Select non-sequential item groups by holding down the **Ctrl** key and clicking on each desired item.
3. Set the command type to permanent, semi-permanent or timed.
4. Right click on the Item(s) highlighted and then choose a command from the list provided.

The command is then immediately sent to the appropriate IRC-2000-2 controller(s) for execution.

## Command Type

From the drop down menu select one of the three options available for command type.

### Permanent

Permanent commands are used to perform actions and to manually override system operation. When the status of an input, output or access point is changed by a permanent command, the scheduler no longer controls the device. For example, if a door is normally armed from 6 p.m. to 8 am by the scheduler and a permanent command is issued to arm the door, the door will remain armed forever and will not be disarmed by the scheduler.

A permanent command remains in effect until cleared by a second operator command or fresh files are downloaded to the controller.

### Semi-Permanent

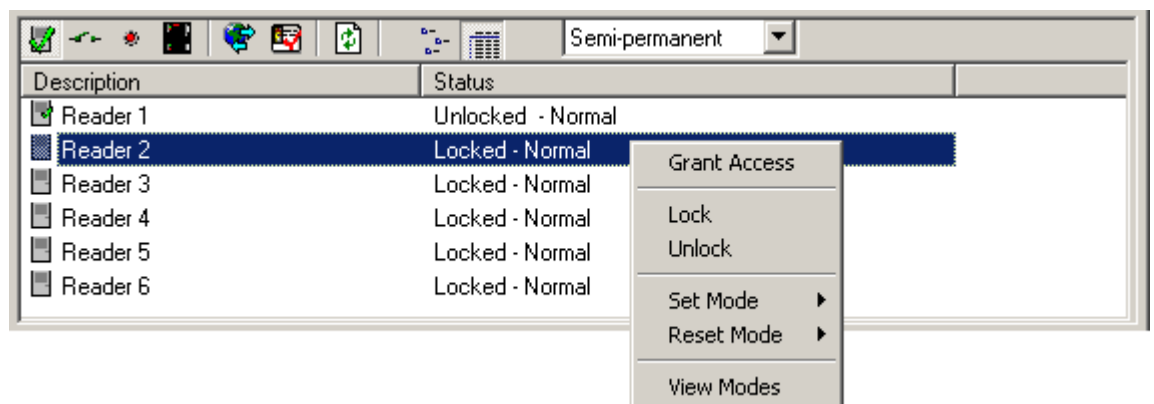
Semi permanent commands are executed like permanent commands but do not override operation of the scheduler. In the above example of the door armed by scheduler between 6pm and 8am, if a semi permanent command is issued at 4 p.m. to arm the door, the command is executed. The scheduled operation remains unaffected and on the next day at 8:00 am the door will disarm and revert to the normal arming schedule.

### Timed

Timed commands allow an action to be performed for a specified duration. For example, turn on an output for 5 minutes. The time can be specified from 1 to 127, seconds or minutes.

## Access Points Commands

Clicking the Access Points button on the *Command Toolbar* depicts the status of Access points on the *Monitor Screen*.



The following commands for Access points are available by right clicking the selected Access points.

## Commands

### Grant Access

Unlock the access point for the duration of the access point *Unlock Time*. This command has the same effect on an access point as presenting a valid card.

### Lock

Lock an access point or access point group on a permanent, semi-permanent or timed basis.

### Unlock

Unlock an access point or access point group on a permanent, semi-permanent or timed basis.

### Set Mode

The access point has several operating modes that are normally controlled by the scheduler. The operator can override the scheduler and manually control these modes.

### Reset Mode

Reset Mode button is used to turn off the option turned on in Set mode.

### High Security

In High Security mode, only cards with high security privileges, may gain access at this access point.

### APB Enabled

Antipassback is an access control feature that prevents cardholders' misuse, by putting certain restrictions on the use of their cards. When the Antipassback feature is enabled, cardholders must present their card for entry to and exit from all areas. Antipassback prevents a cardholder from using his/her card twice at the same access point.

### Facility Code

Use this option to turn on/off the Facility Code mode, when the system checks only the Facility Code portion of the card code. All cards with valid Facility Codes will be granted access. This feature is typically used when the system is being configured for the first time and the cardholder information is not entered in the database.

### Interlock

With this feature enabled a door will not be unlocked if the other door is opened. The open door must be closed before the other door will grant access.

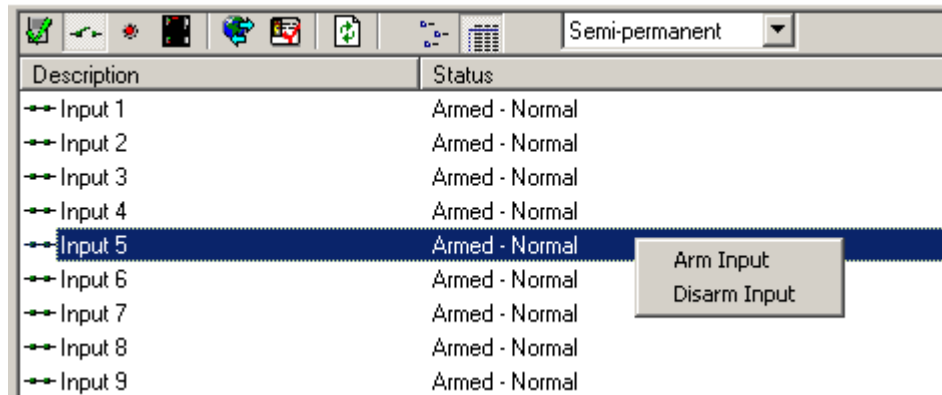
### View Mode

Select this option to view all the modes available and their status.



## Input Points Commands

Clicking the *Input Points* button on the *Command Toolbar* depicts the status of input points on the *Monitor Screen*.



The following commands for Input points are available by right clicking the selected Input points.

### Commands

#### Arm Input

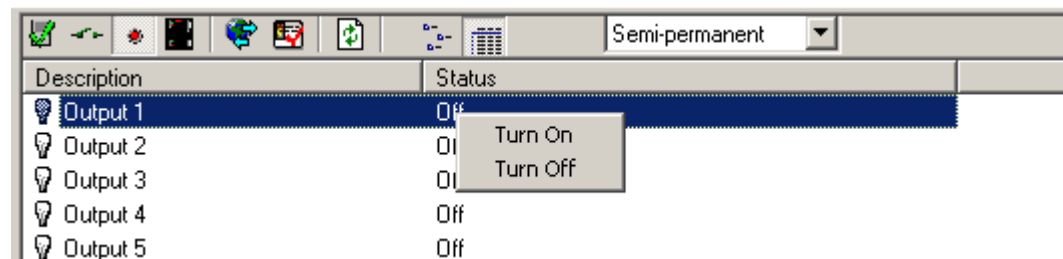
Arm the input. When an input is armed, an alarm is generated if the input is violated. In the case of a door, opening an armed door generates an alarm.

#### Disarm Input

Disarm an input. While an input is disarmed, no alarm is generated when the input is violated. In the case of a door, opening the door while disarmed does not generate an alarm. The system however will still generate and log a “door opened” event and report it to the *Log Screen*.

## Output Points Commands

Clicking the *Output Points* button on the *Command Toolbar* depicts the status of output points on the *Monitor Screen*.



The following commands for output points are available by right clicking the selected *Output Points*.

## Commands

### Turn On

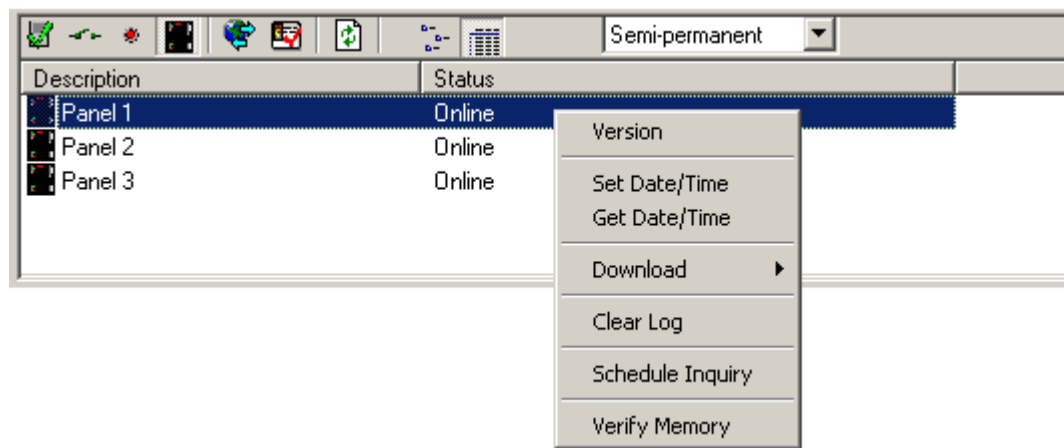
Turn on an output.

### Turn Off

Turn off an output.

## Panels Commands

Clicking the *Panels* button on the *Command Toolbar* depicts the status of panels on the *Monitor Screen*.



The following commands for panels are available by right clicking the selected panels.

## Commands

### Version

The *Version* queries all or selected IRC-2000-2 for the firmware version they are running. The version number will be displayed on the *Log Screen*.

### Set Date/Time

Click on the *Set Date/Time* to launch the *Set Panel Date/Time Screen*.

- The *Get Local* button is used to retrieve the current date and time settings from the PC's internal clock.
- The *Set* button is used to upload the selected *Date/Time* settings to the selected IRC-2000-2 controller(s).
- The *Close* button is used to close the *Set Panel Date/Time Window*.

## Get Date/Time

This command queries the controller for its current date and time, and displays it on the *Log Screen*.

## Download

The *Download* function allows the operator to manually repopulate the IRC-2000-2 memory from the database on the server. Select any of the listed files to download or select the *All Files* option to download all files.

Download messages are posted to the log as files are sent, verifying the number of records sent in each file. Card records are sent individually and will indicate the card number, and whether it was added or deleted. (*Edited cards are displayed as added.*)

- If the panel is offline at the time of the download the files that failed to download will be logged on the *Log Screen*. When the panel comes back on line the download will be executed then, again logging the files that are downloaded.

## Clear Log

The *Clear Log* option clears the event log of all or selected controllers. The database portion of memory is untouched. The results will be displayed on the *Log Screen*.

## Schedule Inquiry

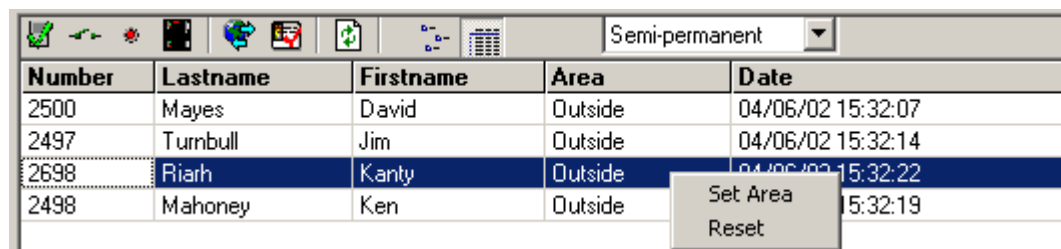
This query is used to find out the current state of the time schedules. It will list on the *Log Screen* which schedules are on and which is off.

## Verify Memory

This command will check the files in the panel and compare them to those in the database. The files verification will be displayed on the *Log Screen*.

## Area and Cardholder Commands

Clicking either the *Areas* or the *Cardholders* button will bring up a selection window. From the *Areas* selection window you can choose the area or areas you wish to view. The *Cardholders* selection window allows you to choose from the list of cardholders. The display will show a list of cardholders based on your selections. You will see the area the cardholder is logged into and the date/time they were logged into that area.



Number	Lastname	Firstname	Area	Date
2500	Mayes	David	Outside	04/06/02 15:32:07
2497	Turnbull	Jim	Outside	04/06/02 15:32:14
2698	Riarh	Kanty	Outside	04/06/02 15:32:22
2498	Mahoney	Ken	Outside	15:32:19

Semi-permanent ▼

Set Area  
 Reset

The following commands for areas are available by right clicking the selected cardholder.

## *Commands*

### **Set Area**

Set Area is used to change the area that a cardholder is logged into. This may be necessary if a cardholder get into an area without reading into that area.

### **Reset**

The Reset command will clear the area the cardholder is in. The cardholder will not be logged into any area; therefore the next card read cannot violate Antipassback.

## Chapter 4

# Alarm Screen

---

The *Alarms Screen* displays alarm events and pops up automatically when the *Alarms* option is turned on in the toolbar of the main screen.

Site	Date	Alarm message	Operator
001	05/10/2001 11:20:21	Access Point: Forced entry alarm Main Entrance	
001	05/10/2001 11:20:32	Access Point: Forced entry alarm Employee Entrance	rbh

### Acknowledge/Unacknowledged/Clear

Right clicking the alarm event on the *Alarm Screen* gives the option to acknowledge the Alarm. Right clicking on an Acknowledged Alarm gives the options to either unacknowledged or clear the alarm. Once an alarm is acknowledged only the operator that acknowledged that alarm could clear it.

A maximum of one hundred and fifty alarms can be held in the alarm buffer. Any alarms received when the buffer is full are logged to history but do not get sent to the *Alarm Screen*.

### Alarm Details

The user can see the details of an alarm event in *Alarm Details Window* by double clicking the alarm event in the *Alarm Screen*.

#### Date

This box shows the date and time that the alarm occurred.

#### Age

The age of an alarm is the number of seconds since the alarm happened.

#### Status

Status shows whether the alarm has been acknowledged.

#### Alarm

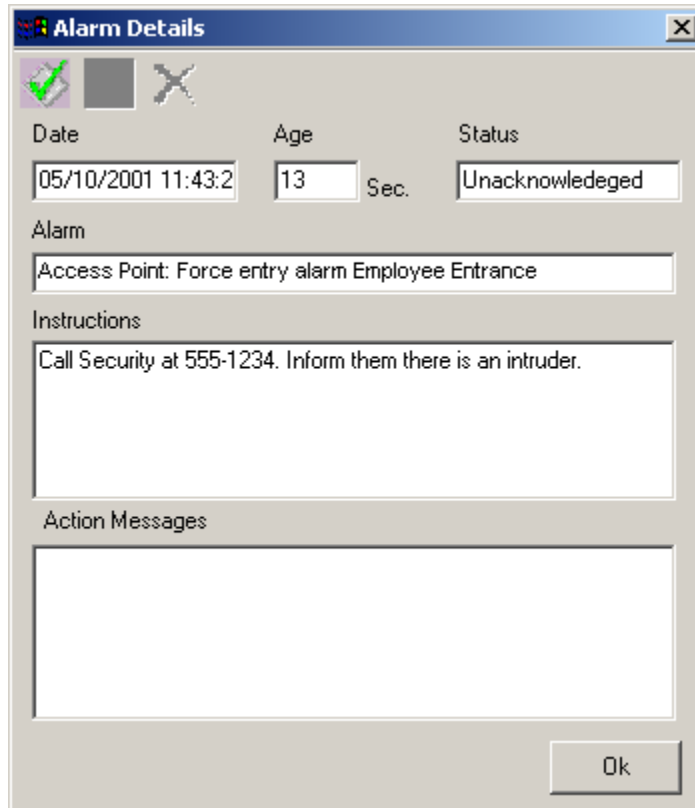
Alarm provides a description of the alarm.

## Instructions

This box will display instruction messages assigned to the alarm.

## Action Messages

The operators can enter their own message into this box indicating what action was taken because of this alarm.



The screenshot shows a window titled "Alarm Details" with a close button (X) in the top right corner. Below the title bar are three icons: a green checkmark, a grey square, and a grey X. The window contains several fields:

Date	Age	Status
05/10/2001 11:43:2	13 Sec.	Unacknowledged

Below these fields are three text boxes:

- Alarm:** Access Point: Force entry alarm Employee Entrance
- Instructions:** Call Security at 555-1234. Inform them there is an intruder.
- Action Messages:** (Empty text box)

An "Ok" button is located at the bottom right of the window.

## Acknowledge



Acknowledge the alarm by clicking the *Acknowledge* button in the *Alarm Details Window*.

## Unacknowledged



Unacknowledged the alarm by clicking the *Unacknowledged* button in the *Alarm Details Window*.

## Clear



Clear the alarm by clicking the *Clear* button in the *Alarm Details Window*.

## Chapter 5 Programming

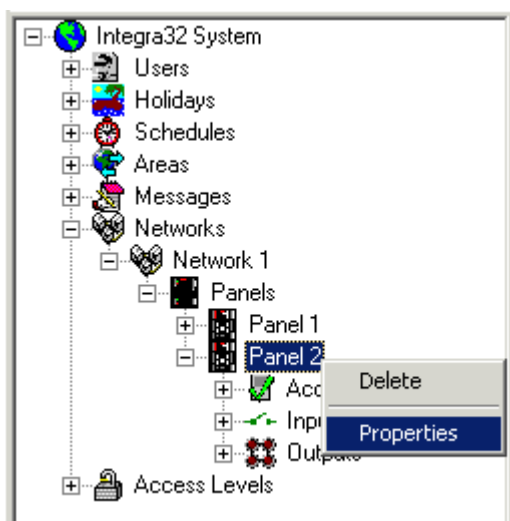
---

Click on the + sign to expand the tree view of your Invision32™ system in the *Database Screen*. Click on the – sign to compress it. Double clicking the description will either expand or compress the view depending on the sign associated with the text. Items that do not have a sign (+ or –) associated with them will take you to their properties when they are double clicked.

Right clicking the description brings up a small menu selection. From these menus you can add, delete, or go to properties for the selected item. Right clicking the access point, the input, or the output will not bring up a menu (*there are no options to select*), but will expand the tree view instead.

### Invision32 Database

The User/Operator can configure the Invision32™ system in the *Database Screen*.



### Users

#### General

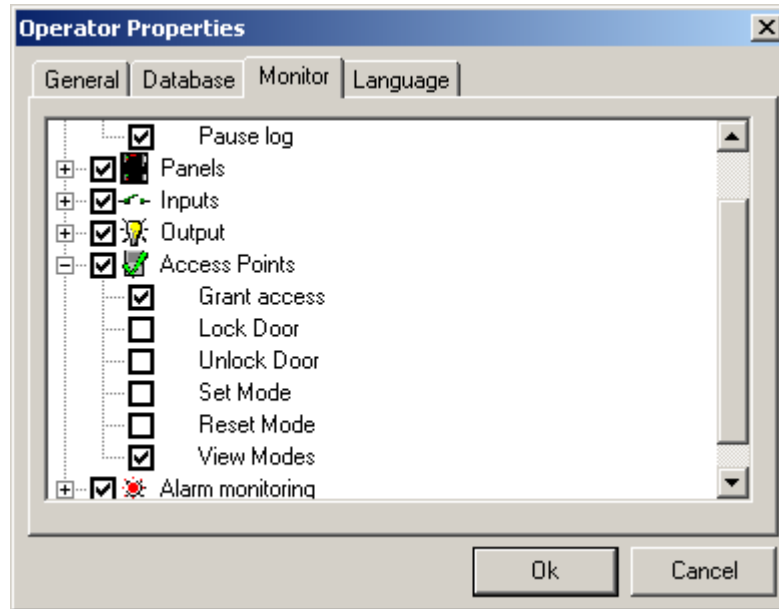
Name, user Id and password can be changed/entered in the *General* tab. of *Operator Properties Window*

#### Database

The access to database can be defined/changed in the *Database* tab. Access to each module of the database can be chosen as 'No Access', 'Read Only', or 'Read & Write'.

## Monitor

Access to commands used in the *Monitor Screen* and the *Alarm Screen* can be defined/changed in the *Monitor* tab. Check commands that the user is to have access to and uncheck commands that he/she is not to have access to.



## Language

The language the system will operate in, for this operator, is selected in the *Language* tab.

## Holidays

Up to forty holidays can be assigned.

You can edit/create the name of a holiday and the date of a holiday in the *Holiday Properties*. Then you can *Select A Date* for the holiday. Holidays replace the day of the week for the day specified. (E.g. *Good Friday 13 April, 2001 as far as schedules are concerned this day will not be a Friday it will be H1.*)

## Schedule

Before cardholders are entered, any additional *Time Groups* that are required should be programmed. Up to 32 schedules can be programmed for Invision32 system.

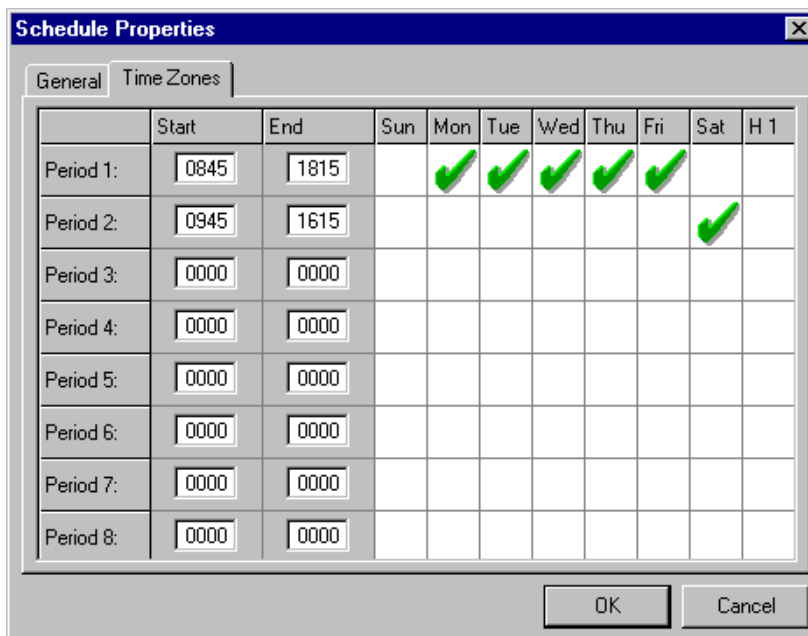
## General

Change the *Description* of the Schedule under the *General* tab of the *Schedule Properties Window*.

## Time Zones

Program the *Time Zones* for the *New Schedule* in the *Time Zones* tab of the *Schedule Properties Window*.

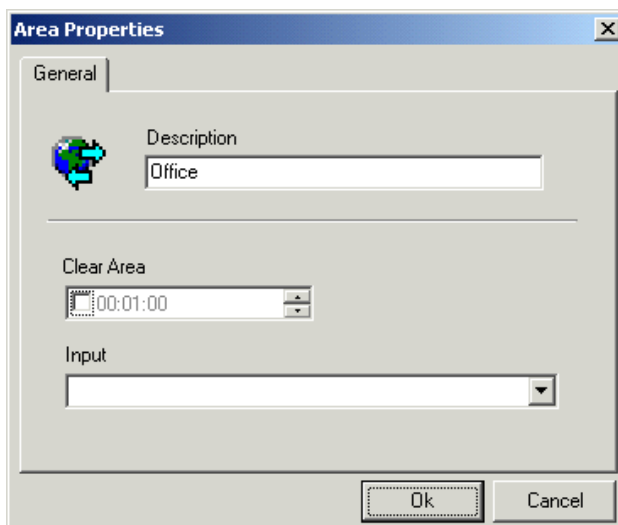




- Eight time periods can be programmed.
  - Click to check or uncheck a day for the period.
  - End time must be later than start time.
  - Valid times are from 00:00 to 24:00, (even though 24:00 is never actually reached [it represents the end of the day]).
    - Schedules that cross, midnight will require two periods. One to go up to 24:00 on the first day, and a second to start at 00:00 of the next day.

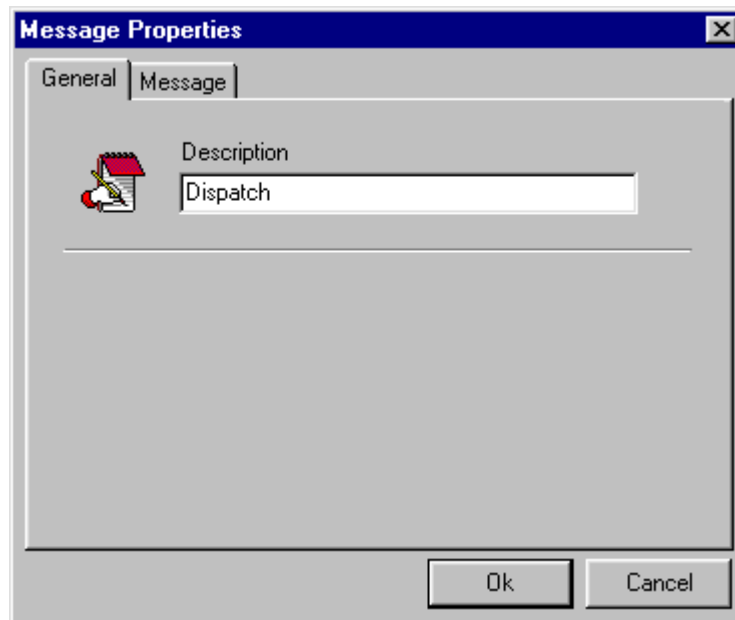
## Areas

In the *Area Properties window* the name of the area is entered. Access points from which a cardholder can enter or exit the area define the actual area. A 'Clear Area' time can also be entered here. As well an input (*general purpose*) can be chosen, to print out a report of all the cardholders in the area, when the input goes into alarm.



## Messages

Messages/Instruction that operators need to follow under certain circumstances can be created and saved here.



### General

Under the *General* tab of the *Message Properties Window* message descriptions can be edited.

### Message

The message is entered under the *Message* tab.

## Networks

Up to sixteen networks can be connected on the Invision32™ system. The description of each *Network* can be changed in the *Description* box under the *General* tab of the *Network Properties Window* for each network. Under the *Comms* tab, properties of the port are configured. Choose one of the four options available for *Port Type*.

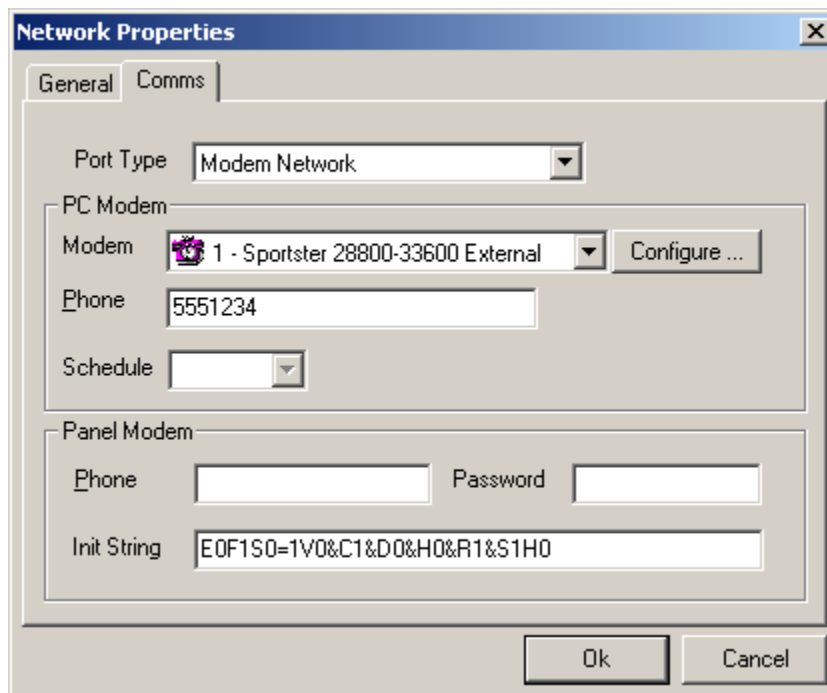
### Connection Type

#### *Direct Connect*

The controller network (*IRC-2000-2*) is connected directly to the PC serial port via a RS232 or a RS485 cable.

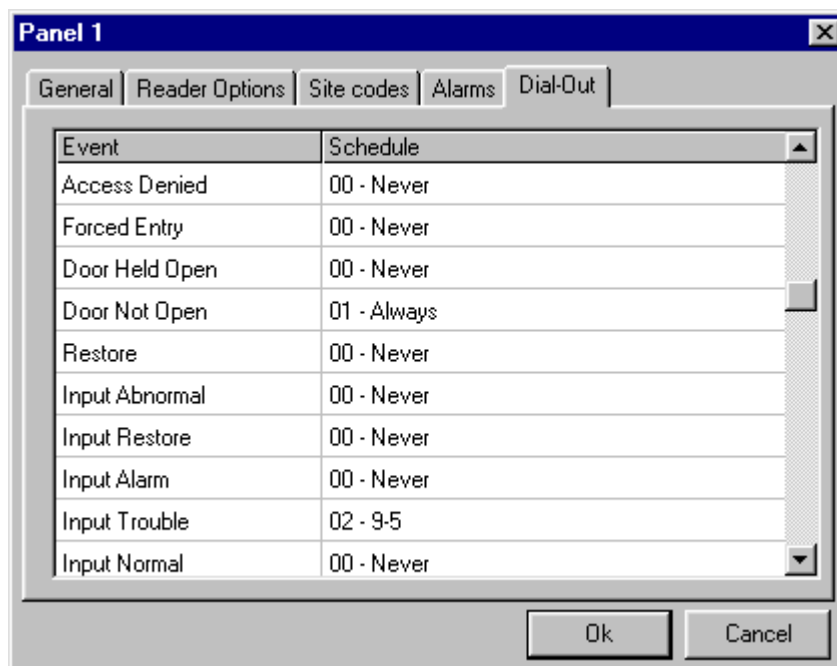
#### *Modem Connect*

The controller network (*IRC-2000-2*) is located remotely and is connected to the PC via dial up modems.



Select a modem and configure it in the *Control Panel* to a maximum baud rate equal to that set at the panel (e.g. 9600). Enter the phone number for the network (to be called by the PC) and the call back phone number (for the panel to call).

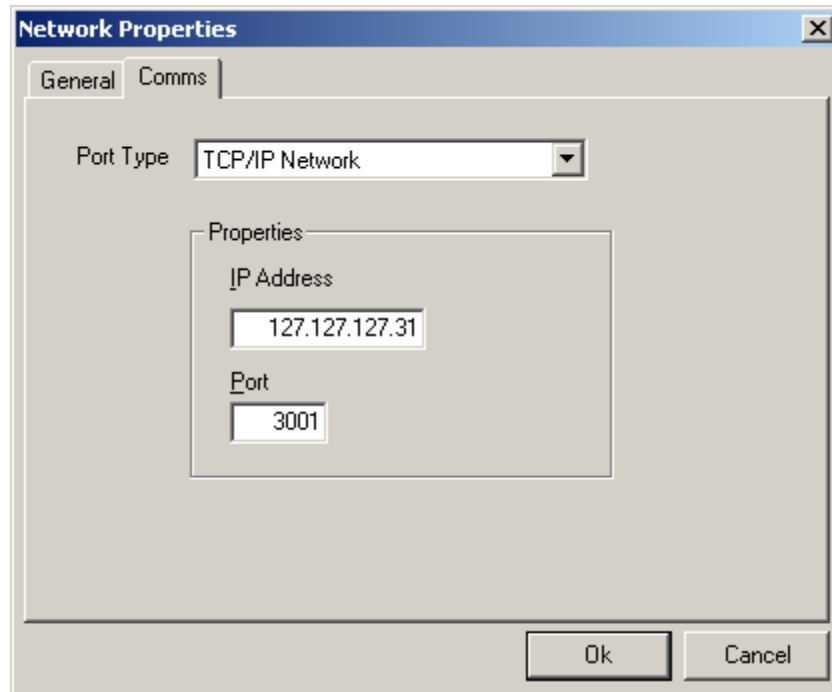
The call back criteria are set under the *Dial-out* tab of each panel. Which events will cause the panel to call up the PC can only be set in the panels of a modem network.



To reset the password, connect the panel directly to the Invision32™ system and execute a full download to the panel.

### ***Ethernet Connect***

The controller network (IRC-2000-2) is connected to the PC through a standard Ethernet network.



For an Ethernet connection to work **TCP** must be installed on your computer.

Enter the specific address and proper port value for the Ethernet interface assigned to the network. (*Enter a port value of which must match programming of Interface*)

## ***Panels***

Up to sixteen panels in total can be connected to the Invision32™ system.

### **General**

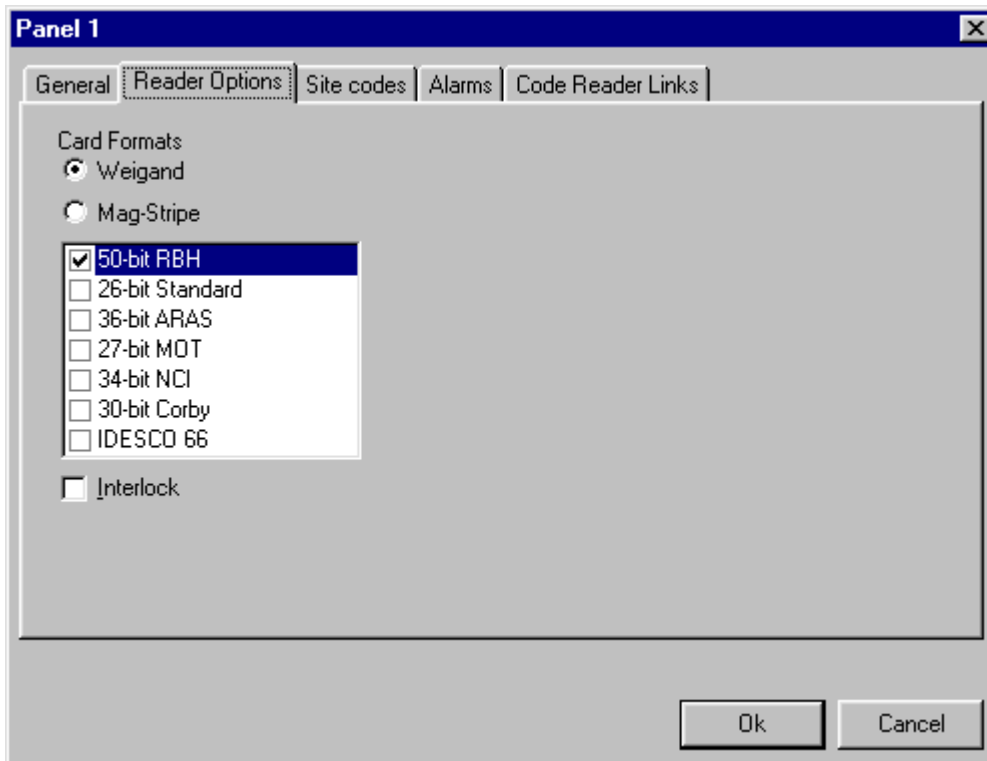
#### ***Description***

To change the default description simply type over it.

#### ***Enable***

If the enable check box is not checked then the panel will not be shown in the status screen. All Access Point, Inputs, and Outputs under that panel will also be disabled. Disabled items are still in the database but are not considered to be part of the system.

## Reader Options



### ***Card Format***

This is where the card format is selected (*only a limited number of formats are supported- list provided*).

### ***Interlock***

With Interlock checked only one of the two doors on the one panel may be opened at a time. If one door is open then access will not be granted at the other door until the first door is closed.

## **Site Codes**

Under the *Site Codes* tab the facility code to be used by the IRC-2000-2 is entered. (*Only 1 facility code per IRC-2000-2 is supported.*)

## **Alarms**

Under the *Alarms* tab the schedules are set for when *Panel Online*, *Panel Offline*, and *Panel Trouble* cause an alarm. An instruction message can be assigned to these alarms as well from this tab. Instruction messages are created elsewhere.

## **Code Reader Links**

Intgra32™ provides for access codes (*cards*) to be linked to one or multiple inputs, outputs, and access points on a local basis. A single access code with a card read is

capable of invoking different links dependent on which access point it is presented at. This linking is done at the controller level without the Host PC online.

Code reader links are used primarily in HVAC control, lighting control and intrusion alarm control systems where it is necessary to control inputs, outputs, and other access points from a single card read. With code reader links, the same cardholder can perform different functions at each access point. Also, every cardholder can perform a unique function at every access point. Further, links can have several entries, allowing execution of multiple commands at each access point when a card is presented.

This window contains the following fields and options:

ID	Code	Description
1	1403	Code Reader Link 1

Reader Side A  
 Reader Side B

	Command	Device	Duration	Schedule
1.	Arm Input	Input 3	10 Sec	01 - Always
2.	Output On	Output 4	5 Sec	01 - Always
3.	Disable forced en			01 - Always
4.				

***ID***

The number of the code reader link may be system generated by pressing up and down button or user-defined. A maximum of 16 code reader links can be generated.

***Code***

Put in the code number. These codes can be in the range of 1-32767.

***Description***

The user specified description of link.

Choose one of the two radio buttons- Reader side A or B on which code reader link has to be executed.

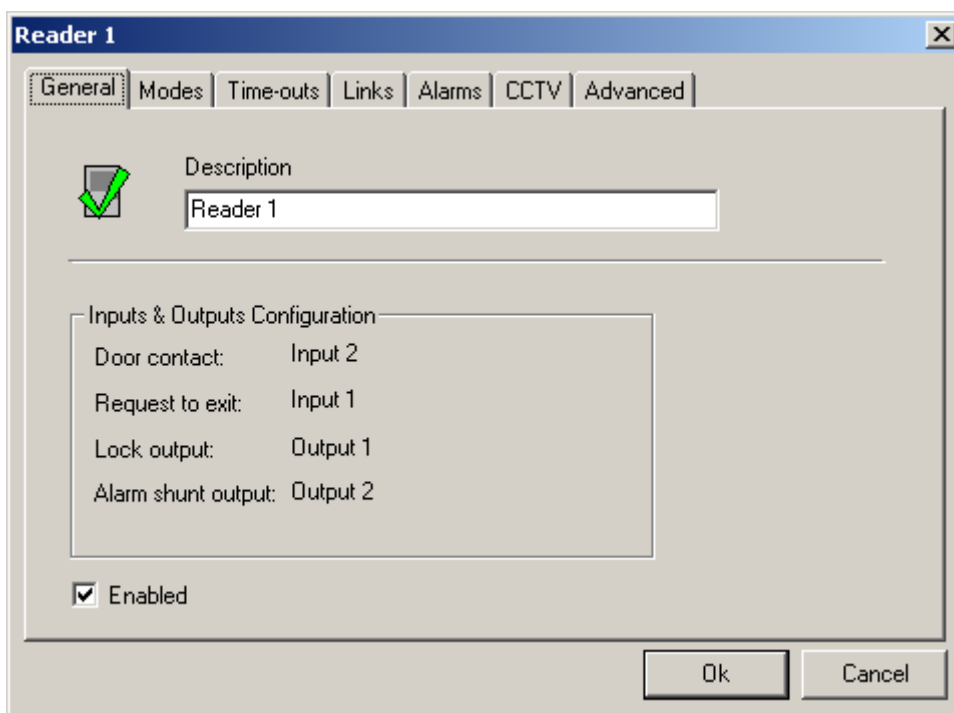
Then as with local links you choose which event on what device will cause the link to be executed. You can choose up to four things to have happen with one code.

## Dial-Out

This tab is visible only if the Network to which the panel is connected is Modem Network. (*Explained earlier on page 21 and 22*)

## Access Points

### General



### ***Description***

To change the default description simply type over it.

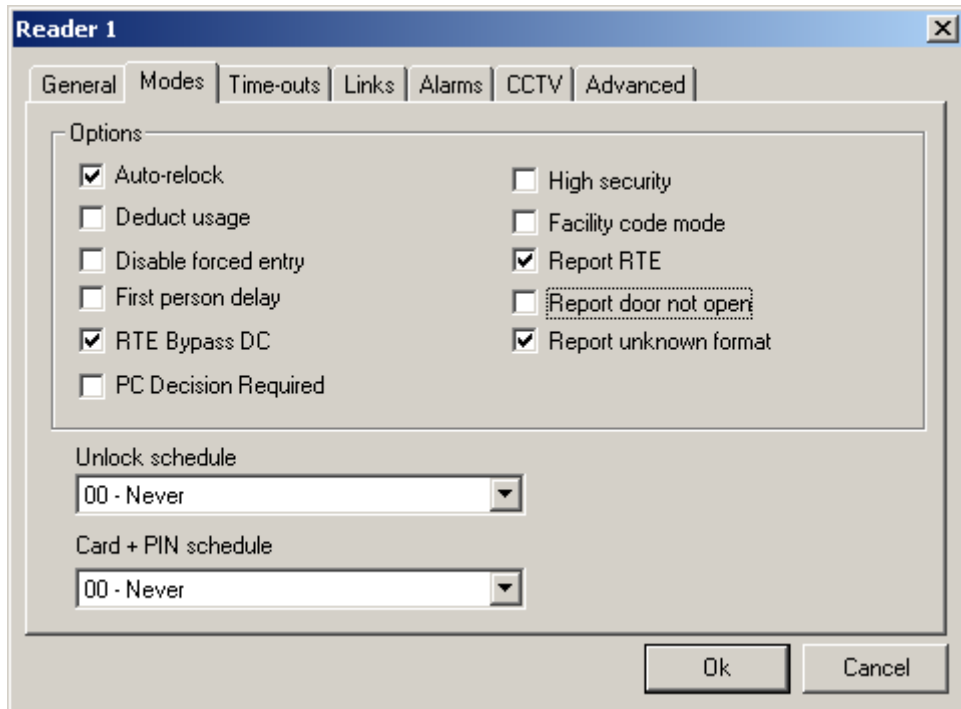
### ***Input & Output Configuration***

This section of the tab tells you which inputs and outputs are assigned to the access point.

### ***Enable***

If the enable check box is not checked then the access point will not be shown in the status screen and will not be considered to be part of the system.

## Modes



### ***Auto-Relock***

After a grant access the door locks again at the end of the unlock time. With auto-relock checked if the door closes before the unlock time expires, then the door will lock when the door closes and won't wait until the timer expires.

### ***Deduct Usage***

Readers selected to deduct usage will reduce the usage count of cards granted access if card's the usage count is less than 255. Card with a usage count of zero will not be granted access.

### ***Disable Forced Entry***

If Forced Entry is disabled then opening the door without an access granted will not cause a Forced Entry alarm but instead will start the access granted sequence. This is generally used on a door with a mechanical egress and no request to exit device.

### ***First Person Delay***

Access points with lock/unlock schedules will lock and unlock according to the schedule. If First Person Delay is selected the door will remain locked until the first card is granted access after the start of the schedule.



### ***RTE Bypass DC***

This feature is used with the doors having mechanical egress. The Request to Exit device will bypass the door contact but will not unlock the door. The door can be opened without causing an alarm since the contact is bypassed.

### ***PC Decision Required***

Selecting *PC Decision Required* takes the decision to grant access away from the panel. If the panel would normally grant access, it wouldn't. Instead it simply sends a message to the PC "Access Requested". An operator at the PC can then decide to grant access or not. Other software functions can also use this feature (e.g. *global Antipassback*).

### ***High Security***

Cards with High Security privilege can only access access points in High Security mode.

### ***Facility Code Mode***

Access points in Facility Code Mode will grant access based upon the card's facility code and not on the card's card number. Cards not entered into the system that have the correct facility code will be granted access.

### ***Report RTE***

Access granted by a request to exit device will report that event if this feature is checked.

### ***Report Door Not Open***

The fact that a door was not opened after access was granted at that door can be reported if this feature is checked.

### ***Report Unknown Format***

An Unknown Format message indicates that the data received does not correspond to any of the card formats useable by the IRC-2000-2. This message can be turned off if it is not required.

### ***Unlock Schedule***

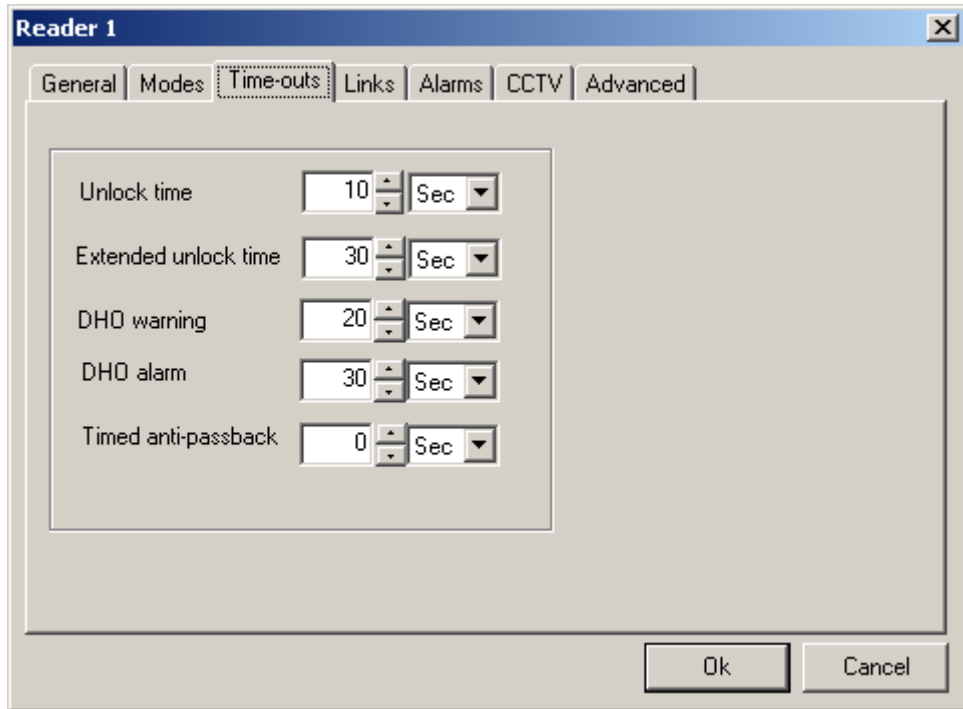
Select a schedule when unlocking and locking of this access point is required.

### ***Card + PIN Schedule***

Select a schedule when both Card and PIN are required.

## **Time-Outs**

Timers can be set from 0-127 seconds or minutes. Setting a timer to zero will disable it.



### ***Unlock Time***

This is the time the Door Unlock output is turned on for.

### ***Extended Unlock Time***

For the Cards given the Extended Unlock Time privilege the Door Unlock output will turn on for this length of time instead of the regular Unlock Time.

### ***DHO Warning***

If a door is still open after the Lock Time expires, the Access Point will go into Door Held Open Warning after the Door Held Open Warning time expires.

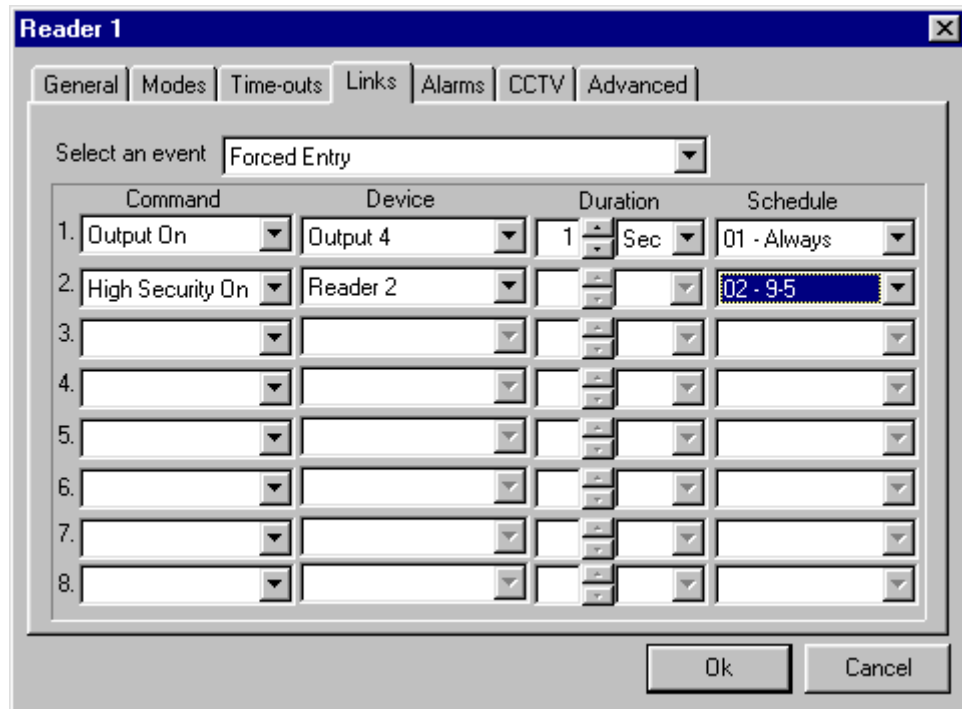
### ***DHO Alarm***

If a door is still open after the Lock Time expires, the Access Point will go into Door Held Open Alarm after the Door Held Open Alarm time expires. This timer starts at the end of the lock timer and not at the end of the DHO Warning timer. If DHO Alarm time is less than the DHO Warning time there won't be a warning.

### ***Timed Antipassback***

Set the amount of time for Timed Antipassback here. See Reader Options for description of Antipassback.

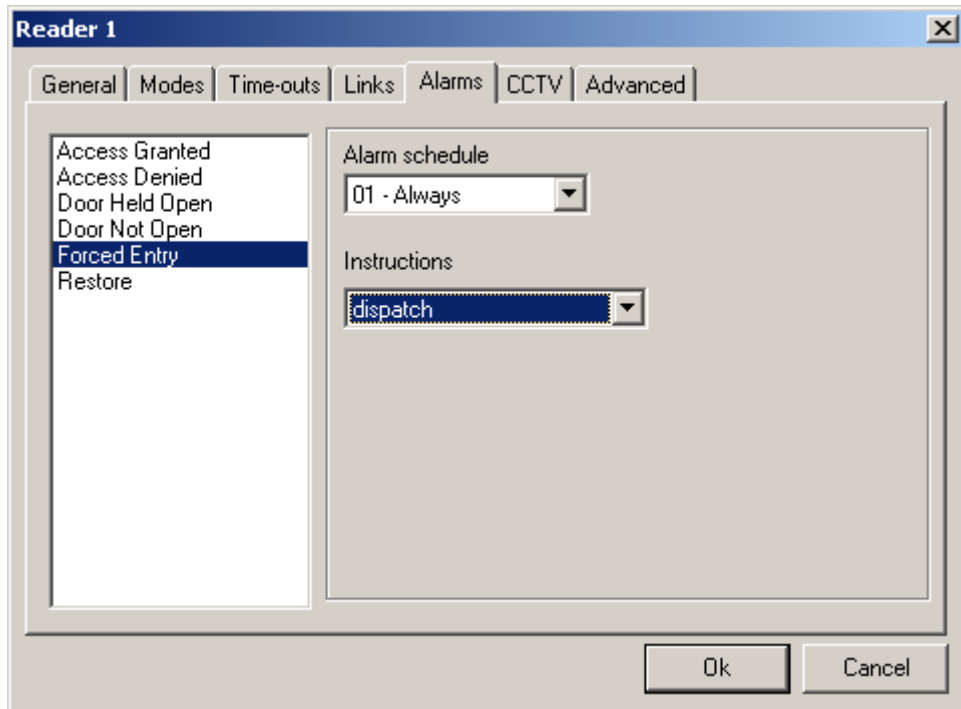
## Links



- First select an event.
  - The selectable events are Access Granted, Access Denied, Door Locked, Door unlocked, Door Held Open, Door Not Open, Forced Entry, and Restore.
- Then select up to eight commands to be executed with that event.
  - The command selection list includes; arming or disarming an input, turning on or off an output, locking or unlocking an access point, setting High Security mode on or off for an access point, and turning Disable Forced Entry on or off.
- After you have selected a command an appropriate device needs to be selected (*input, output, or access point*).
- Choose the duration of the command (*0-127 seconds or 0-126 minutes*).
  - Not all commands can be timed. *High Security* on and off, and *Disable Forced Entry* on and off cannot be timed.
- A schedule can also be selected for each command (*the command will only be executed when the schedule is on*).

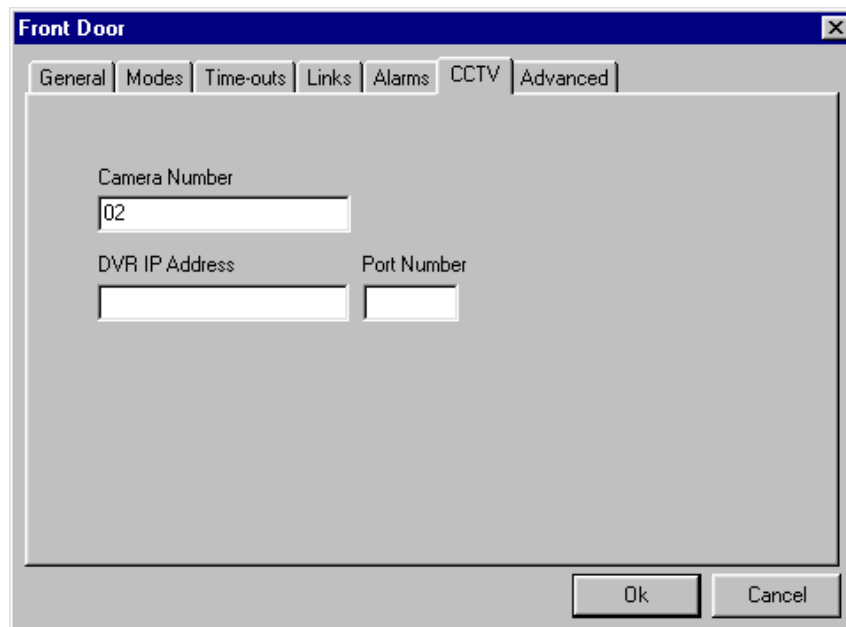
The example above has the Output 4 being turned on for one second whenever there is a forced entry at Reader 1. If this forced entry occurs when schedule 2 is on, then High Security Mode will be turned on for Reader 2.

## Alarms



- First select an event from list on the left.
  - The alarm will occur when the message appears in the log screen.
- Then select an *Alarm Schedule*. (*Causes an alarm when?*)
- Then you can select (*if required*) an instruction message for the alarm. (*Message creation is described earlier.*)

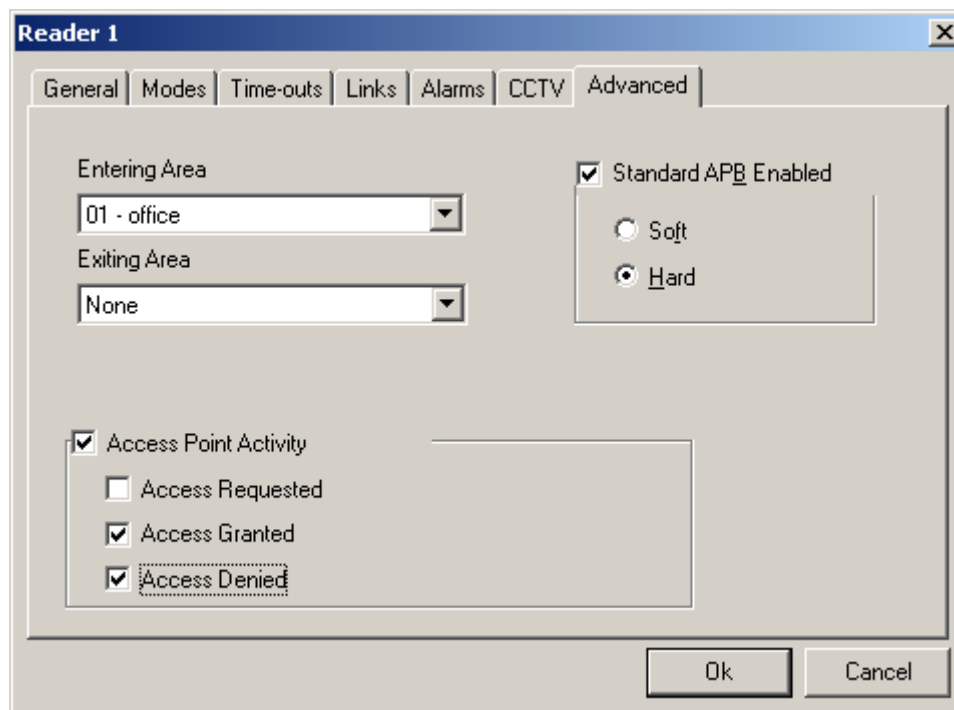
## CCTV



The information in this tab is required only for DVR interface.

- First select the camera number for the activity you want to display from DVR
- Select the DVR IP address and Port Number for the camera you selected as you could be using more than one DVR (This is related to the *DVR* tab in the *History Reports* explained later in Chapter 7)

## Advanced



### ***Standard APB Enabled***

The check box is used to turn on Antipassback. Soft Antipassback will still grant access even though APB has violated, hard APB will not.

**Note:** For Global Antipassback<sup>5</sup> to work, the *PC Decision Required* box need to be clicked on in the *Modes* tab of the Reader Properties' window for all the readers, otherwise it will ignore the multiple panels (*IRC-2000-2*) used and will work as local antipassback<sup>6</sup> (*within a panel IRC-2000-2*).

Areas need to be created first for global antipassback to work.

<sup>5</sup> Anti-passback tracked across multiple IRC-2000-2s is called *global Anti-passback*

<sup>6</sup> Anti-passback tracked on one panel (*IRC-2000-2*) is called *local Anti-passback*

### ***Entering Area & Exiting Area***

An entering area must be selected for APB to work. Selecting only an Entering Area will setup Reader APB. In Reader APB the entering area is compared to the cardholders current location. If they match there is an APB violation. By adding an Exiting Area you setup Area APB. Area APB not only check that the area the cardholder is entering isn't the area they are in, but also verifies that the area they are exiting is the area they currently are in, providing a higher level of APB.

### ***Access Point Activity***

By checking this box you enable the automatic displaying of the Access Point Activity window when the selected event(s) occur at the access point. Often this is used with a CCTV system for video verification of access.



**Note:** The above window is automatically displayed only if *Access Point Activity* is turned on from the *Options* menu of the main screen toolbar.



## Inputs

### General

From *General* tab the user can change the description of the input. The *Type* of input is also chosen here.

- The input type can be:
  - General Purpose
  - RTE for Reader A
  - RTE for Reader B
  - Door Contact for Reader A
  - Door Contact for Reader B

### Details

Select the *Circuit type* and *Abort Delay* under the *Details* tab.

- Inputs can be:
  - Normally Open or Normally Closed
  - One resistor, Two resistor, or No resistor
- Abort Delay is set in second/minutes (*maximum 127 minutes*).
  - The input must be tripped for this amount of time to cause an alarm. If the input is cleared before the time expires then there won't be an alarm.

For *General Purpose* inputs additional programming is required under the *Details* tab.

The screenshot shows a dialog box titled "Input 4" with a "Details" tab selected. The "Circuit type" dropdown menu is set to "NO, No Resistor". The "Abort Delay" is set to "0" seconds. Under the "Options" section, the checkboxes for "Report while armed" and "Report while disarmed" are checked, while "Forced arm alarm" is unchecked. The "Disarm during time group" dropdown menu is set to "00 - Never".

- Reporting, or Non-reporting. (*Are messages from this input to be displayed on the Log Screen and logged?*)

- Forced Arm Alarm or Not Forced Arm Alarm. (*Forced Arm Alarm will force an input into alarm if it is armed while it is abnormal.*)
- Disarm during Time Group. (*Disarm the input during a schedule.*)

## CCTV

The screenshot shows a configuration window titled "Input 4" with a close button in the top right corner. Below the title bar are five tabs: "General", "Details", "CCTV", "Links", and "Alarms". The "CCTV" tab is selected. The main area contains three input fields: "Camera Number" (a single text box), "DVR IP Address" (a single text box), and "Port Number" (a smaller text box). At the bottom right are "Ok" and "Cancel" buttons.

- As for Access Point, select Camera Number, DVR IP Address and Port Number accordingly if the event selected for DVR display is an input.

*Links and Alarms* tabs are available only for general-purpose inputs.

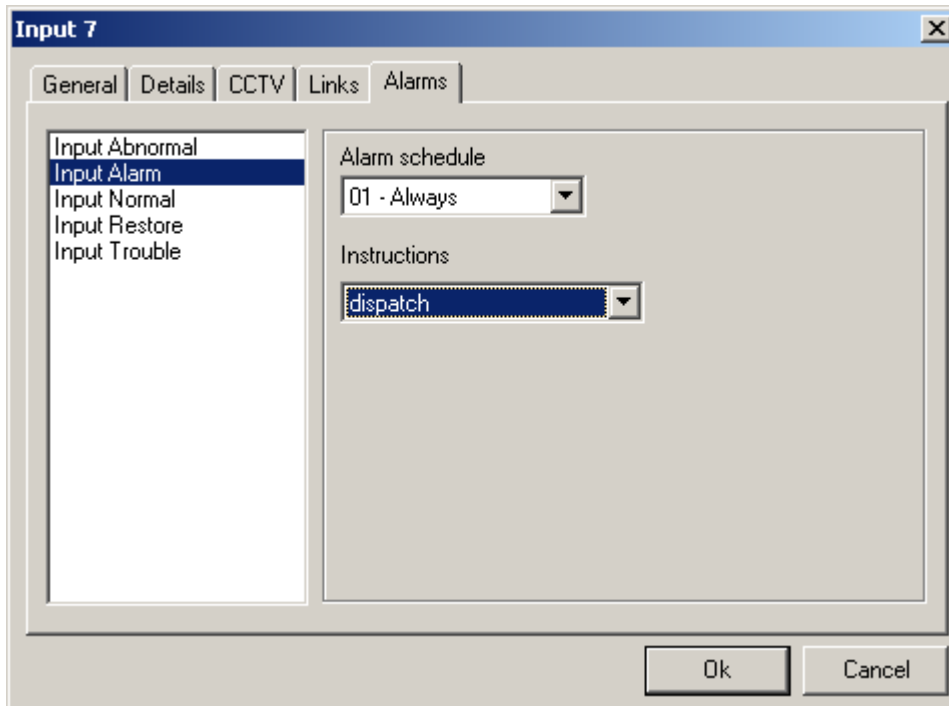


## Links

	Command	Device	Duration	Schedule
1.	High Security On	Reader 1		01 - Always
2.				
3.				
4.				
5.				
6.				
7.				
8.				

- First select an event.
  - Selectable events are Input Abnormal, Input alarm, Input Normal, Input Restore, and Input Trouble.
- Then select up to eight commands to be executed with that event.
  - The command selection list includes; arming or disarming an input, turning on or off an output, locking or unlocking an access point, setting High Security mode on or off for an access point, and turning Disable Forced Entry on or off.
- After you have selected a command an appropriate device needs to be selected (*input, output, or access point*).
- Choose the duration of the command (*0-127 seconds or 0-126 minutes*).
  - Not all commands can be timed. *High Security* on and off, and *Disable Forced Entry* on and off cannot be timed.
- A schedule can also be selected for each command (*the command will only be executed when the schedule is on*).

## Alarms



- First select an event from the list on the left.
  - The alarm will occur when the message appears in the log screen.
- Then select an *Alarm Schedule*. (*Causes an alarm when?*)
- Then you can select (*if required*) an instruction message for the alarm. (*Message creation is described earlier.*)

## Outputs

### General

The *Description* and *Type* of the output can be changed/programmed in the *General* tab.

- The output type can be:
  - General Purpose
  - Lock for Reader A
  - Lock for Reader B
  - Handicap for Reader A
  - Handicap for Reader B
  - Alarm Shunt A
  - Alarm Shunt B
  - Modem Power

### Details

Choose *Energized/De-energized On State* and select a schedule for *Output State On During Time Group* from the *Details* tab. Also select the option of *Report to PC*, if it is

needed. *Output State On During Time Group* and *Report to PC* are programmable for general-purpose outputs only.

## CCTV

Input the DVR information for the output event as in case of inputs.

## Links

The *Links* tab is only available for programming for general-purpose outputs.

	Command	Device	Duration	Schedule
1.	Disarm Input	Temperature Sensc	1 Sec	02 - Mon-Fri
2.				
3.				
4.				
5.				
6.				
7.				
8.				

- First select an event.
  - Either Output On or Output Off.
- Then select up to eight commands to be executed with that event.
  - The command selection list includes; arming or disarming an input, turning on or off an output, locking or unlocking an access point, setting High Security mode on or off for an access point, and turning Disable Forced Entry on or off.
- After you have selected a command an appropriate device needs to be selected (*input, output, or access point*).
- Choose the duration of the command (*0-127 seconds or 0-126 minutes*).
  - Not all commands can be timed. *High Security* on and off, and *Disable Forced Entry* on and off cannot be timed.
  - A schedule can also be selected for each command (*the command will only be executed when the schedule is on*).

## *Access Levels*

Assigning access points to schedules create access levels. They are created so that cardholders can be easily given access rights. Before cardholders are entered, any additional access levels that are required should be programmed. The only default access level is *Master*, which always provide access to all doors.

### **General**

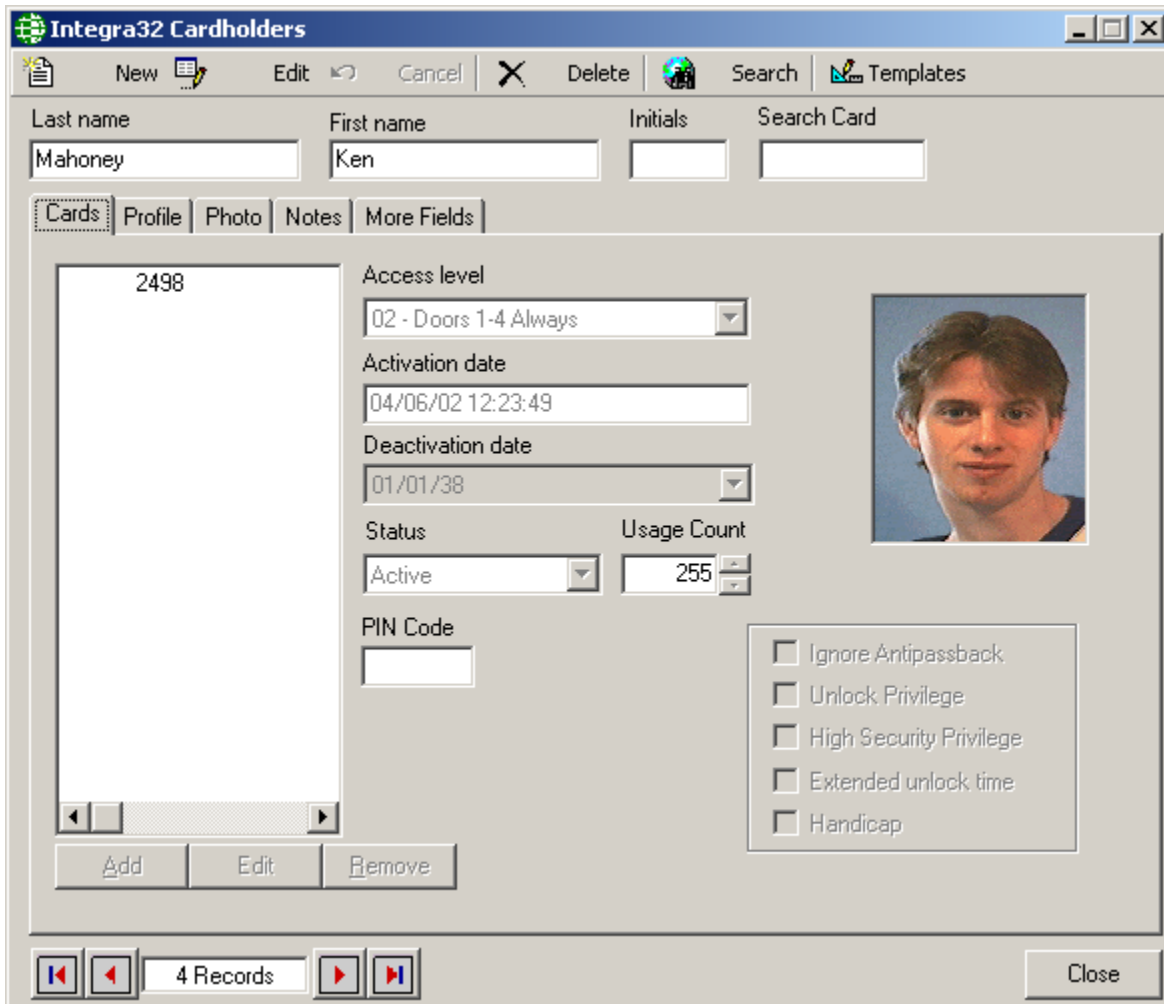
Change the *Description* of the *Access Level* in the *General* tab.

### **Access Level**

Program the *Schedule* corresponding to the Reader (*e.g. front door & rear door*) in *Access Level* tab.

# Chapter 6 Cardholders

Cardholders are entered/edited by clicking the cardholder button from the toolbar of the *Main Window*.



## Fields and Options

The cardholder window contains following fields and options:

### New

To add a new cardholder click on the *New* button, then the cardholder's information can be entered.

### Edit

To make changes to an existing cardholder click *Edit*, then make the necessary changes.

### **Save**

To save changes made to a cardholder click *Save*.

### **Cancel**

*Cancel* will exit the edit mode without saving any changes to cardholder.

### **Delete**

Cardholders that are no longer required can be removed from the database with the *Delete* button. All cards with this cardholder are deleted with it.

### **Search**

To search for a cardholder click *Search*. There are many fields to search by, select one and enter your perimeters then click *Search*.

### **Templates**

*Templates* will open a utility to create your own ID badge templates (explained later). This button is visible only if optional badging software is added with Invision32™

### **Last Name**

Enter the cardholder's surname.

### **First Name**

Enter the cardholder's given name.

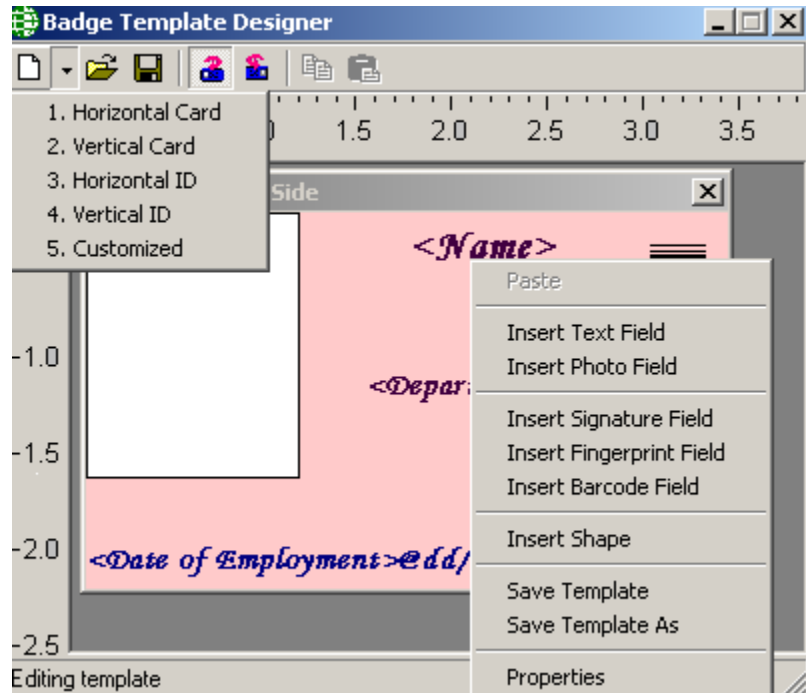
### **Initials**

Up to six characters can be entered.

### **Search Card**

Enter a number here to be used as a search parameter.

## Templates



The Badge Template Designer can create standard or customized badge sizes. Select one of the five options available from the *Create a new template* button of the toolbar. Templates can be saved and re-opened.

Right clicking on the badge will bring up a menu list. From here you can add a text, photo, fingerprint, signature, or barcode field.

- Text fields can be static (*type in your own information*) or it can get data from a field in the database (*e.g. name or card number*).
- Photo fields can also be *static* (so that you can insert your own picture or logo) or *picture field* where you can display the cardholder's image that is stored in the database or acquire the picture of the cardholder if a camera is installed on your computer.
- Fingerprint fields\* can be added to the badge.
- Signature fields\* can be added to the badge.

\*To use these options you may need optional hardware devices.

- Barcode fields\*\* can be added to the badge.

\*\*To use the Barcode field, you need to install barcode fonts in your control panel, which are available in the *fonts\ Resources* folder of your Invision CD.

- A shape field can also be added to enhance your badge.
- In the properties of the badge you can set the background colour of the badge, you can also add a background picture.
  - You can right click on a field to modify its properties or to delete it.

**Magnetic Encoding for the Badges** can be done under the *Options* menu of toolbar (explained later in Chapter 8).

## Cardholders Tabs

### Cards

#### Access Level

Select previously defined access levels from the pop-up window. Access levels determine when and where an access code is valid.

#### Activation Date

MM-DD-YYYY<sup>7</sup>. This field is automatically populated with the current date and time when a new cardholder is added to the system.

#### Deactivation Date

MM-DD-YYYY<sup>8</sup>. To deactivate a cardholder, enter the current date, or a date in the future, on which that cardholder is to be deactivated. The cardholder will be deactivated automatically on the specified date. This field defaults to 1 January 2038.

#### Status

Card status is shown here, generally active or inactive (*depending on the activation and deactivation dates*). This status can be changed to stolen, destroyed, expired, lost, or suspended.

#### Usage Count

Valid range is 1—255. Enter the maximum number of times the card can be used. It reduces the count by one, every time the card is used (*at specific readers*) to gain access. When the count reaches zero the card can no longer be used. To specify that a card is valid for unlimited number of uses, enter 255.

#### Pin Code

The PIN - Personal Identification Number - is the code required at access points with a keypad.

---

<sup>7</sup> Date is displayed in the format selected in the Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.

<sup>8</sup> Date is displayed in the format selected in the Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.



## Options

Choose from the five options available, if required: *Ignore Antipassback*, *Unlock Privilege*, *High Security Privilege*, *Extended Unlock Time*, and *Handicap*.

### ***Ignore Antipassback***

Cards that are given this option will bypass antipassback checks when presented to a reader.

### ***Unlock Privilege***

Cards with this option can unlock or lock access points with a double grant access. Two consecutive grant accesses by the same card can toggle the lock/unlock mode of an access point.

### ***High Security Privilege***

Cards with this option will be granted access on doors in high security mode. As well high security mode on a door can be toggled with four consecutive grant accesses.

### ***Extended Unlock Time***

Cards with this option will use the *Extended Unlock Time* instead of the regular *Unlock Time*.

### ***Handicap***

Cards with this option will activate the *Handicap Output* associated with the access point. The *Handicap Output* follows the activation of the *Lock Output* by a short delay, and is used to trigger a door operator to open the door.

## Cards

Up to twenty cards can be added per cardholder. New cards can be added for an existing cardholder with the *Add* button. All the cards assigned to a cardholder can be seen on the left-hand window of the *Cardholder Screen* when a cardholder is selected. The card number and description of the card are put into this window.

Use the *Edit* button to edit the description of any card assigned to the cardholder, and use the *Delete* button to remove a card assigned to the cardholder.

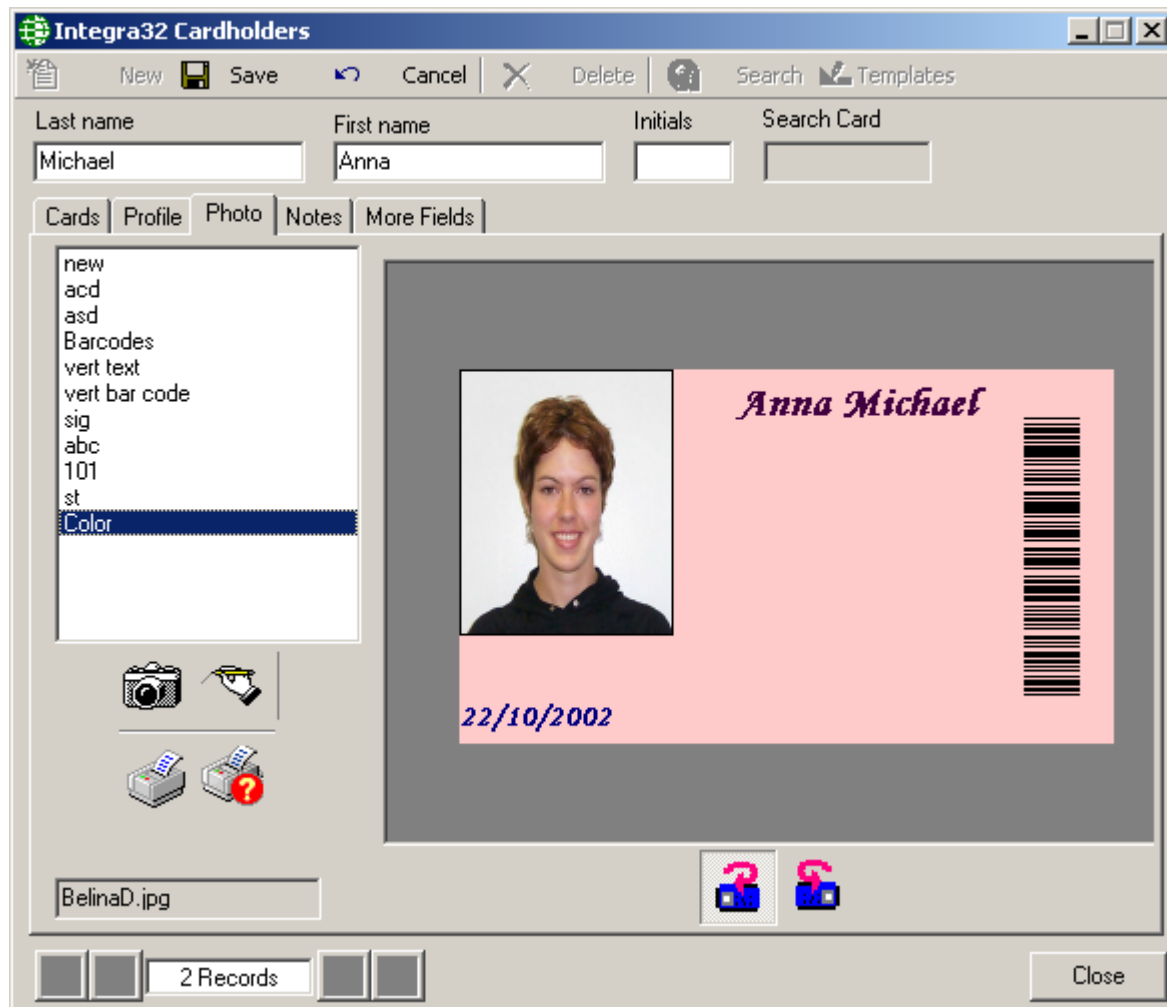
### ***Profile Tab***

The profile information (*like address, phone number and email address*) of a cardholder can be entered in the *Profile* tab.

### ***Photo Tab***

You can select an already saved picture of the cardholder in the *Photo* tab or you can acquire a cardholder's image. The picture is then saved in the Invision32\Images folder.

You can select/ print one of the already saved templates for the cardholder in this tab if the badging option is part of the software.



### Notes Tab

Any other relevant information concerning a cardholder can be saved under the *Notes* tab.

### More Fields Tab

Any additional information required for cardholders can be saved in *More Fields* tab. The user can rename the fields under this tab by right clicking on the label to be renamed. There are two numeric fields, six text fields, and two date fields for the user. These fields can be used in searches and can be displayed on badges.

The screenshot shows the 'Integra32 Cardholders' application window. At the top, there is a menu bar with options: New, Edit, Cancel, Delete, Search, and Templates. Below the menu bar, there are four input fields: 'Last name' (Mahoney), 'First name' (Ken), 'Initials' (empty), and 'Search Card' (empty). A tabbed interface below shows 'Cards', 'Profile', 'Photo', 'Notes', and 'More Fields' tabs, with 'More Fields' currently selected. The main area contains several fields: 'User Number1' (0), 'User Number2' (0), 'User Text 1' (with a 'Rename' button), 'User Text 2', 'User Text 3', 'User Text 4', 'User Text 5', and 'User Text 6'. To the right of these fields is a photo of a man and two date pickers: 'User Date1' (06/06/02) and 'User Date2' (06/06/02). At the bottom, there are navigation buttons (back, forward, search, refresh), a '4 Records' indicator, and a 'Close' button.

# Chapter 7

## Reports

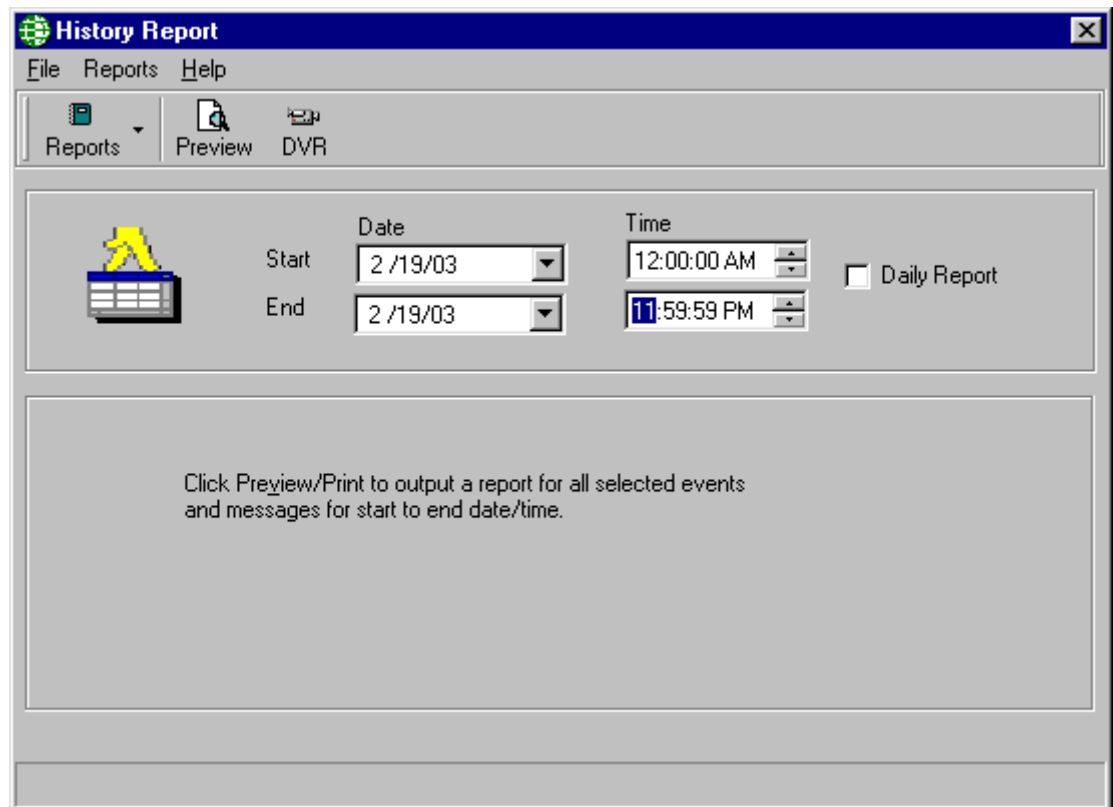
---

The Invision32™ report creation facilities allow you to customize an almost unlimited number of reports and can be used as an extremely valuable management tool.

From *Reports* menu you can choose to launch *History Report* or *Database Report Window*.

### History Reports

Select *History Reports* from the *Reports* menu to launch the following window, where the user has the option of selecting from many history reports available.



#### *File*

From the file menu the user can *Print*, *Select History Path* or *Exit* from the History Report window.

#### **Print**

This menu selection will function the same as the *Print Preview* button described below.

## Select History Path

If your history files are not being saved to the Invision32 folder, then the path to their location will be required.

## Reports

The user can select the kind of report they want to preview or print from the *Reports* menu. The options available are: *Main, Cardholders, Access Points, Inputs, Outputs, Controllers, Alarms, Operators, and Time & Attendance.*

The same options are available from the *Reports* button of the toolbar.

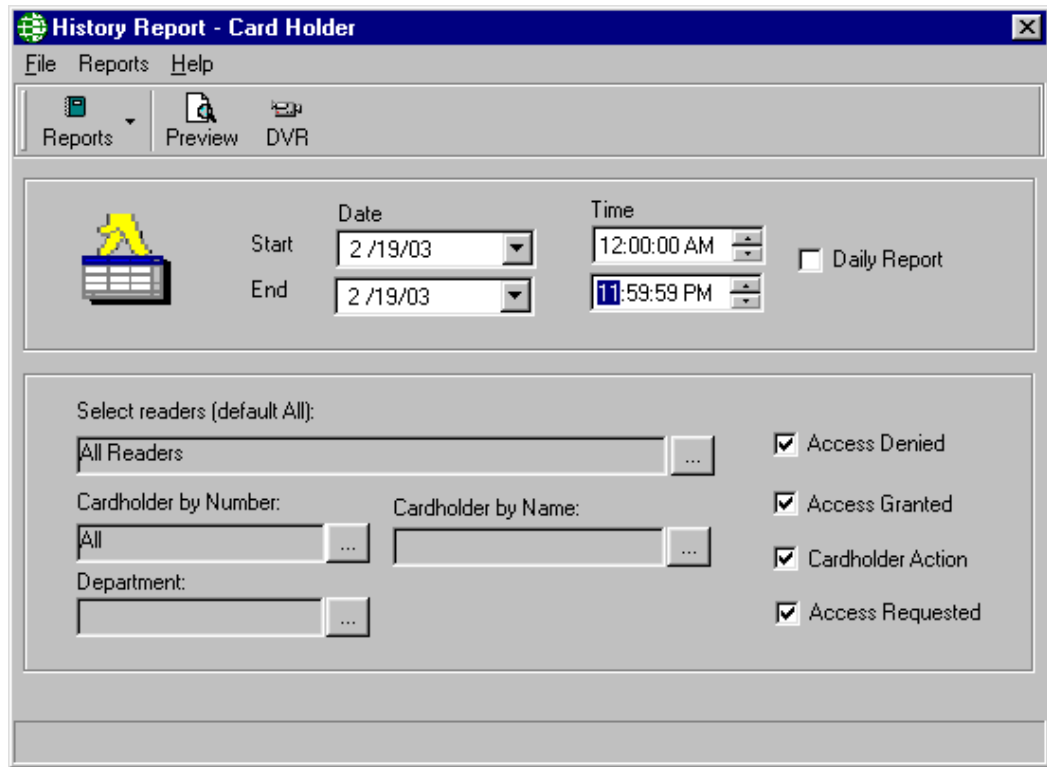
The user sets the *Start Date, End Date, Start Time, and End Time* for any report they have selected to preview or print. The report will span from the start time of the start date to the end time of the end date unless the daily report box is checked. If the daily report box is checked then the report will still span from the start date to the end date, but only include the times between the start time and end time of each day.

## Preview

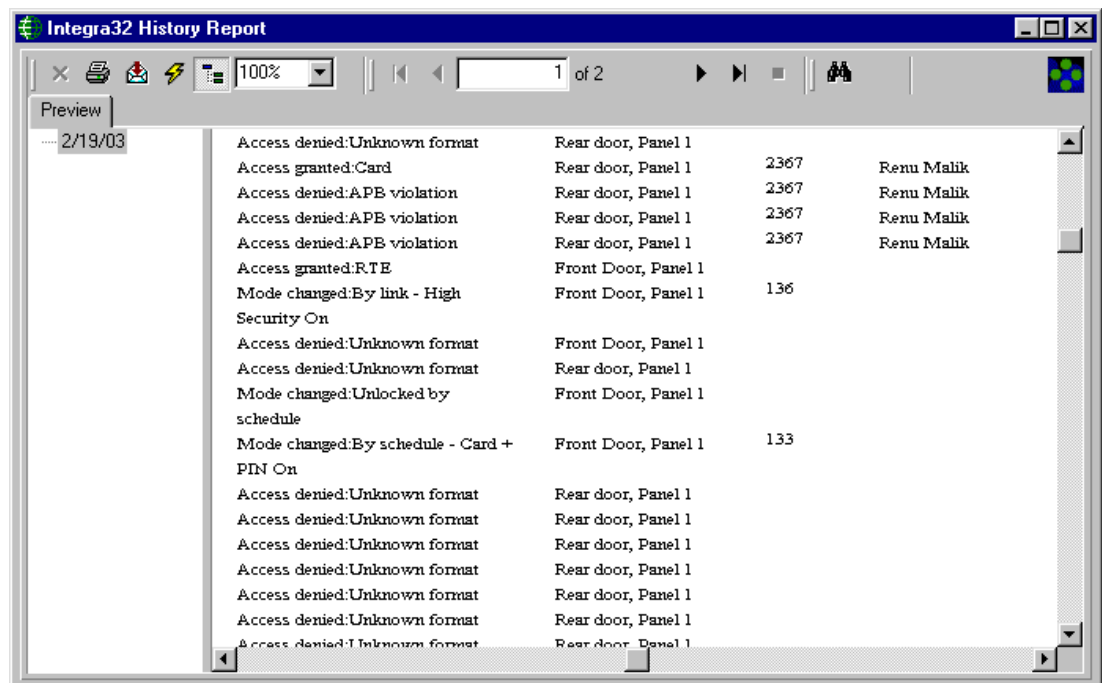
Clicking the *Preview* button of the toolbar, the user can preview or print any of the selected reports for selected time period.

To understand the *History Reports Window* in detail, let's take the example of one of the selected options: *Cardholders*

From *Reports* menu or *Reports* button, select *Cardholders* to show the following screen:



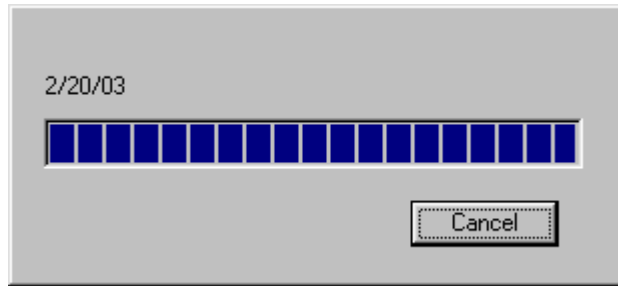
- Select the *Start* and *End, Date* and *Time* for the time period you want to preview the report for.
  - If the report is to cover only specific hours each day then check *Daily Report* so that the *Start* and *End Time* will be applied each day.
- Click the *Select Readers* button to select the readers you want on this report to preview or print. All readers will be shown by default.
- Click the '*Cardholder by Number*' or '*Cardholder by Name*' to select cardholders for your report. All cardholders are selected by default.
- The user can customized the report by clicking in the checkboxes for *Access Denied, Access Granted* and *Cardholder Action*. These selections will determine which messages are to be reported on.
- Click the *Preview* button to preview the customized cardholder's report.




From this report, the user has the option of *Printing, Exporting* the file, *Refreshing* the preview of the report, or changing the current view of the report.

## DVR

Clicking the *DVR* button from the toolbar of the *History Report-Cardholders* window, the user can preview the *Send Camera Commands* window to select the History Event Command he/she wants to send to DVR.



Date	Message	Location	Name/Num:	Operator	
2/20/03 10:13:03 AM	System:Panel offline	Panel 1			
2/20/03 10:16:56 AM	System:Panel online	Panel 1			
2/20/03 10:16:57 AM	System:Panel online	Panel 2			
2/20/03 10:16:57 AM	Audit message:Operator log			rbh	
2/20/03 10:30:59 AM	Audit message:Record char			rbh	
2/20/03 10:31:14 AM	Access denied:Unknown fo	Rear door, P			
2/20/03 10:31:29 AM	Access denied:Unknown fo	Rear door, P			
2/20/03 10:31:54 AM	Access denied:Unknown fo	Rear door, P			
2/20/03 10:32:03 AM	Access denied:Invalid card i	Front Door, F			
2/20/03 10:32:05 AM	Access denied:Invalid card i	Front Door, F			
2/20/03 10:32:07 AM	Access denied:Invalid card i	Front Door, F			
2/20/03 10:32:09 AM	Access denied:Unknown fo	Rear door, P			
2/20/03 10:32:11 AM	Access denied:Unknown fo	Rear door, P			
2/20/03 10:32:14 AM	Access denied:Invalid card i	Front Door, F			
2/20/03 10:32:17 AM	Access granted:RTE	Front Door, F			
2/20/03 10:32:27 AM	Access point:Door not open	Front Door, F			
2/20/03 10:32:39 AM	Input:In alarm	Input 4, Pan			
2/20/03 10:32:42 AM	Input:Restore	Input 4, Pan			
2/20/03 10:32:44 AM	Input:In alarm	Input 3, Pan			

Double clicking *Camera sign*  for the event will display the respective event on screen.

## Database Report

Select *Database Reports* from the *Reports* menu to launch the following window, where the user has the option of selecting from many database reports available.

### Options

The options available for *Database Report* are:

- **Access Levels Report**
- **Access Points Report**

- **Areas Report**
  - **Cardholders Report**
  - **Global Links Report**
  - **Holidays Report**
  - **Input Points Report**
  - **Network Controllers Report**
  - **Operators Report**
  - **Output Points Report**
  - **Time groups Report**
- Select one of the reports available (*e.g. Access Points Report*). Click the *Next* button to select the options available in for the chosen report:
  - Select the items to include in the report or click in the check box for *Select All* if you want to include all the items available in your report.
  - Click the *Next* button to select from the available fields to include in the report, or check the *Select All* box to include all fields.
    - By default four fields are selected. If up to five fields are selected a simple report will be produced. For more than five fields a detailed report is produced.
    - For some reports there is a main report and sub report. If you select *Show Subreport*, which is selected by default, the *ID* field can not be unselected. It is required to link the main and sub report. The fields selected in this list are for the main report only. Up to ten fields can be selected. If you select more than ten fields the first ten will be shown.
  - Click the *Next* button to select the sort order for the report
    - Use the *Move All*, *Forward* and *Back* arrows to select sort fields.
    - Then choose *Ascending* or *Descending* for that field.
    - Click the *Next* button to go to next screen.
  - Click on *Preview Report* to see the report or click on *Begin Again* to view a new report or click on *Finish* to end.

The user can follow similar steps to preview or print other kinds of *Database Reports* as well.



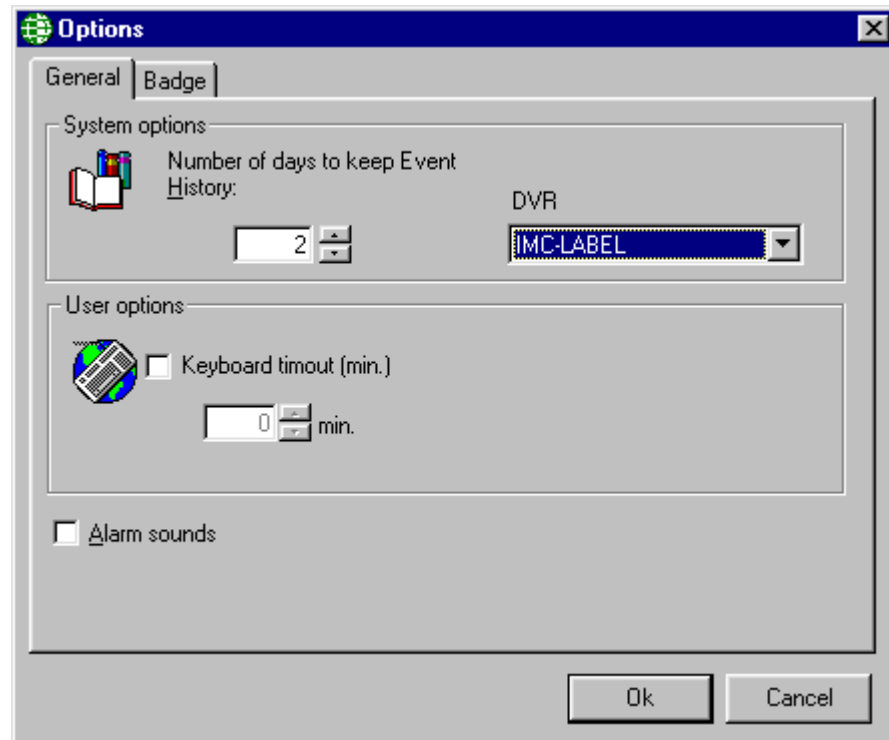
# Chapter 8

## Options

---

### System Options

#### General



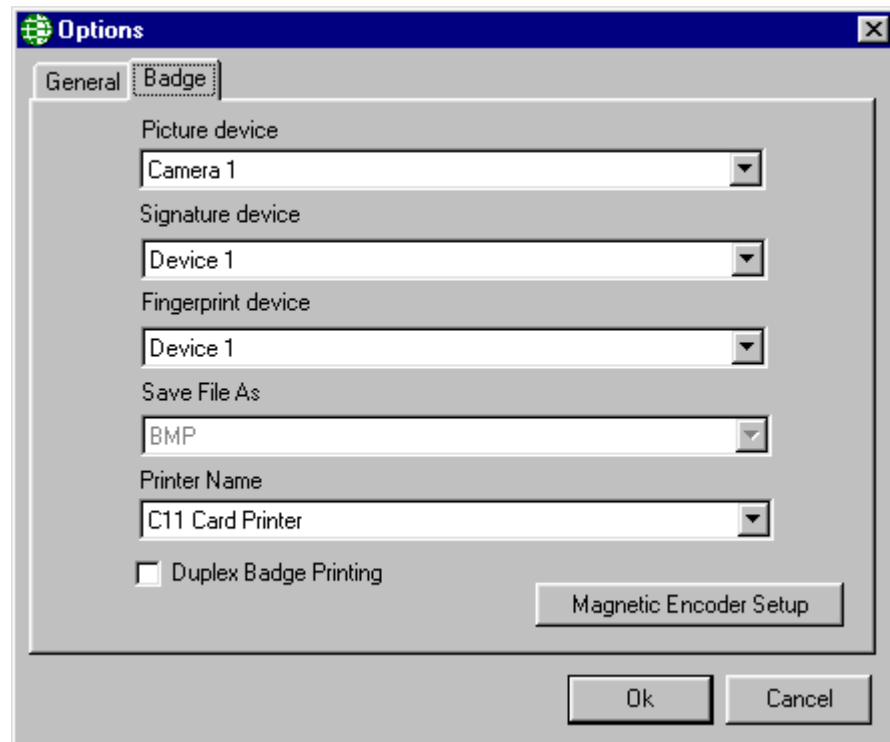
The *System Options* window allows the user to customize number of days to keep *Event History* and *Keyboard* time-out in minutes. The default "number of days" to keep *Event History* is 365 days. Each history file keeps the history information of one calendar day. If 365 days of history is being kept then only 365 files will be kept. When a new history file is created, the oldest file will be deleted so that only 365 files are maintained.

If a user has entered a keyboard time-out, Invision32™ will automatically log-out if there is no mouse activity for the duration of keyboard time-out period.

DVR box allows choosing one of the two options available for video display: IMC-HISTORY or IMC-LABEL which displays a label as well for the history event command the user has sent to DVR.

Also click in the check box to turn on the alarm sound, which are heard through the computer speaker. (*Click again in the check box to turn it off.*)

## Badge



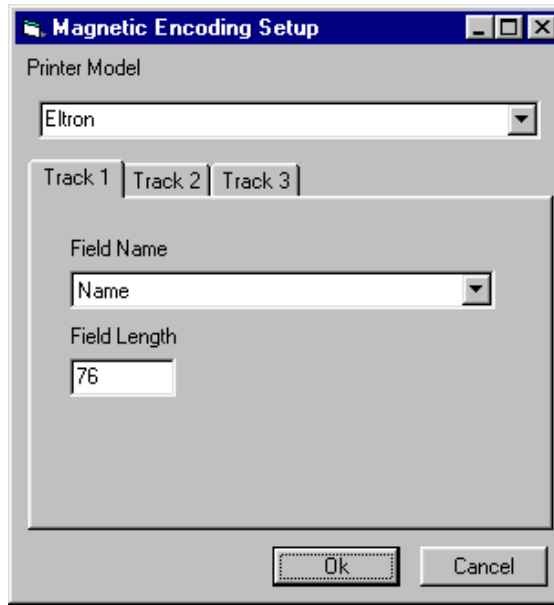
Use this tab to define properties of the badging utilities. Designate where the cardholder's image, signature, and fingerprint will be acquired. For devices to be listed here they must first be installed in the operating system according to the requirements of Badges. They must also be Twain devices.

Designate as well the format to save the image as and what printer to use for printing badges.

Also click in the check box for double sided printing of badges.

### Magnetic Encoder Setup

Clicking in the *Magnetic Encoder Setup* button under the *Badge* tab of *System Options* window will launch the following window to setup properties for magnetic encoding.

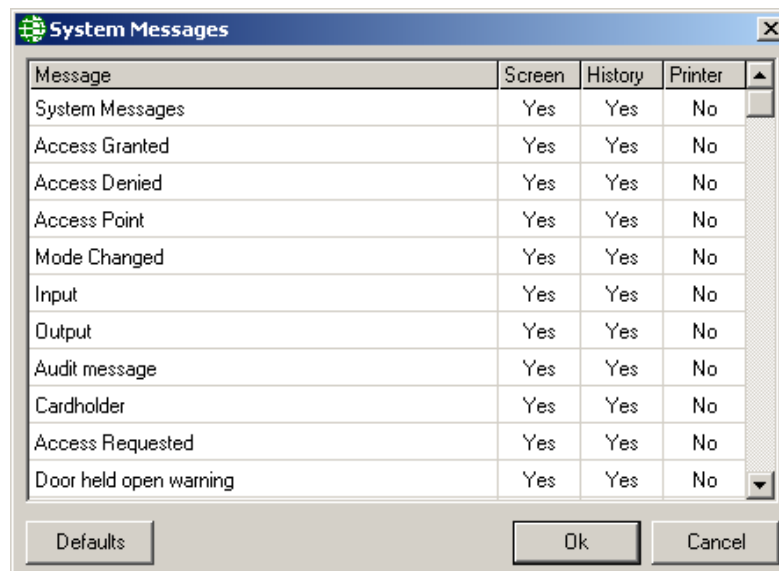


Select the printer model in this window. The fields to encode can be selected for each track once the printer model is selected.

Note:

- The field length is fixed and cannot be changed.
- If *None* is selected for the printer model, the track fields for encoding will not be available.
- The printer properties for encoding should be setup for the printer from the control panel.

## System Messages



The user can customize the system activity on screen and history. (E.g. if the user doesn't want a particular message to appear on screen, like cardholder messages. By simply double clicking you can change 'Yes' to 'No', and stop the displaying of cardholder activity on screen.) Each user can also send messages to the computers default printer (selectable by message).

## Access Point Activity



The Access Point Activity feature can be used with a CCTV system for video verification. To do this enable PC Decision in the *Modes* tab of the *Access Point's Properties* window and check Access Point Activity – Access Requested in the *Advanced* tab of the *Access point's properties* window. Now whenever a valid card is read at the access point the Access Point Activity window will open displaying the cardholder's picture, name, and card number, the date/time of the event and at which reader the event happened.

If PC Decision is not used in the *Modes* tab then the Access Point Activity window will show all access granted and/or access denied events that occur at selected access points.

### *More/Less*

The *More* button will add a section to the bottom of the window that will display the contents of the cardholder's notes tab. Information about the cardholder that needs to be readily available can be display this way. The *Less* button will remove this extension.

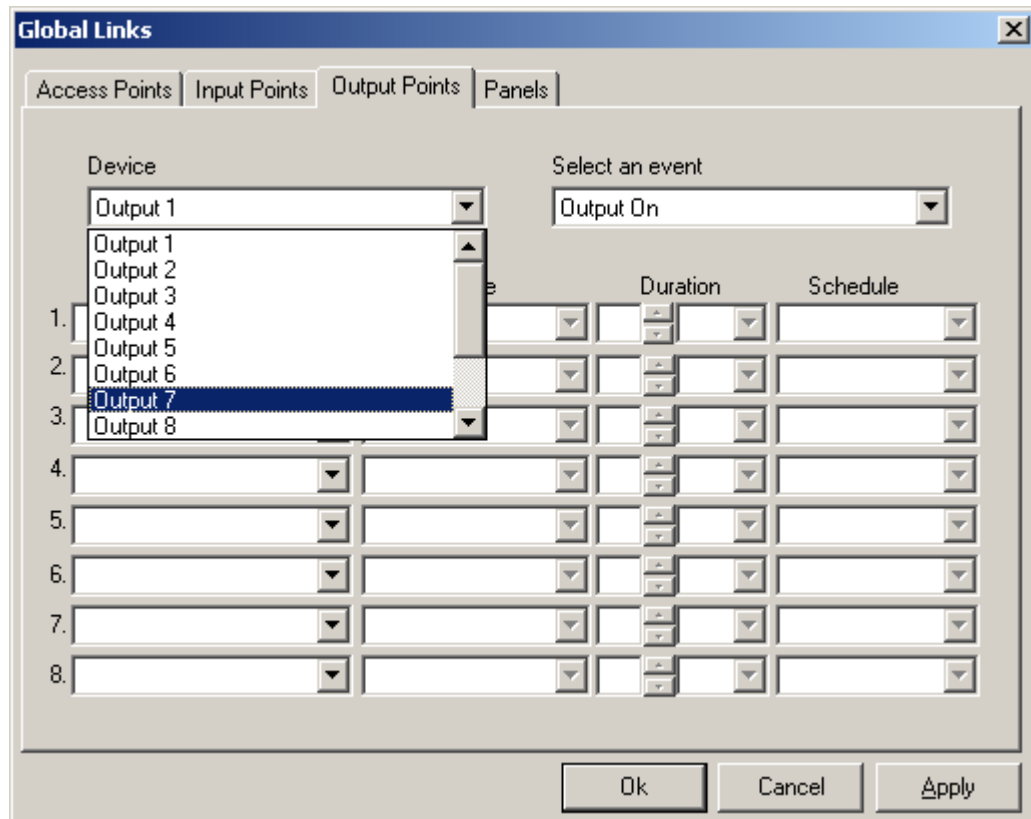
### *Hide*

The *Hide* button will remove the Access Point Activity window from view without turning it off. You can also minimize this window. The difference between hiding and minimizing is that a hidden window won't show up on the task bar.

# Chapter 9

## Links

### Global Links



Global Links like Global APB require the interaction of the PC. These links cannot be executed if the PC is not online. As with local links you choose which event on what device will cause the link to be executed. Then you can choose up to eight things to have happen. These links can be executed on any panel in the system.

Details on programming links can be found in Chapter 5 under Access Point, Inputs, and Outputs.

# Chapter 10

## Tools

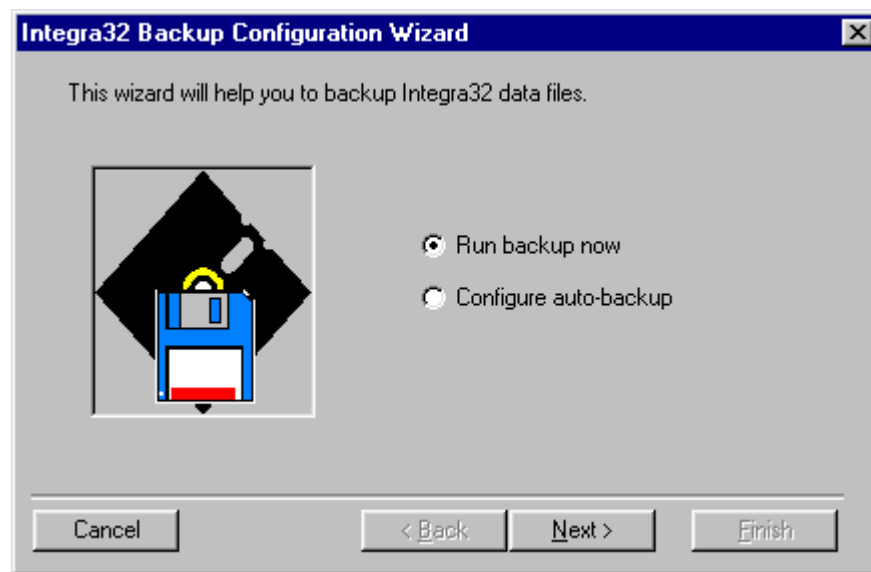
---

### Backup

The Invision32™ *Backup Configuration Wizard* is used to backup your data files. You can run the *Backup* immediately or configure the auto-backup to run at a later time.

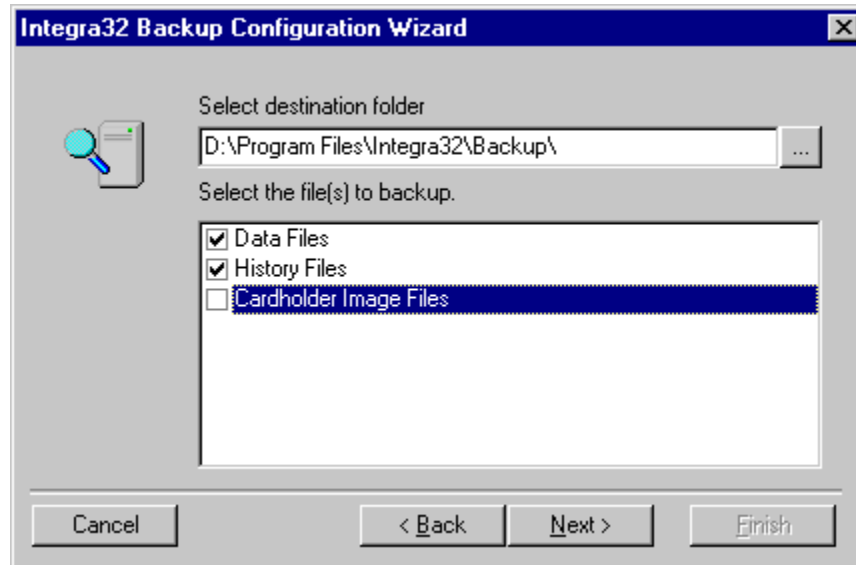
Your Operating System most likely will also have its own backup utility. It doesn't matter what method you use as long as you backup your files regularly.

[“Its not a matter of if a hard drive fails, but when.” *Unknown*]



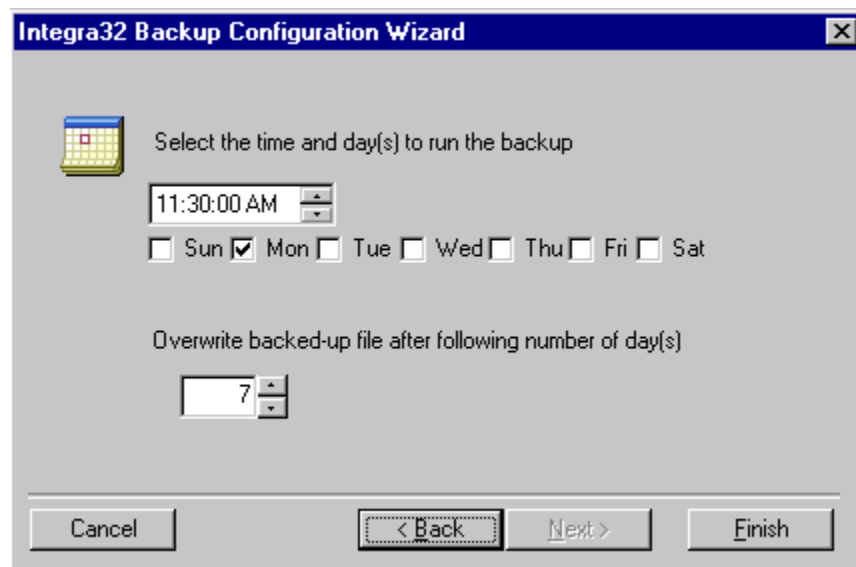
### Run Backup Now

*Run Backup Now* option is used to run an immediate backup. Follow the wizard for this option. From the *Backup Configuration Screen* the destination folder into which the backup files will be saved is selected. (*The default destination setting is ...\Integra32\backup\.*) Checking *Data Files* will backup the data files (*particularly AxlogxLT.mdb, AxsystLT.mdb, & AxuserLT.mdb*). While checking *History Files* will backup all of the currently held history files. *Cardholder Image Files* when checked will backup the cardholder pictures. The *Log Screen* will display these files as they are backed-up.



## Configure Auto-Backup

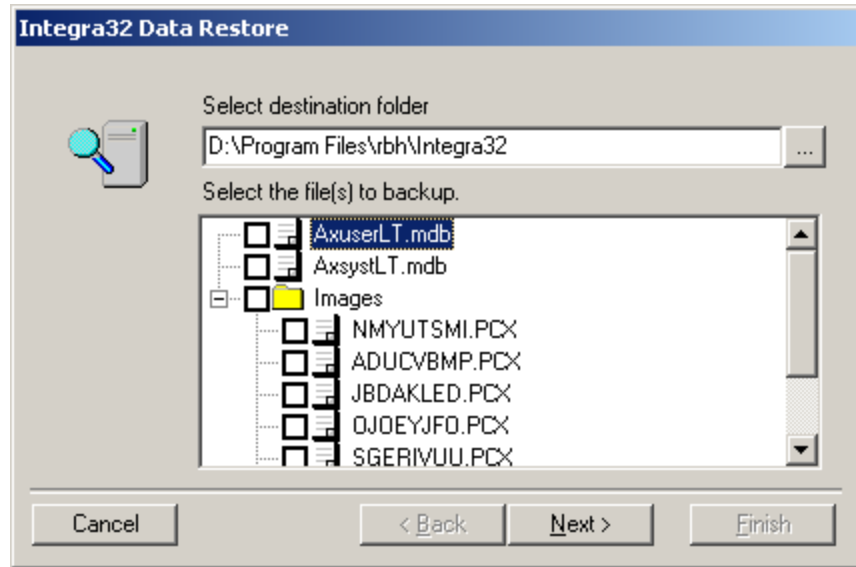
The auto-backup can be configured to happen at a specified time on specified days of the week. For example the backup can be performed at 11:30am every Monday, or at 10:15pm every Tuesday and Thursday. These backed-up files are saved by date (*the file is designed bkpYYYYMMDD where YYYYMMDD is the backup date*), and you can set how long they are to be kept. If for example you set the backup for every Monday and Friday to be kept for 31 days. Backups older than 31 days will be over written.



Click *Finish* to allow the system to run the auto-backup at the specified day and time.

## Restore

To restore backed-up files you must log into *Invision32 Data Restore*. *Invision32 Data Restore* is located under Programs > Invision32 Security System which is accessed by clicking *Start*. You will be required to login before getting to the *Data Restore Screen*.



The *Data Restore Screen* allows you to select which files are to be restored. You can even select which image files are to be restored.



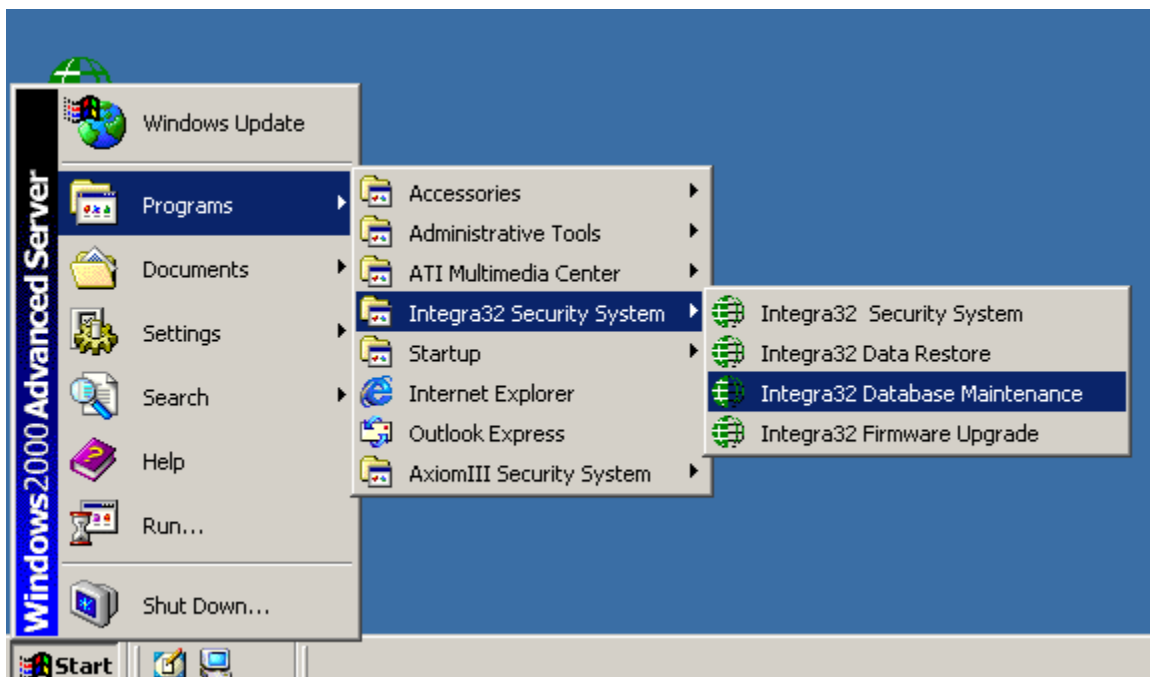
# Chapter 11

## Program Groups

---

### Invision32™ Security System

Insure that the Invision32™ system is not be running before making a selection here in the 'Program Groups'. All selections here made will bring up the login window as shown in Chapter 2 on page 4.



### *Invision32™ Security System*

There are two ways to start the Invision32™ system. You can either double click the icon that was create when the system was installed, or you can click on '*Invision32™ Security System*' in program groups. Both methods will start Invision32™ system.

### *Invision32™ Data Restore*

Data restore is described at the end of Chapter 10.

### *Invision32™ Database Maintenance*

Running the '*Database Maintenance*' will compact and repair the Invision32™ databases. The '*Repair*' will correct most corruptions in the databases. Those that can't be repaired will produce an error message.

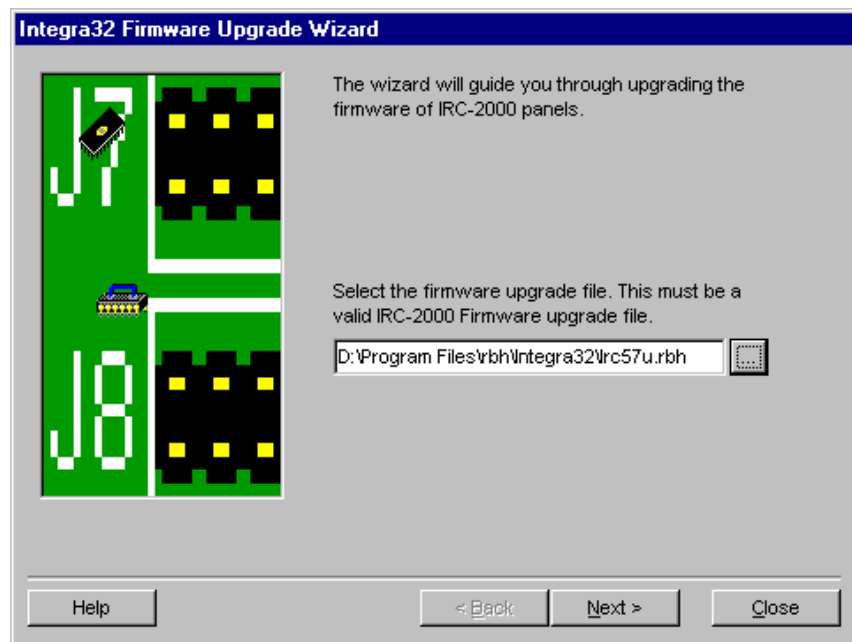
## Invision32™ Firmware Upgrade

### Before Upgrading

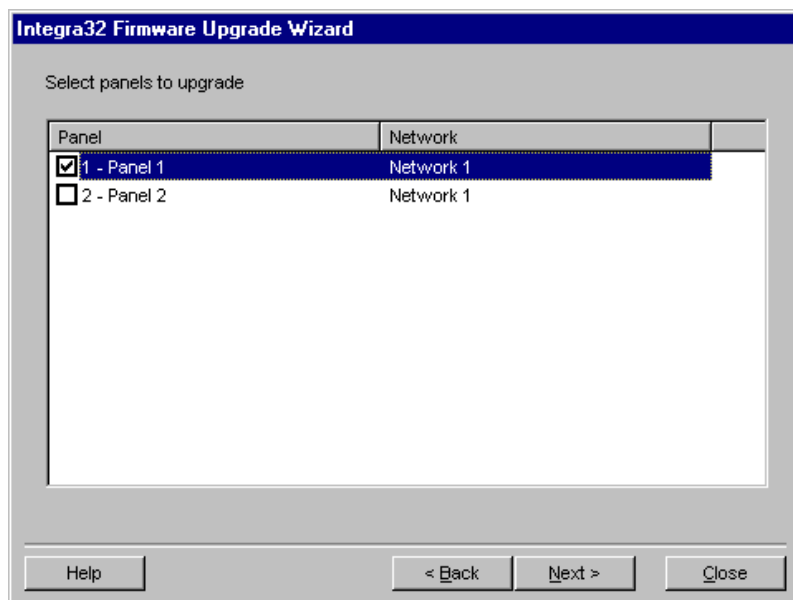
1. Before starting the firmware upgrade be sure to know where the upgrade file (\*.rbh) is located.
2. Although upgrading will not affect the panel's memory, it is recommended that you download all files to the panel after upgrading to ensure that any new features are properly installed.

### Upgrading

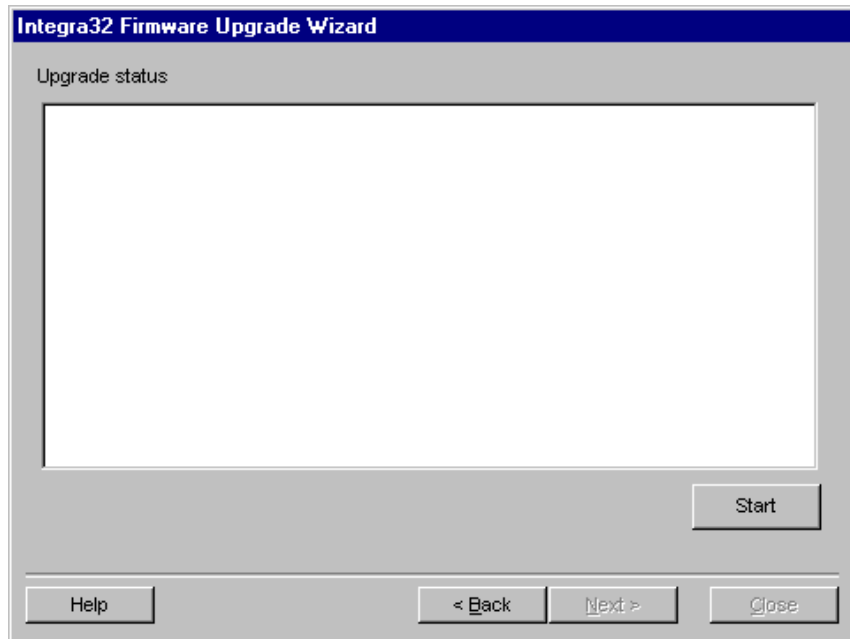
After logging in the Upgrade Wizard will come up. Browse and select the upgrade file (\*.rbh). The upgrade file's path will be shown in the box next to the browse button.



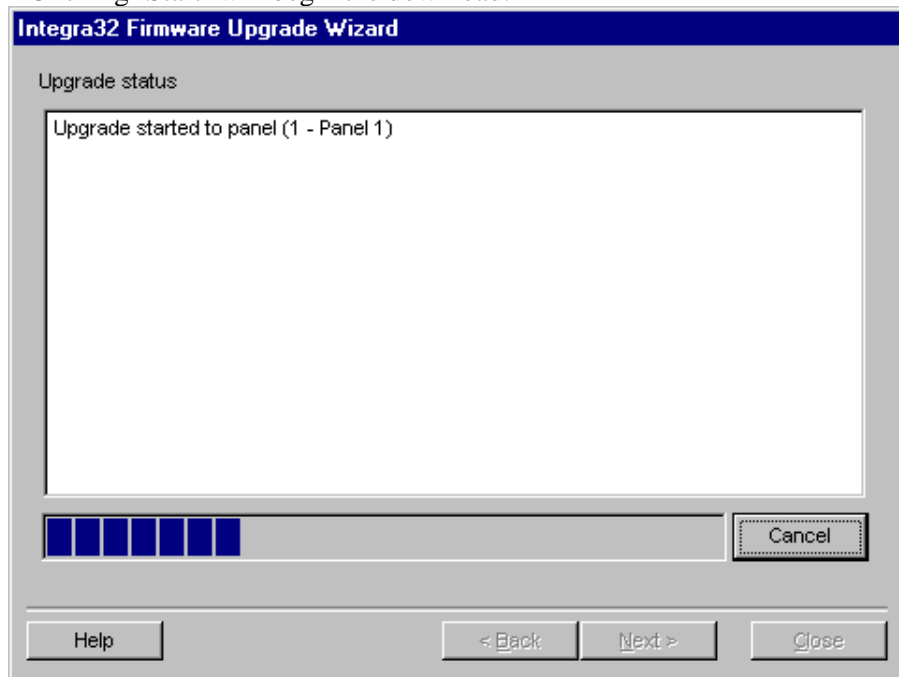
Click 'Next' after the appropriate file has been selected.



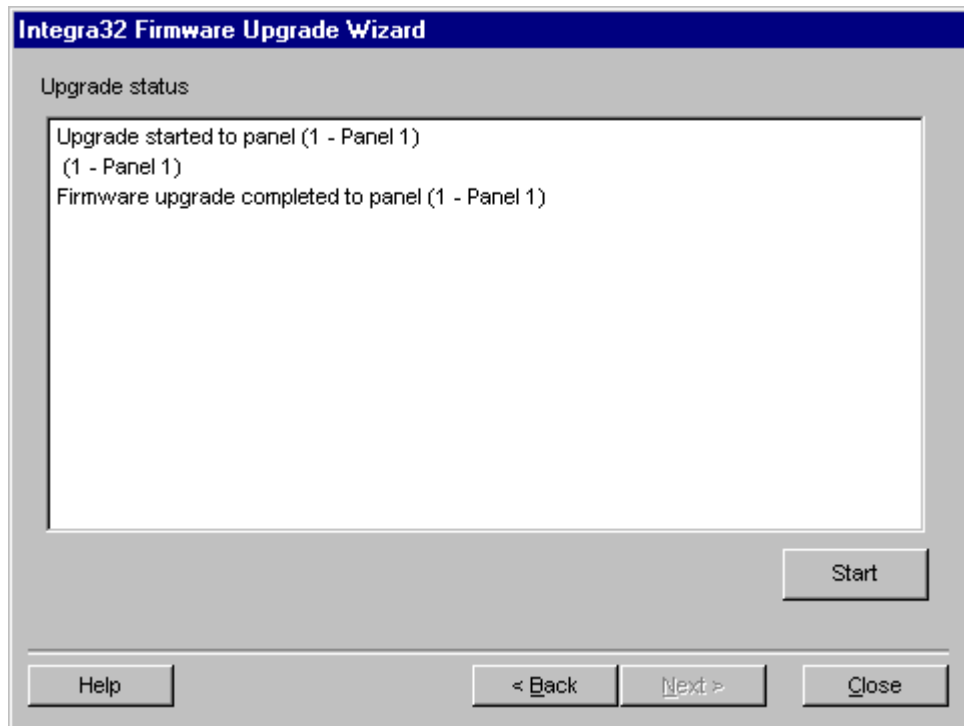
Next select which panel(s) should be downloaded to. Then click 'Next'. You don't have to select all the panels at this time. After upgrading you can come back to this screen.



Clicking 'Start' will begin the download.



A progress bar and messages will keep informed during the proceedings.



There will be a 'completed' message after each panel download. You can go back to select other panels or close if you are finished downloading.

# Glossary

---

Many of the words or terms in this guide have more common definitions than used in industry. In this guide, we've used them specifically in the context of security access control. For this reason, the following glossary of terms defines these terms as used in this guide.

<b>Access Point</b>	A point of entry or exit, for an <u>area</u> whose access is controlled and monitored by Invision32™. (E.g. a door, parking gates.)
<b>Antipassback (APB)</b>	An <u>Access Control</u> feature designed to prevent improper usage of a valid card.
<b>Ethernet</b>	A widely used LAN developed by Xerox, Digital, and Intel. Ethernet networks connect up to 1,024 nodes at 10 megabits per second over twisted pair, coax, and optical fiber.
<b>Holiday</b>	Any days in which the regular weekly Invision32™ time group schedules are not appropriate. Statutory holidays and summer shut down periods are two examples. In Invision32™, <i>Holidays</i> may be assigned special irregular time group schedules that override the regular time group schedule for that day.
<b>Input</b>	Any field apparatus that provides information to an Invision32™ system with respect to conditions or status of a monitored component. Examples include door contacts, thermometers etc.
<b>Operator</b>	Any individual authorized to log-on to the Invision32™ system for purposes of data-entry or monitoring.
<b>Output</b>	Any field apparatus that receives commands from an Invision32™ system and executes the action specified in the command. (Examples include door locks, and lights.)
<b>PIN</b>	Personal Identification Number.
<b>RTE</b>	Request to exit.
<b>TAPI</b>	Telephony Application Programming Interface. TAPI is a Microsoft® Windows set of functions that allows programming of telephone line-based devices in a device-independent manner, giving personal telephony to users.
<b>TCP/IP</b>	Transfer Control Protocol/Internet Protocol. TCP/IP is the protocol that networks use to communicate with each other on the Internet.
<b>Time Group</b>	A <i>Time Group</i> (e.g., <i>Business Hours</i> ) is a pre-defined time slot/day combination that may be assigned to schedules, thereby governing how the Invision32™ system operates from day to day.

# License & Warranty

---

## Notice 1.01

This Software is licensed (**not sold**). It is licensed to sublicenses, including end-users, without either express or implied warranties of any kind on an “as is” basis. Camden Door Controls Inc. makes no express or implied warranties to sublicenses, including end-users, with regard to this software, including merchantability, fitness for any purpose or non-infringement of patents, copyrights, or any other proprietary rights of others. Camden Door Controls Inc. shall not have any liability or responsibility to sublicenses, including end-users for damages of any kind, including special, indirect or consequential damages arising out of or resulting from any program, services or materials made available hereunder or the or the modification thereof.

## Notice 1.02

Camden Door Controls Inc. makes no claim or warranty with respect to the fitness of any product or software for a specific application and assumes no responsibility for installation. This warranty is in lieu of all other warranties expressed or implied. No representative or agent of Camden Door Controls Inc. may make any other claims to the fitness of any product for any application.

# Reader Comments

---