

# Integra32™

*Integrated Alarm Monitoring  
and Access Control*

---

***USER MANUAL***

**Integra 32™**  
A SECURITY MANAGEMENT SOLUTION BY RBH

## Copyright Notice

---

Copyright© 1995 – 2022 by RBH Access Technologies 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 RBH Access Technologies Inc., Brampton, Ontario, Canada.

### **Trademark**

Integra32™ is the trademark of RBH Access Technologies 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 RBH Access Technologies Inc., nor its dealers or distributors shall be liable to any person or entity with respect to any liability, loss, nor damage, caused, or alleged to have been caused directly or indirectly by this information. Further RBH Access Technologies Inc. reserves the right to revise this publication, and to make changes to the content hereof from time to time, without the obligation of RBH Access Technologies Inc. to notify any person or organization of such revision or changes.

## **RBH ACCESS TECHNOLOGIES INC.**

2 Automatic Road, Suite 108  
Brampton, Ontario  
CANADA L6S 6K8

Tel: (905) 790-1515  
Fax: (905) 790-3680  
Email: [support@rbh-access.com](mailto:support@rbh-access.com)  
Web: [www.rbh-access.com](http://www.rbh-access.com)

Printing Date June 1, 2022

Integra32 Revision 5.0

# Table of Contents

---

<b>ABOUT THIS MANUAL .....</b>	<b>6</b>
BEFORE READING THIS MANUAL .....	6
CONVENTIONS IN THIS MANUAL .....	6
<b>CHAPTER 1 .....</b>	<b>7</b>
<b>INTRODUCING INTEGRA32™ .....</b>	<b>7</b>
INTEGRA32 SERVER CLIENT NETWORK SETUP .....	7
<b>CHAPTER 2 .....</b>	<b>8</b>
<b>GETTING TO KNOW INTEGRA32™ .....</b>	<b>8</b>
COMMAND BAR .....	8
Menu Options .....	9
Command Bar Buttons .....	16
DATABASE SETUP SCREEN .....	21
STATUS SCREEN .....	21
ALARM SCREEN .....	22
EVENT LOG SCREEN .....	22
<b>CHAPTER 3 .....</b>	<b>23</b>
<b>MONITOR SCREEN .....</b>	<b>23</b>
SYSTEM STATUS .....	23
HOW TO EXECUTE A COMMAND .....	23
COMMAND TYPE .....	23
Permanent .....	24
Semi-Permanent .....	24
Timed .....	24
ACCESS POINTS COMMANDS .....	25
Commands .....	25
INPUT POINTS COMMANDS .....	27
Commands .....	27
OUTPUT POINTS COMMANDS .....	28
Commands .....	28
PANELS COMMANDS .....	29
Commands Reader Panels .....	30
Commands PC100 (Summit) .....	31
Commands PC100 (Bosch/Risco/DSC) .....	32
IOC COMMANDS .....	32
AREA AND CARDHOLDER COMMANDS .....	33
Commands .....	33
VISITORS .....	33
FLOORS .....	34
<b>CHAPTER 4 .....</b>	<b>35</b>
<b>ALARM SCREEN .....</b>	<b>35</b>
ACKNOWLEDGE/UNACKNOWLEDGE/CLEAR .....	35
ALARM DETAILS .....	35
<b>CHAPTER 5 .....</b>	<b>38</b>
<b>PROGRAMMING .....</b>	<b>38</b>
INTEGRA32 DATABASE .....	38
Operators .....	38
Holidays .....	40
Schedules .....	41

<i>Areas</i> .....	43
<i>Messages</i> .....	44
<i>Networks</i> .....	45
<i>Panels</i> .....	48
<i>Access Points</i> .....	67
<i>Outputs</i> .....	83
<i>Elevators</i> .....	87
<i>Floor Groups</i> .....	88
<i>Access Levels</i> .....	90
<b>CHAPTER 6</b> .....	<b>93</b>
<b>CARDHOLDERS</b> .....	<b>93</b>
FIELDS AND OPTIONS .....	93
<i>File</i> .....	93
<i>Multi Cards</i> .....	95
<i>F Print</i> .....	96
<i>Receipt</i> .....	96
<i>Cards</i> .....	97
<i>Profile Tab</i> .....	100
<i>Photo Tab</i> .....	101
<i>Notes Tab</i> .....	102
<i>More Fields Tab</i> .....	103
<b>CHAPTER 7</b> .....	<b>106</b>
<b>VISITOR MANAGEMENT</b> .....	<b>106</b>
GENERAL .....	108
MORE FIELDS .....	109
<b>CHAPTER 8</b> .....	<b>113</b>
<b>REPORTS</b> .....	<b>113</b>
HISTORY REPORTS.....	113
<i>File</i> .....	113
<i>Reports</i> .....	114
<i>Preview</i> .....	114
DATABASE REPORTS .....	116
<i>Options</i> .....	116
<b>CHAPTER 9</b> .....	<b>119</b>
<b>OPTIONS</b> .....	<b>119</b>
SYSTEM OPTIONS .....	119
<i>General</i> .....	119
<i>Badge</i> .....	121
<i>Font</i> .....	122
<i>Email</i> .....	123
AP ACTIVITY .....	124
VISITOR CONFIGURATION .....	125
<i>Email Configuration</i> .....	125
<b>CHAPTER 10</b> .....	<b>127</b>
<b>LINKS</b> .....	<b>127</b>
GLOBAL LINKS .....	127
<b>CHAPTER 11</b> .....	<b>128</b>
<b>TOOLS</b> .....	<b>128</b>
BACKUP .....	128
<i>Run Backup Now</i> .....	128
<i>Configure Auto-Backup</i> .....	129

VOID CARDS .....	129
FINGER PRINT/QUERY FPR .....	130
BADGE TEMPLATE DESIGNER .....	130
CARD IMPORT .....	132
<i>Configure Import Utility</i> .....	132
<i>Run Import Utility</i> .....	140
<i>View Log File</i> .....	141
DEVICE DISCOVERY .....	142
SEARCH .....	142
<i>Controllers</i> .....	143
<i>Accessories</i> .....	143
<b>CHAPTER 12</b> .....	<b>144</b>
<b>PROGRAM GROUPS</b> .....	<b>144</b>
INTEGRA32™ SECURITY SYSTEM .....	144
<i>Integra32™ Security System</i> .....	145
<i>Integra32™ Data Restore</i> .....	146
<i>Integra32™ Database Maintenance</i> .....	146
<i>Integra32™ Firmware Upgrade</i> .....	146
<i>Integra32™ Server</i> .....	148
<b>GLOSSARY</b> .....	<b>149</b>
<b>LICENSE &amp; WARRANTY</b> .....	<b>150</b>
<b>INDEX</b> .....	<b>151</b>
<b>READER COMMENTS</b> .....	<b>154</b>

# About This Manual

---

This manual documents how to install and use the Integra32™ Security Management System as developed by RBH Access Technologies Inc. The **Integra32™** 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 **Integra32™** with a minimal amount of training.

Read this manual if you are:

- ◆ An operator who monitors security and access using Integra32™.
- ◆ A system administrator who updates Integra32™'s database.
- ◆ The system technician that installs and configures the Integra32™ onsite.

## Before reading this manual

This manual 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 manual

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”.

*Cross-references* are displayed in [blue](#), and will take you to the associated or mentioned part of the manual. **Ctrl + Click** on the *cross-reference* when the curser changes to move to that place in the manual.

# Chapter 1

## Introducing Integra32™

---

The Integra32™ system integrates Access Control, Photo-Badging, Digital Video Recording and Alarm Monitoring into an elegant building management and security system specifically designed for the smaller application

Integra32™'s 32-bit software architecture together with, Windows 10, Windows 11, Windows Server 2012R2, Windows Server 2016, Windows Server 2019 and Windows Server 2022 operating system ensures that security management needs are met easily and economically with a minimal amount of training.

The IRC-2000 Intelligent Field Panels utilize flash firmware for easy upgrades. This panel uses fully distributed intelligence for off-line operations. In addition to supporting two card readers, each IRC-2000 Intelligent Field Panel also has eight fully supervised alarm inputs along with eight outputs. The IRC2000's memory has been increased to now hold 5,000 card and can be further extended to hold 8,000 cards.

One of the alternate panel URC2000 can be used along with or instead of the original IRC2000. This panel also uses fully distributed intelligence for off-line operations. In addition to supporting two card readers, each URC-2000 panel has four fully supervised alarm inputs and four outputs as well as a 3,000 card capacity. Communication is handle through an RS485 port.

Another alternate panel the UNC100 can be used along with or instead of the other two panels. This panel also uses fully distributed intelligence for off-line operations. In addition to supporting two card readers, each UNC100 panel has four fully supervised alarm inputs and four outputs as well as a 8000 card capacity. Communication is handle through an RS485 port.

### Integra32 Server Client Network Setup

Please see technical document TB95\_InstallIntegra32r5.0 for a step-by-step guide to installing Integra32™.

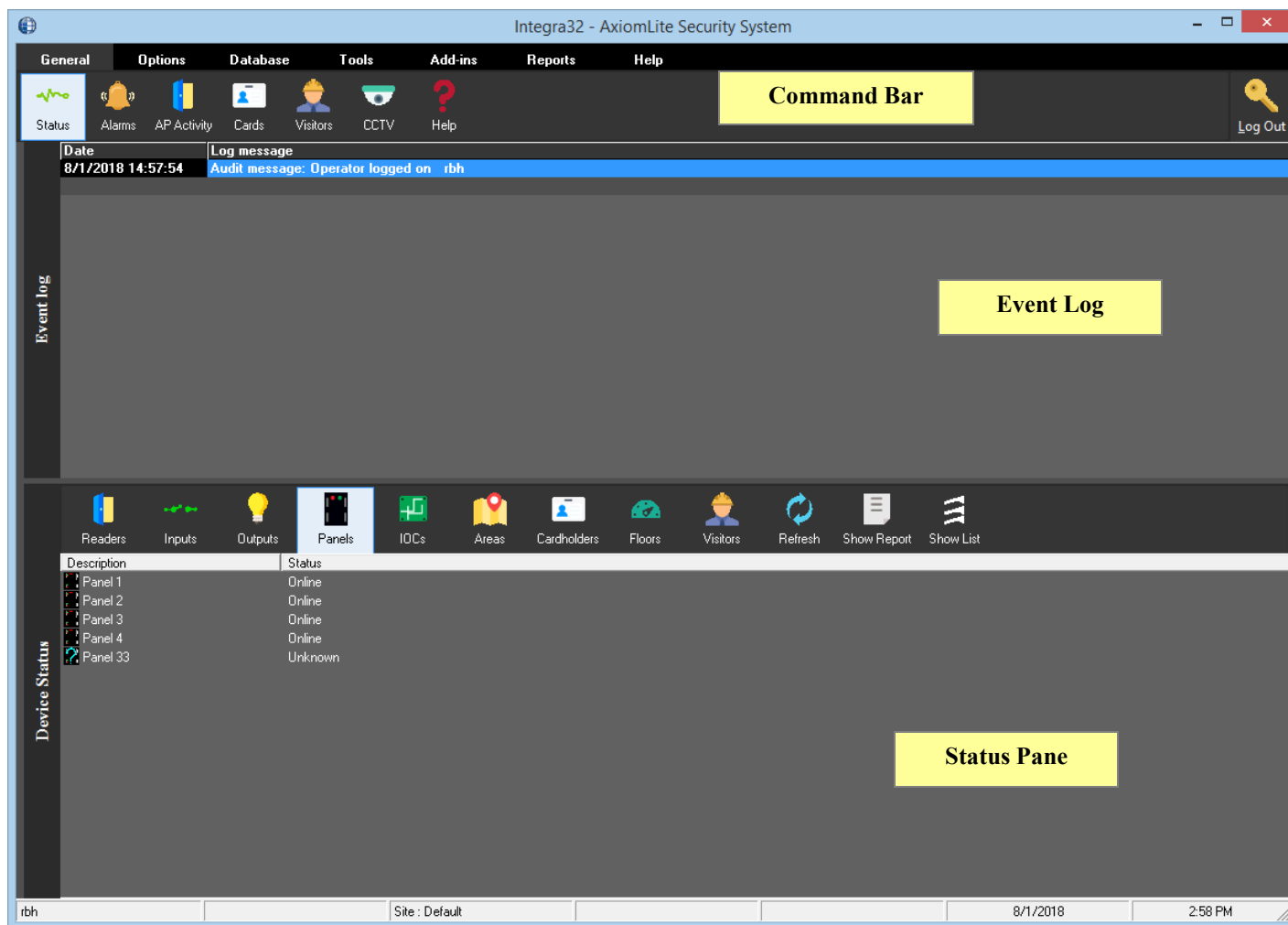


**In order for a remote client to connect to the server, the server must first be running. This should not be a problem since the Integra32 server runs as a service and should be running at all times.**

## Chapter 2

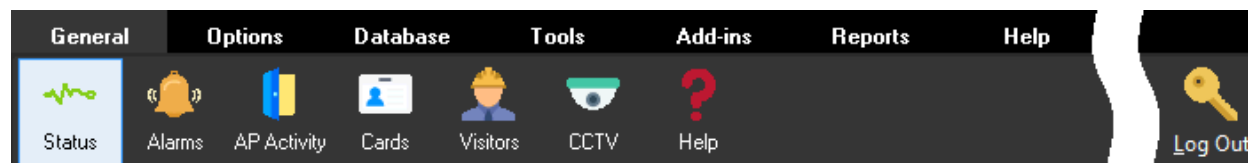
# Getting to Know Integra32™

Integra32™ lets you manage and monitor all your security access needs using a standard PC. There are three separate parts to the Integra32's™ main screen:



## Command Bar

Menus and buttons to access other features of the system are available on the *Command Bar*. Integra32™ has the following menu options:





Each of these selections has a set of buttons that "launch" functions contained in new windows (e.g. Cardholder window).



### **Log In & Out (Alt+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.

Connect to Server

**Axiom Lite Integra** v5.1.10

Login Name:

Password:

Server:

Ok Cancel

To log in, enter your full login Name and password. The default login name is "rbh" and default password is "password". 'Login Name' is not case sensitive, but 'Password' is.

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

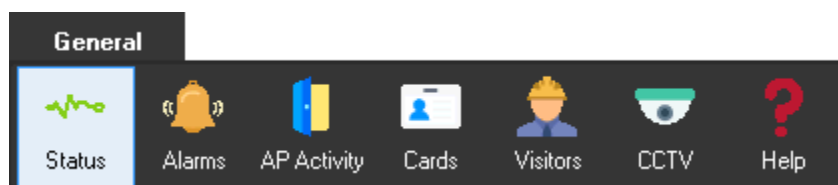


### **Exit**

Exit will shut down the Integra32™ System Client software.

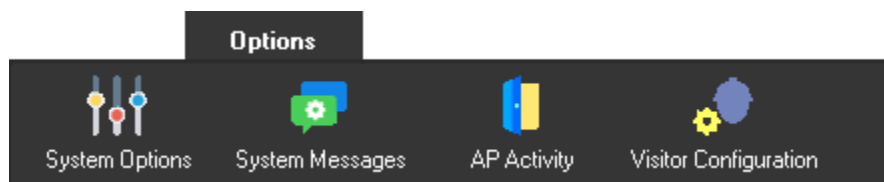
## **Menu Options**

### **General**



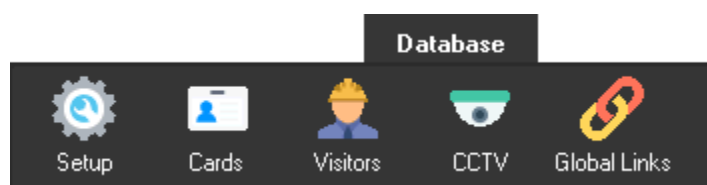
The General option has the main selection an operator should require; the [Status Screen](#), the [Alarm Screen](#), [Access Point Activity \(AP Activity\)](#), the [Cardholders](#) Screen, the [Visitor Management](#) screen, the [CCTV](#) screen, and the [Help](#) screen.

## Options



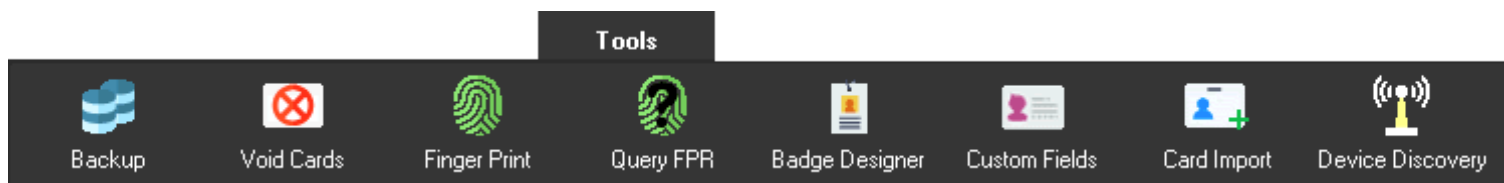
Use this menu option to customize user preferences *through* [System Options](#) or customize the [System Messages](#) that are displayed on the Status Screen and in the History Reports. The Access Point Activity window is also enabled here. Details of the [AP Activity](#) window option will be discussed in Chapter 9. Visitor Management configuration is accessed by selecting [Visitor Configuration](#)<sup>1</sup>.

## Database



This menu option has configuration selections; [Database Setup Screen](#), [Error! Reference source not found.](#), [Visitor Management](#), [CCTV](#), and [Global Links](#).

## Tools



The *Tools* menu gives the options for [Backup](#), [Void Cards](#), [Finger Print](#)<sup>2</sup>, [Error! Reference source not found.](#)<sup>2</sup>, [Badge Template Designer](#)<sup>3</sup>,

[Card Custom Fields](#), [Card Import](#)<sup>4</sup>, and [Device Discovery](#) which are covered in more detail in [Chapter 11](#).

<sup>1</sup> This selection is only available if the optional license for the Visitor System has been purchased and installed.

<sup>2</sup> This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.

<sup>3</sup> This selection is only available if the optional license for the Badging Software has been purchased and installed.

<sup>4</sup> This selection is only available if the optional license for the Card Import Utility has been purchased and installed.

## Add-ins



Both [CCTV-RBHView](#) and [Visitor Module](#) are additions that require the appropriate licensing to use and opens Presentations slides for requested module.

## Reports



Use this menu option to customize and generate [History Reports](#), [Database Reports](#), and [Visitor Reports](#)<sup>5</sup>.

### ***History Reports***

Reports are explained later in [Chapter 8](#).

### ***Database Reports***

Reports are explained later in [Chapter 8](#).

### ***Visitors Reports***

Reports are explained later in [Chapter 8](#).

## Help

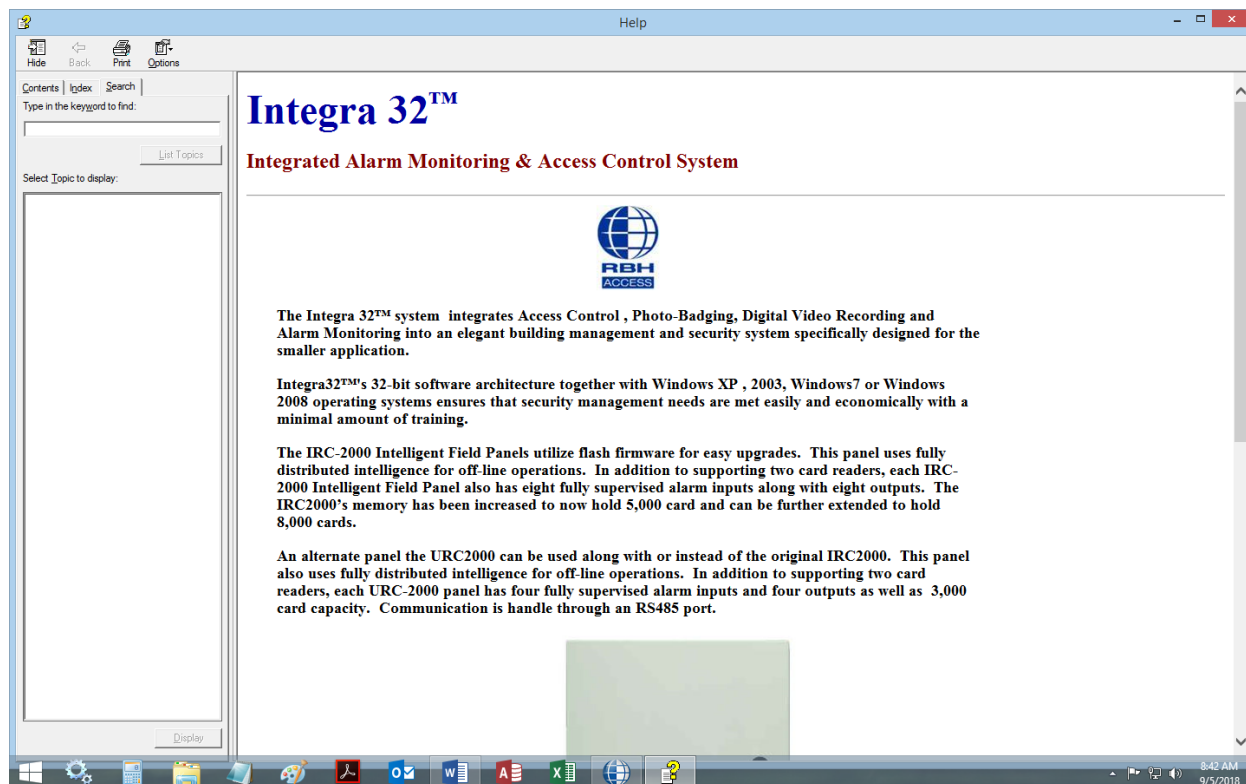


Use this menu option to go to online Help by clicking on *Contents*, display information regarding your Integra32™ software version, as well as dealer information by clicking on *About*. The licensing of the software is done through *Register* and *Activate*.

---

<sup>5</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

## Contents



Use *Contents* to search for the information you require.

### ***Contents***

You can browse through the online manual for the information you require.

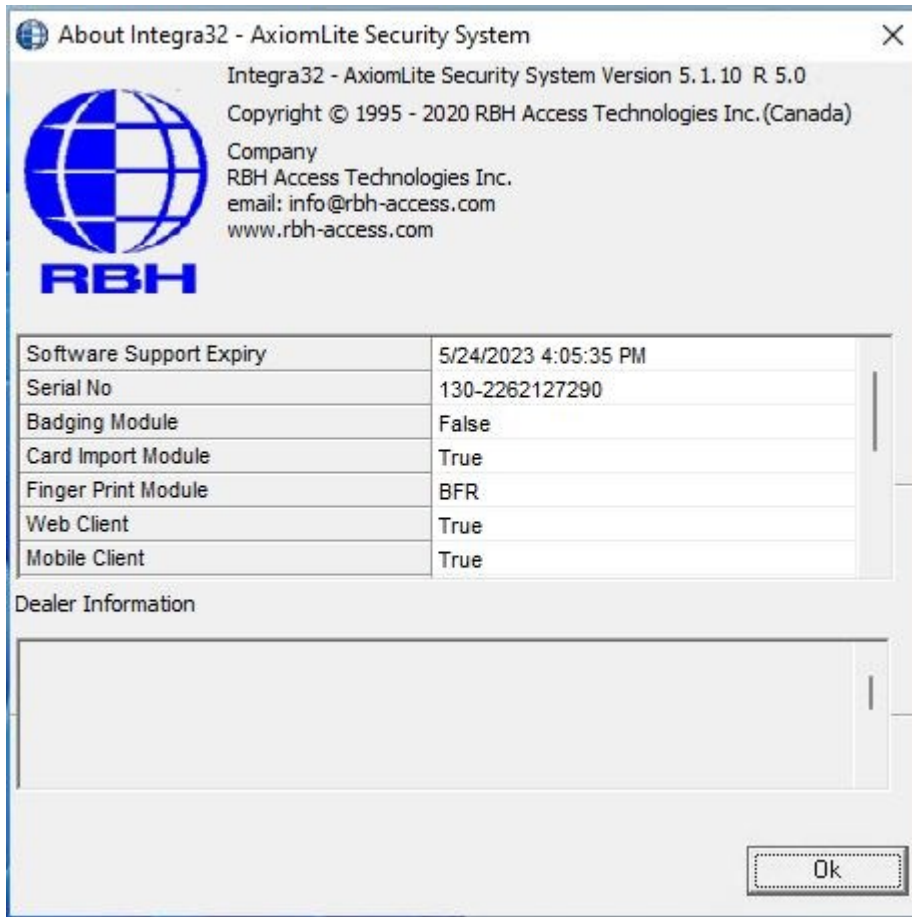
### ***Index***

Select from a list of the most popular topics for the information you require.

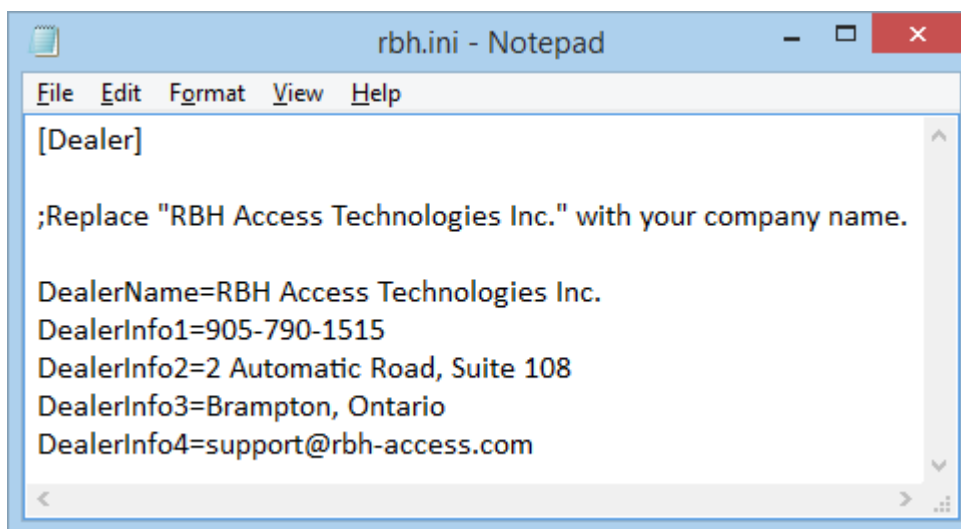
### ***Search***

Enter a keyword to provide a list of selections to help you find the information you require.

## About



Create a text file in the site folder (e.g. default) named `rbh.ini` (as shown below) to display **Dealer information** in the *About* screen. Up to nine lines of information (`DealerInfo#`) can be included.



## Activation

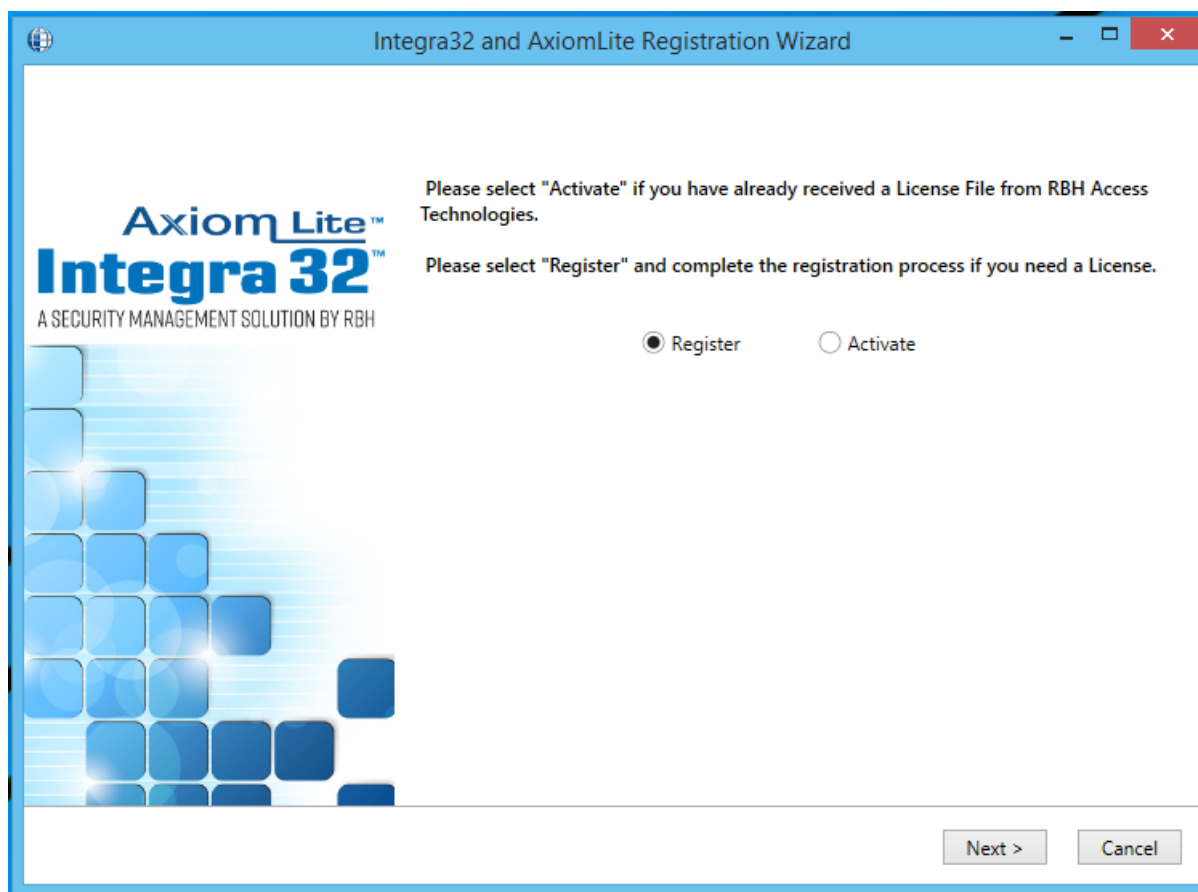
After your software has been registered you will receive an Activation File.



Follow the online instructions to activate your software with all its licenses.

## Registration

The software must be registered in order to enable the Badging software, the Card Import Utility, the Finger Print Reader, the CCTV integration software, and/or the Visitor Management System. None of these features will be accessible or even visible if the license hasn't been registered. Only the feature ordered will be included on a license.



Follow the on screen instructions. Fill in the site information and the dealer information. Optionally you may include the distributor information as well. Once completed you can email the information directly or you can save the attachment to email latter.

## Command Bar Buttons

### General



#### **Login/Logout**

Press this button to log in or log out of Integra32™ system.



#### **System Status**

Press this button to change the *Monitor Screen* to display the status of access points, inputs, outputs, and panels.



#### **Alarms**

Press this button to change the *Status Screen* to display alarm messages, time and date of alarm and operator ID. This change will take place automatically when an Alarm Event occurs.



#### **AP Activity**

Press this button to toggle on and off the *Access Point Activity* screen pop-up.



#### **Cards**

Press this button to launch Integra32™'s *Cardholder* window to program new cards or edit existing cards.



#### **Visitors<sup>6</sup>**

Press this button to launch the Integra32™'s *Visitor* window to administer visitors in the system.



#### **CCTV<sup>7</sup>**

Press this button to launch the *CCTV Configuration* screen.

---

<sup>6</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

<sup>7</sup> This selection is only available if the optional license for the CCTV system has been purchased and installed.



**Help**

Press this button to get online *Help*.

**Options****System Options**

*System Options* will allow you to custom configure your system by enabling you to change things like ‘number of day to keep Event History’ or ‘keyboard timeout’. Other system related options can also be configured under this selection.

**System Messages**

Press this button to configure where messages are send. Messages can be sent to the *Event Log Screen*, to the *History Log*, to a *Printer*, or to ...

**AP Activity**

Press this button to toggle on and off the *Access Point Activity* screen pop-up.

**Visitor Configuration**

Press this button to launch the *Visitor Configuration* screen.

**Database****Setup**

Press this button to access the system *Setup* screen.

**Cards**

Press this button to launch the *Cardholder* configuration screen.

**Visitors**

Press this button to launch the *Visitor Management* screen.

**CCTV**

Press this button to launch the *CCTV Configuration* screen.

**Global Links**

Press this button to launch the *Global Links Configuration* screen.

**Tools****Backup**

Press this button to configure and run *Backups*.

**Void Cards**

Press this button to launch the *Void Card Utility*.

**Finger Print**

Press this button to launch the *Finger Print* reader configuration screen.

**Query FPR**

Press this button to launch the *Finger Print Reader* query screen.

**Badge Designer**

Press this button to launch the *Badge Template Designer*.

**Custom Fields**

Press this button to launch the Cardholder *Custom Fields* configuration screen.

**Card Import**

Press this button to launch the *Card Import Utility*.



### **Device Discovery**

Press this button to launch the *RBH IP Locator* Utility.

## **Add-ins**



### **CCTV-RBH View**

Press this button to learn how to configure CCTV-RBH View through this Video.



### **Visitors Module**

Press this button to learn how to configure Visitor module through this Video.

## **Reports**



### **History Reports**

This button will open the History Report screen.



### **Database Reports**

This button will open the Database Report screen.



### **Visitor Reports**

This button will open the Visitor Report screen.

## **Help**



### **Contents**

Press this button to get online *Help*.



### **About**

Clicking on *About* will display information regarding your Integra32™ software version as well as dealer information.



### ***Activate***

Press this button to go the screen to *Activate* your Integra32™ software's warranty extension/options

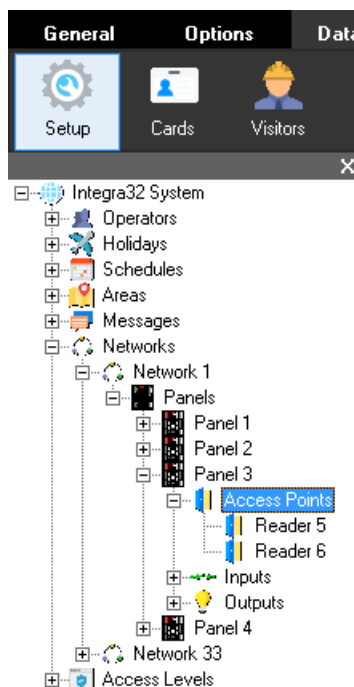


### ***Register***

Press this button to go the screen to *Register* your Integra32™ software.

## Database Setup Screen

The system is configured for a particular installation from this screen. Setup and programming of hardware devices (e.g. IRC-2000), and programming of all records such as, access levels, schedules, and holidays are done here, with the exception of cardholders.



Up to thirty-two networks can be configured and up to thirty-two panels can be configured, for each Integra32™ system. These panels can be distributed across the thirty-two networks, as you like with no more than sixteen panels on any one network. A maximum of thirty schedules, each with up to eight periods, can be added to the existing schedules (*Never* and *Always*). The system is capable of handling up to forty holidays and one hundred messages.

## Status Screen

This screen gives the operator control of the system through Operator Commands, and it provides viewing of the status of the items that have been selected (e.g. *Access Points*, *Input Points*, and *Output Points*).

	Readers	Inputs	Outputs	Panels	IOCs	Areas	Cardholders	Floors	Visitors	Refresh	Semi-permanent	Show Report	Show List
Device Status	Description	Status	Cardnumber	Checked In									
	Output 1	Off											
	Output 2	Off											
	Output 3	On											
	Output 4	On											
	Output A	Off											
	Output B	Off											
	Output C	On											
	Output D	Off											
	Output 5	Off											

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 *Status Screen*. From here alarms are acknowledged and cleared.

Alarms	Date	Alarm message	Operator
	8/16/2018 15:35:36	Input: In alarm Input 6 Panel 2 (128)	rbh
	8/16/2018 15:36:02	Input: In alarm Input 6 Panel 2 (128)	

Instruction messages can be obtained from the *Alarm Details* by double clicking or by the right click menu on the alarm messages, and actions taken can be noted there as well.

## Event Log Screen

This screen displays all system activity such as cardholder activity, input activity, output activity and panel activity. All system messages are also displayed here.

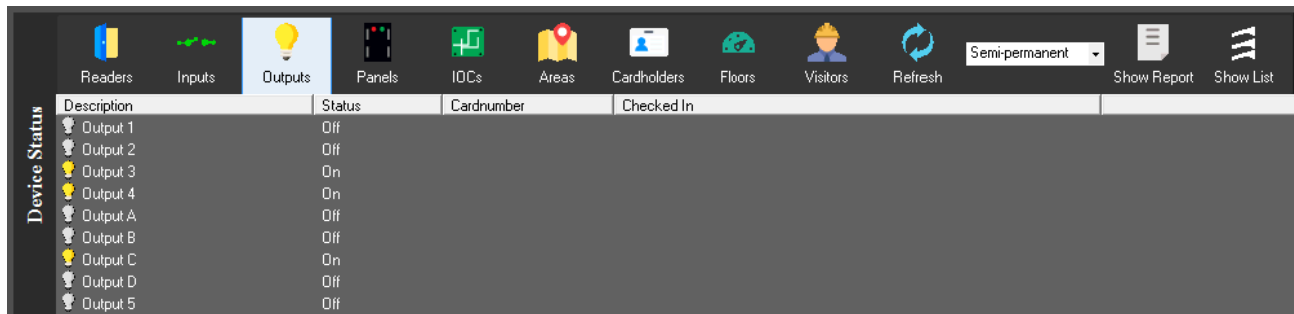
Event log	Date	Log message
	8/16/2018 16:03:48	Audit message: Alarm cleared
	8/16/2018 16:03:49	Audit message: Alarm cleared
	8/16/2018 16:04:28	Access granted: Card Oswald Boelke (41042) Reader 3 Panel 2
	8/16/2018 16:04:37	Access granted: Card Ernst Udet (2384) Reader 3 Panel 2
	8/16/2018 16:04:54	Access granted: RTE Reader 6 Panel 3
	8/16/2018 16:05:08	Access granted: Card Max Immelmann (53071) Reader 3 Panel 2
	8/16/2018 16:05:34	Input: In alarm Input 3 Panel 1
	8/16/2018 16:05:34	Output: On by link Output 3 Panel 1
	8/16/2018 16:05:36	Input: Restore Input 3 Panel 1
	8/16/2018 16:05:36	Output: Off by link Output 3 Panel 1

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 *Device Status Pane* the operator can issue commands, as well as view status. Commands can be sent to access points, inputs, outputs, and panels. Areas can be cleared and cardholders can have their area set or cleared.



### System Status

Clicking on the *Status* button on the toolbar of the main screen will change the *Alarm Screen* to the *Monitor Screen* or the *System Status Pane*. From the *System Status Pane* 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 seven buttons will bring up Readers, Inputs, Outputs, Panels, IOCs, Areas, and Cardholders respectively. Floors and Visitor buttons are also available here. *Refresh* is used to update/verify the status of the items shown. The Status of the selected items can be shown either in *List View* or *Report View*. The next two buttons

### 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 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 6:00 p.m. to 8:00 a.m. 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 6:00 p.m. and 8:00 a.m., if a semi-permanent command is issued at 4:00 p.m. to arm the door, the command is executed. The scheduled operation remains unaffected and on the next day at 8:00 a.m. the door will disarm and revert to the normal arming schedule.

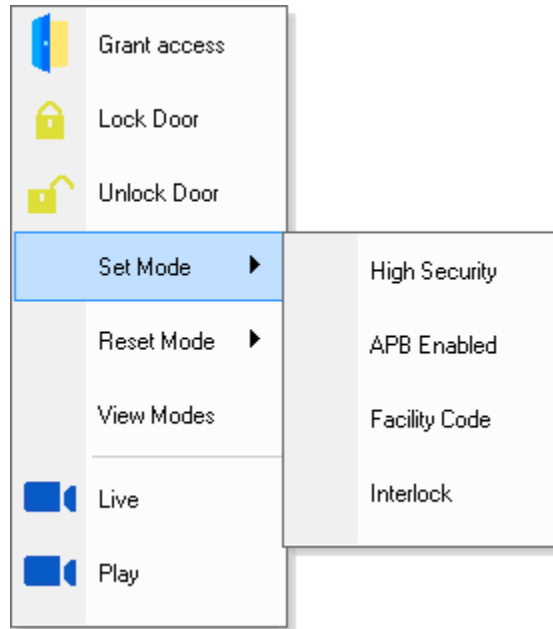
## ***Timed***

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



## Access Points Commands

Clicking the *Reader* button on the *Command Toolbar* depicts the status of Access points on the *Device Status 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 group of access points on a permanent, semi-permanent, or timed basis.



#### Unlock

Unlock an access point or group of access points 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.



Select *Live* to display live video from the CCTV camera associated with the selected access point.



*Play* will bring up a CCTV history selection screen so that video connected to an event for the chosen access point can be played back.

---

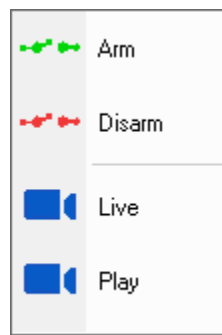
<sup>8</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.

<sup>9</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.

History				
Date	Message	Device	Card Holder	Play
7/21/2011 4:19:19 PM	Access point-Forced entry alarm	Reader 1test email, Panel 76-1		
7/21/2011 4:19:15 PM	Access point-Forced entry alarm	Reader 1test email, Panel 76-1		
7/21/2011 4:19:13 PM	Access point-Forced entry alarm	Reader 1test email, Panel 76-1		
7/21/2011 3:41:16 PM	Access granted-Operator	Reader 1test email, Panel 76-1		
7/21/2011 3:40:07 PM	Access granted-Operator	Reader 1test email, Panel 76-1		
7/21/2011 3:37:58 PM	Access granted-Operator	Reader 1test email, Panel 76-1		
7/21/2011 3:36:53 PM	Access point-Forced entry alarm	Reader 1test email, Panel 76-1		
7/21/2011 3:33:38 PM	Access granted-Operator	Reader 1test email, Panel 76-1		
6/17/2011 4:22:33 PM	Access point-Door not open	Reader 1test email, Panel 76-1		
6/17/2011 4:22:30 PM	Access granted-Card	Reader 1test email, Panel 76-1	Kanty Riarh	

## Input Points Commands

Clicking the *Input* button on the *Command Toolbar* depicts the status of input points on the *Device Status Screen*.



The following commands for Inputs are available by right clicking the selected Input(s).

### 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*.



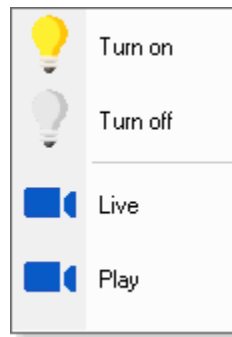
Select *Live* to display live video from the CCTV camera associated with the selected input point.



*Play* will bring up a CCTV history selection screen so that video connected to an event for the chosen input point can be played back.

## Output Points Commands

Clicking the *Output* button on the *Command Toolbar* depicts the status of output points on the *Device Status Screen*.



The following commands for outputs are available by right clicking the selected *Output*.

### Commands



Turn on an output.



Turn off an output.



Select *Live* to display live video from the CCTV camera associated with the selected output point.

---

<sup>10</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.

<sup>11</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.

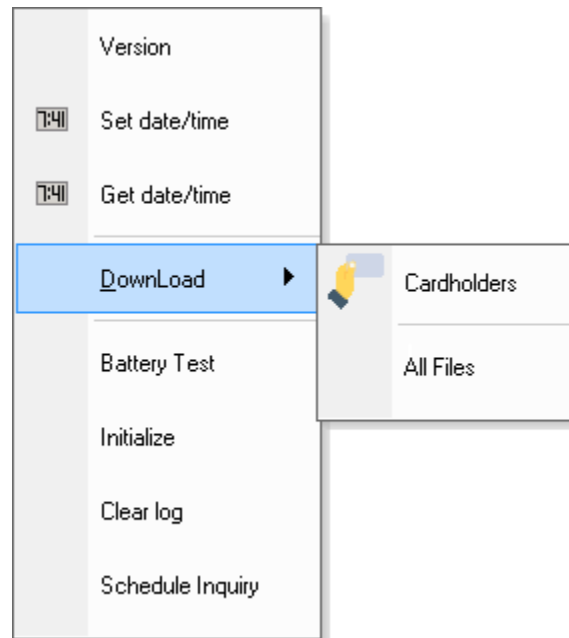
<sup>12</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.



*Play* will bring up a CCTV history selection screen so that video connected to an event for the chosen output point can be played back.

## Panels Commands

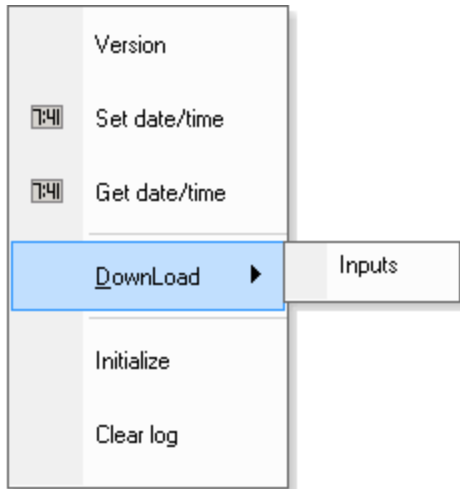
Clicking the *Panels* button on the *Command Toolbar* depicts the status of panels on the *Device Status Screen*.



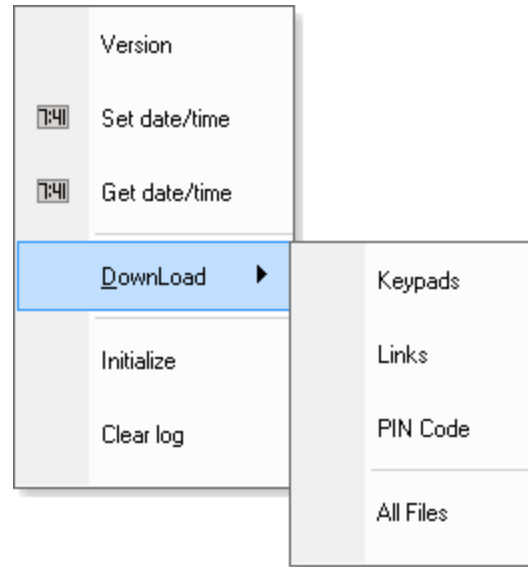
### Reader Panels

---

<sup>13</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.



**PC100 (Summit)**



**PC100 (Risco, Bosch or DSC-IT)**

## Commands Reader Panels

The following commands for panels are available by right clicking the selected reader panel(s).

### Version

The *Version* queries all or selected reader panel 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 reader panel.
- 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 panel's memory from the database on the server. Select *Cardholder* files to download or select the *All Files* option to download all files.

Download messages are posted to the log as files are sent. 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*. Panel download does not execute itself; after the panel comes back online have manually re-start the download on that panel.**

## Reset

The *Reset* option initializes the panel.

## Clear Log

The *Clear Log* option clears the event log of selected controller(s). 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.

## Commands PC100 (Summit)

The following commands for panels are available by right clicking the selected PC100 (Summit) panel.

## Version

The *Version* queries the selected PC100 for the firmware version it is 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 PC-100
- The *Close* button is used to close the *Set Panel Date/Time Window*.



## Get Date/Time

This command queries the PC100 for its current date and time, and displays it on the *Log Screen*.

## Download

The *Download* function allows the operator to manually repopulate the PC100 memory from the database on the server. Click on '*Inputs*' to download the data.

Download messages are posted to the log as files are sent, verifying the number of records sent for the file.



**If the panel is offline at the time of the download any files that fail to download will be logged on the *Log Screen*. Panel download does not execute itself; after the panel comes back online have manually re-start the download on that panel.**

## Commands PC100 (Bosch/Risco/DSC)

The following commands for panels are available by right clicking the selected PC100 (Bosch/Risco/DSC) panel.

### Version

The *Version* queries the selected PC100 for the firmware version it is 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 PC-100
- The *Close* button is used to close the *Set Panel Date/Time Window*.



### Get Date/Time

This command queries the PC100 for its current date and time, and displays it on the *Log Screen*.

### Download

The *Download* function allows the operator to manually repopulate the PC100 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.

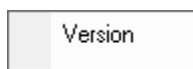
Download messages are posted to the log as files are sent, verifying the number of records sent in each file.



**If the panel is offline at the time of the download any files that fail to download will be logged on the *Log Screen*. Panel download does not execute itself; after the panel comes back online have manually re-start the download on that panel.**

## IOC Commands

Clicking the *IOC* button on the *Command Toolbar* depicts the status of IOC boards on the *Device Status Screen*.





## Version

The *Version* queries the selected IOC board for the firmware version it is running. The version number 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.



The following commands for cardholders 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.



#### Print

The Print command will produce a printed report showing the data provided in the status pane. It will show all of the cardholders displayed and the areas they are in.

## Visitors<sup>14</sup>

Clicking the *Visitors* button on the *Command Toolbar* will display the visiting cardholders and who they are visiting.

---

<sup>14</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

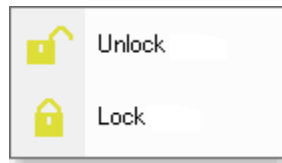


## **Check Out**

Click *Check Out* to check-out the selected visitor.

## **Floors**

Clicking the *Floors* button on the *Command Toolbar* depicts the status of floor outputs on the *Device Status Screen*.



## **Unlock**

*Unlock* will release the floor button in the cab so that anyone may access the floor.

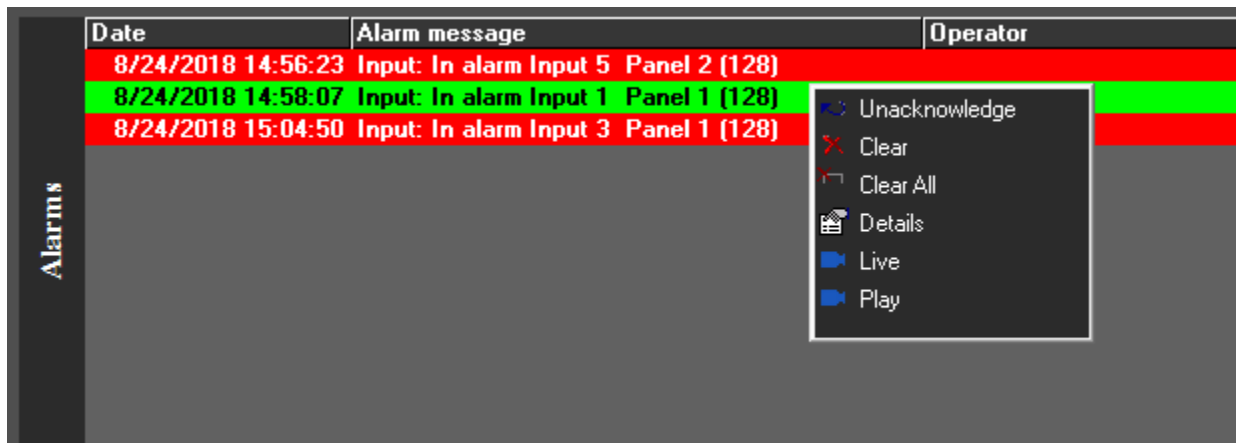
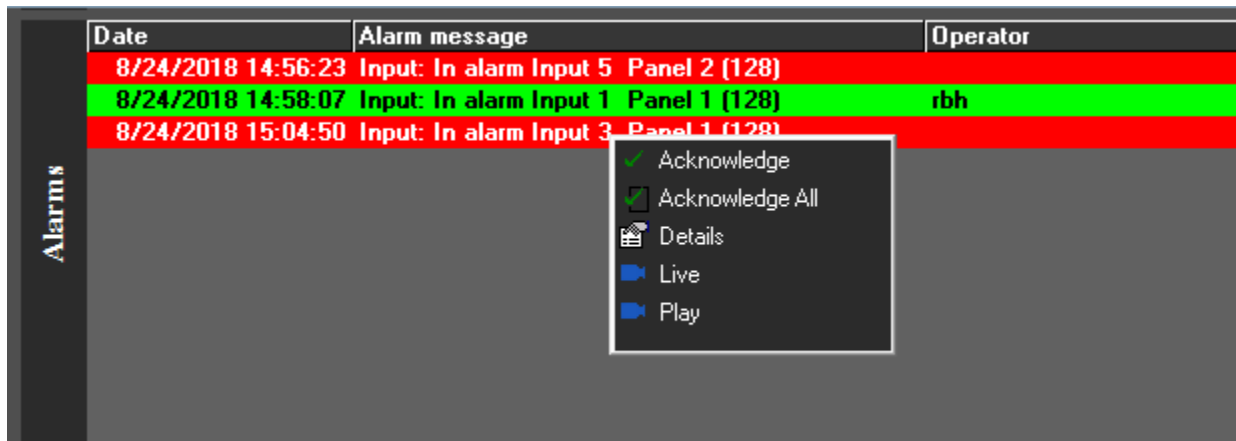
## **Lock**

*Lock* will energize the floor output and disconnect the floor button in the cab. A card with the appropriate access level can release the floor temporarily.

# 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.



### Acknowledge/Unacknowledge/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 clear or unacknowledge the alarm. Once an alarm is acknowledged, only the operator that acknowledged that alarm can 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

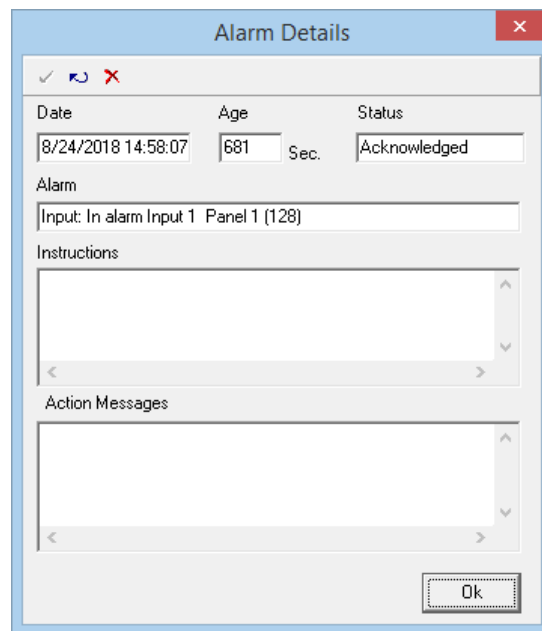
Alarm provides a description of the alarm.

## 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 dialog box titled "Alarm Details" with a close button (X) in the top right corner. Inside the dialog, there are several sections: a header bar with checkmark, refresh, and delete icons; a table with columns "Date", "Age", and "Status"; an "Alarm" section with a text field; an "Instructions" section with a scrollable text area; and an "Action Messages" section with a scrollable text area. At the bottom right is an "Ok" button.

Date	Age	Status
8/24/2018 14:58:07	681 Sec.	Acknowledged

Alarm  
Input: In alarm Input 1 Panel 1 (128)

Instructions

Action Messages

Ok



## Acknowledge

*Acknowledge* the highlighted alarm with this selection.



## Acknowledge All

*Acknowledge all* of the alarms in the Alarm Window with this selection.

## **Unacknowledge**

*Unacknowledge* the highlighted alarm with this selection.

## **Clear**

*Clear* the highlighted acknowledged alarm with this selection.

## **Clear All**

*Clear all* of the acknowledged alarms in the Alarm Window with this selection.

## **Live<sup>15</sup>**

Select *Live* to display live video from the CCTV camera associated with the selected alarm event.

## **Play<sup>16</sup>**

*Play* will play back the video connected to the selected alarm event for the chosen time period configured in CCTV tab.

---

<sup>15</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.

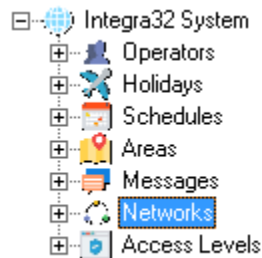
<sup>16</sup> This selection is only available if the optional license for the CCTV Software has been purchased and installed.

# Chapter 5

## Programming

---

Click on the + sign to expand the tree view of your Integra32™ 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 on the different selections will bring up small menus. 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.**

## Integra32 Database

### Operators

The Integra32™ system comes with user 'rbh' by default, with password 'password'. Additional Users/Operators can be added and configured in the *Database Screen*.

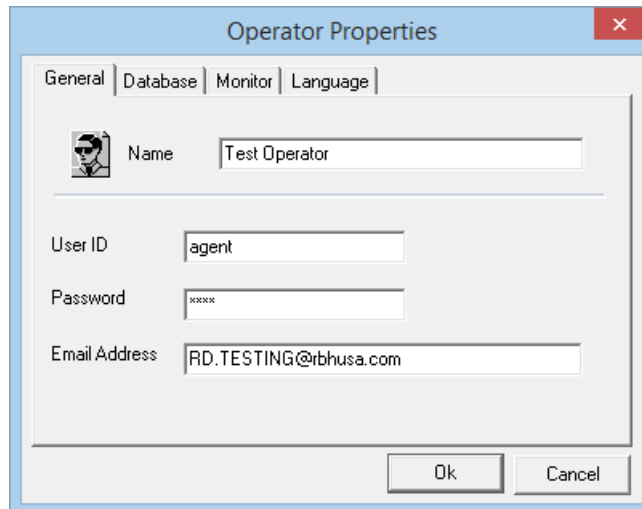


### General

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

Email Address is used by the message server to send the emails for Access point messages configured in Access Point Properties to send the email.

For more information, see page [72](#) (Message server service should be running for this functionality to work)



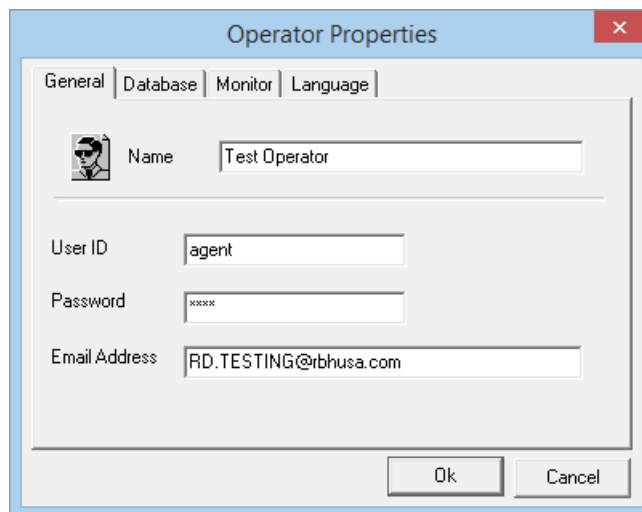
The image shows the 'Operator Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a close button (X). Inside, there are four tabs: 'General', 'Database', 'Monitor', and 'Language'. The 'General' tab contains the following fields:

- Name:** Test Operator
- User ID:** agent
- Password:** (masked with asterisks)
- Email Address:** RD.TESTING@rbhusa.com

At the bottom right, there are 'Ok' and 'Cancel' buttons.

## Database

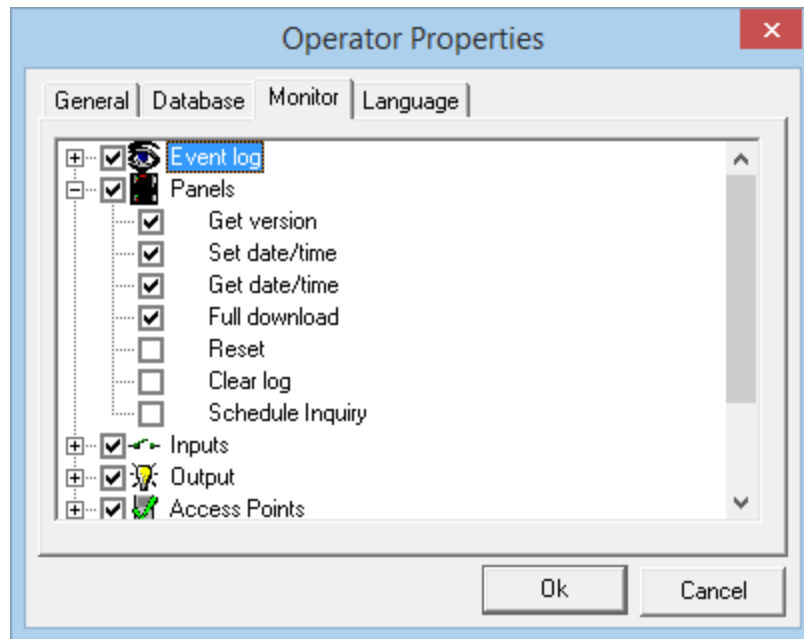
The access to database can be defined/changed in the *Database* tab. Access to each module of the database can be chosen as 'No Access', 'Read Only', or 'Read & Write'. (For some items 'Read Only' access may not be relevant. If 'Read Only' access is selected for these items their access will actually be 'Read & Write'.)



This image is identical to the one above, showing the 'Operator Properties' dialog box with the 'General' tab selected. The fields and values are the same: Name (Test Operator), User ID (agent), Password (masked), and Email Address (RD.TESTING@rbhusa.com).

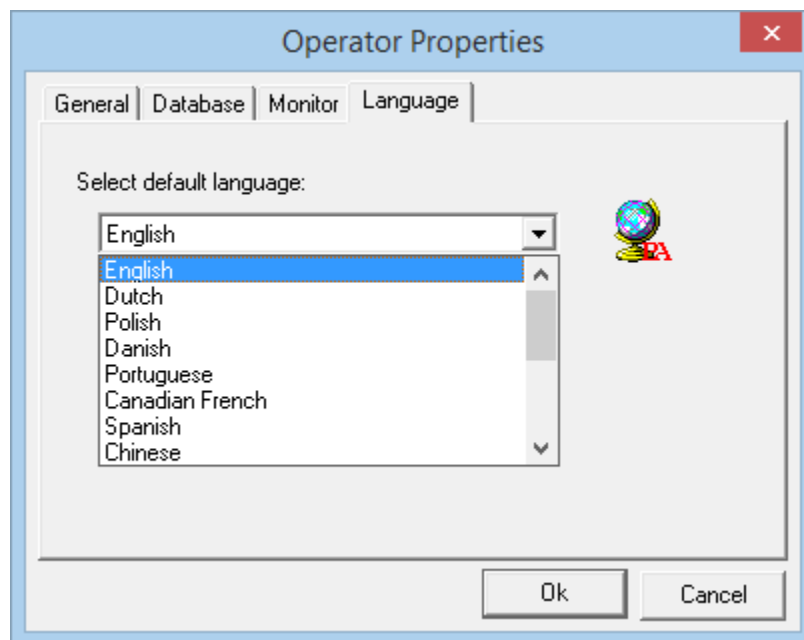
## Monitor

Access to commands allowed 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

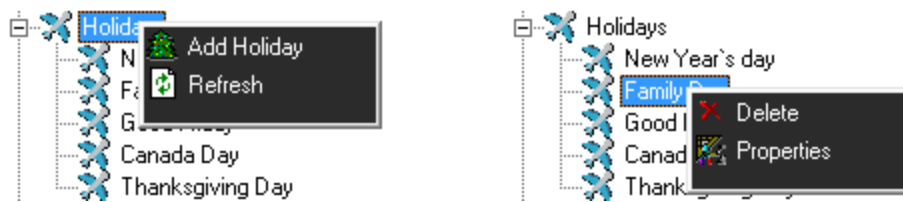
The language the system will operate in, for this operator, is selected in the *Language* tab.



## Holidays

Up to forty holidays can be assigned.





You can edit/create the name of a holiday and the date(s) of a holiday in the *Holiday Properties*. You can select a *Start Date* for the holiday and an *End Date* for the holiday. Any date designated as a holiday, will replace the regular day of the week for the day specified. (E.g. Good Friday 6 April, 2012 as far as schedules are concerned this day will not be a Friday it will be H1.)

Start and end times can also be specified for the holidays. In the example shown below the holiday starts on 24 December 2018 at noon. Up until noon the day is Monday, at noon the day becomes H1. The holiday remains until 10:00am on 27 December 2018 when the day of the week changes from H1 to Thursday.

## Schedules

Before cardholders are entered, any additional *Time Groups* that are required should be programmed. Up to thirty-two schedules can be programmed for Integra32™ system.



## General

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

## Time Zones

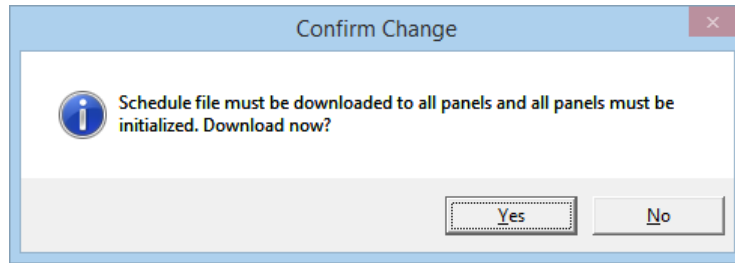
Program the Time Zones for the New Schedule in the Time Zones tab of the Schedule Properties Window.

	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H 1
Period 1:	0000	0700		✓	✓	✓	✓	✓		
Period 2:	0000	2400	✓						✓	✓
Period 3:	1800	2400		✓	✓	✓	✓	✓		
Period 4:	0000	0000								
Period 5:	0000	0000								
Period 6:	0000	0000								
Period 7:	0000	0000								
Period 8:	0000	0000								

Ok Cancel

1. Eight time periods can be programmed.
2. Click to check or uncheck a day for the period.
3. End time must be later than start time.
4. Valid times are from 00:00 to 24:00, (even though 24:00 is never actually reached [it represents the end of the day]).
5. 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.
6. *H1* is checked if selected period should be active on *Holidays* programmed in the system as well.

After you create a new schedule, edit an existing schedule, or delete a schedule, you will be asked if the changes are to be downloaded and the panel initialized now or will it be done later.



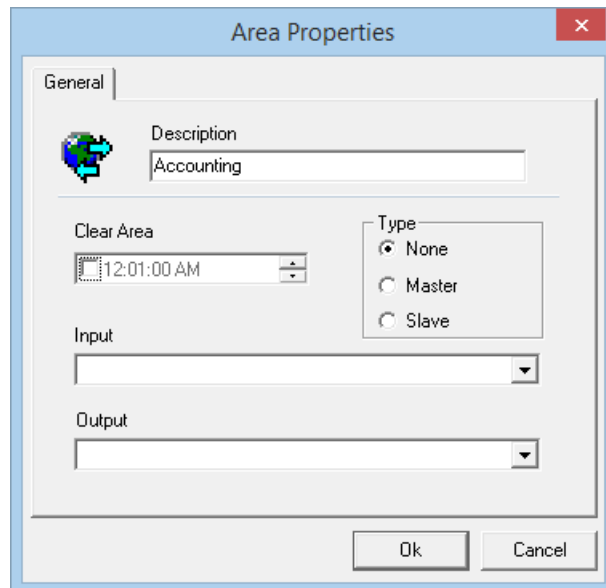
## Areas



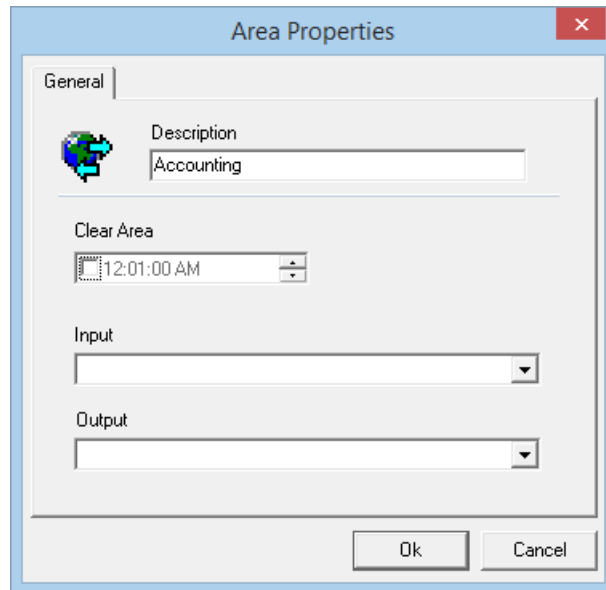
In the *Area Properties* window the name of the area is entered. Access points from which a cardholder can enter or exit the area define the actual area. A 'Clear Area' time can also be entered here. As well an input and an output (both general purpose) can be chosen. To print out a report of all the cardholders in the area simply put the input into alarm. The output will Turn ON automatically when there are no cardholders in the area, it must be turned off manually (operator command).



**A new selection 'Type' is added for an optional (License is required) Antipassback functionality. (See TB67 Integra32 Area Type GAPB)**



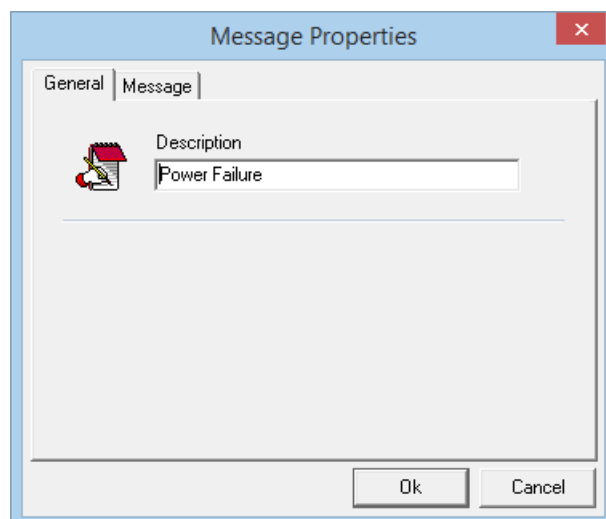
- **If no license for *Area Type* Global APB, *Type* option will not be available in Area configuration.**



## 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.

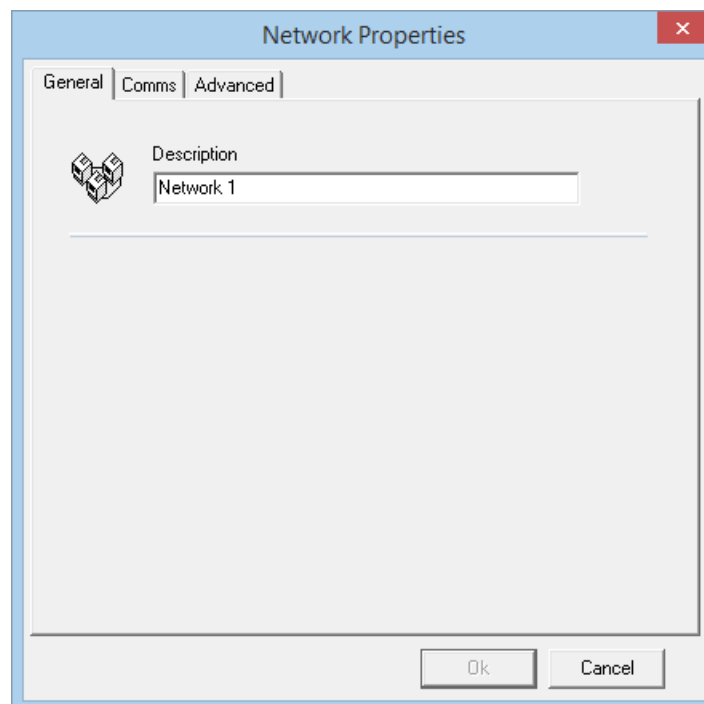
## Networks

Up to thirty two networks can be connected on the Integra32™ 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*.



## General

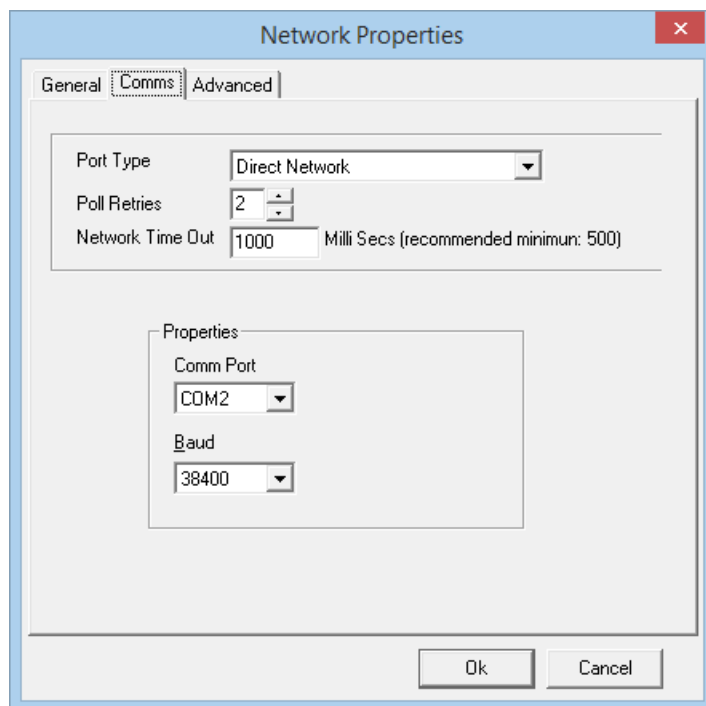
Under the *General* tab of the *Networks Properties Window* network descriptions can be edited.



## Comms

### Direct Connect

The controller network (*IRC-2000/URC-2000/UNC100*) is connected directly to the PC serial port via a RS232 or a RS485 cable.

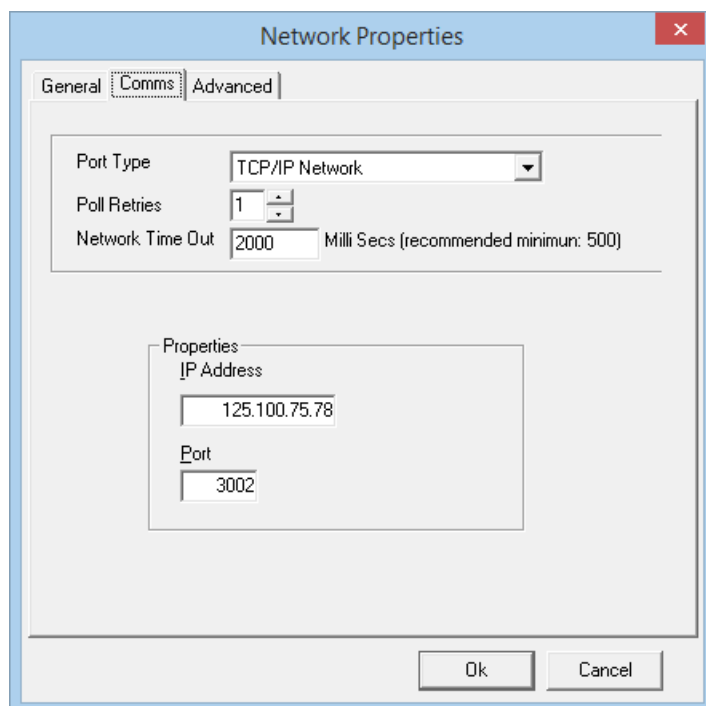


The image shows the 'Network Properties' dialog box with the 'Comms' tab selected. The 'Port Type' is set to 'Direct Network'. The 'Poll Retries' is set to 2, and the 'Network Time Out' is set to 1000 Milli Secs (recommended minimum: 500). The 'Properties' section shows 'Comm Port' set to 'COM2' and 'Baud' set to '38400'. The 'Ok' and 'Cancel' buttons are at the bottom right.

Property	Value
Port Type	Direct Network
Poll Retries	2
Network Time Out	1000 Milli Secs (recommended minimum: 500)
Comm Port	COM2
Baud	38400

### ***Ethernet Connect***

The controller network is connected to the PC through a standard Ethernet network.



The image shows the 'Network Properties' dialog box with the 'Comms' tab selected. The 'Port Type' is set to 'TCP/IP Network'. The 'Poll Retries' is set to 1, and the 'Network Time Out' is set to 2000 Milli Secs (recommended minimum: 500). The 'Properties' section shows 'IP Address' set to '125.100.75.78' and 'Port' set to '3002'. The 'Ok' and 'Cancel' buttons are at the bottom right.

Property	Value
Port Type	TCP/IP Network
Poll Retries	1
Network Time Out	2000 Milli Secs (recommended minimum: 500)
IP Address	125.100.75.78
Port	3002

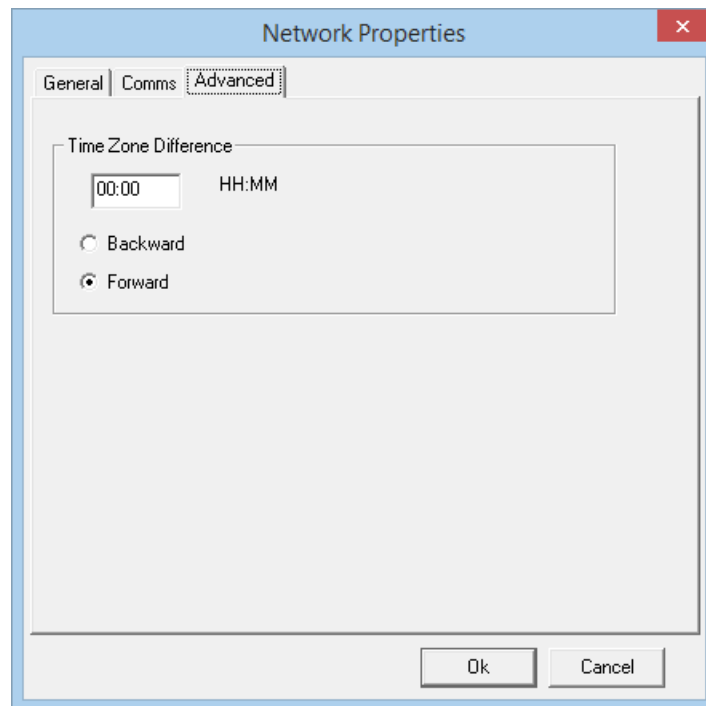
For an Ethernet connection to work **TCP must** be installed on your computer (e.g. IP Locator for LIF-200, and RBH Device Locator for UNC100 panels).

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.)

## Advanced

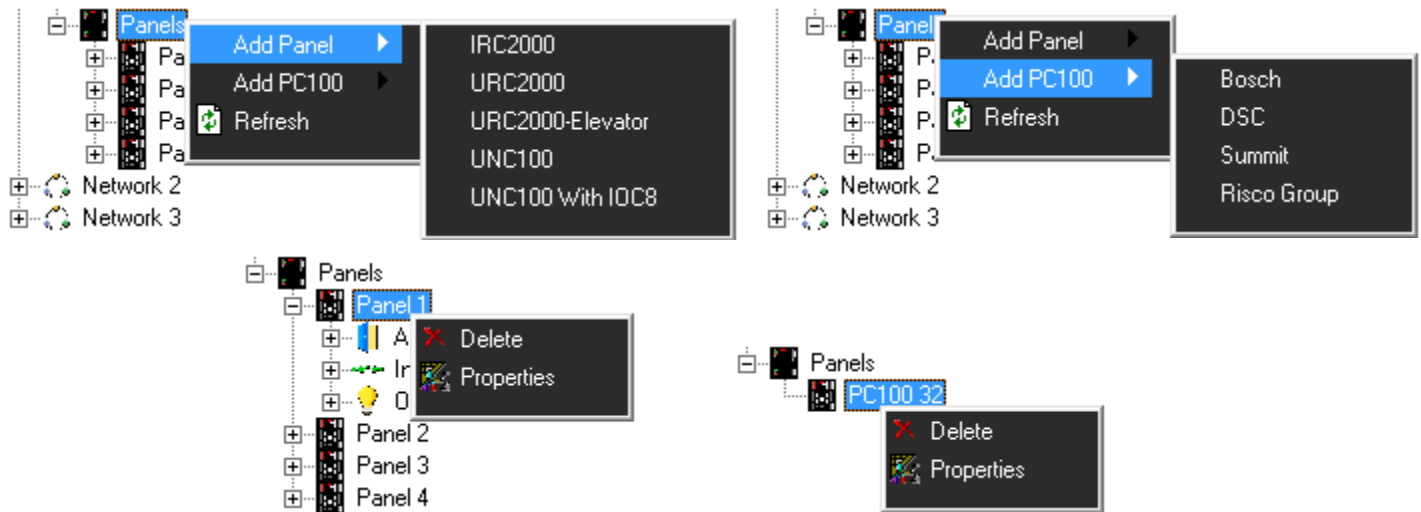
### ***Time Zone Difference***

If a network is located in an area within a different time zone you can set the difference here. Set the number of hours either ahead or behind of the time where the server is located.



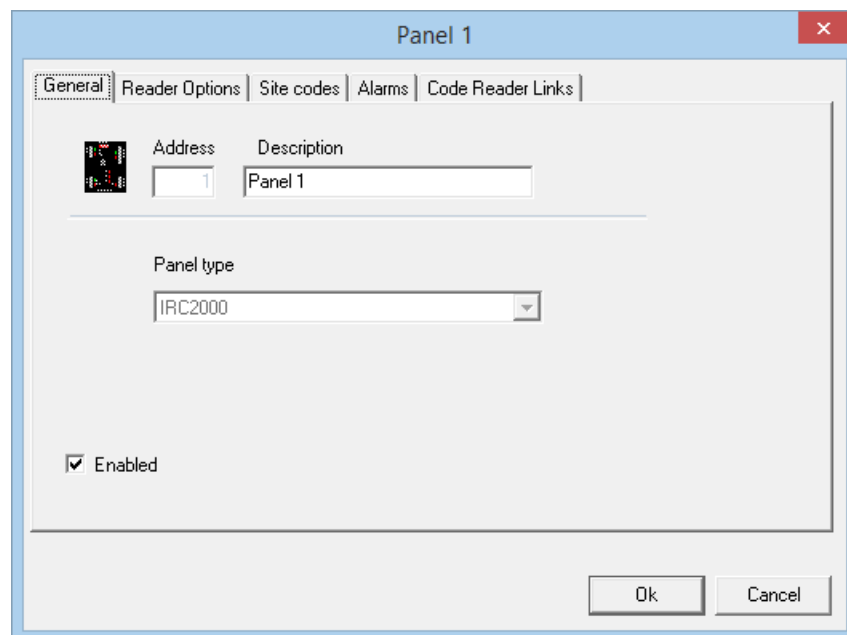
## Panels

Up to thirty-two panels<sup>17</sup> in total can be connected to the Integra32™ system.



## IRC2000/URC2000/UNC100/UNC100 with IOC8

### General



### Address

The address is selected at the time of creation and cannot be edited later.

### Description

<sup>17</sup> Number of panels installed can go up to 128, license required.



To change the default description simply type over it.

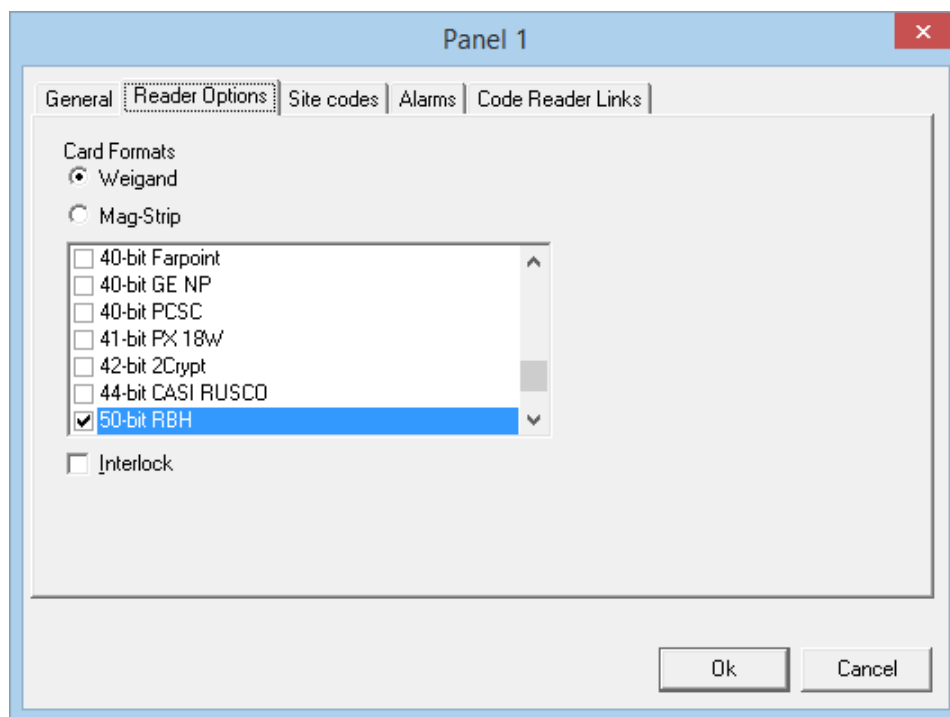
### **Panel Type**

The panel type is chosen when the new panel is added and cannot be edited later.

### **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 for both Wiegand and Mag-Strip formats).

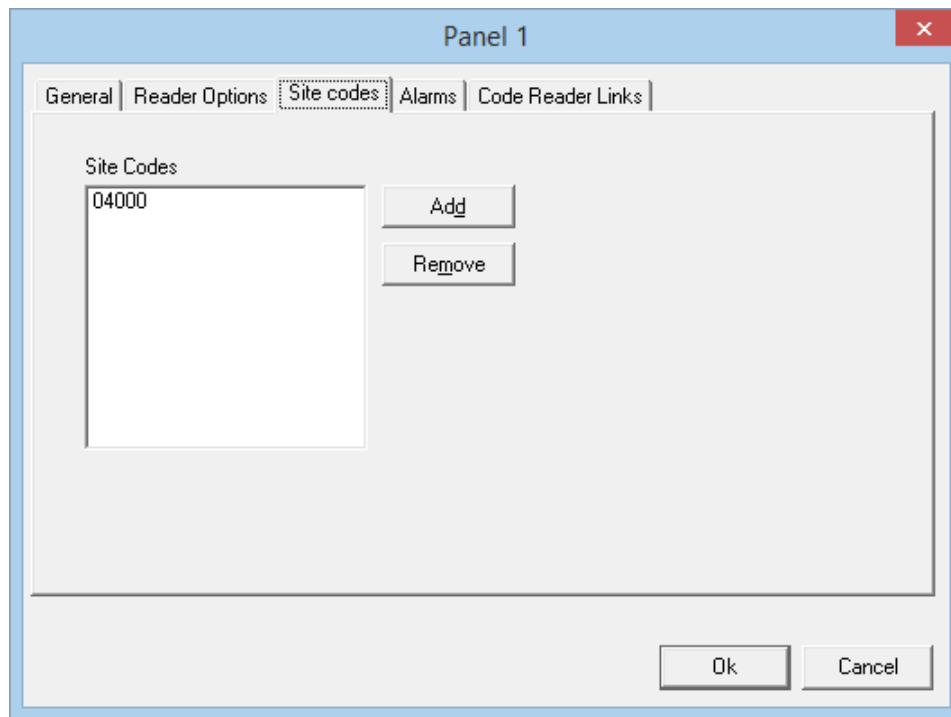
### **Interlock**

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**

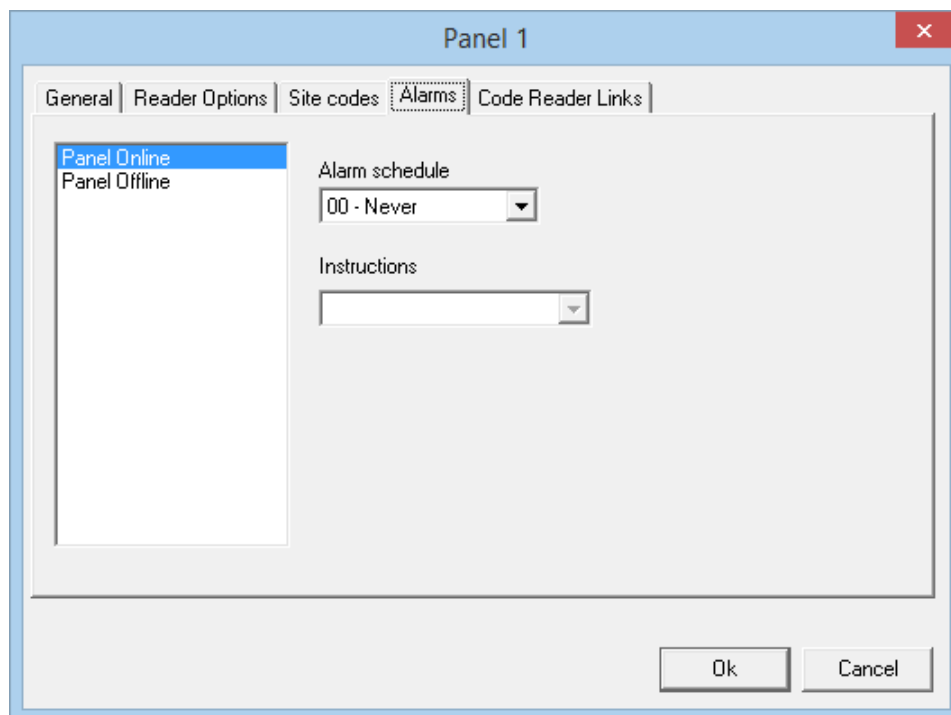
Under the *Site Codes* tab the facility code to be used by the Reader Controller is entered. (Each Reader Controller panel will support up to ten facility/site codes.)

Leading zeros are not required when entering a site codes, even though the display does show them.



## Alarms

Under the *Alarms* tab the schedules are set for when *Panel Online* and *Panel Offline* 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

Code reader links can 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. A combination card reader and keypad is needed to utilize this function. The programmed link is executed for the appropriate key code after a grant access has been executed at the specified access point. In the example below 'Code Reader Link 1' (High Security Mode off for both Reader 1 & Reader 2 at specified schedules) will be executed after a grant access and a key code entry of '1234', on the side A reader of Panel 1.

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. In addition, 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:

The screenshot shows a software window titled "Panel 1" with a close button in the top right corner. Inside the window, there are five tabs: "General", "Reader Options", "Site codes", "Alarms", and "Code Reader Links". The "Code Reader Links" tab is selected. Below the tabs, there is a table with three columns: "ID", "Code", and "Description". The first row of the table has the values "1", "1234", and "Code Reader Link 1". Below the table, there are two radio buttons: "Reader Side A" (which is selected) and "Reader Side B". At the bottom of the window, there are two buttons: "Ok" and "Cancel".

ID	Code	Description
1	1234	Code Reader Link 1

☒ Reader Side A  
☐ Reader Side B

	Command	Device	Duration	Schedule
1.	High Security Off	Reader 2		03 - After Hours
2.	High Security Off	Reader 1		01 - Always
3.				
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.


## URC2000 with ELV

The first five tabs (General, Reader Options, Site Codes, Alarms, & Code Reader Links) are *almost* the same as above for the regular URC-2000. URC-2000 Elevator panels have a sixth tab (Outputs). These outputs, on the ELC-08 boards, are the only outputs that can be used for elevator control.

Reader ports on an elevator board can be used for either elevator control or with very limited functionality as access control (It is usually recommended not to combine elevator control and access control on the same board). When an access point is used for elevator control change all of its default inputs and outputs to general purpose, the elevator reader won't need them. If you use the access point for access control it won't have all of the features that access points on other panels have. Access points on an elevator control board will not have 'Deduct Usage', 'Disable Forced Entry', 'Unlock Schedule', 'First Person Delay', 'RTE Bypass DC', 'Report RTE', 'Antipassback', or an 'Alarm Shunt' output. Timed commands will act as semi-permanent commands. Extended Unlock time will be fixed at thirty seconds, Door Held Open warning will be fixed at twenty seconds, and Door Held Open alarm will be fixed at thirty seconds.

Panel 4

General | Reader Options | Site codes | Alarms | Code Reader Links | Outputs

 Address: 4 Description: Panel 4

Panel type: URC2000 with ELC

☒ Enabled

Ok Cancel

### Outputs

Up to four eight-output relay boards may be used with each URC2000 Elevator Control. These outputs may be split between the two readers of the panel or all outputs may be used with just one reader. Use the scroll buttons to select the number of relay boards that are connected.

Panel 4

General | Reader Options | Site codes | Alarms | Code Reader Links | **Outputs**

Number of ELC boards

4

	Floor description
24	Output 24
25	Output 25
26	Output 26
27	Output 27
28	Output 28
29	Output 29
30	Output 30
31	Output 31
32	Output 32

Ok Cancel

Rename the outputs for your convenience.

Panel 4

General | Reader Options | Site codes | Alarms | Code Reader Links | **Outputs**

Number of ELC boards

4

	Floor description
11	Cab A 12th Floor
12	Cab A 13th Floor
13	Cab A 14th Floor
14	Cab A 15th Floor
15	Cab A 16th Floor
16	Cab A 17th Floor
17	Cab B 2nd Floor
18	Cab B 3rd Floor
19	Cab B 4th Floor

Ok Cancel

## PC100

IRC2000 panels connected along with the PC100 must be running firmware version 76 or higher for the PC100 and the IRC2000 panels to function together correctly.

## Bosch

It is recommended that the user be familiar with the DS7400Xi panel and has the ability to program PIN codes and parameters into the panel.

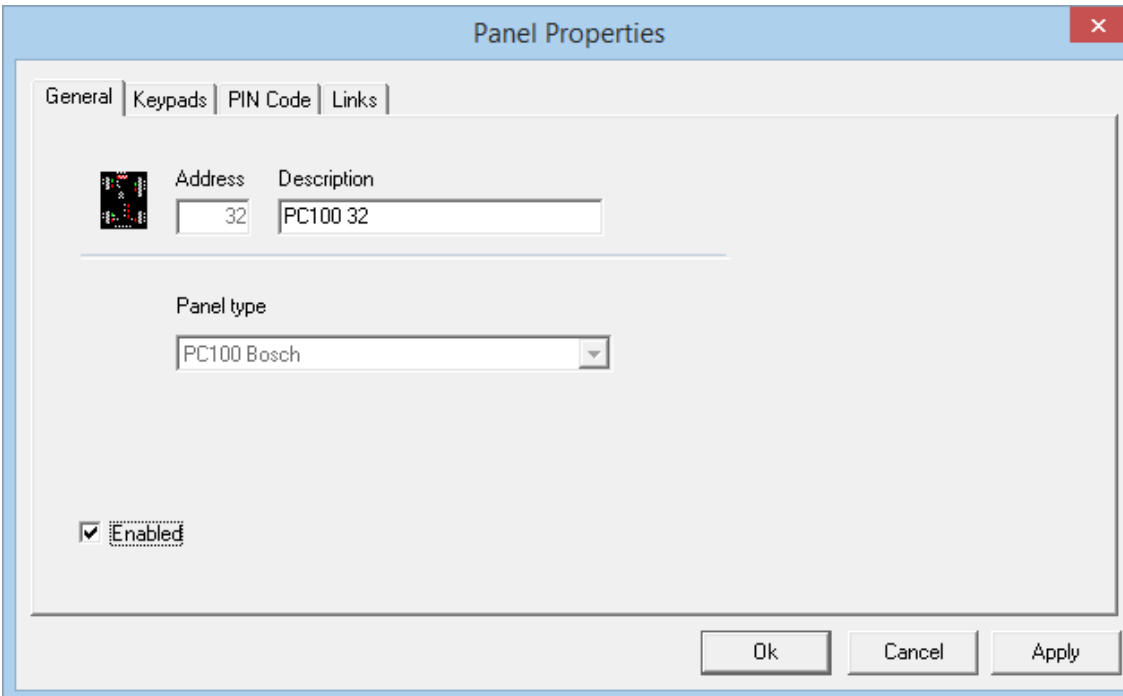
The PC100 interface has been designed to connect the Integra32 network to the DS7400Xi alarm panel through the option or keypad bus. It will emulate a keypad when a link has been provided and report status to the Integra network when included in the list of keypads.

In order for the alarm panel to poll the emulated keypad the keypad assignment for the alarm panel should be programmed. Keypad addresses 1-10 connect to the keypad bus and addresses 11-15 is connected to the option bus.

The PC100 can monitor all keypads on the bus that are listed under panel properties “Keypads”.

A Link to an Event will use an emulated keypad to enter a password followed by a command. If the password is not programmed into the alarm panel no operation will take place. Whenever a command is executed the green “Health” LED will turn on. The green “Health” LED will turn off when the alarm panel finishes its poll to the keypad.

## General



The screenshot shows the 'Panel Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a close button (X). Inside, there are four tabs: 'General', 'Keypads', 'PIN Code', and 'Links'. The 'General' tab contains a small keypad icon, an 'Address' field with the value '32', and a 'Description' field with the value 'PC100 32'. Below these is a 'Panel type' dropdown menu showing 'PC100 Bosch'. At the bottom left, there is a checked checkbox labeled 'Enabled'. At the bottom right, there are three buttons: 'Ok', 'Cancel', and 'Apply'.

Address	Description
32	PC100 32

Panel type: PC100 Bosch

☒ Enabled

Ok Cancel Apply

## Address

The address 32 is automatically selected at the time of creation and cannot be edited.

## Description

To change the default description simply type over it.

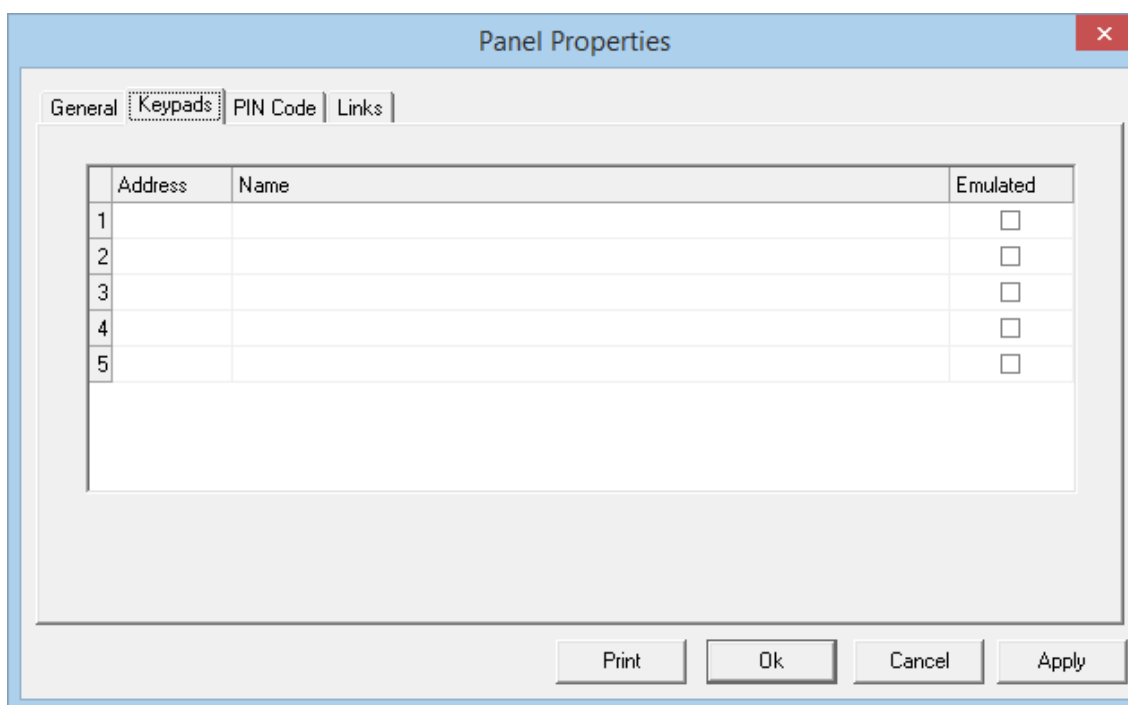
### **Panel Type**

The panel type is chosen when the new panel is added and cannot be edited later.

### **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.

### **Keypads**



The image shows a 'Panel Properties' dialog box with a blue title bar and a red close button. It has four tabs: 'General', 'Keypads' (selected), 'PIN Code', and 'Links'. The 'Keypads' tab contains a table with three columns: 'Address', 'Name', and 'Emulated'. The table has five rows, numbered 1 to 5 in the first column. The 'Emulated' column contains checkboxes, all of which are currently unchecked. Below the table is a large empty text area. At the bottom of the dialog are four buttons: 'Print', 'Ok', 'Cancel', and 'Apply'.

Address	Name	Emulated
1		<input type="checkbox"/>
2		<input type="checkbox"/>
3		<input type="checkbox"/>
4		<input type="checkbox"/>
5		<input type="checkbox"/>

### **Address**

This is the address of the keypad in the Bosch system (1-15). Only five of the possible fifteen keypads can be selected for use with the PC100.

### **Name**

Enter here a description or name of the keypad to be shown in the Integra32™ system.

### **Emulated**

Check this box if the Integra32™ system will be emulating this keypad and leave it unchecked to monitor an existing keypad. Signals from an emulated keypad will be the same as signals from an existing keypad; therefore to the Bosch system there is no difference between an emulated keypad and an existing keypad.

### **Pin Codes**

Panel Properties

General | Keypads | **PIN Code** | Links

☒ 4 Digit pin codes  
☐ 6 Digit pin codes

PIN Code	Pin code name

Print Ok Cancel Apply

Select either:

☒ Digit Pin Codes

Or

☒ Digit Pin Codes

### Pin Codes

Enter the four or six digits of each PIN code. These PIN codes must match PIN codes programmed into the Bosch system in order for commands from the emulated keypads to affect the Bosch system. Only five of the possible two hundred PIN codes may be entered here.

### Pin Code Name

Enter here a description or name for each PIN code.

### Links

Panel Properties

General | Keypads | PIN Code | **Links**

	Event	Device	Card	Command	Keypads	PIN Code
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

Print Ok Cancel Apply



### ***Event***

Select from a pull down list the triggering event.

### ***Device ID***

Choose the appropriate device to execute the selected command from a pull down for the selected event.

### ***Card***

Enter the card number (if applicable) that will trigger the selected command when it is associated with the chosen device and selected event (e.g. execute the command when card 1234 is granted access at reader 1).

### ***Command***

Select the command to be executed on the chosen keypad from a pull down list (Arm Keypad, Disarm Keypad, or Arm Perimeter).

### ***Keypad***

Choose which keypad the command is to be executed on.

### ***Pin Code***

Select a valid PIN code. The command will be executed as though this PIN code had been entered.

## ***Summit***

The PC100 when made for the Summit application will interface the Electronics Line Gold alarm panel to the IRC2000 access control system.

The PC100 comes with three channels of communication all of which are programmed for a baud rate of 9600, eight data bits, and no parity.

The PC100 passes data to and from the host to the IRC network and listens for log messages. In the event where the host is disconnected the PC100 sends request for status from each panel in the network. This prevents log messages from being lost. It takes about 5 seconds for the PC100 to time out and take over the network. When the PC100 has control of the network it will request time and date and keep updating the latest time every 32 polls. When the host comes back on lines all log messages are ignored that are time stamped with a date and time earlier than last recorded. This prevents old messages from triggering false alarms while allowing the host to update its log file. All log messages are passed through the event filter transforming all 128 different log messages into a few events.

All activity is synchronized to the Summit LSCP bus. If the bus is disconnected all activity on the PC100 will halt. The PC100 acts like a zone expander to the Summit panel allowing up to 32 zones. Each zone is mapped to an element in the IRC network. The state of each element in the IRC network will cause a zone to appear open or closed.

The PC100 acts like an IRC panel at address 32 to the host. The host can poll the PC100 to see if it is online, request status, write to memory, and update flash memory.

## ***General***

The image shows a 'Panel Properties' dialog box with a blue title bar and a red close button. It has two tabs: 'General' and 'Inputs'. The 'Inputs' tab is active. Inside the tab, there is a table with two columns: 'Address' and 'Description'. The 'Address' field contains the value '32' and the 'Description' field contains 'PC100 32'. Below the table, there is a 'Panel type' dropdown menu showing 'PC100 Summit'. At the bottom left, there is a checked checkbox labeled 'Enabled'. At the bottom right, there are three buttons: 'Ok', 'Cancel', and 'Apply'.

### **Address**

The address 32 is automatically selected at the time of creation and cannot be edited.

### **Description**

To change the default description simply type over it.

### **Panel Type**

The panel type is chosen when the new panel is added and cannot be edited later.

### **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.

### **Inputs**

The inputs of a Summit panel can be affected by the events from Integra32™ access panels. They can follow the access panel's inputs by mimicking them, going into alarm when the access panel's input goes into alarm. Alternatively, they can arm/disarm the Summit panel when access is granted at a reader (the Summit panel's input must be set as an arm/disarm input). On the other hand, they can follow an output on the access panel as if the output was wired to the input.

Zone	Description	Panel	Command	Output
1	Input 1			
2	Input 2			
3	Input 3			
4	Input 4			
5	Input 5			
6	Input 6			
7	Input 7			
8	Input 8			
9	Input 9			
10	Input 10			

### **Zone**

There are 32 zones.

### **Description**

The zone name or description can be edited here.

### **Panel**

Designate which panel the input will be affected by.

### **Command**

Choose the function for the input from the pull down list. Does it follow an input or an output, or is it used to arm or disarm the Summit panel.

### **Output**

If the input follows an output designates which output from the pull down list.

### **Risco Group**

It is recommended that the user be familiar with the (“Risco Group”) panel and has the ability to program PIN codes and parameters into the panel.

The PC100 interface has been designed to connect the Integra32 network to the (“Risco Group”) alarm panel through the option or keypad bus. It will emulate a keypad when a link has been provided and report status to the Integra network when included in the list of keypads.

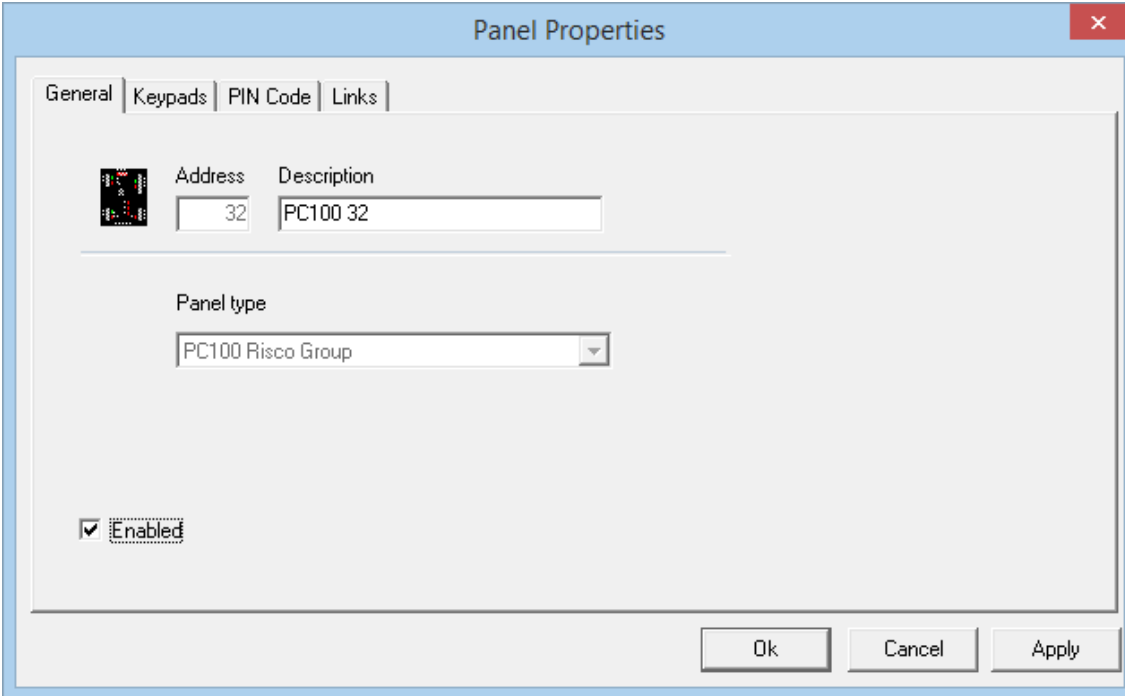
In order for the alarm panel to poll the emulated keypad the keypad assignment for the alarm panel should be programmed. Keypad addresses 1-10 connect to the keypad bus and addresses 11-15 is connected to the option bus.

The PC100 can monitor all keypads on the bus that are listed under panel properties “Keypads”.

A Link to an Event will use an emulated keypad to enter a password followed by a command. If the password is not programmed into the alarm panel no operation will take place. Whenever a command is

executed the green “Health” LED will turn on. The green “Health” LED will turn off when the alarm panel finishes its poll to the keypad.

## General



The image shows a 'Panel Properties' dialog box with a blue title bar and a red close button. It has four tabs: 'General', 'Keypads', 'PIN Code', and 'Links'. The 'General' tab is active. Inside the tab, there is a table with two columns: 'Address' and 'Description'. The first row has '32' in the 'Address' column and 'PC100 32' in the 'Description' column. Below the table, there is a 'Panel type' dropdown menu with 'PC100 Risco Group' selected. At the bottom left, there is a checked checkbox labeled 'Enabled'. At the bottom right, there are three buttons: 'Ok', 'Cancel', and 'Apply'.

Address	Description
32	PC100 32

Panel type: PC100 Risco Group

☒ Enabled

Ok Cancel Apply

### Address

The address 32 is automatically selected at the time of creation and cannot be edited.

### Description

To change the default description simply type over it.

### Panel Type

The panel type is chosen when the new panel is added and cannot be edited later.

### 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.

## Keypads

	Address	Name	Emulated
1			<input type="checkbox"/>
2			<input type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>

### **Address**

This is the address of the keypad in the Risco Group system (#?).

### **Name**

Enter here a description or name of the keypad to be shown in the Integra32™ system.

### **Emulated**

Check this box if the Integra32™ system will be emulating this keypad and leave it unchecked to monitor an existing keypad. Signals from an emulated keypad will be the same as signals from an existing keypad; therefore to the Risco Group system there is no difference between an emulated keypad and an existing keypad.

### **PIN Code**

☒ 4 Digit pin codes

PIN Code	Pin code name

☒ 4 Digit Pin Codes

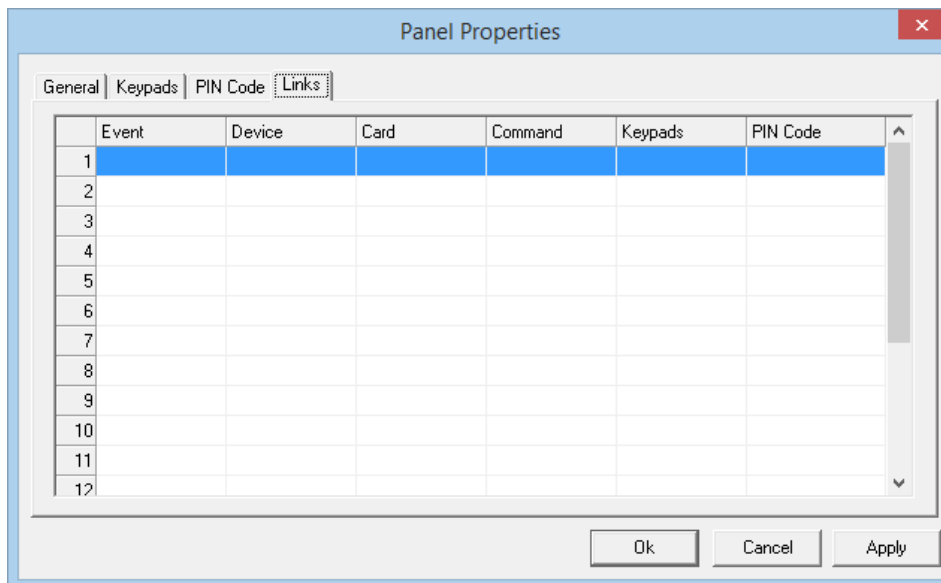
## **Pin Codes**

Enter the four digits of each PIN code. These PIN codes must match PIN codes programmed into the Risco Group system in order for commands from the emulated keypads to affect the Risco Group system. Only five of the possible two hundred PIN codes may be entered here.

## **Pin Code Name**

Enter here a description or name for each PIN code.

## **Links**



The image shows a 'Panel Properties' dialog box with the 'Links' tab selected. The dialog has a title bar with a close button. Inside, there are four tabs: 'General', 'Keypads', 'PIN Code', and 'Links'. The 'Links' tab contains a table with 12 rows and 7 columns. The columns are labeled 'Event', 'Device', 'Card', 'Command', 'Keypads', and 'PIN Code'. The first row is highlighted in blue. Below the table are three buttons: 'Ok', 'Cancel', and 'Apply'.

	Event	Device	Card	Command	Keypads	PIN Code
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

## **Event**

Select from a pull down list the triggering event.

## **Device ID**

Choose the appropriate device to execute the selected command from a pull down for the selected event.

## **Card**

Enter the card number (if applicable) that will trigger the selected command when it is associated with the chosen device and selected event (e.g. execute the command when card 1234 is granted access at reader 1).

## **Command**

Select the command to be executed on the chosen keypad from a pull down list (Arm Keypad, Disarm Keypad, or Arm Perimeter).

## **Keypad**

Choose which keypad the command is to be executed on.

## **Pin Code**

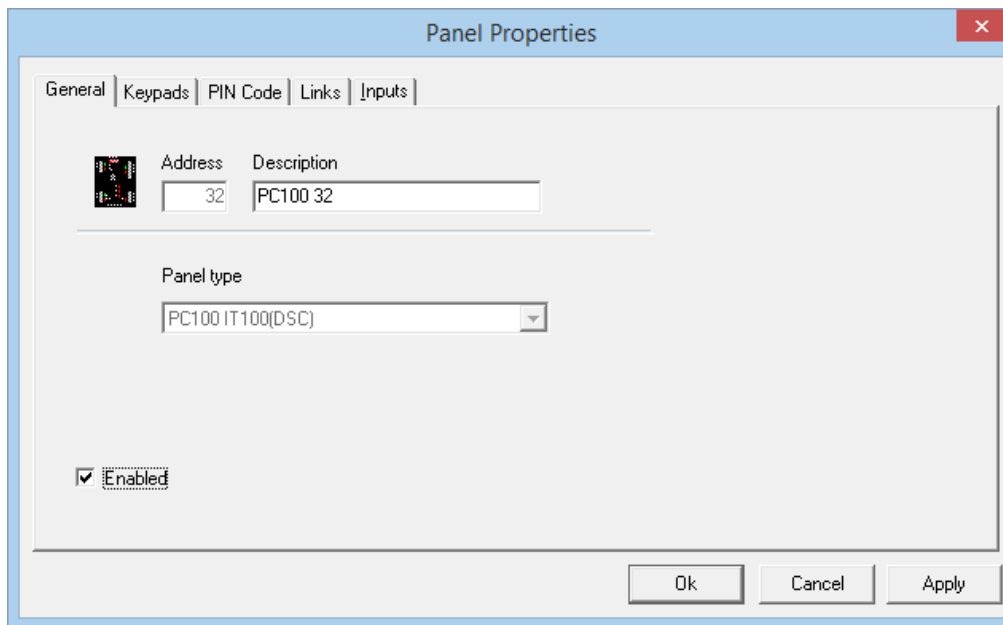
Select a valid PIN code. The command will be executed as though this PIN code had been entered.

## **DSC (IT-100)**

This PC100 interface uses the DSC “IT100” to allow communications between the Integra Access Control System and the DSC Power Series Burglar Alarm panel.

The PC100 is programmed through the Integra32 Software Version 3.7.18 (or higher) and is designed to be “Stand Alone”. While the host is offline the PC100 continues to monitor activity in the Access Control System allowing interaction between the Access and Alarm Systems.

## General



The screenshot shows the 'Panel Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a close button. Inside, there are tabs for 'General', 'Keypads', 'PIN Code', 'Links', and 'Inputs'. The 'General' tab contains a small icon of a panel, an 'Address' field with the value '32', a 'Description' field with the value 'PC100 32', a 'Panel type' dropdown menu showing 'PC100 IT100(DSC)', and an 'Enabled' checkbox which is checked. At the bottom right are 'Ok', 'Cancel', and 'Apply' buttons.

Address	Description
32	PC100 32

Panel type: PC100 IT100(DSC)

☒ Enabled

### Address

The address 32 is automatically selected at the time of creation and cannot be edited.

### Description

To change the default description simply type over it.

### Panel Type

The panel type is chosen when the new panel is added and cannot be edited later.

### 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.

## Keypads

	Address	Name
1		
2		
3		
4		
5		
6		
7		
8		

### **Address**

This is the address of the keypad in the DSC system.

### **Name**

Enter here a description or name of the keypad to be shown in the Integra32™ system

### **PIN Code**

☒ 4 Digit pin codes  
☐ 6 Digit pin codes

PIN Code	Pin code name

Select either:

- ☒ 4 Digit Pin Codes



Or

⦿ 6 Digit Pin Codes

### **Pin Codes**

Enter the four or six digits of each PIN code. These PIN codes must match PIN codes programmed into the DSC system in order for commands from the emulated keypads to affect the DSC system. Only eight PIN codes may be entered here.

### **Pin Code Name**

Enter here a description or name for each PIN code.

### **Links**

	Event	Device	Card	Command	Keypads	PIN Code
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

### **Event**

Select from a pull down list the triggering event.

### **Device ID**

Choose the appropriate device to execute the selected command from a pull down for the selected event.

### **Card**

Enter the card number (if applicable) that will trigger the selected command when it is associated with the chosen device and selected event (e.g. execute the command when card 1234 is granted access at reader 1).

### **Command**

Select the command to be executed on the chosen keypad from a pull down list (*Arm Keypad*, *Disarm Keypad*, or *Arm Perimeter*).

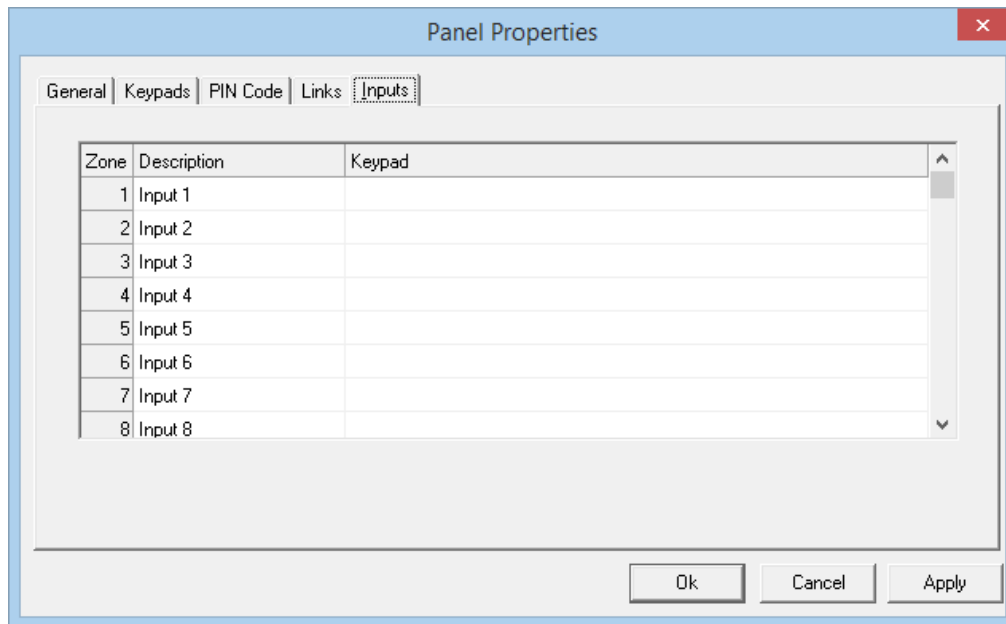
### **Keypad**

Choose which keypad the command is to be executed on.

### **Pin Code**

Select a valid PIN code. The command will be executed as though this PIN code had been entered.

## Inputs



The image shows a software window titled "Panel Properties" with a close button (X) in the top right corner. Inside the window, there are five tabs: "General", "Keypads", "PIN Code", "Links", and "Inputs". The "Inputs" tab is currently selected. Below the tabs is a table with three columns: "Zone", "Description", and "Keypad". The table contains eight rows, each with a zone number (1-8) and a description "Input 1" through "Input 8". The "Keypad" column is empty for all rows. A vertical scrollbar is on the right side of the table. At the bottom right of the dialog are three buttons: "Ok", "Cancel", and "Apply".

Zone	Description	Keypad
1	Input 1	
2	Input 2	
3	Input 3	
4	Input 4	
5	Input 5	
6	Input 6	
7	Input 7	
8	Input 8	

### **Zone**

There are 256 zones.

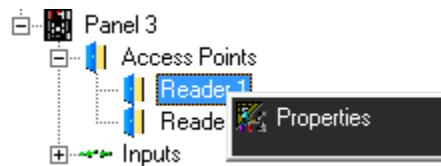
### **Description**

The zone name or description can be edited here.

### **Keypad**

Select the Keypad assigned to various zones from the drop down menu.

## Access Points



### General

Reader 1

General | Modes | Time-outs | Links | Alarms | CCTV | Advanced

☒ Description  
Reader 1

Inputs & Outputs Configuration

Door contact:	DC Reader 1
Request to exit:	RTE Reader 1
Lock output:	Lock Reader 1
Alarm shunt output:	Shunt Reader 1

☒ Enabled

Ok Cancel

### Description

To change the default description simply type over it.

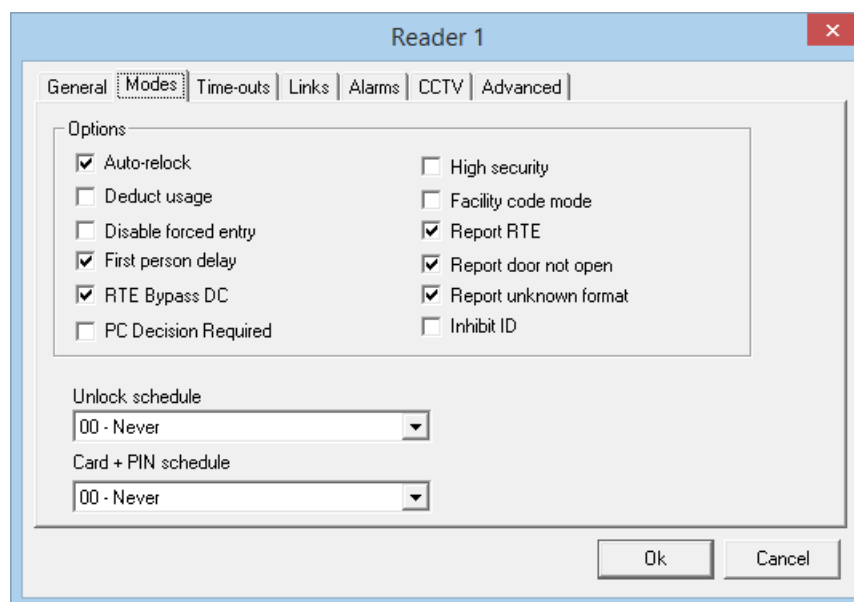
### Input & Output Configuration

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 as 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 the cards' usage count is less than 255. Card with a usage count of zero will not be granted access. Usage count works per panel if the system is run offline. Systems that are run online will have the usage count of a cardholder updated in all panels when any reader reduces that cardholder's count.

### *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***

Only cards with High Security privilege will be granted access at 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 Reader Controller. This message can be turned off if it is not required.

### ***Inhibit ID***

The cardholder name and card number will be blocked for access granted messages if this feature is checked. 'Access granted RTE' message will be shown in place of 'Access granted by card'. This feature is not applicable for **Card + PIN** schedule.

### ***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. When this schedule is off only a Card is needed for access to be granted.

### ***Time-Outs***

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

Reader 1

General Modes **Time-outs** Links Alarms CCTV Advanced

Unlock time 5 Sec

Extended unlock time 30 Sec

DHO warning 20 Sec

DHO alarm 30 Sec

Timed anti-passback 0 Sec

Repeat ignore time 0 Sec

Ok Cancel

### *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 when the Lock Time expires, the Door Held Open Warning timer will start. When the Door Held Open Warning time expires the Access Point will go into Door Held Open Warning (posting DHO Warning message and pulsing the reader's buzzer).

### *DHO Alarm*

If a door is still open when the Door Held Open Warning time expires, the Door Held Open Alarm timer will start. When the Door Held Open Alarm time expires the Access Point will go into Door Held Open Alarm (posting DHO Alarm message and turning on the reader's buzzer continuously). Since the DHO Alarm timer starts when the DHO Warning timer expires, if the DHO Warning time is set to zero then the DHO Alarm timer won't be started.

### *Timed Antipassback*

Set the amount of time for Timed Antipassback here. Timed Antipassback will reset at the end of the programmed time allowing the cardholder to be granted access through a reader they are already logged into. If a cardholder tries to re-enter through the same reader before the timer expires they will cause a Timed Antipassback violation.



**Timed Antipassback and Area/Reader Antipassback (Local/Global) cannot be combined together.**

## Repeat Ignore Time

Set the amount of time after a card is read until that card can be used again at that door. After the card is read, that card will be ignored for the set amount of time. Other cards can be used and each will be subject to the ignore time individually.

## Links

	Command	Device	Duration	Schedule
1.	Output On	Output 3	5 Sec	01 - Always
2.	Disarm Input	Input 4	0 Sec	03 - After Hours
3.				
4.				
5.				
6.				
7.				
8.				

### Select an event

The selectable events are Access Granted, Access Denied, Door Locked, Door unlocked, Door Held Open, Door Not Open, Forced Entry, Restore, High Security On, High Security Off, 3\* Links, and 5\* Links (3\* Links and 5\* Links indicate either three or five consecutive Access Granted to execute the link).

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*).

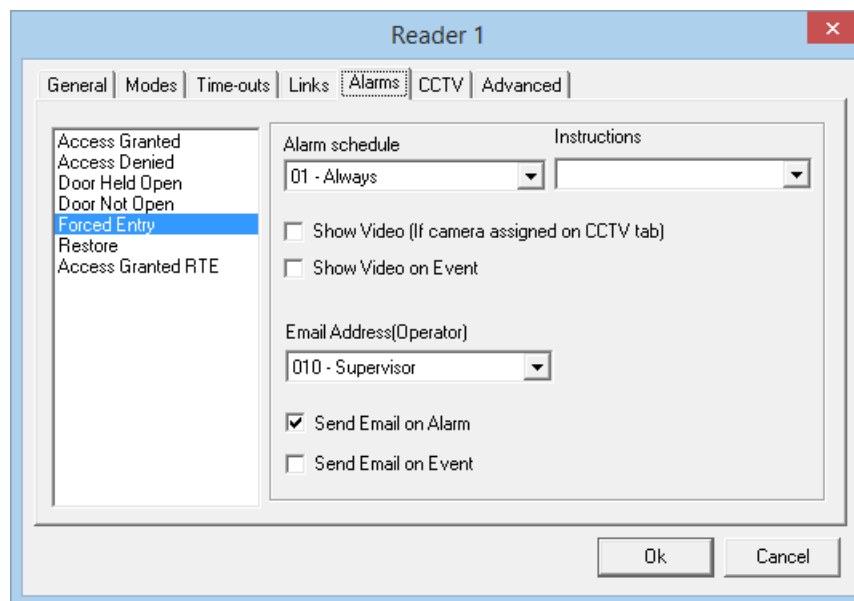
Choose the duration of the command (0-127 seconds or 0-126 minutes).

- 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 3 being turned on for five seconds and Disarm Input 7 when there is a forced entry at Reader 1 (but only during the specified schedule associated with output/input).

## Alarms

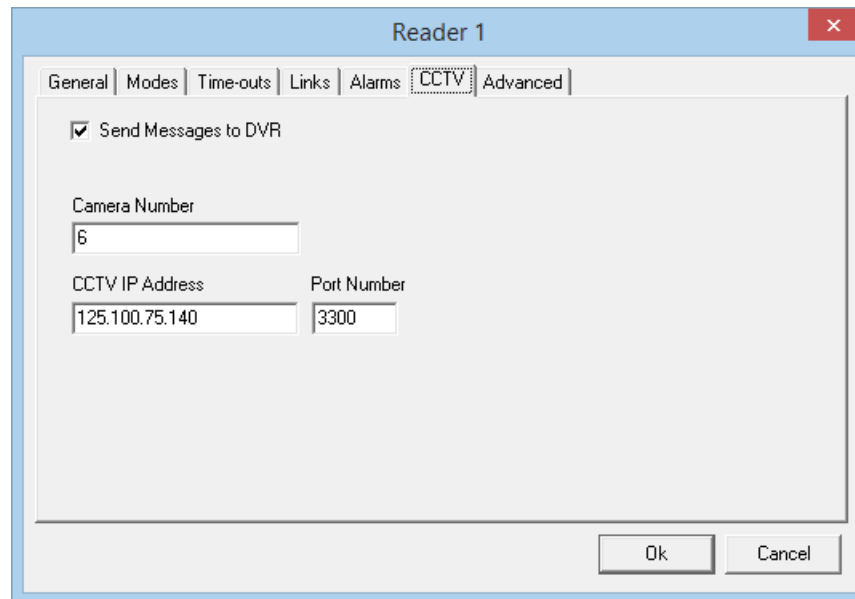


- 1) First select an event from list on the left.
    - (a) The alarm will occur when the message appears in the log screen.
  - 2) Then select an *Alarm Schedule*. (Causes an alarm when?)
  - 3) Then you can select (if required) an instruction message for the alarm. (Message creation is described earlier.)
- ☒ Show Video (If camera assigned on CCTV tab): Check this box to have the DVR show the camera configured on the CCTV tab for this access point on the configured Alarm.
  - ☒ Show Video on Events: Check this box to have the CCTV show the camera configured on the DVR tab for this access point on the configured message (Alarm is not required).
- Select an operator if need to send an email on the message.
- ☒ Send Email on Alarm: Check this box to send the email address configured for the operator selected on Alarm.
  - ☒ Send Email on event: Check this box to send the email address configured for the operator selected on Event.(Alarm configuration is not required)



## CCTV<sup>18</sup>

This tab is available for editing only if CCTV license has been installed, otherwise we can only send messages to DVR servers.



The information in this tab is used to interface with a CCTV.

There are two ways that this interface can be accomplished.

- 1) The first is by sending messages to DVR servers. Two types of messages can be sent to DVRs: ASCII or XML, selection of which is made in *DVR Message Format*: as explained under *System Options*

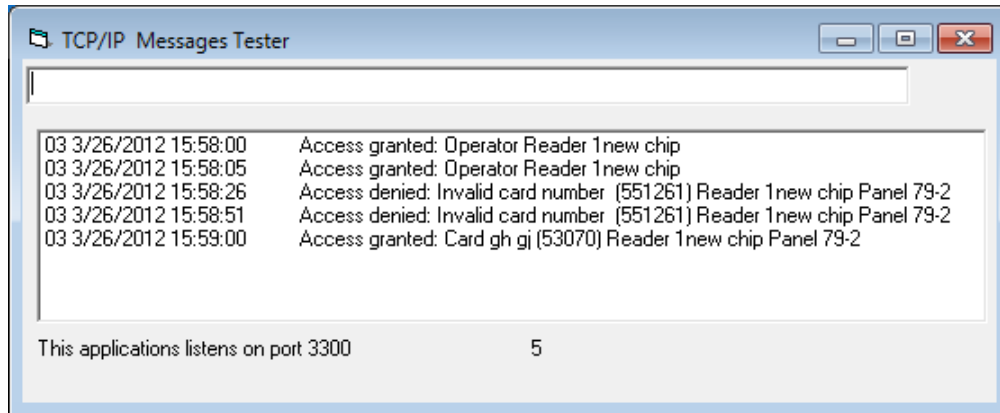
☒ Send Message to DVR

- First select the camera number you want to display from DVR.
- Then enter the DVR's IP address and Port Number associated with the camera you selected as you could be using more than one DVR. For this functionality to work, messages need to be configured in system messages tab as explained on page [123](#).

The ASCII messages are sent to DVR in the following format:

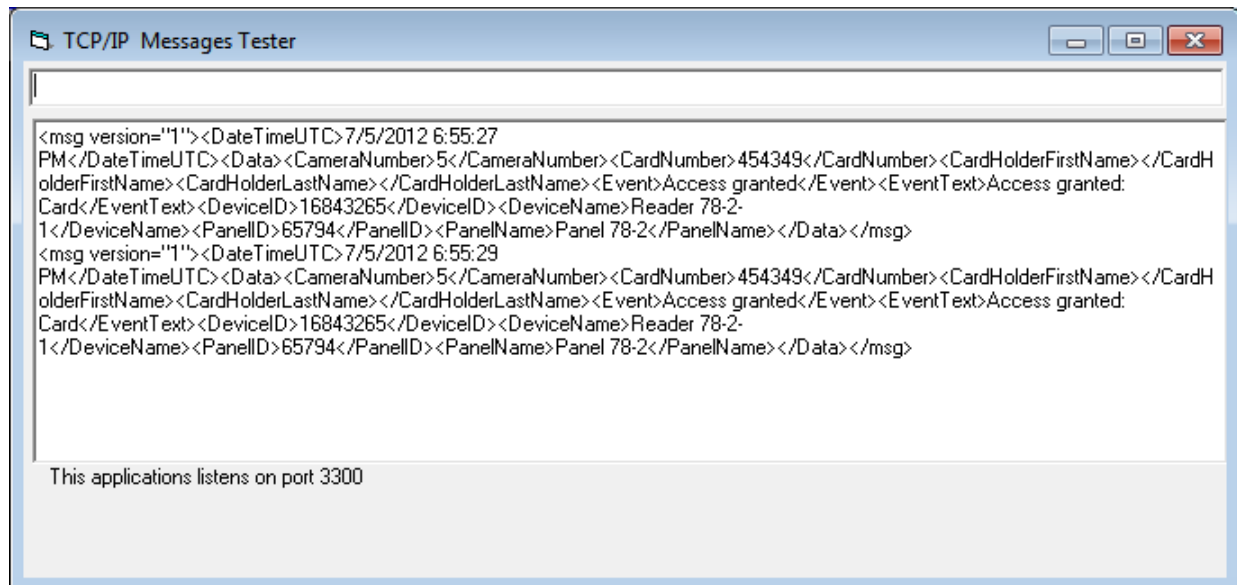
---

<sup>18</sup> This selection is only available if the optional license for the DVR Software has been purchased and installed.



And

XML messages are sent in the following format:



XML format string is:

<msg Version="1">

<DateTimeUTC></DateTimeUTC><Data><CameraNumber></CameraNumber><CardNumber></CardNumber><CardHolderFirstName></CardHolderFirstName><CardHolderLastName></CardHolderLastName><Event></Event><EventText></EventText><DeviceID></DeviceID><DeviceName></DeviceName><PanelID></PanelID><PanelName></PanelName></Data></msg>

☞ **When <Event> is Access Granted, Access Denied or Access point then <Device ID> = Reader ID and <Device Name> = Reader name.**

**NOTE:** Integra32™ server services need to be restarted whenever switching between the *DVR Message Format: ASCII and XML in System Options.*

- 2) The second way the interface can be used is to associate with a specific CCTV. CCTV are set up in the *Main window's toolbar* under CCTV

The screenshot shows the 'Reader 1' configuration window with the 'CCTV' tab selected. The window has a title bar with a close button. Below the title bar is a tabbed interface with tabs for 'General', 'Modes', 'Time-outs', 'Links', 'Alarms', 'CCTV', and 'Advanced'. The 'CCTV' tab is active. It contains a checkbox for 'Send Messages to DVR' which is unchecked. Below this is a 'CCTV Name' dropdown menu currently set to 'None'. There are two main sections: 'Camera Information' and 'History Information'. 'Camera Information' includes a 'Camera Number' spinner set to '0' and a 'PTZ Camera' checkbox which is unchecked. 'History Information' includes 'Pre Event Time' and 'Post Event Time' spinners, both set to '0' with a 'Min' dropdown. At the bottom are 'Ok' and 'Cancel' buttons.

- First select a CCTV for the pull down list under *CCTV Name*.
- Next configure the *Camera Information*. Select a camera number, indicate whether it's a PTZ camera or not, and if it is enter a preset number if applicable.
- Then set the *History Information*. Set the *Pre Event Time*, and the *Post Event Time*. These times set playback start time (how much time before the event time) and the playback end time (how long to continue the playback after the event time). This configuration is used by the [History Reports](#) DVR tab to playback video associated with a logged event.

## Advanced

The screenshot shows the 'Reader 1' configuration window with the 'Advanced' tab selected. The window has a title bar with a close button. Below the title bar is a tabbed interface with tabs for 'General', 'Modes', 'Time-outs', 'Links', 'Alarms', 'CCTV', and 'Advanced'. The 'Advanced' tab is active. It contains 'Entering Area' and 'Exiting Area' dropdown menus, with '03 - Sales' and '01 - Main Office' selected respectively. There are checkboxes for 'Exit Reader Installed' and 'AP Activity', both unchecked. On the right, there is a checkbox for 'Standard APB Enabled' which is checked, and a group box containing 'Soft' and 'Hard' radio buttons, with 'Hard' selected. At the bottom are 'Ok' and 'Cancel' buttons.

### **Standard APB Enabled**

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

#### *Global/Local Antipassback*

For Global Antipassback<sup>19</sup> to work the Integra32™ system must be online, and *PC Decision Required* must be turned on in the *Modes* tab of the Reader Properties' window for all of the appropriate readers, otherwise the panel will default to Local Antipassback<sup>20</sup> (within a Reader Controller). Global Antipassback allows a cardholder's area to be reset/cleared, meaning they are not logged into any area. With Local Antipassback the cardholder is either 'In' or 'Out' (never neither, always one or the other). Local Antipassback may be used with or without the Exit Reader Interface.



**If the Exit Reader Interface is not used when Local Antipassback is configured, then either the 'A' side or the 'B' side reader port (not both) needs to have its TAM terminal grounded. The side with the grounded TAM terminal will be the 'Out' reader and the side without will be the 'In' reader.**

### **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 cardholder's 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.

APB Access Points work well with Exit Reader Interfaces. The 'In' reader uses the configuration of Entering Area and Exiting Area as programmed while the 'Out' reader uses the inverse. (The 'Out' reader gets its Entering Area from the data programmed into Exiting Area and vice versa.)

### **Exit Reader Installed**

Selection of this option will configure the system to allow separate Global links for the 'In' reader as for the 'Out' reader.

The Exit Reader Interface module is used to connect two readers to a single reader port providing both 'In' and 'Out' readers.



**To use the Exit Reader Interface module the IRC2000 must be running firmware 100 or higher.**



**Timed Antipassback and Area/Reader Antipassback (Local/Global) cannot be combined together.**

### **Access Point Activity (AP Activity)**

---

<sup>19</sup> Antipassback tracked across multiple panel is called *Global Antipassback*.

<sup>20</sup> Antipassback tracked on one side of a panel is called *Local Antipassback*.

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

Multiple readers may have been selected to be displayed with this window. Only the last event is displayed though, all previous displays are deleted.

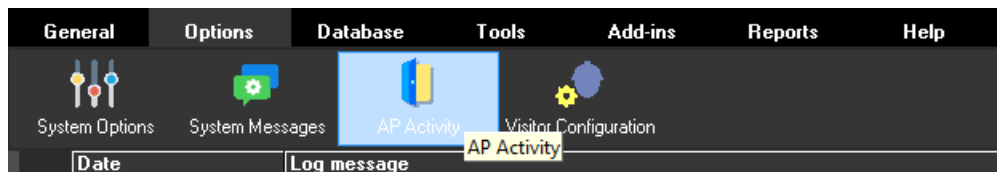
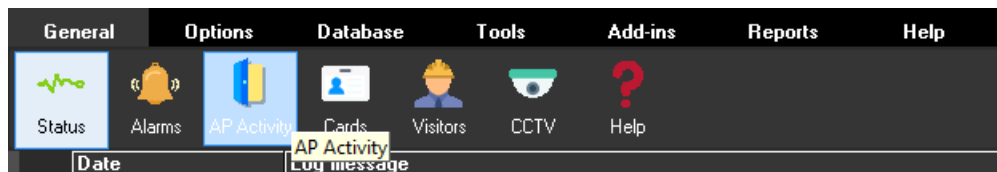
The image shows a window titled "AP Activity" with a "Grant access" section. It contains a "Reader" field with a green checkmark icon, a "Number" field, a "Date" field, an "Event" field, and a "Name" field. There are "More" and "Hide" buttons at the bottom right of the form area.

### Grant Access

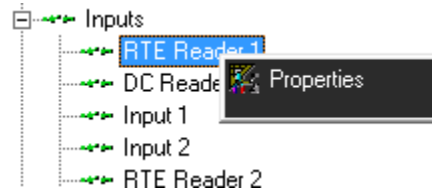
*Grant access* will grant access at the reader currently shown in the *Reader* box of the *Access Point Activity* window.



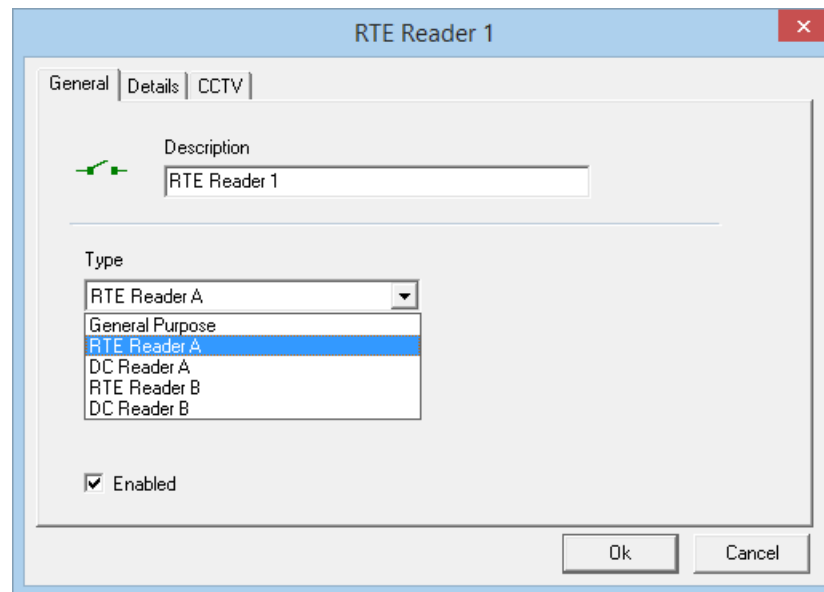
**Note:** The above window is automatically displayed only if *Access Point Activity (AP Activity)* is turned on either under *General* or *Options*.



## 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
- DC for Reader A
- RTE for Reader B
- DC 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.

RTE Reader 1

General Details CCTV

Circuit type  
NC, No Resistor

Abort Delay  
0 Sec

Ok Cancel

- 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<sup>21</sup>

RTE Reader 1

General Details CCTV

☒ Send Messages to DVR

Camera Number

CCTV IP Address Port Number

Ok Cancel

This tab is available for editing only if CCTV license has been installed, otherwise we can only send messages to DVR servers.

<sup>21</sup> This selection is only available if the optional license for the DVR Software has been purchased and installed.

The information in this tab is used to interface with a DVR.

There are two ways that this interface can be accomplished.

1. The first is by sending messages to DVR servers. Two types of messages can be sent to DVRs: ASCII or XML, selection of which is made in *DVR Message Format*: as explained under *System Options*

☒ Send Message to DVR

- First select the camera number you want to display from DVR.
- Then enter the DVR's IP address and Port Number associated with the camera you selected as you could be using more than one DVR. For this functionality to work, messages need to be configured in *system messages* menu as explained on page 123.
- The ASCII/XML messages are sent to DVR.

☞ **When <Event> is *Input*, then <Device ID> = Input ID and <Device Name> = Input name.**

**NOTE: Integra32™ server services need to be restarted whenever switching between the *DVR Message Format: ASCII and XML in System Options.***

2. The second way the interface can be used is to associate with a specific CCTV. CCTV are set up in the *Database Screen* under CCTV.

The screenshot shows a dialog box titled "RTE Reader 1" with a close button in the top right corner. It has three tabs: "General", "Details", and "CCTV", with "CCTV" being the active tab. Inside the dialog, there is a checkbox labeled "Send Messages to DVR" which is currently unchecked. Below this is a "CCTV Name" label followed by a dropdown menu showing "None". Further down, there are two sections: "Camera Information" and "History Information". The "Camera Information" section contains a "Camera Number" label with a numeric input field and a "PTZ Camera" checkbox. The "History Information" section contains "Pre Event Time" and "Post Event Time" labels, each followed by a time selection control (a numeric input field and a dropdown arrow). At the bottom right of the dialog are "Ok" and "Cancel" buttons.

- First select a DVR for the pull down list under *DVR Name*.
- Next configure the *Camera Information*. Select a camera number, indicate whether it's a PTZ camera or not, and if it is enter a preset number if applicable.
- Then set the *History Information*. Set the *Pre Event Time*, and the *Post Event Time*. These times set playback start time (how much time before the event time) and the playback end time (how long to continue the playback after the event time).

This configuration is used by the *History Reports* DVR tab to playback video associated with a logged event.





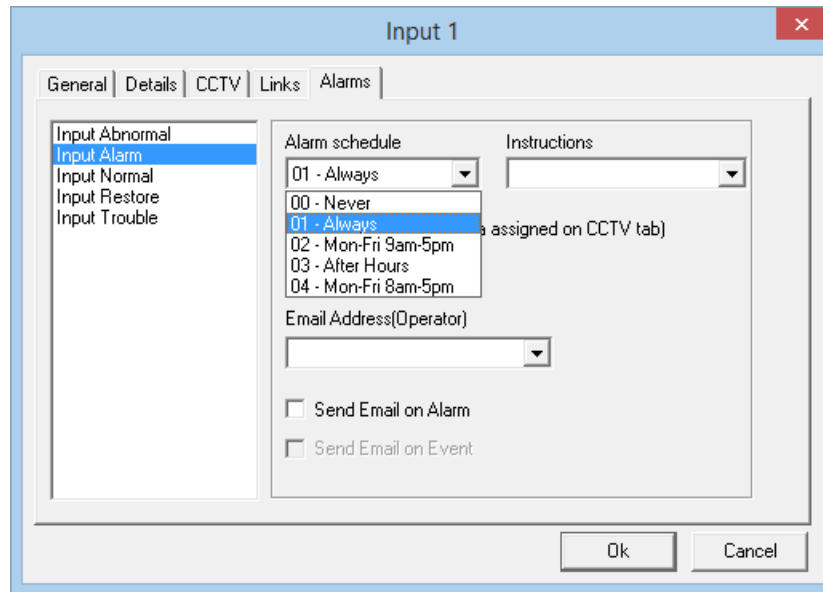
**Links and Alarms tabs are available only for general-purpose inputs.**

## Links

	Command	Device	Duration	Schedule
1.	Output On	Output 3	0 Sec	03 - After Hours
2.	Disable forced entry On	Reader 1	0 Sec	01 - Always
3.	Unlock Door	Reader 2	0 Sec	01 - Always
4.				
5.				
6.				
7.				
8.				

- First select an event.
  - i) 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, turning Disable Forced Entry on or off, and Clear Area.
- 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

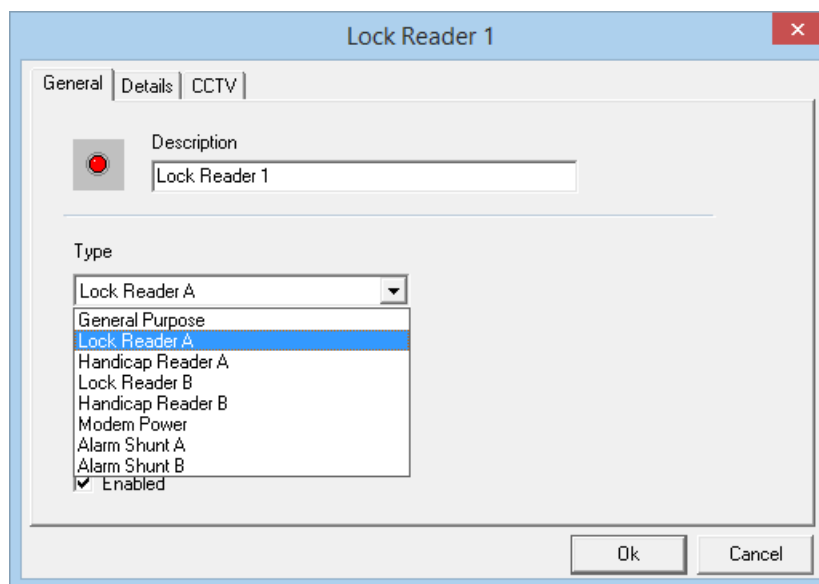


- First select an event from the list on the left.
  - The alarm will occur when the message appears in the log screen.
  - Then select an Alarm Schedule. (Causes an alarm when?)
  - Then you can select (if required) an instruction message for the alarm. (Message creation is described earlier.)
- 
- ☒ Show Video (If camera assigned on DVR tab): Check this box to have the DVR show the camera configured on the DVR tab for this input on configured Alarm
  - ☒ Show Video on Event: Check this box to have the DVR show the camera configured on the DVR tab for this input on configured event.

## Outputs



### General

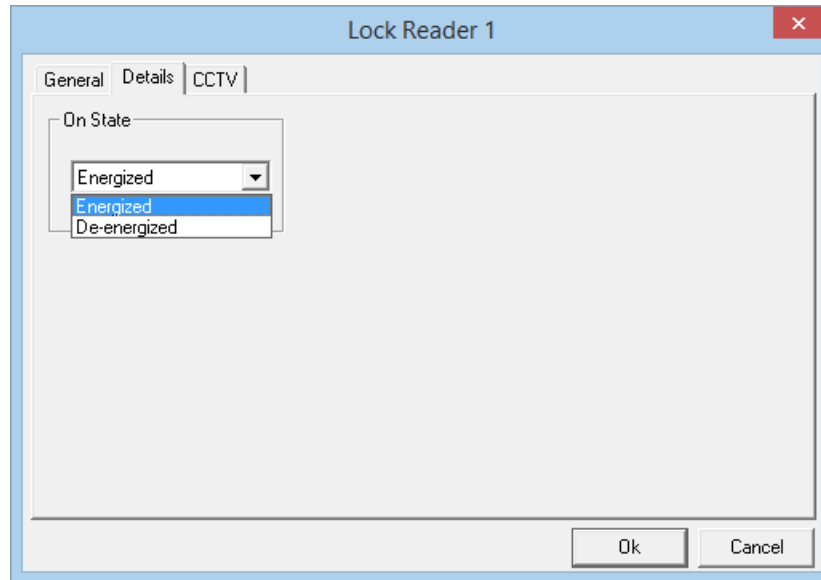


The *Description* and *Type* of the output can be changed/programmed in the *General* tab.

The output type can be:

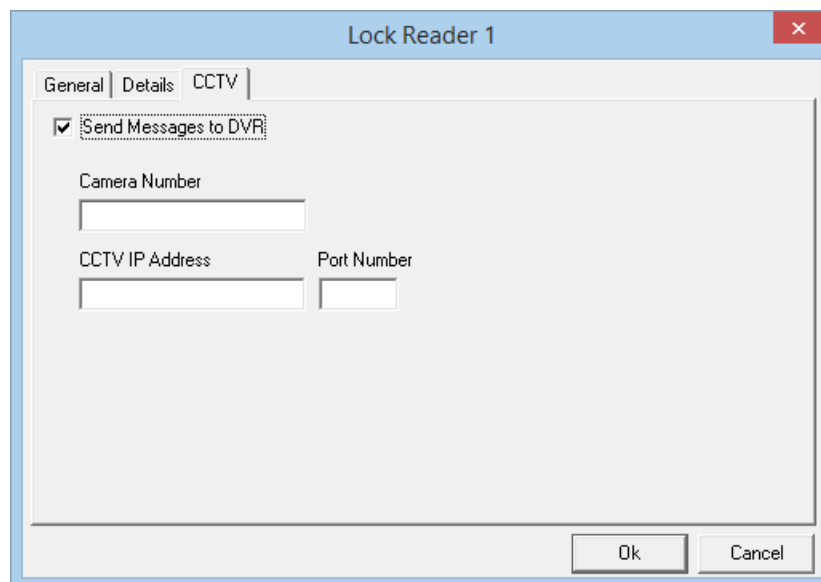
- General Purpose
- Lock for Reader A
- Handicap for Reader A
- Lock for Reader B
- Handicap for Reader B
- Modem Power
- Alarm Shunt A
- Alarm Shunt B

### 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<sup>22</sup>



This tab is available for editing only if CCTV license has been installed, otherwise we can only send messages to DVR servers.

The information in this tab is used to interface with a DVR.

---

<sup>22</sup> This selection is only available if the optional license for the DVR Software has been purchased and installed.

There are two ways that this interface can be accomplished.

- 1) The first is by sending messages to DVR servers. Two types of messages can be sent to DVRs: ASCII or XML, selection of which is made in [DVR Message Format](#): as explained under [System Options](#)

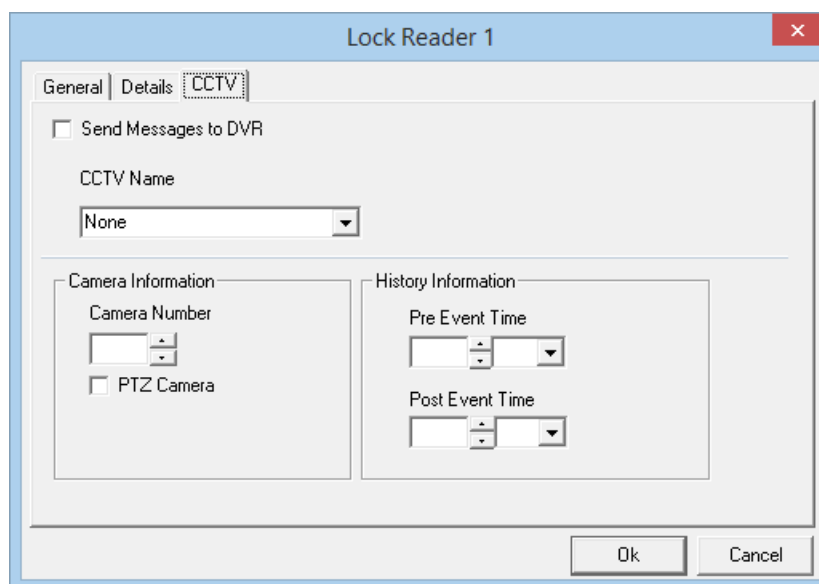
☒ Send Message to DVR

- First select the camera number you want to display from DVR.
- Then enter the DVR's IP address and Port Number associated with the camera you selected as you could be using more than one DVR. For this functionality to work, messages need to be configured in System messages menu as explained on page [123](#).
- The ASCII/XML messages are sent to DVR.

 **When <Event> is *Output*, then <Device ID> = Output ID and <Device Name> = Output name.**

**NOTE: Integra32™ server services need to be restarted whenever switching between the [DVR Message Format: ASCII and XML](#) in [System Options](#)**

- 2) The second way the interface can be used is to associate with a specific CCTV. CCTV are set up in the *Main windows' toolbar* under CCTV.



- First select a DVR for the pull down list under *DVR Name*.
- Next configure the Camera Information. Select a camera number, indicate whether it's a PTZ camera or not, and if it is enter a preset number if applicable.
- Then set the History Information. Set the Pre Event Time, and the Post Event Time. These times set playback start time (how much time before the event time) and the playback end time (how long to continue the playback after the event time).

This configuration is used by the [History Reports](#) DVR tab to playback video associated with a logged event.



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

## Links

Output 1

General | Details | CCTV | **Links**

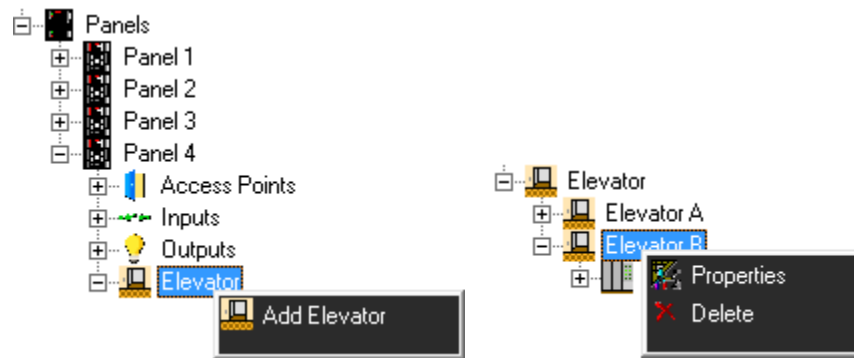
Select an event: Output Off

	Command	Device	Duration	Schedule
1.	Arm Input	Input 1	10 Sec	03 - After Hours
2.	Disable forced entry Off	Reader 2		01 - Always
3.	Lock Door	Reader 1	0 Sec	01 - Always
4.				
5.				
6.				
7.				
8.				

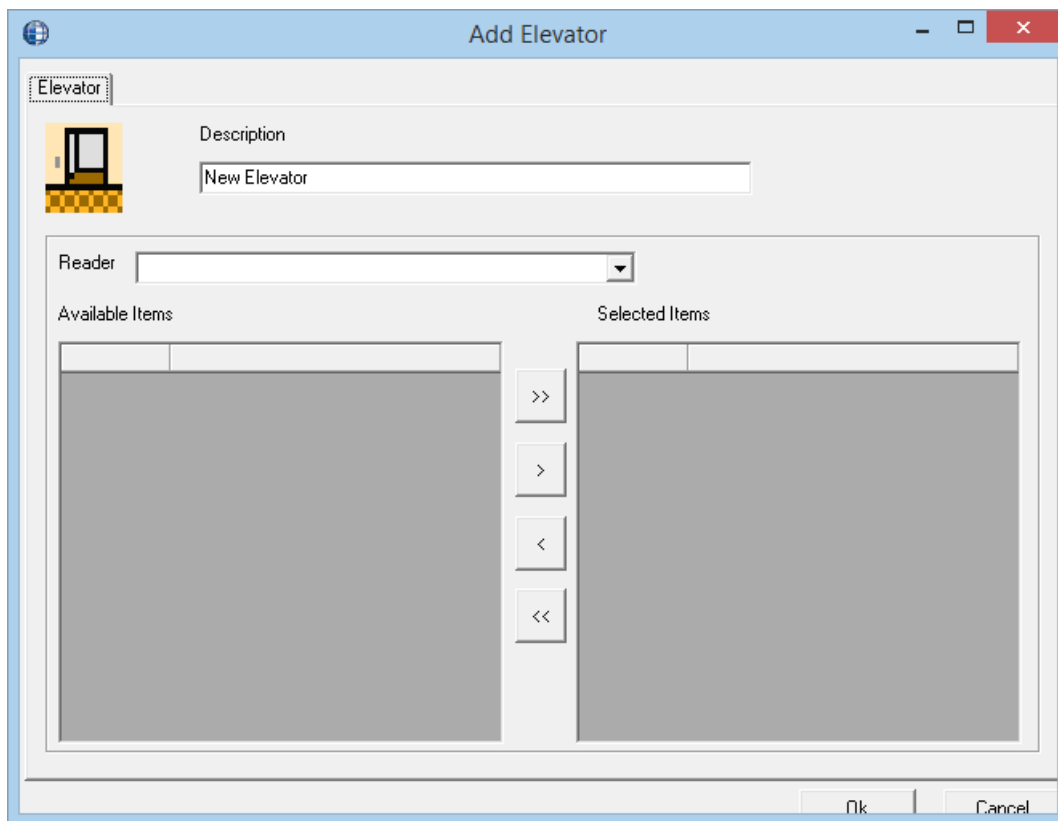
Ok Cancel

- 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).

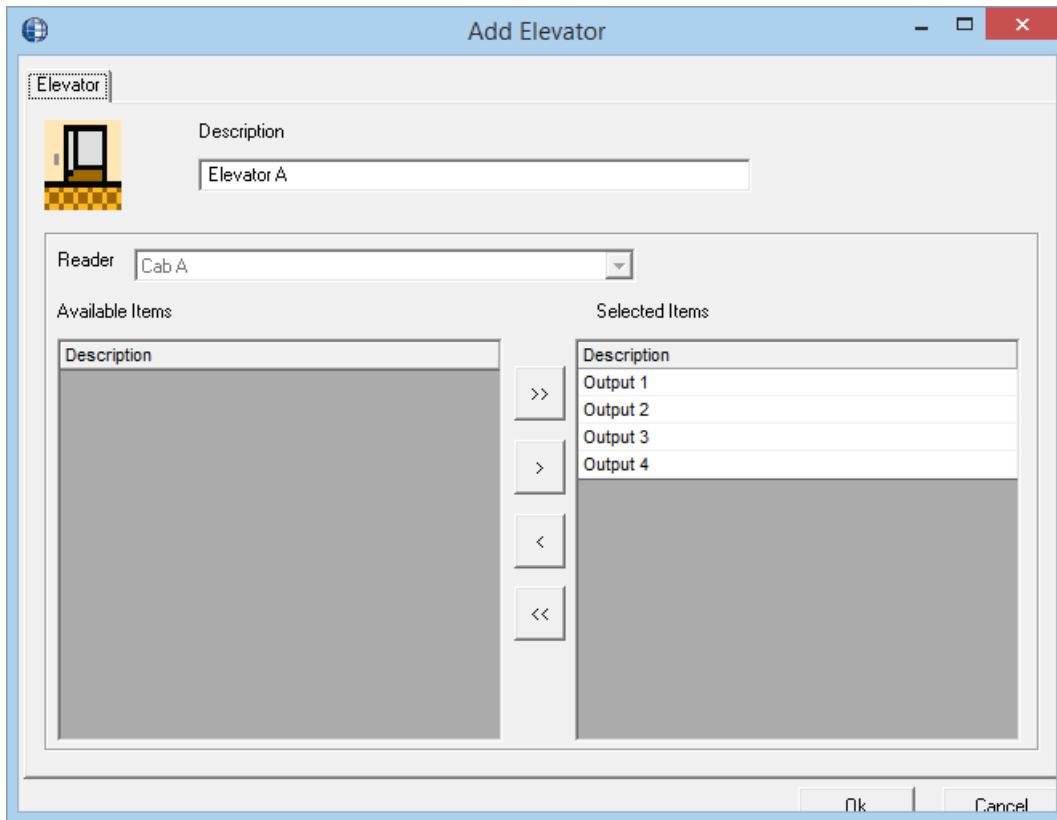
## Elevators



The URC2000 Elevator Control can control up to two elevator cabs and thirty-two floors. You can split the thirty-two floors between the two doors any way you like.

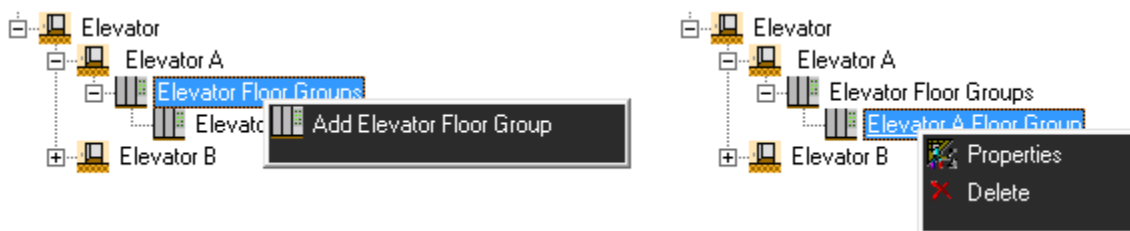


Access Points used for elevator control will have all the standard functionality of regular Access Points except for Antipassback and Interlock, and unlocking these Access Point will only affect the outputs assigned to the URC2000 controller and not the floor outputs.



Change the Description, select a reader, and for that reader determine which outputs (floors) are to be controlled on this elevator. You can create up to two elevators (per controller) by using both the A side and B side readers.

## Floor Groups




Add Floor Groups as required. Change the description and select which floors are to be member of the group. Each group can be given an Unlock Schedule so that its floors can have free access during that time. Maximum 15 floor groups can be added per elevator.



Elevator Floor Groups

Elevator Floor Groups |

 Description Elevator A Floor Group

Elevator Elevator A Unlock Schedule 00 - Never

Available Items

Description
-------------

>>

>

<

<<

Selected Items

Description
Cab A 1st Floor
Cab A 2nd Floor
Cab A 3rd Floor
Cab A 4th Floor

Ok Cancel

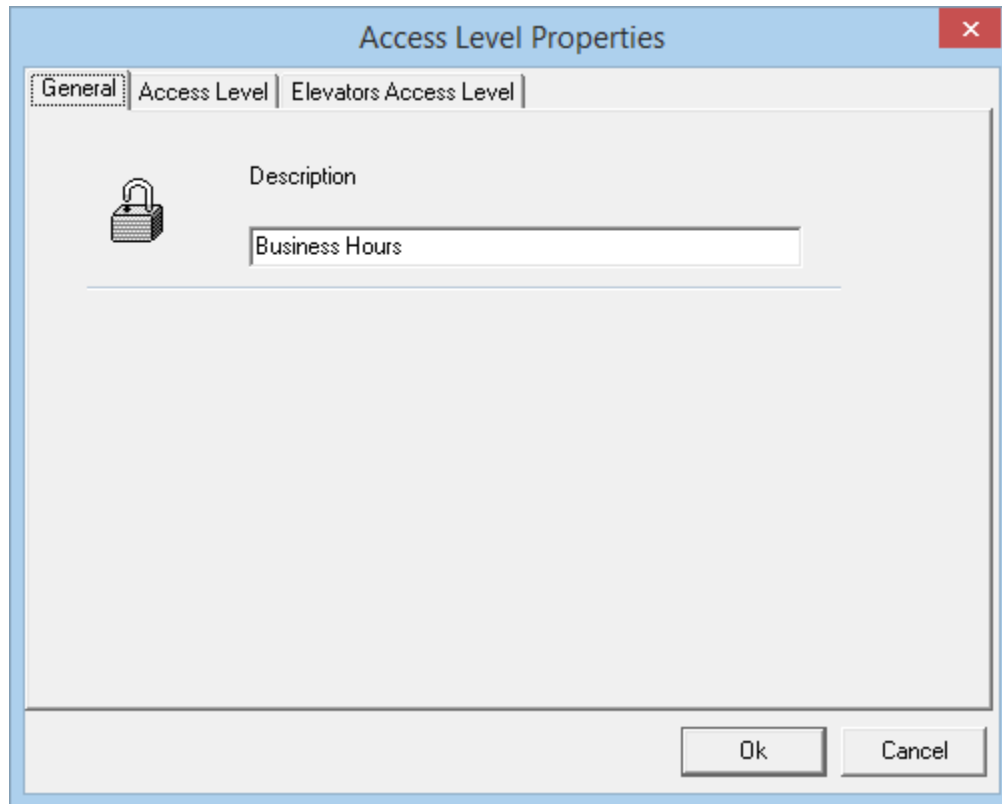
## Access Levels



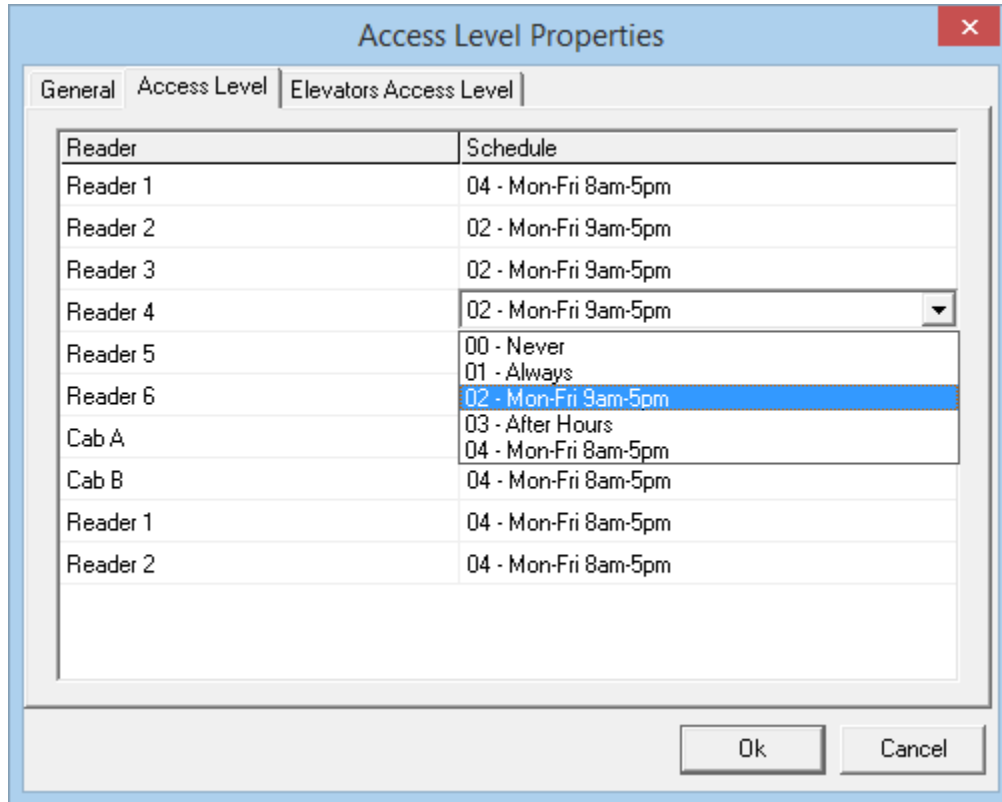
Assigning schedules to access points and floor groups creates access levels. They are created so that cardholders can be easily given access rights. Before cardholders are entered, any additional access levels that are required should be programmed. The only default access level is *Master*, which always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

### General

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



## Access Level



The image shows a software window titled "Access Level Properties" with a close button (X) in the top right corner. It has three tabs: "General", "Access Level", and "Elevators Access Level". The "Access Level" tab is selected. Inside the tab is a table with two columns: "Reader" and "Schedule".

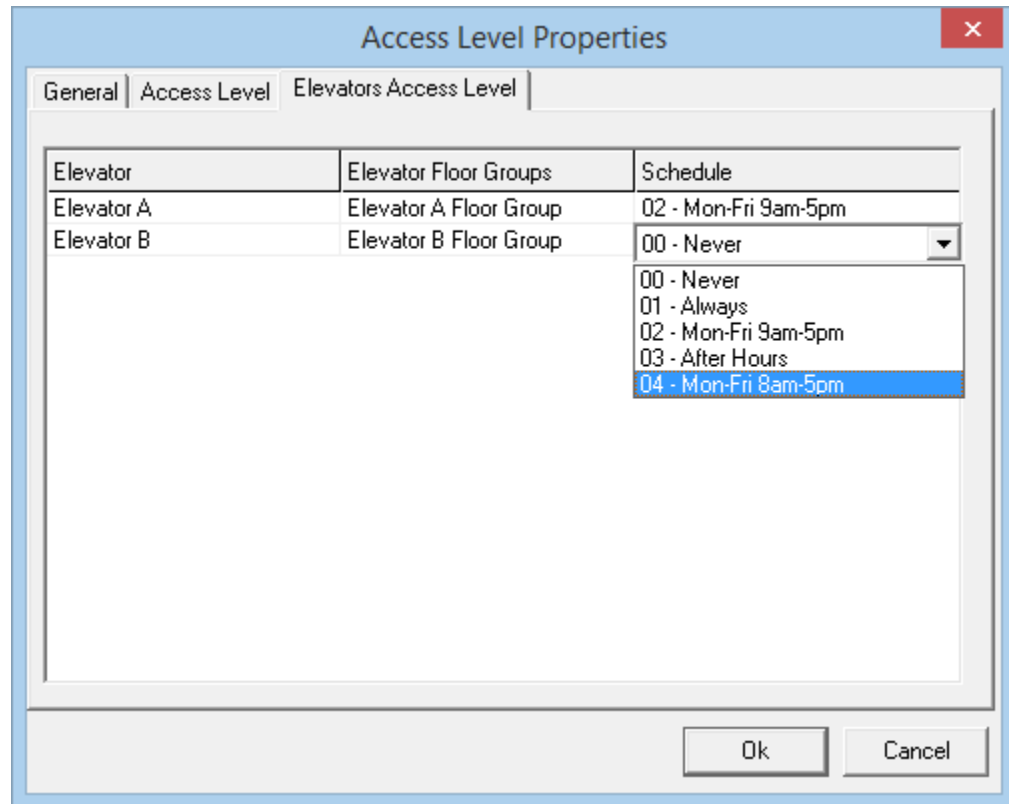
Reader	Schedule
Reader 1	04 - Mon-Fri 8am-5pm
Reader 2	02 - Mon-Fri 9am-5pm
Reader 3	02 - Mon-Fri 9am-5pm
Reader 4	02 - Mon-Fri 9am-5pm
Reader 5	00 - Never 01 - Always
Reader 6	02 - Mon-Fri 9am-5pm
Cab A	03 - After Hours 04 - Mon-Fri 8am-5pm
Cab B	04 - Mon-Fri 8am-5pm
Reader 1	04 - Mon-Fri 8am-5pm
Reader 2	04 - Mon-Fri 8am-5pm

At the bottom of the window are "Ok" and "Cancel" buttons.

Program the *Schedule* corresponding to the Reader (e.g. front door & rear door) in *Access Level* tab. Assign one schedule to each access point. Use the *Never* schedule if no access is to be allowed at the access point. Any access points added after the creation of the Access Level will be given the schedule *Never*. Access levels can easily be edited any time after they are created if changes are required.

Elevator readers require a schedule but the actual schedule selected is irrelevant. The actual Cardholder's access is determined by the Schedules on the Floor Groups.

## Elevator Access Level



The image shows a software dialog box titled "Access Level Properties" with a close button (X) in the top right corner. It has three tabs: "General", "Access Level", and "Elevators Access Level", with the third tab being the active one. Inside the dialog, there is a table with three columns: "Elevator", "Elevator Floor Groups", and "Schedule".

Elevator	Elevator Floor Groups	Schedule
Elevator A	Elevator A Floor Group	02 - Mon-Fri 9am-5pm
Elevator B	Elevator B Floor Group	00 - Never

Below the table, a dropdown menu is open, showing a list of schedule options: "00 - Never", "01 - Always", "02 - Mon-Fri 9am-5pm", "03 - After Hours", and "04 - Mon-Fri 8am-5pm". The option "04 - Mon-Fri 8am-5pm" is currently selected and highlighted in blue. At the bottom right of the dialog, there are "Ok" and "Cancel" buttons.

The schedule of any Floor Group can be changed to any schedule, as long as no more than **four** schedules are changed from Never. Maximum of 4 Floor groups can be assigned per elevator panel in an Access level. If multiple Floor Groups, that are given schedules, have floors in common than the cardholder will have access to those floors if any schedule allows it.

# Chapter 6

## Cardholders

---

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

The screenshot shows the 'Integra32 - AxiomLite Cardholders' application window. It features a standard Windows-style interface with a title bar, a menu bar (File), and a toolbar with icons for New, Edit, Cancel, Delete, Search, Multi Cards, F Print, and Receipt. Below the toolbar, there are input fields for 'Last name' (Udet), 'First name' (Ernst), 'Initials', and 'Cardnumber'. A tabbed interface is present, with 'Cards' selected, and other tabs for 'Profile', 'Photo', 'Notes', and 'More Fields'. The main content area is divided into two parts: a list of cardholders on the left (showing '2384 Ernst') and a detailed form on the right for the selected cardholder '2384'. The form includes fields for 'Access level' (1 ... Master), 'Activation date' (2 /13/2018), 'Deactivation date' (1 /1 /2038), 'Usage Count' (255), 'Status' (Active), 'PIN Code', and 'Type' (Normal). There are also checkboxes for 'Ignore Antipassback', 'Ignore Auto Void', 'Unlock Privilege (2)', 'High Security Privilege (4)', 'Link Execute Privilege (3/5)', 'Extended unlock time', and 'Disabled'. At the bottom of the form are buttons for 'Add', 'Edit', 'Remove', and 'Copy'. The status bar at the bottom indicates '1 of 11'.

## Fields and Options

The cardholder window contains following fields and options:

### File

#### Exit:

Select this option to leave the Cardholder screen.

**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*.

**Multi Cards**

Multi Cards will open a utility to add multiple cards in a sequence to the cardholder utility as well as to the panels.

**F Print<sup>23</sup>**

F Print will open the finger print enrolment screen depending upon the manufacturer selected in *Badge* tab of *system options*.

**Last Name**

Enter the cardholder's surname.

**First Name**

Enter the cardholder's given name.

**Initials**

Up to six characters can be entered.

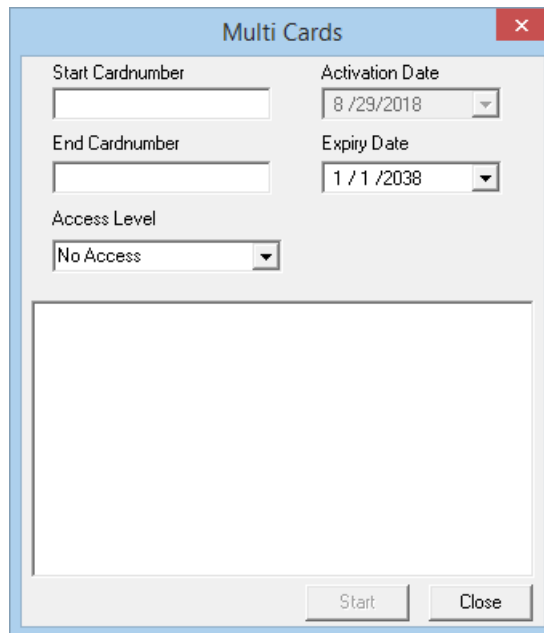
**Cardnumber**

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

---

<sup>23</sup> This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.

## Multi Cards



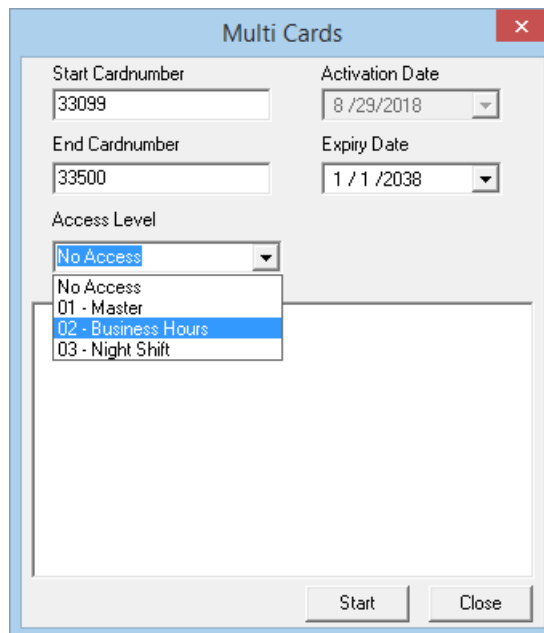
The screenshot shows a dialog box titled "Multi Cards" with a close button (X) in the top right corner. The dialog contains the following fields:

- Start Cardnumber:** An empty text input field.
- End Cardnumber:** An empty text input field.
- Activation Date:** A date picker showing "8 / 29 / 2018".
- Expiry Date:** A date picker showing "1 / 1 / 2038".
- Access Level:** A dropdown menu currently showing "No Access".

Below these fields is a large empty rectangular area. At the bottom right of the dialog are two buttons: "Start" and "Close".

Multi Cards utility can add multiple cards in a sequence in the cardholder window.

- Put in the Start and End card number.
- Assign the Expiry date, if any.
- Assign the Access Level from the drop down menu of the Access Levels configured in your system.



This screenshot shows the same "Multi Cards" dialog box, but with the "Access Level" dropdown menu open. The input fields are now populated:

- Start Cardnumber:** "33099"
- End Cardnumber:** "33500"
- Activation Date:** "8 / 29 / 2018"
- Expiry Date:** "1 / 1 / 2038"

The dropdown menu for "Access Level" is open, showing the following options:

- No Access
- 01 - Master
- 02 - Business Hours
- 03 - Night Shift

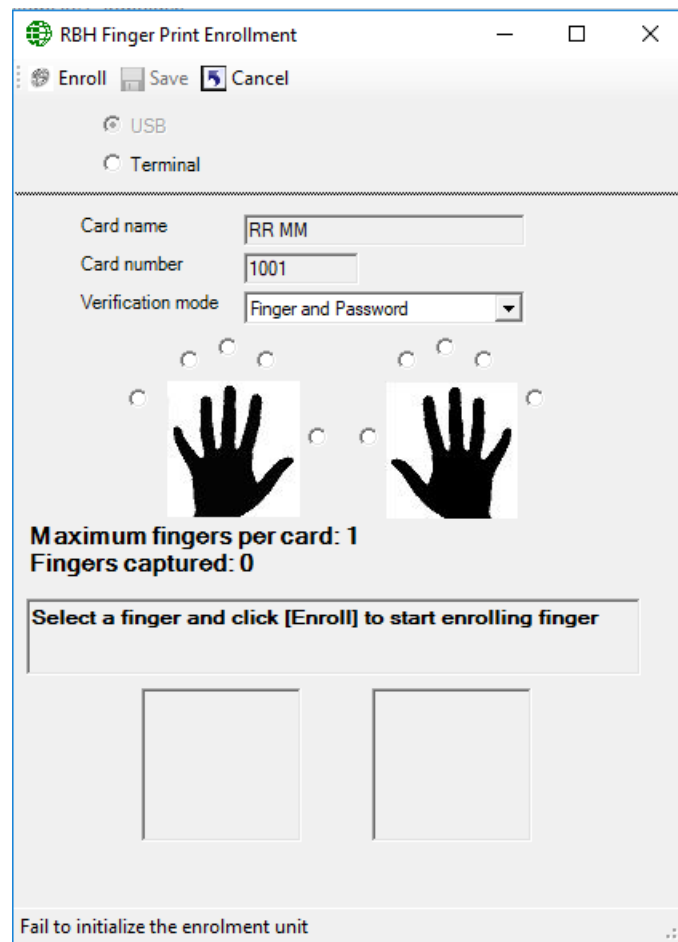
The "02 - Business Hours" option is currently selected and highlighted in blue. The "Start" and "Close" buttons remain at the bottom right.

- Click on Start button to add the cards

- ☞ Cards added through *Multi Card* utility do not get downloaded to panels. The operator needs to do a full download to the panels to download the cards added through Multi Cards.

## *F Print*<sup>24</sup>

Finger Print enrolment window varies for different manufactures of fingerprint readers



The image shows a software window titled "RBH Finger Print Enrollment". At the top, there are three buttons: "Enroll", "Save", and "Cancel". Below these are two radio buttons: "USB" (which is selected) and "Terminal". The main area of the window contains three input fields: "Card name" with the text "RR MM", "Card number" with the text "1001", and "Verification mode" with a dropdown menu showing "Finger and Password". Below these fields are two hand icons, each with five small circles above the fingers, representing the areas to be scanned. Under the hand icons, it says "Maximum fingers per card: 1" and "Fingers captured: 0". Below this is a text box with the instruction "Select a finger and click [Enroll] to start enrolling finger". At the bottom of the window, there are two empty rectangular boxes for fingerprints. A status bar at the very bottom says "Fail to initialize the enrolment unit".

## *Receipt*

Receipt will create a printable document for the cardholder to sign indicating that the cardholder has taken possession of the card.

---

<sup>24</sup> This selection is only available if the optional license for the Finger Print Reader has been purchased and installed.



Receipt	
	4/18/2012 4:18:15PM
Card Name	STEPHEN ANDRULIS
Card Number	449968
Department	Support
User Number1	0
User Number2	0
User Text 1	
User Text 2	
Access Level	Master
	
<p>I have received the above card and accept that I have to report it immediately if it is lost. The card is personal and never to be handed to anybody else.</p>	
Signature	_____
Card Name	STEPHEN ANDRULIS
Date	4/18/2012

## Cardholders' Tabs

### Cards



Since cardholders can have multiple cards, card features will only be shown for selected (highlighted) card number only. When adding or editing cards ensure that the proper card number is selected (highlighted).

## 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>25</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>26</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.

<sup>25</sup> Date is displayed in the format selected under *Windows – Control Panel – Regional Settings Properties-Date*. If a two-digit year was chosen then it will be displayed in that form here.

<sup>26</sup> Date is displayed in the format selected under *Windows – Control Panel – Regional Settings Properties-Date*. If a two-digit year was chosen then it will be displayed in that form here.

## 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.

## Type<sup>27</sup>

There are currently only two card types to choose from, *Normal*, and *Visitor*. *Normal* cards are for your regular permanent cards while *Visitor* cards are for a group of continually changing cards. These cards are for the people who only need a card for a short period of time; they use the card while they are on site and then hand it back in when they leave. These are the only cards can be assigned in Visitor module.

## Options

Choose from the seven options available, if required: *Ignore Antipassback*, *Unlock Privilege*, *High Security Privilege*, *Link Execute Privilege*, *Extended Unlock Time*, *Disabled* and *Ignore Auto void*.

### ***Ignore Antipassback***

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

### ***Unlock Privilege (2)***

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 (4)***

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.

### ***Link Execute Privilege (3/5)***

Cards with this option can execute *Global Links* with either three or five consecutive *grant accesses*. Three consecutive *grant accesses* can be programmed with a different link then five consecutive *grant accesses*.

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

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

### ***Disabled***

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.

---

<sup>27</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

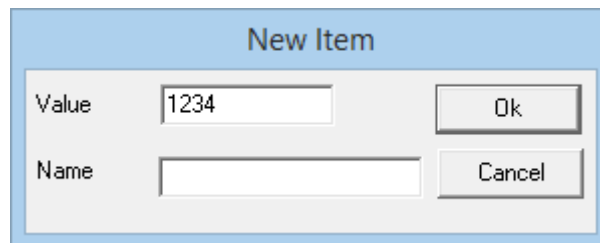
### ***Ignore Auto Void***

Cards with this option will ignore Auto void, if selected any in system settings.

### **Cards**

Up to fifty 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.

Click the *Add* button to add a card to the cardholder. Enter the card number in *Value*. *Name* is optional and is used to distinguish a cardholder's different cards from one another. Click OK to enter the card number.

A screenshot of a 'New Item' dialog box. The dialog has a light blue title bar with the text 'New Item'. Inside, there are two text input fields. The first is labeled 'Value' and contains the text '1234'. The second is labeled 'Name' and is empty. To the right of the 'Value' field is an 'Ok' button, and to the right of the 'Name' field is a 'Cancel' button.

*Copy* will enter a new card, with a different *Value*, and an activation date of the current date. All other parameters will be the same as the selected (highlighted) card.

*Edit* button is used to edit the description of any card assigned to the cardholder, and *Remove* button to delete 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. All of this data is optional, and does not affect the functioning of the Access Control System.

Integra32 - AxiomLite Cardholders

File

New Save Cancel Delete Search Multi Cards F Print Receipt

Last name First name Initials Cardnumber

Udet Ernst

Cards Profile Photo Notes More Fields

Street: 123 Main Street

City: Anytown

Province: Ontario

Country: Canada

Postal: L6S 6K8

Phone: 555-987-6543 Ext: 21

E-mail: ernstudet@gmail.com

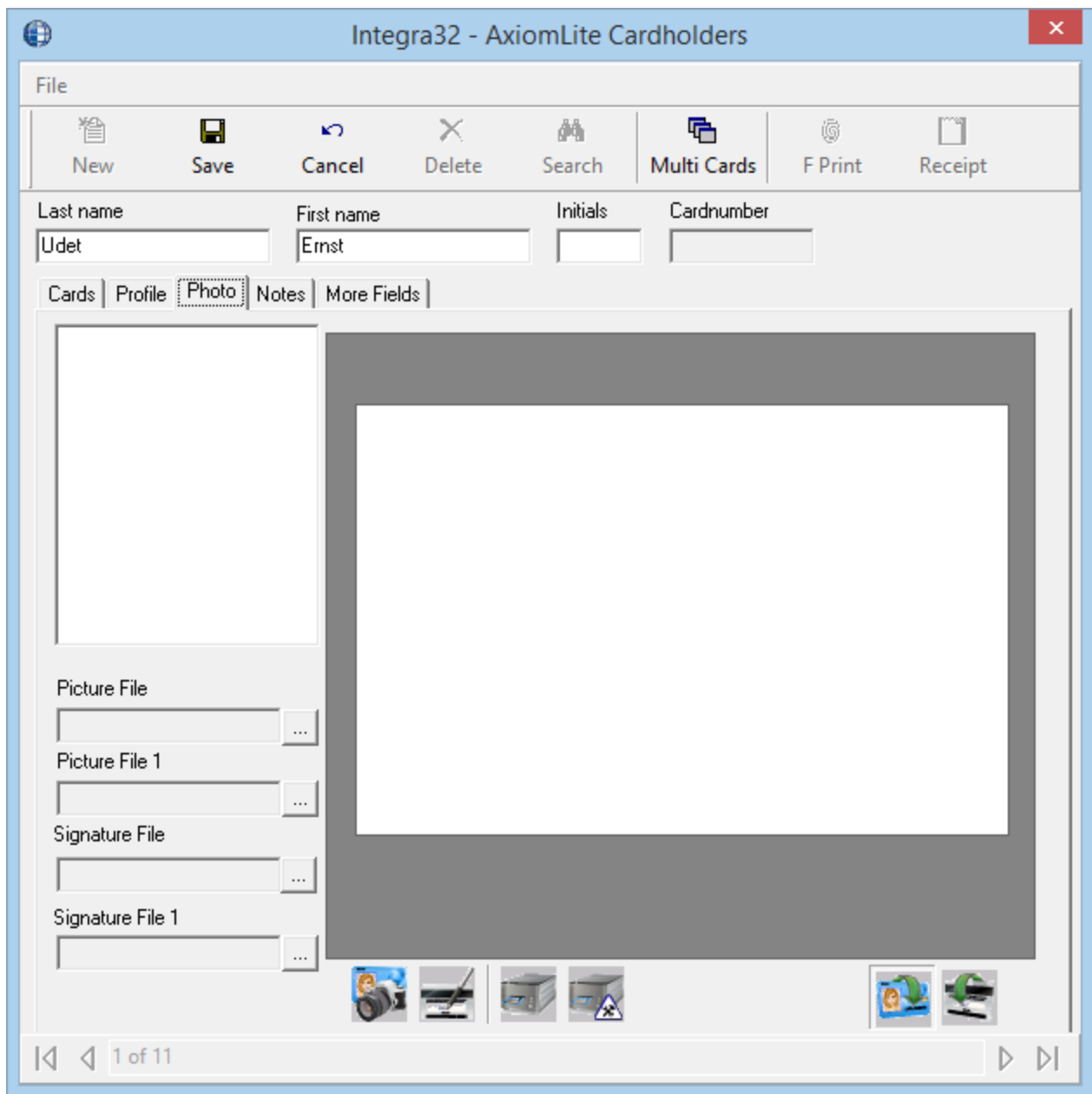
Department

1 of 11

Department can be selected from the pull down list instead of being typed in.

## 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 Integra32\Images folder. You can select or print one of the already saved templates for the cardholder in this tab if the badging option is part of the software.



Use the Card Front  and Card Back  buttons to view both sides of the badge.

## Notes Tab

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

Integra32 - AxiomLite Cardholders

File

New Save Cancel Delete Search Multi Cards F Print Receipt

Last name First name Initials Cardnumber

Udet Ernst

Cards Profile Photo Notes More Fields

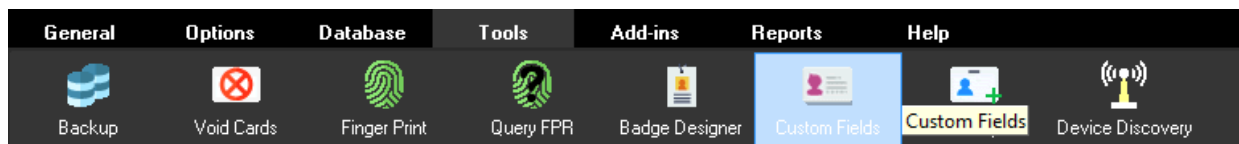
1 of 11

Notes entered here can be displayed in the Access Point Activity window when it is expanded to show *More*.

### ***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 clicking on *Custom Fields* from *Tools* menu



Double click on the Label of any of the fields to be changed in edit mode and rename the field name.



The screenshot shows the 'Integra32 - AxiomLite Cardholders' application window. At the top, there is a toolbar with 'Edit', 'Save', and 'Cancel' buttons. Below the toolbar, the main form has several fields: 'Last name', 'First name', 'Initials', and 'Cardnumber'. A 'More Fields' tab is active, revealing a section with 'User Number 1', 'User Text 1' through 'User Text 6', 'User Date 1', and 'User Date 2'. A 'Rename Control' dialog box is open, prompting the user to 'Enter New Name' for 'User Text 1'. The dialog has 'OK' and 'Cancel' buttons. The background form fields are partially obscured by the dialog box.

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.

# Chapter 7

## Visitor Management<sup>28</sup>

---

Integra32 - AxiomLite Security System Visitor

Add Edit Save Delete Cancel Search Check In Check Out Receipt Track

Lastname: Baumer Firstname: Paul  
National ID: Card Number: 0

General More Fields Assets Track Photo

Personal Information

Reason to Visit: Address:  
Date of Birth: 3/19/2007 City:  
Phone: State:  
E-mail: Country:  
Employer: Postal Code:  
Time allotted: 0 Hours  
Notes:

Visiting

Lastname: Department: Firstname: Employee Card: 0

Last Checked In

Last Visited: William Bishop Checked In: 8/24/2018 2:11:14 PM  
Checked Out: 8/24/2018 2:18:06 PM

1 of 1

The Last Name and First Name fields are mandatory fields and must have data before you can save the visitor while the NationalID field is optional. All three of these fields are 'quick search' fields. Type data into the 'quick search' field and hit Enter. The 'quick search' field will call up the record with matching data or will produce a list of records to choose from.

Card Number is also a 'quick search' field and is ideal for calling up a record when a visitor is checking out.

### Add

Click *Add* to enter a new visitor.

---

<sup>28</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.



### **Edit**

Click *Edit* to modify an existing visitor.



### **Save**

Click *Save* to save changes made by adding a new visitor or modifying an existing one.



### **Delete**

Click *Delete* to permanently remove a visitor from the database.



### **Cancel**

Click *Cancel* to exit edit mode and not save any changes made.



### **Search**

Click *Search* to call up a search screen to look for a specific visitor.

Select the search field, enter the search criteria, and click search. The results of the search will be posted in the lower half of the screen.



### **Check In**

Click *Check In* to have the visitor check in to the system.



### **Check Out**

Click *Check Out* to have the visitor check out of the system.

## Track

Click *Track* to display the access points that the visitor has been granted access to while checked-in.

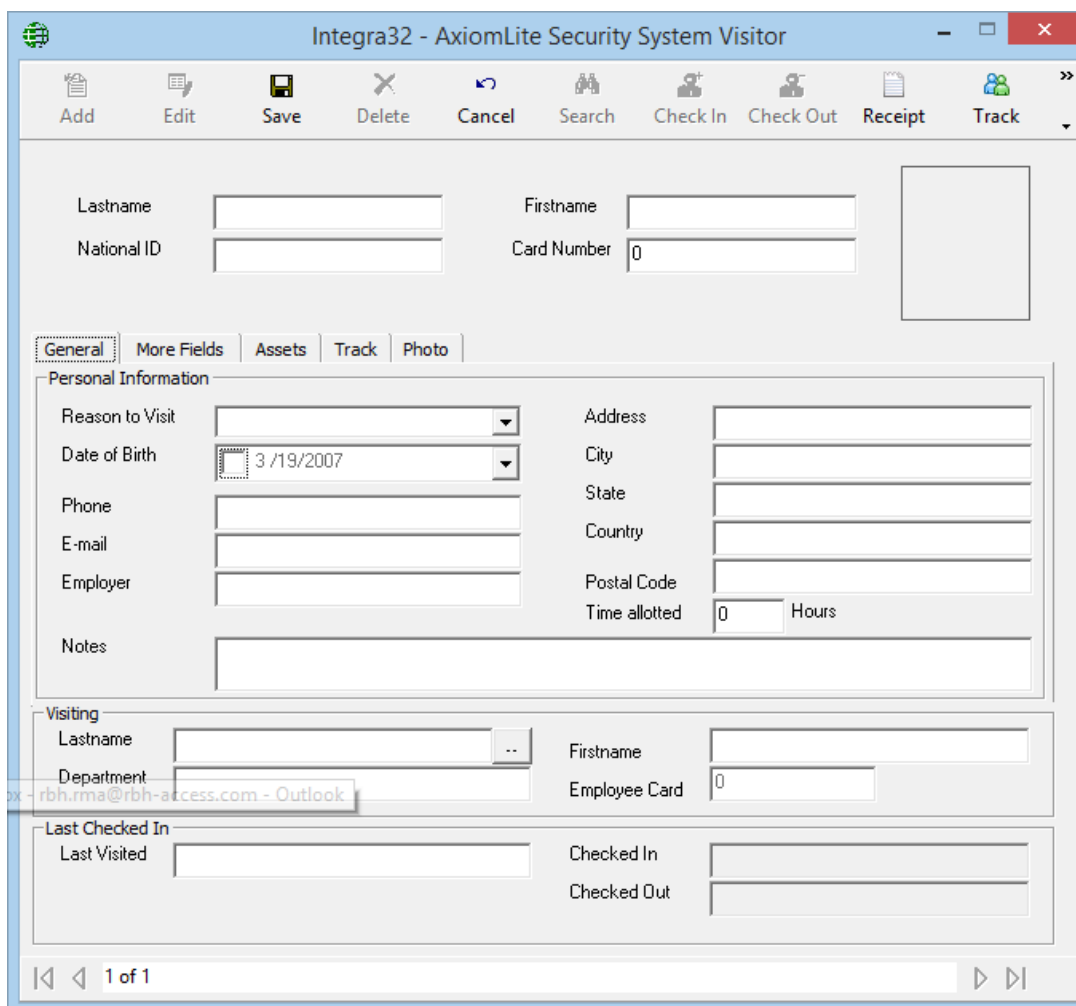
## Receipt

Click *Receipt* to print a receipt for a visitor's assets.

## E Mail

Click on *E Mail* to send an email to the cardholder being visited. For this to work the sender's email information must be configured in VM Configuration under [Email Configuration](#) and the being visited cardholder's [Profile Tab](#) must have an email address.

## General



*Personal Information* data is optional and specific to the visitor and not to the card.

Select who is being visited by clicking on the browse button [...] and search for the appropriate cardholder. *Department* and *Employee Card* will be filled in by the system.

*Last Check In* is also filled in by the system.

## More Fields

The screenshot shows the 'Integra32 - AxiomLite Security System Visitor' application window. The 'More Fields' tab is selected, displaying a form with various input fields. The 'General' tab shows 'Baumer' for Lastname and 'Paul' for Firstname. The 'More Fields' tab includes five 'User Text' fields, two 'User Number' fields, and a 'User Date 1' field set to '3 /19/2007'. Below this, the 'Visiting' section has fields for 'Lastname', 'Firstname', and 'Employee Card'. The 'Last Checked In' section shows 'Last Visited' as 'William Bishop', 'Checked In' as '8/24/2018 2:11:14 PM', and 'Checked Out' as '8/24/2018 2:18:06 PM'. The bottom of the window shows a navigation bar with '1 of 1'.

Field	Value
Lastname	Baumer
Firstname	Paul
National ID	
Card Number	0
User Text 1	
User Text 2	
User Text 3	
User Text 4	
User Text 5	
User Number 1	
User Number 2	
User Date 1	3 /19/2007
Visiting Lastname	
Visiting Firstname	
Visiting Employee Card	0
Last Visited	William Bishop
Checked In	8/24/2018 2:11:14 PM
Checked Out	8/24/2018 2:18:06 PM

*More Fields* are customized fields to hold data pertaining to your visitors. The headings for these fields are set in Visitor management Configuration under the

[More Fields](#) tab.

## Assets

Under the *Assets* tab, in edit mode, the operator can enter data concerning anything that the visitor brought with them to the site.

To print a receipt for these assets click on the *Receipt* button.

If there is any information entered under a visitor's asset then a reminder will pop up when the visitor checks out. After the visitor has checked out this asset data is deleted.

## Track

Integra32 - AxiomLite Security System Visitor

Add Edit Save Delete Cancel Search Check In Check Out Receipt Track

Lastname: Baumer Firstname: Paul  
National ID: Card Number: 0

General More Fields Assets **Track** Photo

Track

Visiting  
Lastname: Department: Firstname: Employee Card: 0

Last Checked In  
Last Visited: William Bishop  
Checked In: 8/24/2018 2:11:14 PM  
Checked Out: 8/24/2018 2:18:06 PM

1 of 1

The *Track* tab will display the access points that the visitor has been granted access to since their check-in time. Simply click on the track button on toolbar to display/refresh the information.



**Only visitors that are checked-in can be tracked. If the visitor has checked-out you can get information on where they have been from the**



**Visitor Reports.**

## Photo

Integra32 - AxiomLite Security System Visitor

Add Edit Save Delete Cancel Search Check In Check Out Receipt Track

Lastname: Baumer Firstname: Paul  
National ID: Card Number: 0

General More Fields Assets Track **Photo**

Photo

Picture Files

Signature

1 of 1

The *Photo* tab shows all the templates from the badging template module. Only the fields valid for the visitor management will be shown on the badging templates in this module.



# Chapter 8

## Reports

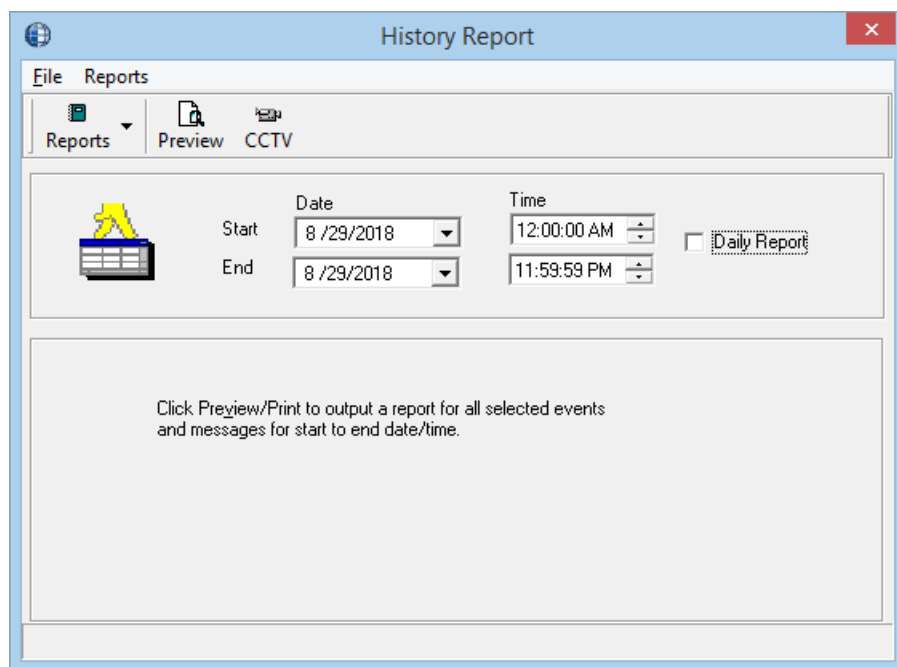
---

The Integra32™ 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*, *Database Report* or *Visitors 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

The *Print* command will produce a printed report showing the data selected for the chosen report.

### Select History Path

If your history files are not being saved to the Integra32 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.

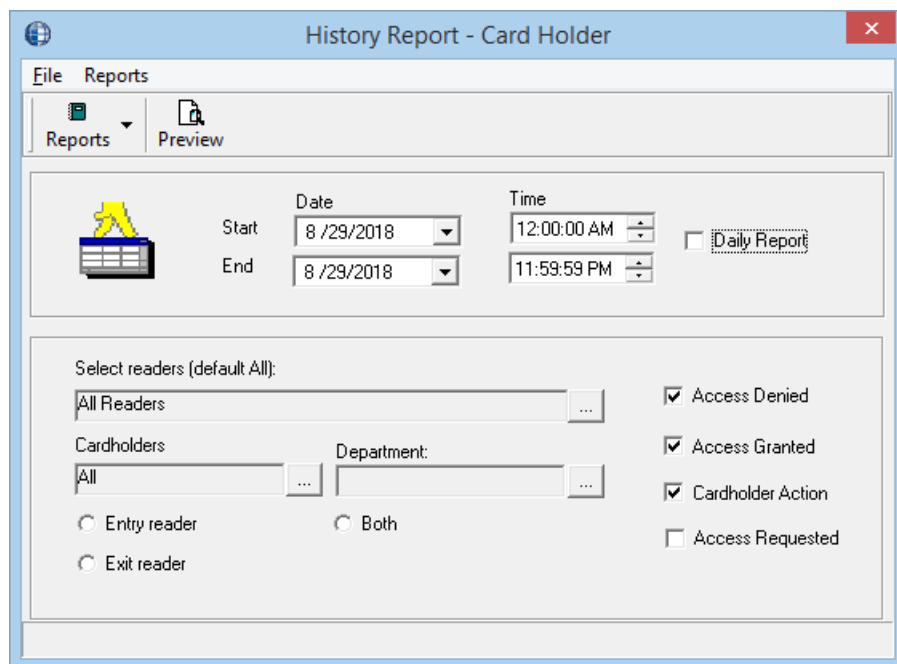
The user sets the *Start Date*, *End Date*, *Start Time*, and *End Time* for any report they have selected to preview or print. The report will span from the start time of the start date to the end time of the end date unless the daily report box is checked. If the daily report box is checked then the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

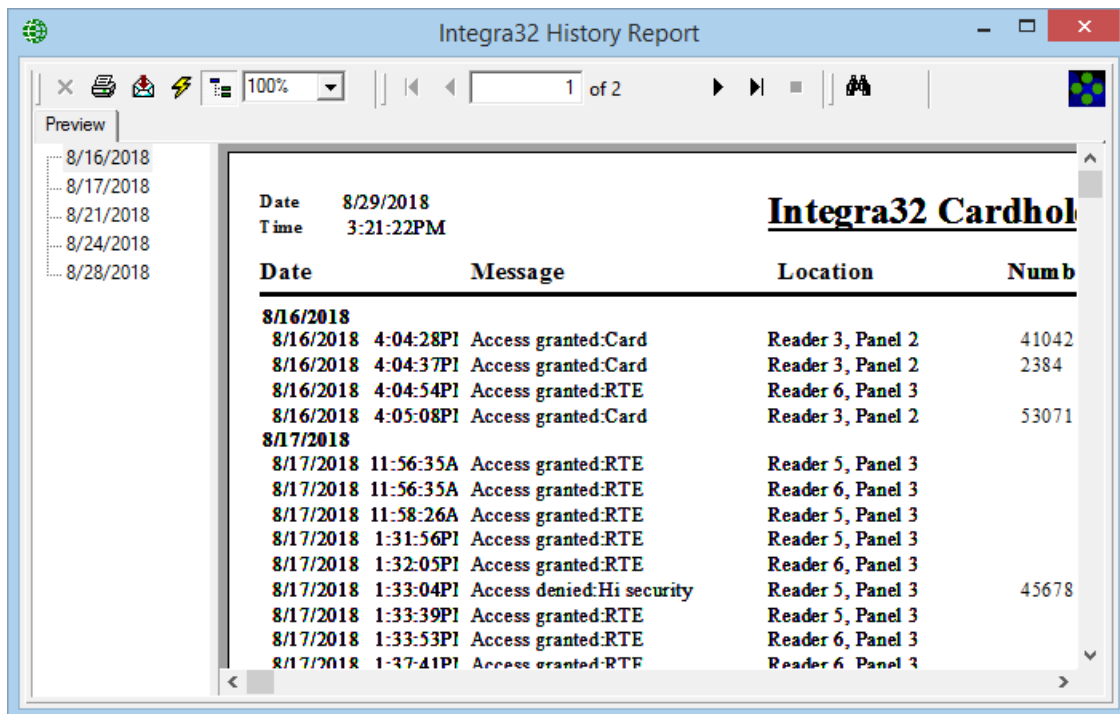


- Select the *Start* and *End*, *Date* and *Time* for the time period you want to preview the report for.
  - If the report is to cover only specific hours each day then check *Daily Report* so that the *Start* and *End Time* will be applied each day.
- Click the *Select Readers* button to select the 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 customize 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.

**Radio buttons:** Select one of *Entry Reader*, *Exit Reader*, or *Both*. Readers are exit readers if they are connected to the Out Reader side of an Exit Reader Module or if their TAM terminal is grounded (IRC2000-4/-5 boards). Otherwise they are entry readers (this includes all readers on IRC2000-3/-2 boards)

- ☐ Entry reader
- ☐ Exit reader
- ☐ Both




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<sup>29</sup>

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

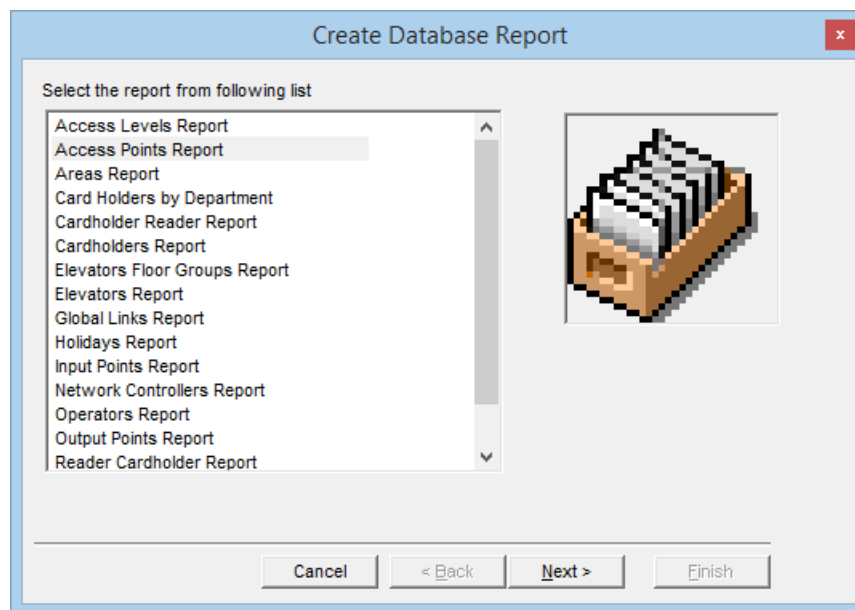
<sup>29</sup> This selection is only available if the optional license for the DVR Software has been purchased and installed.

Send DVR Commands					
Date	Message	Device	Card	Operator	Play
29-Mar-2005 7:45:00 am	Mode changed:Unlock pending fir	Reader 1, Panel 1			
29-Mar-2005 10:41:44 am	Access granted:Card	Reader 13, Panel 7	Harpinder Karm		
29-Mar-2005 10:43:26 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:47:26 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:48:03 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:48:58 am	Access granted:Card	Reader 13, Panel 7	Harpinder Karm		
29-Mar-2005 10:49:07 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:52:23 am	Access granted:Card	Reader 13, Panel 7	Charles Score		
29-Mar-2005 10:52:32 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:55:22 am	Access granted:Card	Reader 13, Panel 7	Steve Taylor		
29-Mar-2005 10:55:40 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:55:54 am	Access granted:Card	Reader 13, Panel 7	Charles Score		
29-Mar-2005 10:56:22 am	Access granted:Card	Reader 13, Panel 7	Melisa Demara		
29-Mar-2005 10:56:40 am	Access granted:Card	Reader 13, Panel 7			

Double click the line that has a *Camera sign* , with the event that is to be played back.

## Database Reports

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

- **Card Holders by Department**
  - **Cardholder Reader Report**
  - **Cardholders Report**
  - **Elevator Floor Group**
  - **Elevator Report**
  - **Global Links Report**
  - **Holidays Report**
  - **Input Points Report**
  - **Network Controllers Report**
  - **Operators Report**
  - **Output Points Report**
  - **Reader Cardholder 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 cannot 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.

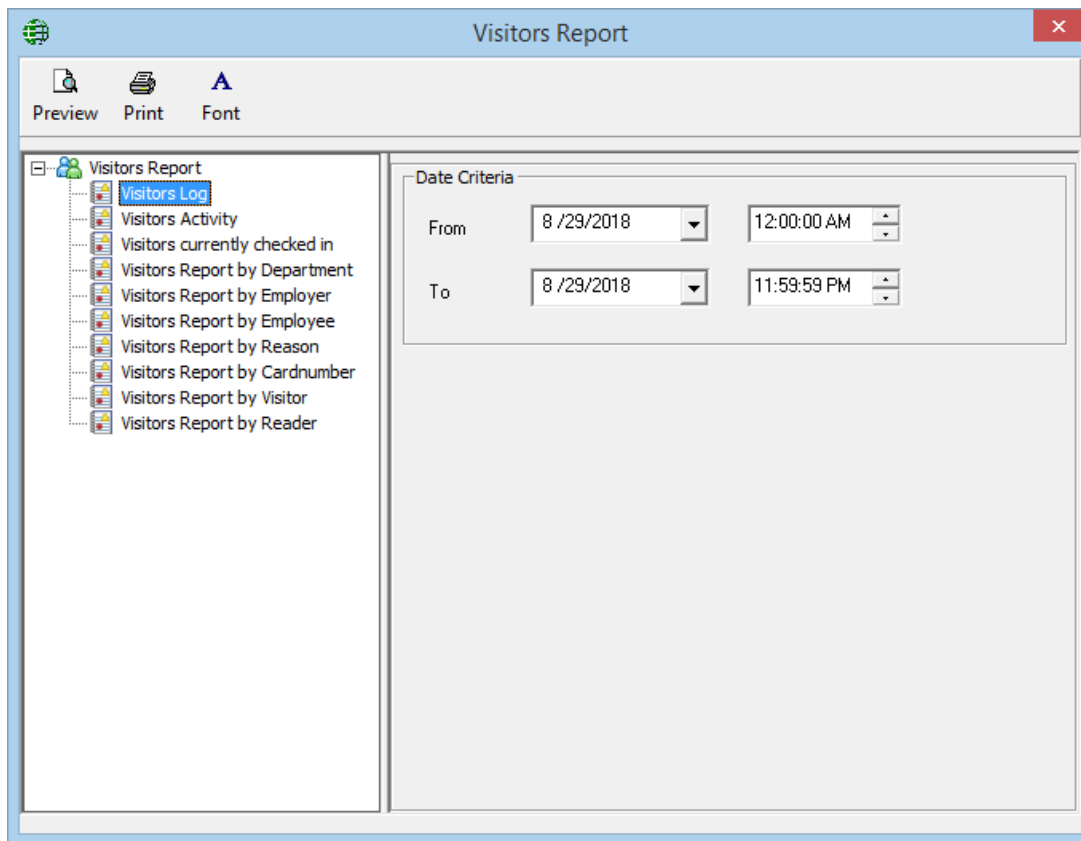
The user can follow similar steps to preview or print other kinds of *Database Reports* as well.

## Visitor Reports<sup>30</sup>

Select *Visitor Reports* from the *Reports* menu to launch the following window, where the user has the option of selecting from many available visitor report formats.

---

<sup>30</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.



Choose a report format and select the *Start* and *End*, *Date* and *Time* for the time period you want to preview the report for.

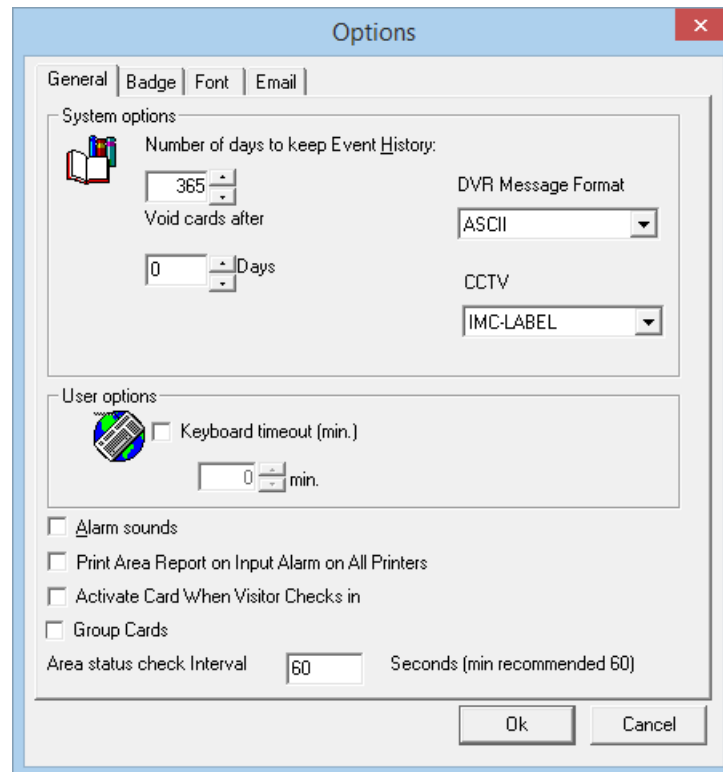
# Chapter 9

## Options

---

### System Options

#### General



### System Options

#### ***Number of days to keep Event History***

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.

#### ***Auto void cards after:***

At 1:00 am cards that have not been used within the specified number of days will be automatically deactivated. No cards will be deactivated if the number of days is set to zero.

### **DVR Message Format:**

- ☒ This option allows sending messages to DVR Servers. You can select one of the two options available: ASCII or XML. For more detailed information, see *Send Message to DVR* on Page [73](#)

**NOTE:** Integra32™ server services need to be restarted whenever switching between the *DVR Message Format: ASCII and XML*.

### **DVR**

The DVR box allows to choose one of the two options available for video display: IMC-HISTORY or IMC-LABEL. IMC-LABEL displays the camera label on the played back history from the DVR.

### **User Options**

If a user has entered a keyboard time-out, Integra32™ will automatically log-out if there is no mouse or keyboard activity for the duration of keyboard time-out period.

### **Alarm sounds**

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

### **Print Area Report on Input Alarm on All Printers**

Click in the check box to turn on the feature (click again in the check box to turn it off). With this box checked all printers listed on the server will print an area report when the input goes into alarm. If the box is not checked the report is printed only on the default printer of the server. An input must be selected in the area properties before any report can be printed.

### **Activate Card When Visitor Checks In**

With this box checked a visitor's card will be activated when the visitor is 'checked in' and deactivated when the visitor is 'checked out'.

### **Group Cards**

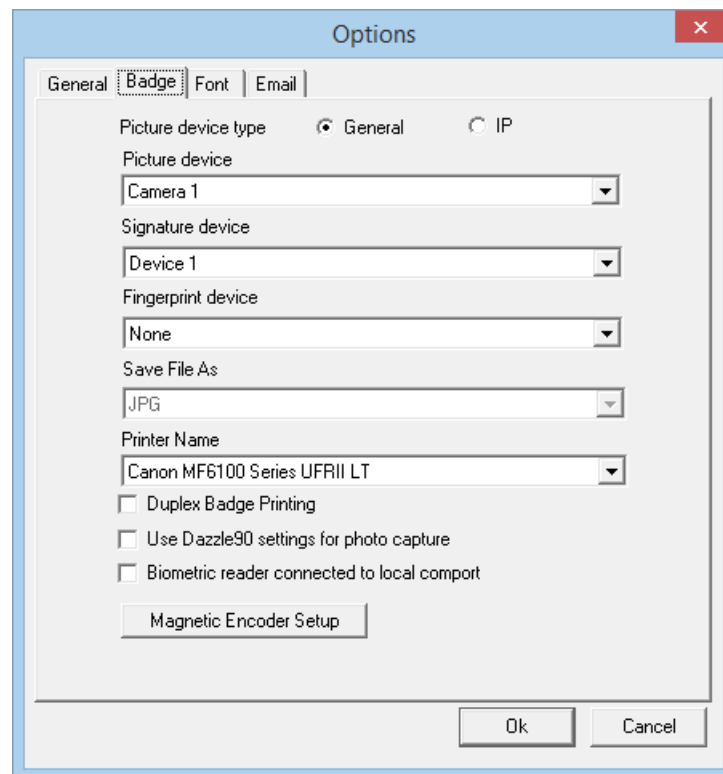
Global Antipassback by Grouping Cards function is an optional feature. This selection tells the system that cards under a single cardholder are to be grouped, so that if one of these cards is used to enter an area, all of the cards in the group will not be allowed to be used to go into the same area. Any one of the cards may be used to go into another area. For this feature to work *PC Decision Required* and *Hard Antipassback* (Page [75](#)) must be ON. For more detailed information refer to TB71 Integra32 Group Cards GAPB.

### **Area Status Check Interval**

60 Seconds is the default time for Area checking intervals to check if any of the Area which has an output configured, is empty so that the specified output is turned on. The users are given the option to change this timing if required.



## 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. IP cameras can be selected as well.

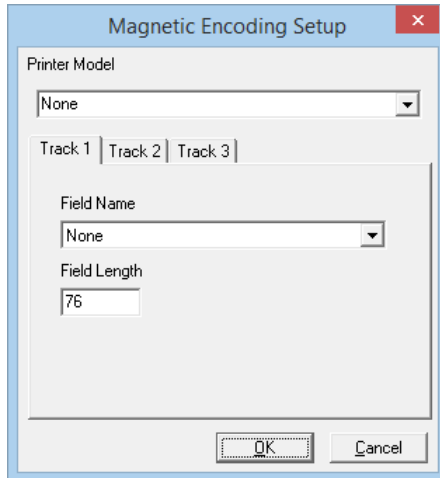
A couple finger print devices are supported. They require their respective integration software to be installed for proper operation.

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.
- ☒ Check 'Use Dazzle 90' if you are using a Dazzle 90 for photo capture.
- ☒ If you are connecting Biometric Readers to your COM port check the box.

### 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.



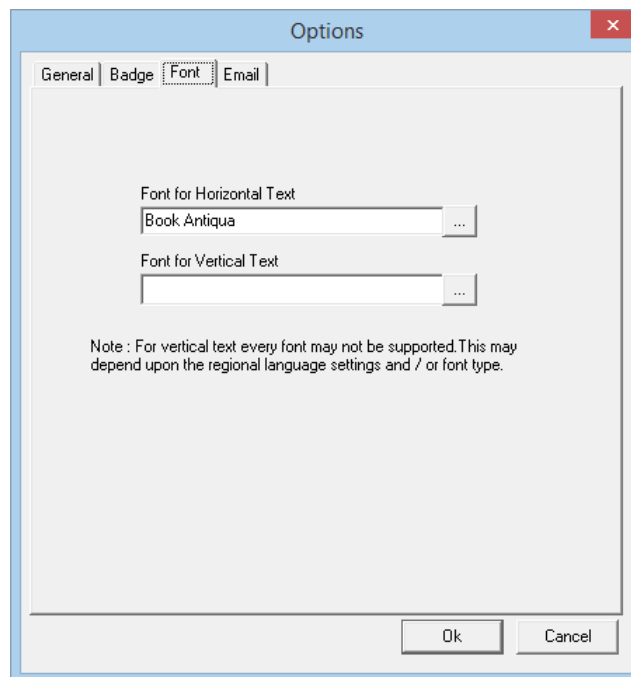
Select the printer model in this window. The fields to encode can be selected for each track once the printer model is selected.

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.

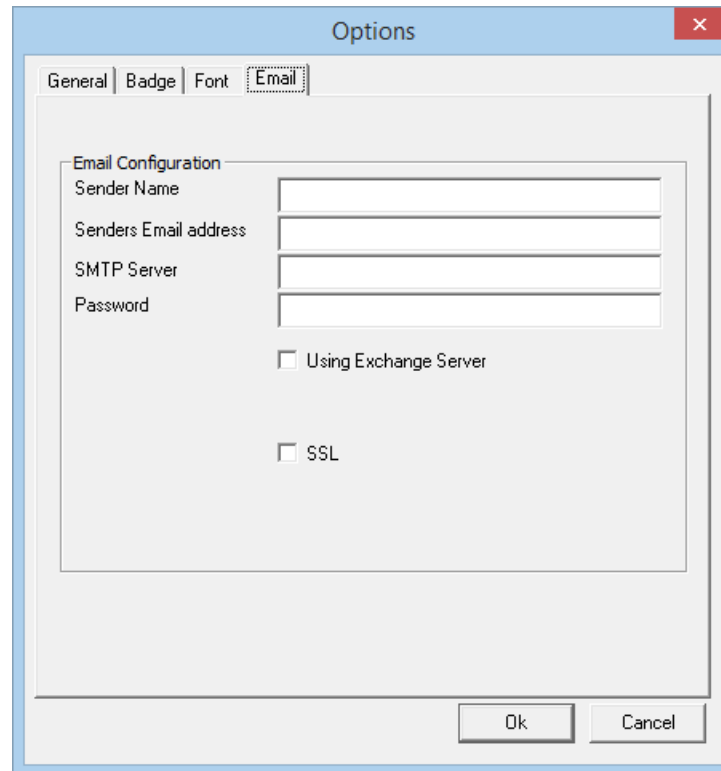
## Font

You can change the default font for the main client screen by browsing the font list, select a font, and click OK. The default font is MS San Serif.



## Email

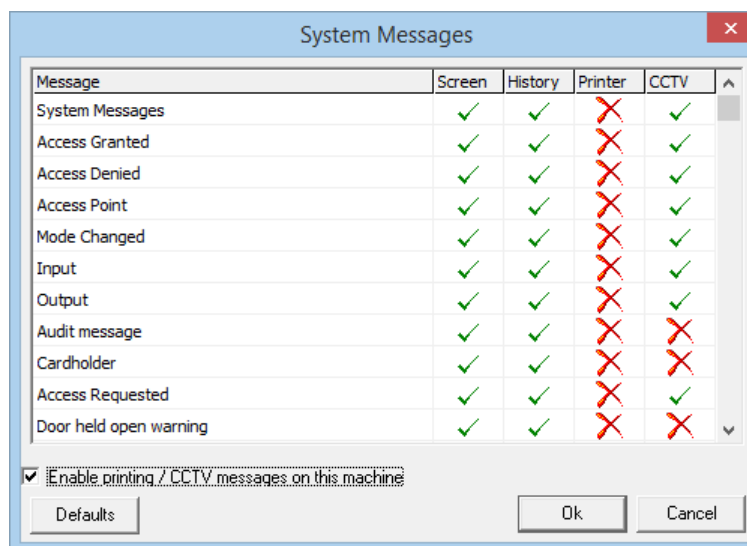
This window is used to configure email settings for Message Server. For more information on how to configure the email information, see page [Error! Bookmark not defined.](#) for users' setup and page [72](#) for configuring the Access point Messages. This option is added in software version 3.8.6R4.2 or higher.



The 'Options' dialog box has four tabs: General, Badge, Font, and Email. The 'Email' tab is selected. It contains an 'Email Configuration' section with four text input fields: 'Sender Name', 'Senders Email address', 'SMTP Server', and 'Password'. Below these fields are two checkboxes: 'Using Exchange Server' and 'SSL'. At the bottom right are 'Ok' and 'Cancel' buttons.

Fill in the required information as per your email settings.

## System Messages



The 'System Messages' dialog box contains a table with columns: Message, Screen, History, Printer, and CCTV. The table lists various system messages and their enabled/disabled status for each output method. Below the table is a checkbox labeled 'Enable printing / CCTV messages on this machine' which is checked. At the bottom are 'Defaults', 'Ok', and 'Cancel' buttons.

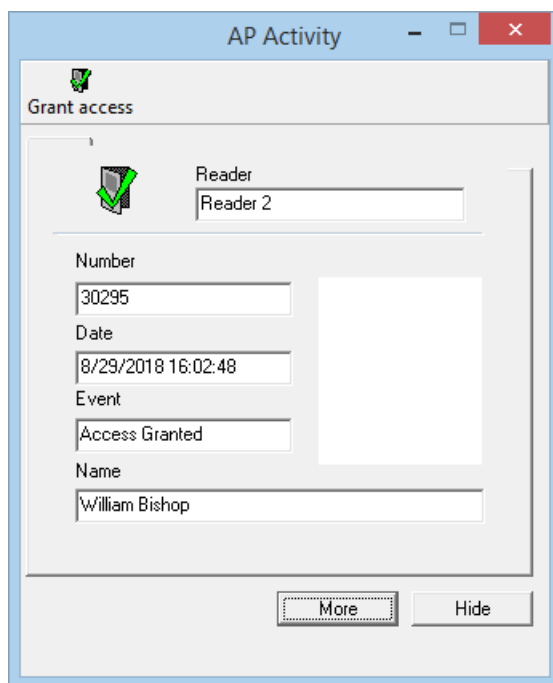
Message	Screen	History	Printer	CCTV
System Messages	✓	✓	✗	✓
Access Granted	✓	✓	✗	✓
Access Denied	✓	✓	✗	✓
Access Point	✓	✓	✗	✓
Mode Changed	✓	✓	✗	✓
Input	✓	✓	✗	✓
Output	✓	✓	✗	✓
Audit message	✓	✓	✗	✗
Cardholder	✓	✓	✗	✗
Access Requested	✓	✓	✗	✓
Door held open warning	✓	✓	✗	✗

The user can customize how the system handles messages. (E.g. If the user doesn't want a particular message to appear on screen, like the Access Requested message, it can easily be turned off with a simple click. Quickly change between 'Yes' ✓ and 'No' ✗, to stop the display of selected messages on the screen or from being sent to history.) The user can also send messages to a printer (selectable by message).

Messages can also be sent as ASCII/XML messages to DVR. CCTV configuration will be required for this to function correctly.

The user can also select what messages to send as ASCII/XML messages by simply changing between 'Yes' ✓ and 'No' ✗ for DVR messages. Check the box Enable printing/DVR messages on this machine if the DVR is configured to send ASCII/XML messages or the printer is on the local machine.

## AP Activity



The AP 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 *AP 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 AP 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 AP Activity window will show all access granted and/or access denied events that occur at selected access points.

### Grant Access

*Grant access* will grant access at the reader currently shown in the *Reader* box of the *AP Activity* window.

## 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 displayed this way. The *Less* button will remove this extension.

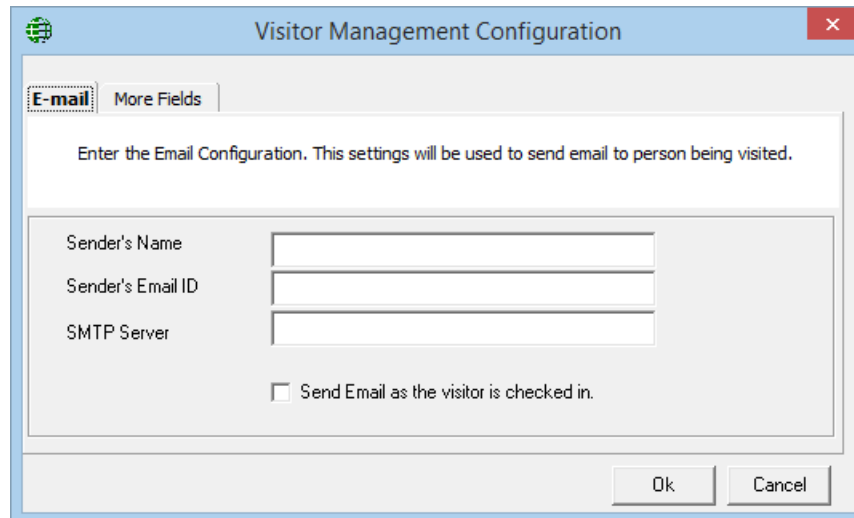
## Hide

The *Hide* button will remove the AP 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.

## Visitor Configuration<sup>31</sup>

### Email Configuration

To send emails to cardholders announcing their visitors you need to configure the sender's email information on the screen depicted below.

The image shows a screenshot of a software window titled "Visitor Management Configuration". It has a blue header bar with a globe icon on the left and a red close button on the right. Below the header, there are two tabs: "E-mail" (which is selected and highlighted) and "More Fields". The main area of the window contains the text "Enter the Email Configuration. This settings will be used to send email to person being visited." Below this text are three input fields: "Sender's Name", "Sender's Email ID", and "SMTP Server". At the bottom of the input fields is a checkbox labeled "Send Email as the visitor is checked in." which is currently unchecked. At the very bottom of the window are "Ok" and "Cancel" buttons.

The *Sender Name* is used to let the cardholder know where the visitor is, or entering from. A site may have more than one entrance that visitors can come in by and the cardholder being visited may need to know where the visitor is.

- ☒ Check the box *Send Email as the visitor is checked in* to have an email sent automatically to the cardholder being visited by the visitor. The being visited cardholder's [Profile Tab](#) must have an email address entered for this feature to work.

## More Fields

---

<sup>31</sup> This selection is only available if the optional license for the Visitor Management System has been purchased and installed.

The screenshot shows a window titled "Visitor Management Configuration" with a close button (X) in the top right corner. Inside the window, there are two tabs: "E-mail" and "More Fields". The "More Fields" tab is selected. Below the tabs, there is a text area with the instruction: "Enter the Description of user fields , this description will be then seen on visitor screen .". Below this text area, there are two columns of input fields. The left column contains five text fields labeled "Text Field 1" through "Text Field 5", each with a corresponding input box containing "User Text 1" through "User Text 5". The right column contains two number fields labeled "Number Field 1" and "Number Field 2", each with a corresponding input box containing "User Number 1" and "User Number 2", and one date field labeled "Date Field 1" with a corresponding input box containing "User Date 1". At the bottom right of the window, there are "Ok" and "Cancel" buttons.

Field Label	Field Value
Text Field 1	User Text 1
Text Field 2	User Text 2
Text Field 3	User Text 3
Text Field 4	User Text 4
Text Field 5	User Text 5
Number Field 1	User Number 1
Number Field 2	User Number 2
Date Field 1	User Date 1

Define the name of the fields for entering data under the *More Fields* tabs of *Visitor*. Use this to customize the visitor data saved in your system.

# Chapter 10

## Links

---

### Global Links

Global Links

Access Points | Input Points | Output Points | Panels

Device: Output 5

Select an event: Output On

	Device	Duration	Schedule
1.	Output 4		
2.	Output 5		
3.	Output 6		
4.	Output 7		
5.	Output 8		
6.			
7.			
8.			

Ok Cancel Apply

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 *Input Links* and *Output Links*.

# Chapter 11

## Tools

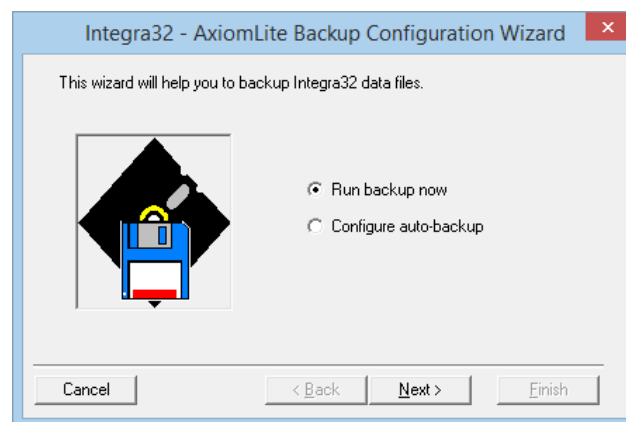
---

### Backup

The Integra32™ *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.

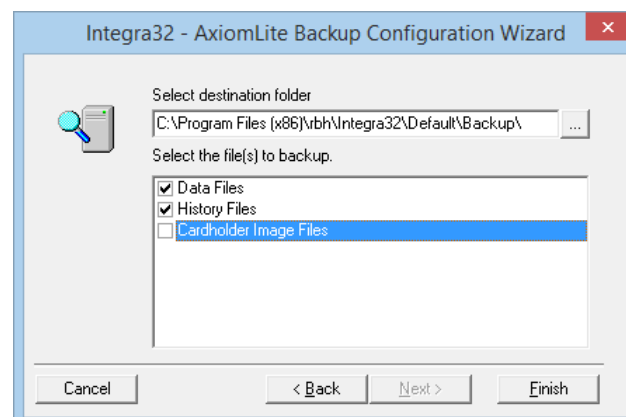
Your Operating System most likely will also have its own backup utility. It doesn't matter what method you use as long as you backup your files regularly.

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



### Run Backup Now

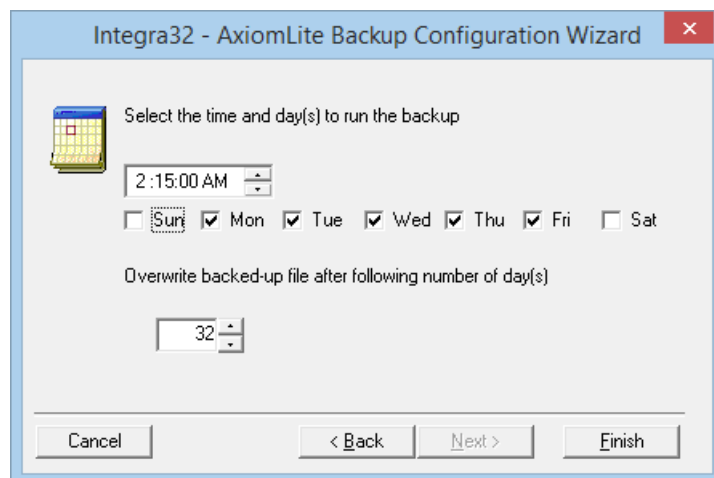
*Run Backup Now* option is used to run an immediate backup. Follow the wizard for this option. From the *Backup Configuration Screen* the destination folder into which the backup files will be saved is selected. (The default destination setting is ...\\Integra32\\backup\\.) Checking *Data Files* will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





## Configure Auto-Backup

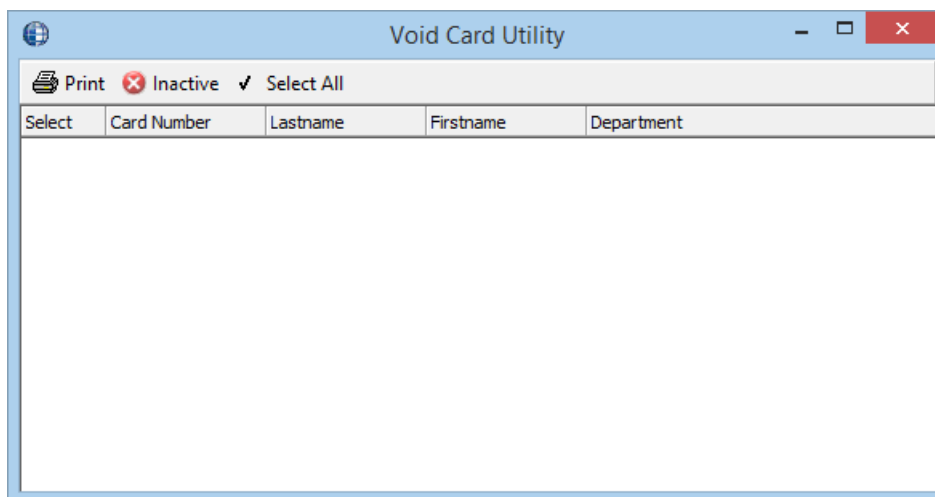
The auto-backup can be configured to happen at a specified time on specified days of the week. For example the backup can be performed at 11:30 a.m. every Monday, or at 10:15 p.m. every Tuesday and Thursday. These backed-up files are saved by date (the file is designed *bkpYYYYMMDD* where *YYYYMMDD* is the backup date), and you can set how long they are to be kept. If for example you set the backup for Monday to Friday to be kept for 32 days, backups older than 32 days will be over written.



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

## Void Cards

From *Void Cards* the operator can manually void (deactivate) cards that have not been used for a preset number of days. The number of days is set under Options – [System Options](#).



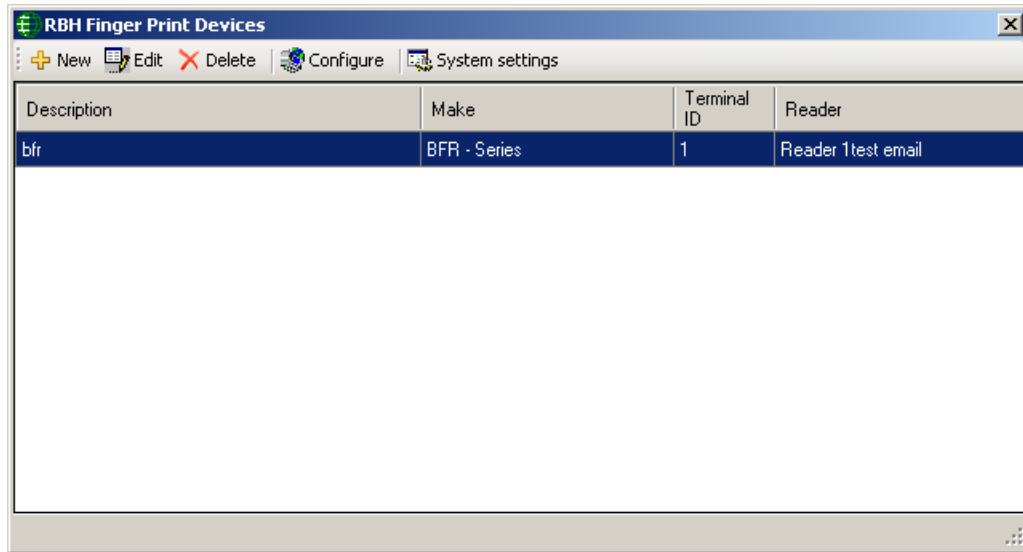
*Print* will produce a hard copy of the cardholders listed at the time *Print* is selected.



*Void* will immediately deactivate all selected cards.

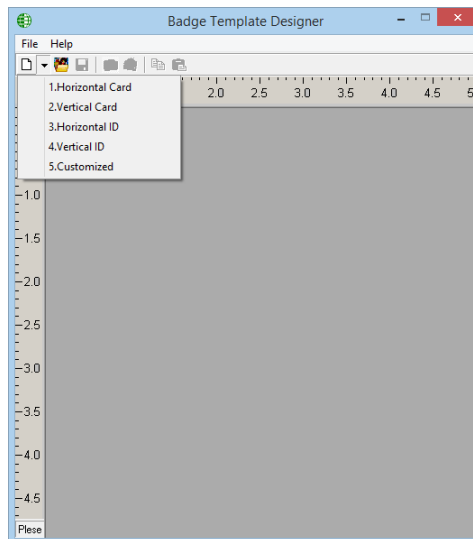
- ✓ Select All will put a check mark in the select field for all of the listed cards.

## Finger Print/Query FPR<sup>32</sup>



*Finger Print/Query FPR* opens a screen from which to configure the Bio readers (Depending upon the integration package installed) and their finger print data.

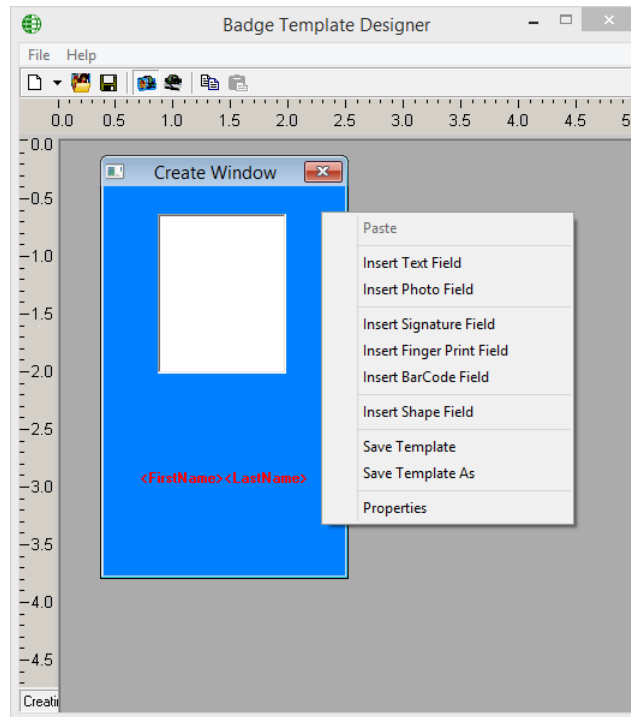
## Badge Template Designer<sup>33</sup>



<sup>32</sup> This selection is only available if the optional license for the Finger Print Reader has been purchased and installed. These windows vary as per the manufacture of FP reader.

<sup>33</sup> This selection is only available if the optional license for the Badging Software has been purchased and installed.

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<sup>34</sup> can be added to the badge.
- Signature fields<sup>35</sup> can be added to the badge.
- Barcode fields<sup>36</sup> can be added to the badge.
- 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.

## Card Custom Fields

<sup>34</sup> To use these options you may need optional hardware devices.

<sup>35</sup> To use these options you may need optional hardware devices.

<sup>36</sup> 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 Integra CD.

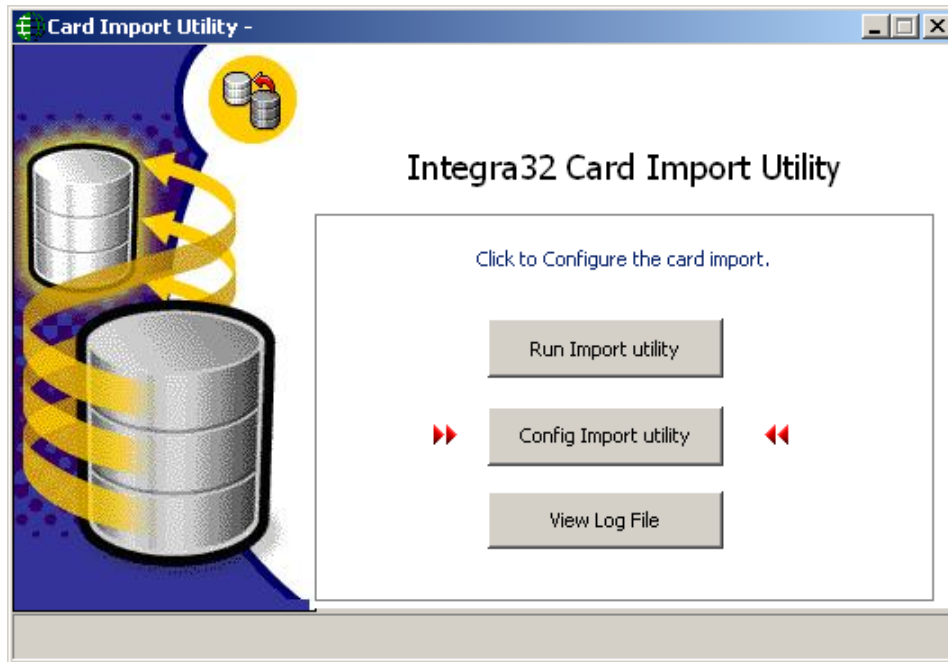
Double click on a header while in the Edit Mode to change the name of the user field. This change will be shown in the *More Fields* tab of every cardholder

## Card Import<sup>37</sup>

### Configure Import Utility

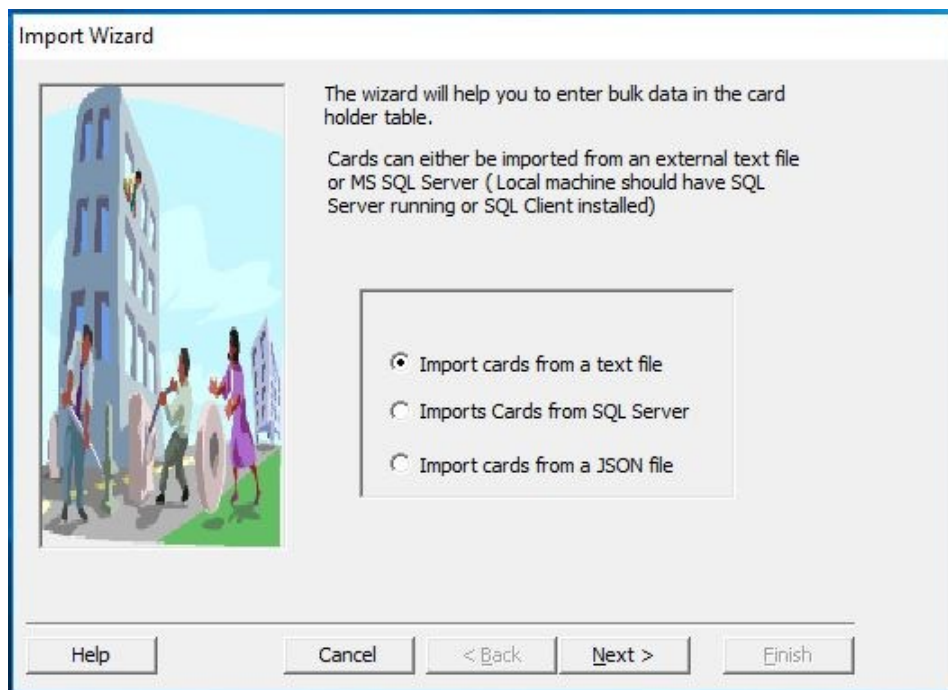
The *Integra32™ Card Import Utility* is used to import cards and cardholder data from a text file or SQL database into your *Integra32™* database.

<sup>37</sup> This selection is only available if the optional license for the Card Import Utility has been purchased and installed.



Select *Config Import Utility* to setup the import parameters.

## Import from a Text File



Enter the source and destination paths as well as the delimiting character.

Use Option:

- ☒ *Delete File upon successful Import:* If want to delete the file you are importing from after the import is complete.
- ☒ *Remove cards not found in Import file:* This option will add/update the cardholders from import file and delete all the records from cardholders which are not existing in import file anymore.(Option added in software version 3.8.20R4.2 and higher)

Click *Next*.

Import Wizard

Enter the path to the text file to import into the Cardholders database of Integra32 system.

Import From Clear  
C:\Documents and Settings\Administrator\Desktop\...

Delimited By: ,

Integra32 Database Folder  
C:\Program Files\Rbh\Integra32\Default\

☐ Delete file upon successfull import  
☐ Remove cards not found in import file

Help Cancel < Back Next > Finish

Then select the appropriate destination fields for the corresponding source fields (e.g. select *Surname* for *Field 1* and *Firstname* for *Field 2*) depending on the data in the text file.

Import Wizard

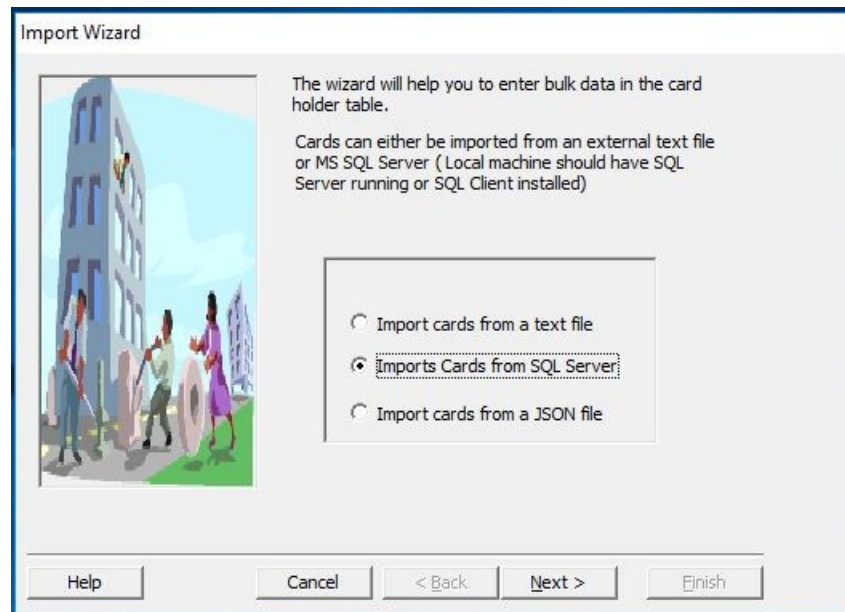
List

Source Field (Text File)	Destination Field (AxUserLT.mdb)
Field 1	Surname
Field 2	Firstname
Field 3	CardNumber
Field 4	
Field 5	
Field 6	Action
Field 7	Name
Field 8	Surname
Field 9	Firstname
Field 10	Initials
	Street
	City

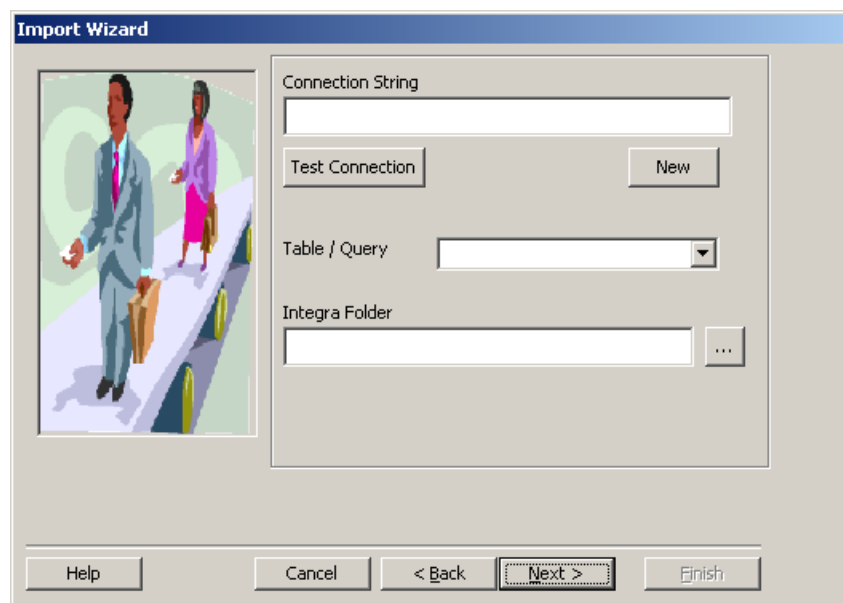
Help Cancel < Back Next > Finish

Click *Next* to continue.

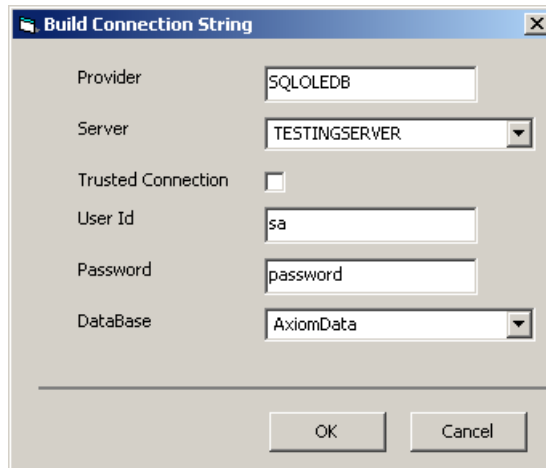
## Import from a SQL File



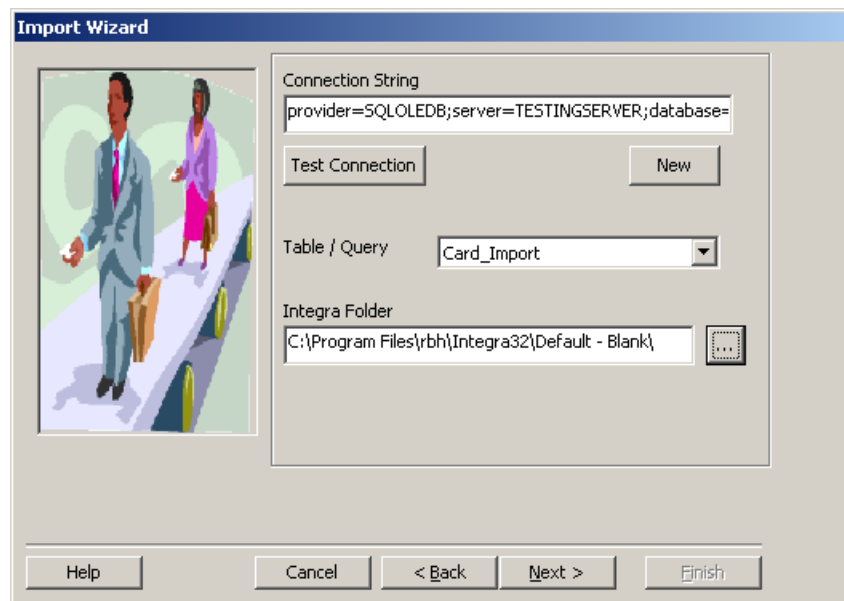
Click *Next* to input the connection string.



Use the pull-down to select the server. Enter the User Id and password. Then select the specific database on the server that holds the source data. Click *OK*.



You can verify the connection with Test Connection. Select the table or query of the database set above, and then provide the path to the target folder (by either typing or browsing).



Then select the appropriate destination fields for the corresponding source fields (e.g. select *Surname* for *lastname* and *Firstname* for *firstname*) depending on the data provided by the table or query.



**Import Wizard**

List


Source Field (Text File)	Destination Field (AxUserLT.mdb)
cardnumber	CardNumber
lastname	Surname
firstname	Firstname
faIid	AccessLevel
expirydate	ExpiryDate
	Text5
	Text6
	CardNumber
	CardName
	ExpiryDate
	AccessLevel
	Status
	PIN

Help Cancel < Back Next > Finish

Click *Next* to continue.

## Import from a Json File

**Import Wizard**



The wizard will help you to enter bulk data in the card holder table.

Cards can either be imported from an external text file or MS SQL Server (Local machine should have SQL Server running or SQL Client installed)

☐ Import cards from a text file  
☐ Imports Cards from SQL Server  
☒ Import cards from a JSON file

Help Cancel < Back Next > Finish

Click *Next* to select Json file.

Import Wizard

Enter the path to the text file to import into the Cardholders database of Integra32 system.

Import From Clear  
C:\License\staff.json ...

Delimited By: ☐

Integra32 Database Folder  
C:\Program Files (x86)\rbh\Integra32\Default\ ...

☐ Delete file upon successfull import  
☐ Remove cards not found in import file

Help Cancel < Back Next > Finish

Then select the appropriate destination fields for the corresponding source fields (e.g. select *Surname* for *lastname* and *Firstname* for *firstname*) depending on the data provided by Json file.

Import Wizard

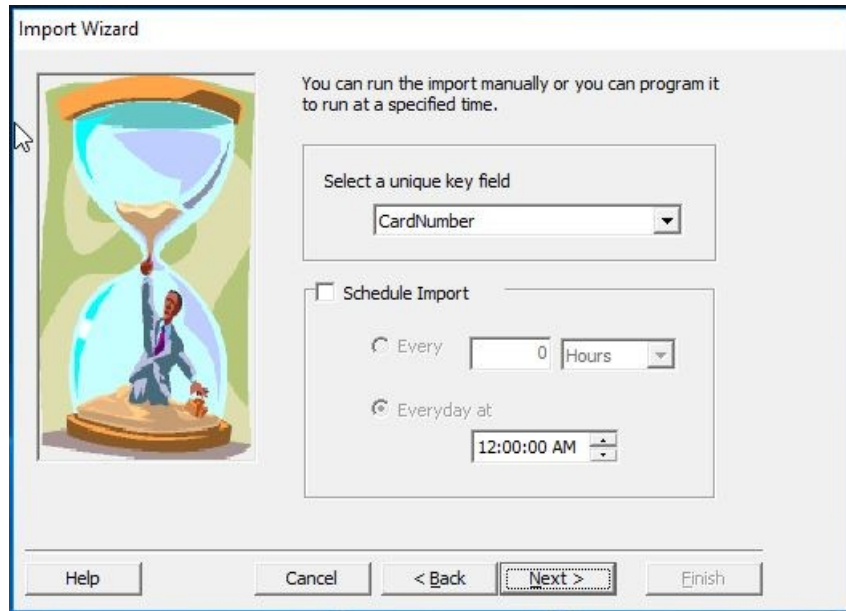
List

Source Field (Text File)	Destination Field (AxUserLT.mdb)
Field 5	
Field 6	
Field 7	
Field 8	
Field 9	
Field 10	Firstname
Field 11	Surname
Field 12	
Field 13	
Field 14	

Help Cancel < Back Next > Finish


### Complete the Configuration.

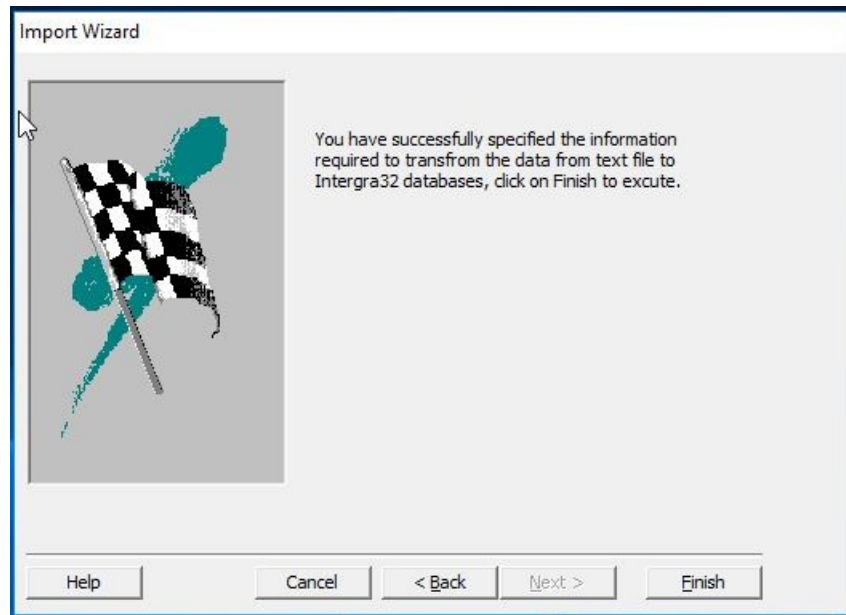
Select a unique key field. If required check Schedule Import and select either 'every x hours or minutes' or 'everyday at x'.



Check the appropriate box to have the import utility start automatically with the Operating System. To have all actions taken by the import utility logged check the second box.



Note the icon  in the windows' *system tray* indicating that the utility is active.



Click *Finish* to complete the setup.

The utility can then run on a schedule or can be opened to run manually.

### ***Run Import Utility***

Run Import Utility will run the utility immediately.



The status bar will display the progress and indicate when the import is complete.



### *View Log File*

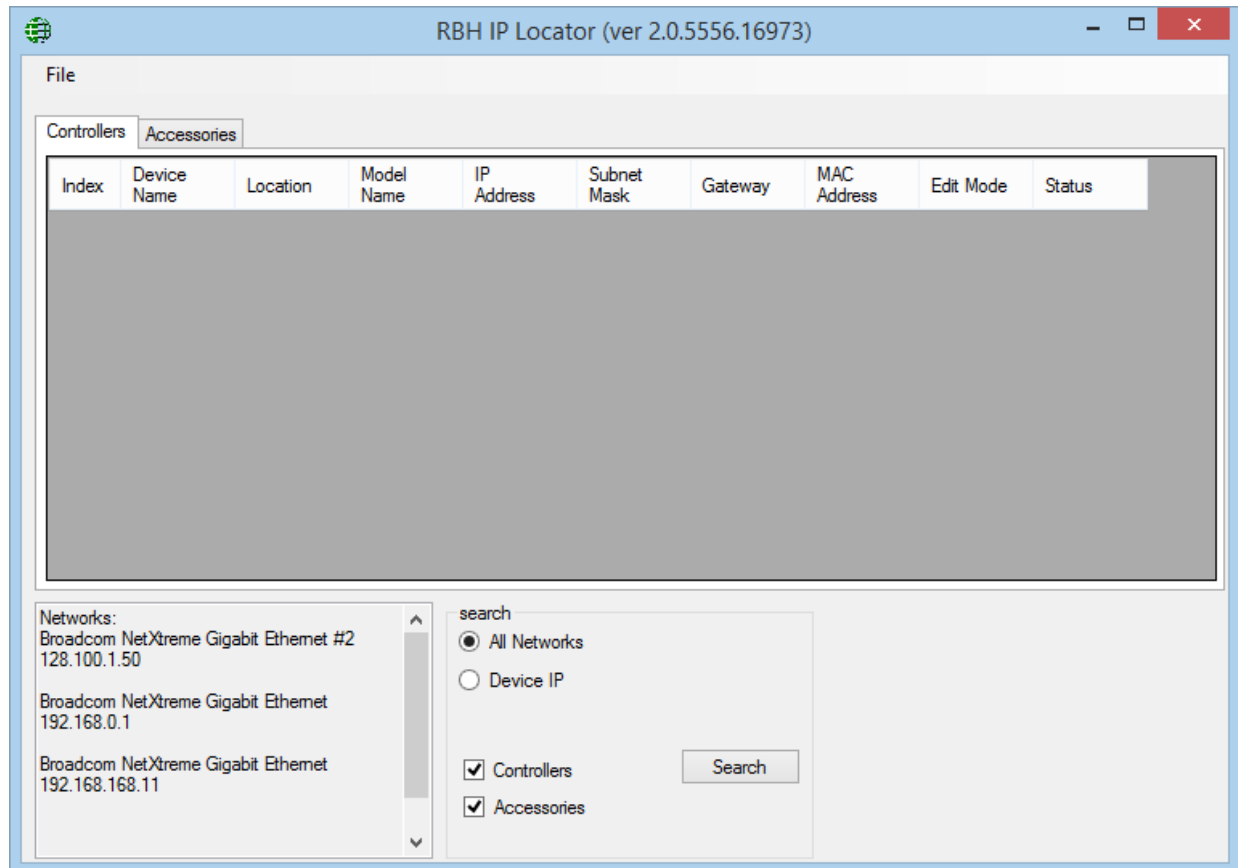


*View Log File* will call up Mimport.log a Notepad file. This file will show when the import started and ended, as well as any errors that occurred.



## Device Discovery

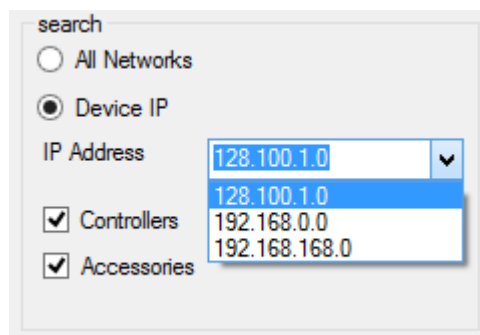
IP Locator is used to find and connect to IP Network devices for the purpose of configuring network and device parameters.



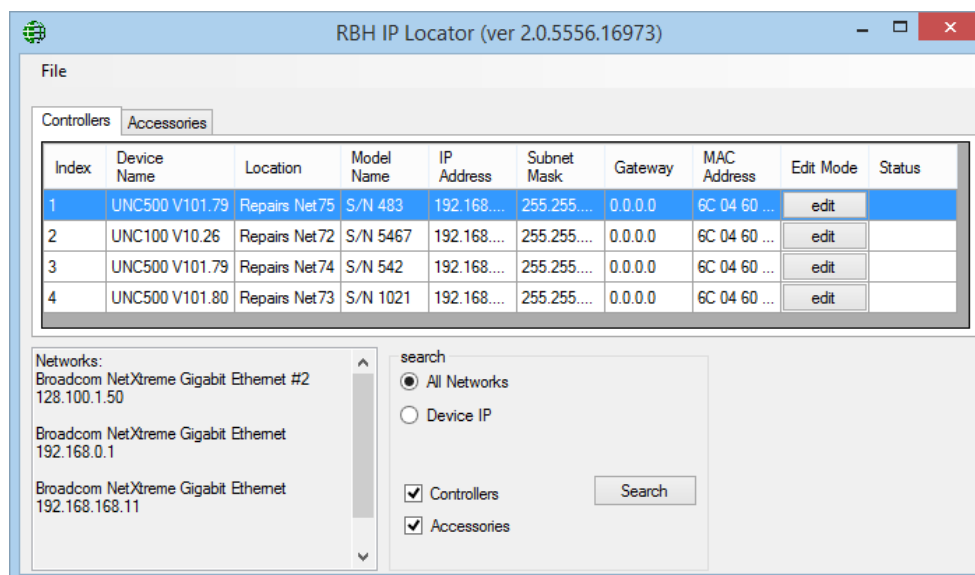
## Search

You search All Network connect to the server or you can narrow down the search with Device IP.

The search can be for controllers only (e.g. UNC100), for utility device like the LIF-100 (Accessories), or for all devices (select both Controllers and Accessories).

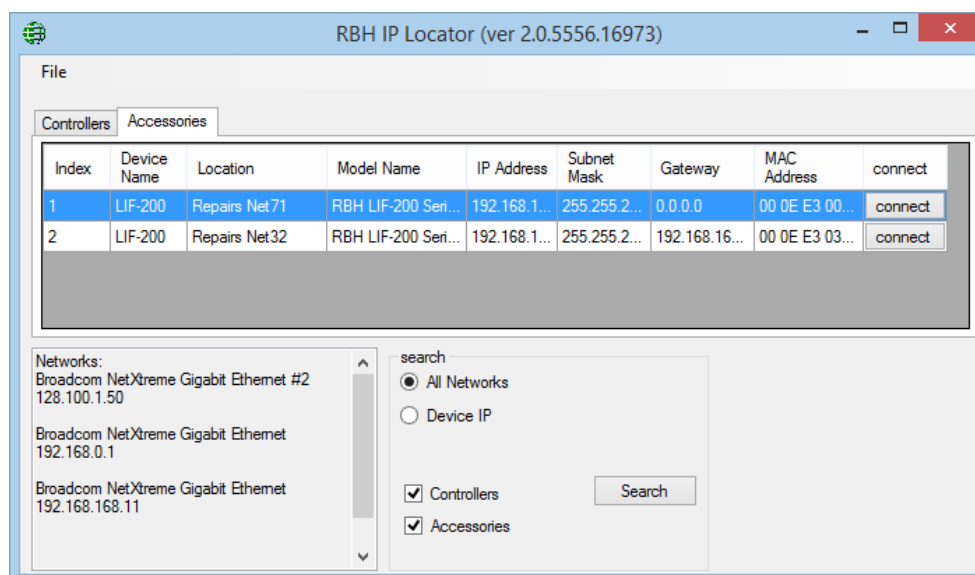


## Controllers



Click on *edit* to change the parameters of the panel.

## Accessories



Click on *connect* to change the parameters of the device.

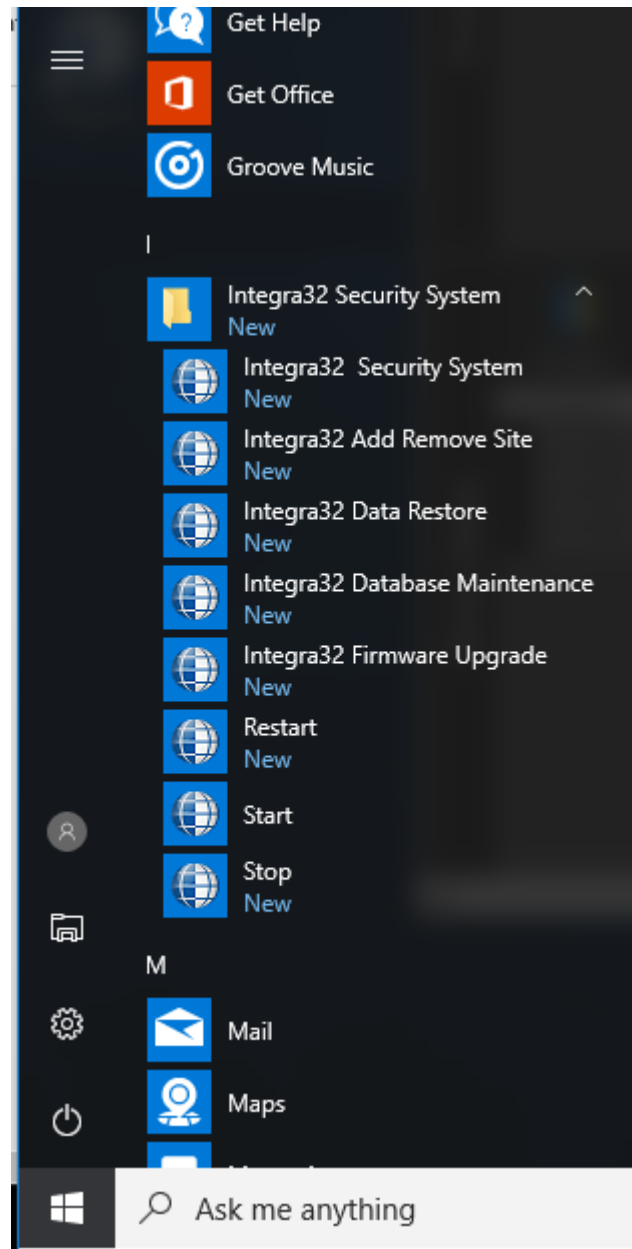
# Chapter 12

## Program Groups

---

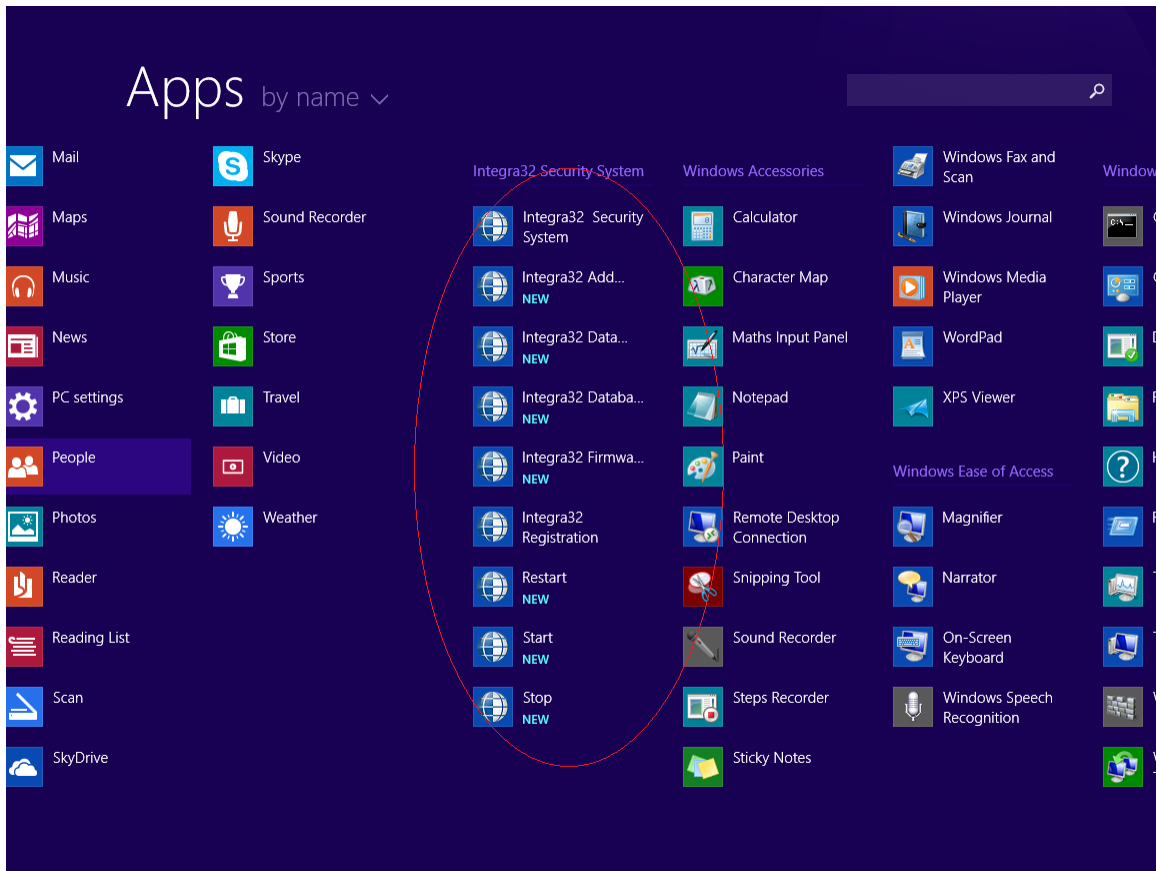
### Integra32™ Security System

Ensure that the Integra32™ system is not running before making a selection here in the ‘*Program Groups*’. All selections made here will bring up the login window for the respective window



OR

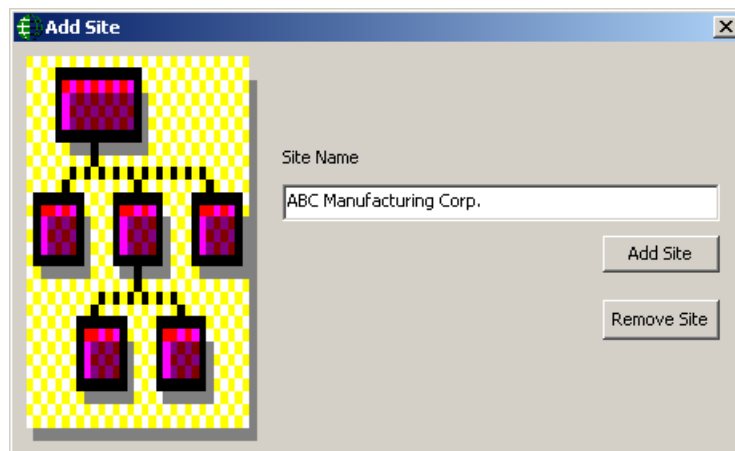




### ***Integra32™ Security System***

There are two ways to start the Integra32™ system. You can either double click the icon that was created when the system was installed, or you can click on ‘Integra32™ Security System’ in program groups in start menu of windows. Both methods will start Integra32™ system.

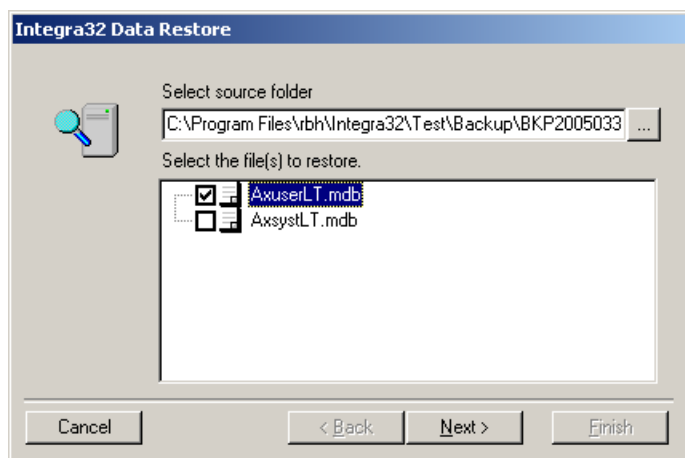
### ***Integra32™ Add Remove Site***



Type in the name of the site and either click *Add Site* or *Remove Site*. Sites added will be selectable on the server pull-down list while logging-on. Each site will have its own database and maintains its own backup (you must be logged-on to the site at the appropriate time for the auto backup for that site to run).

### ***Integra32™ Data Restore***

To restore backed-up files click on '*Integra32™ Data Restore*' in program groups.



The *Data Restore Screen* allows you to select which files are to be restored.

Image files and Purged files (AHB.mdb) cannot be restored through this Restore module. To restore those files, copy them from the backup folder.

### ***Integra32™ Database Maintenance***

Running '*Database Maintenance*' will compact and repair the Integra32™ databases. The '*Repair*' will correct most corruptions in the databases. Those that can't be repaired will produce an error message.

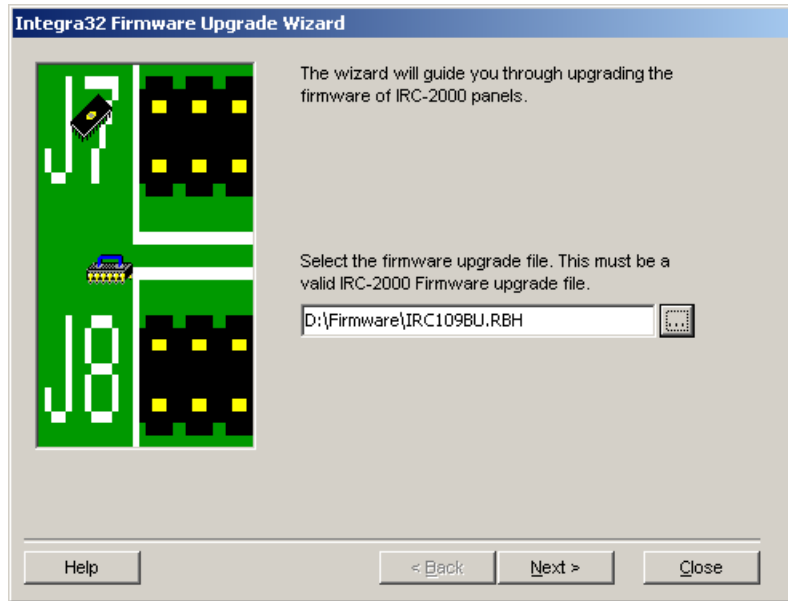
### ***Integra32™ Firmware Upgrade***

#### **Before Upgrading**

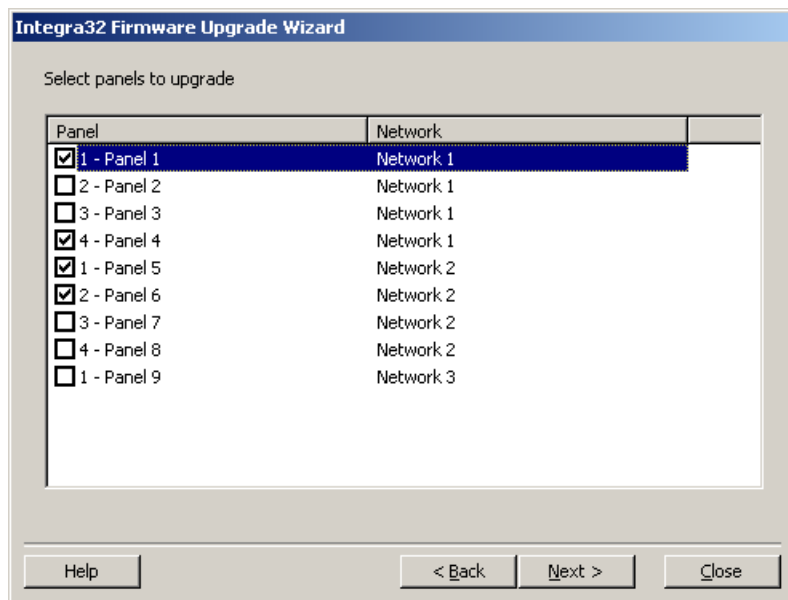
- 1) Before starting the firmware upgrade be sure to know where the upgrade file (\*.rbh) is located.
- 2) Although upgrading will not affect the panel's memory, it is recommended that you download all files to the panel after upgrading to ensure that any new features are properly installed.

#### **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.

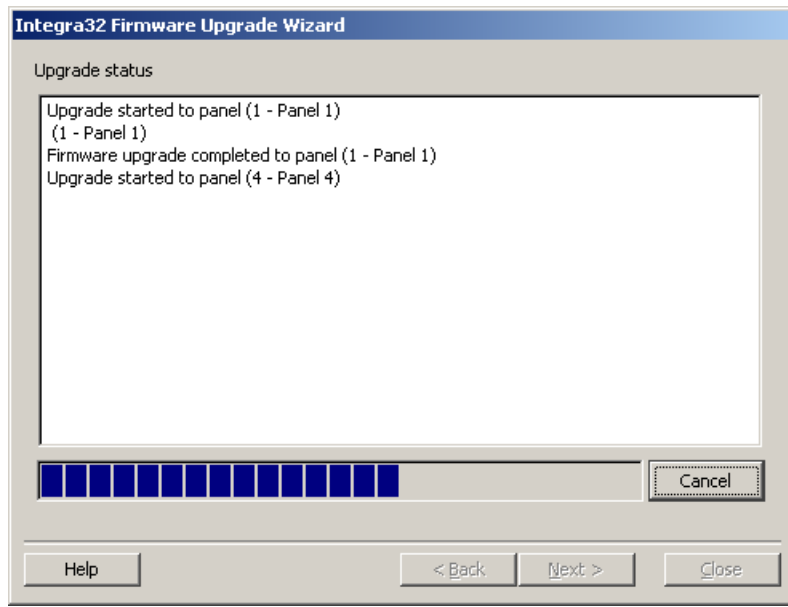


Click *Next* after the appropriate file has been selected.



Next select which panel(s) should be upgraded. 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 firmware upgrade.



A progress bar and messages will keep you informed during the process.

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

### ***Integra32™ Server***

With this option, you can Start, Stop and/or restart Integra 32 Server services.

# 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 Integra32™. (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 Integra32™ time group schedules are not appropriate. Statutory holidays and summer shut down periods are two examples. In Integra32™, <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 Integra32™ 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 Integra32™ system for purposes of data-entry or monitoring.
<b>Output</b>	Any field apparatus that receives commands from an Integra32™ 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., Business Hours) is a pre-defined time slot/day combination that may be assigned to schedules, thereby governing how the Integra32™ system operates from day to day.

# License & Warranty

---

## Notice 1.01

This Software is licensed (**not sold**). It is licensed to sublicensees, including end-users, without either express or implied warranties of any kind on an “as is” basis. RBH Access Technologies Inc. makes no express or implied warranties to sublicensees, 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. RBH Access Technologies Inc. shall not have any liability or responsibility to sublicensees, 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

RBH Access Technologies 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 RBH Access Technologies Inc. may make any other claims to the fitness of any product for any application.

# Index

---

<b><u>A</u></b>			
About This Guide	6	Check In	107
Access Levels	90	Check Out	34, 108
Access Point Activity	76, 124	Clear	37
Access Points	67	Clear Log	31
Advanced	75	Command Bar	8
Alarms	72	Command Type	24
CCTV	73	Conventions in this guide	6
Links	71	<b>Copyright</b>	2
Modes	68		
Time-Outs	69	<b><u>D</u></b>	
Access Points Commands	25	Database Maintenance	145
Acknowledge	37	Database Reports	116
Acknowledge/Unacknowledge/Clear	35	Database Screen	21
Action Messages	36	Deactivation Date	98
Activate Card When Visitor Checks In	120	Deduct Usage	68
Alarm Details	36	Disable Forced Entry	68
Alarm Screen	22, 35	Door Held Open	70
Alarm sounds	120	Download	30, 31, 32
Alarms Toolbar Button	16		
Antipassback	76	<b><u>E</u></b>	
AP Activity Toolbar Button	16	Elevators	87
Area and Cardholder Commands	33	eMail Configuration	125
Areas	43	Event Log Screen	22
Auto void cards	119	Exit	9
Auto-Backup	129	Extended Unlock Time	70, 99
Auto-Relock	68		
<b><u>B</u></b>		<b><u>F</u></b>	
Backup	128	F Print	94, 96
Badge Options	121	Facility Code Mode	26, 69
Badge Template Designer	130	File	9
<b><u>C</u></b>		Finger Print	130
Card + PIN Schedule	69	finger print device	121
<b>Card Custom Fields</b>	131	Firmware Upgrade	145
Card Format	49	First Person Delay	68
<b>Card Import Utility</b>	10, 132	Floor Groups	88
Cardholders	93	Floors	34
More Fields Tab	103	Font	122
Options	99		
Photo Tab	101	<b><u>G</u></b>	
Profile Tab	100	Getting to Know Integra32	8
Type	99	Global Antipassback	76
Cardholders Toolbar Button	16	Global Links	127
		Glossary	148
		Group Cards	120

<b><u>H</u></b>		General	45
Handicap	99, 100	<b><u>O</u></b>	
Help	11	Options	10
Help Toolbar Button	17	Out Reader	76
High Security	69	Output Points Commands	28
High Security Privilege	99	Output Properties	83
History Reports	113	Outputs	
Holidays	40	Details	83
How to Execute a Command	23	Links	86
<b><u>I</u></b>		<b><u>P</u></b>	
Ignore Antipassback	99	Panels	48
<i>Import Utility</i>	132	Alarms	50
Inhibit ID	69	Code Reader Links	51
Input Points Commands	27	Site Codes	49
<i>Input Properties</i>	78	Panels Commands	29, 32
<b>Inputs</b>		PC Decision Required	69
CCTV	79	PC100	54
<b>Details</b>	78	Permanent Command	24
Links	81	Preview Reports	114
Integra32 Database	38	Print Area Report on Input	120
Integra32 Server Client Network Setup	7	Program Groups	143
Integra32™ Database Maintenance	145	Programming	38
Integra32™ Security System	144	Properties	
Interlock	26	Notes Tab	102
Introducing Integra32	7	<b><u>R</u></b>	
IRC2000 Properties	48	rbh.ini	13
<b><u>L</u></b>		Receipt	108
License & Warranty	149	Repeat Ignore Time	71
<i>Link Execute Privilege</i>	99	Reports	11, 113
Links	10	Reset Area	33
Local Antipassback	76	RTE Bypass DC	68
Log In & Out (Ctrl+L)	9	Run Backup Now	128
Login/Logout Toolbar Button	16	<b><u>S</u></b>	
<b><u>M</u></b>		Schedules	41
Magnetic Encoder Setup	121	Semi-Permanent Command	24
Menu Options	9	Set Area	33
Messages	44	Set Date/Time	30, 31, 32
Monitor Screen	23	Status Screen	21
Multi Cards	94, 95	<b>System Messages</b>	123
<b><u>N</u></b>		System Options	119
Networks	45	System Status	23
Advanced	47	System Status Toolbar Button	16
Comms	45	<b><u>T</u></b>	
Direct Connect	45	Time Zone Difference	47
Ethernet Connect	46	Time Zones	42



Timed Antipassback	70	<b>User Fields - Visitors</b>	125
Timed Command	24	User Options	120
Toolbar Buttons	16	Users	38
Tools	10, 128		
<b>Track Visitor</b>	111	<b><u>V</u></b>	
<b><u>U</u></b>		Version	30, 31, 32, 33
Unacknowledge	37	Visitor Manager	106
Unlock Privilege	99	<b>Visitor Reports</b>	117
Unlock Schedule	69	<b>Visitor Tracking</b>	111
URC2000 Properties	48	Visitors' Status	33
URC2000 with ELV	52	Visitors Toolbar Button	16
Usage Count	99	VM Configuration	125
		Void Cards	129

## Reader Comments

---