Axiom V™

Integrated Access Control and

Security Management System

USER MANUAL

Version 5.2.63

new innovative
building security

RBH
ACCESS
TECHNOLOGIES
INC.

Copyright and Trademarks

RBH constantly seeks to innovate and improve on the functionality and reliability of the AxiomV™ system. Therefore, the information contained in this book is subject to change at any time, without notice. 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, distributors, or affiliates 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 the AxiomV™ system.

RBH ACCESS TECHNOLOGIES INC.
2 Automatic Road, Suite 108
Brampton, Ontario
CANADA
L6S 6K8

Printing Date 8 July 2013

Table of Contents

About This Guide

This guide documents how to install and use the AxiomV™ Integrated Access Control and Security Management System as developed by RBH Access Technologies Inc. AxiomV™ is an innovative security access control application that manages and monitors all your security access needs.

Read this guide if you are:

- An operator who monitors security accesses using AxiomV™.
- A system administrator who updates AxiomV's™ database.
- The system engineers whom installs and configures AxiomV™ onsite.

Before reading this guide

This guide assumes that you:

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

Part 1	Read Part 1 for an introduction to AxiomV™.
Part 2	Read Part 2 for information on how to install and setup AxiomV™. *Part 2* is intended for the installers/Dealers.
Part 3	Read Part 3 to get to know AxiomV™. Learn about the basic concepts of access control. *Part 3* will explain portions of the system that are common throughout. This part is intended for everyone that uses the system.
Part 4	Read Part 4 for information on monitoring and operator control. Learn about the monitoring of the status for items in the system and how to send commands to those items. *Part 4* is intended for a system operator.
Part 5	Read Part 5 for information on how to perform administrative functions (i.e., add or update cardholder records in the AxiomV™ Database), and how to create and print reports. *Part 5* is intended for the administrator.
Part 6	Part 6 includes Appendixes, Glossary, License & Warranty, and Reader Comments.

Conventions in this manual

Menu options, window titles, fields, and buttons are indicated by *italic typeface*. For example, "choose *Computer Config* from the *System* 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 jump you to the associated or mentioned part of the manual. Click on the *cross-reference* when the curser changes to move to that place in the manual.

➢ A section beginning with an arrow symbol indicates the start of a task or procedure. Following the introductory statement are step-by-step instructions necessary to complete the procedure.

✎ A section that begins with a pencil symbol indicates special information of which you may want to take additional notice.

☞ A section that begins with a hand symbol indicates cautionary information.

💣 A section that begins with a bomb symbol indicates warning information.

Part 1

Chapter 1
Introducing AxiomV™

Welcome to AxiomV™, an innovative security access control application that manages and monitors all your security access needs.

AxiomV™ combines access control, building management, and security monitoring in a highly integrated and expandable system. AxiomV™ runs on a standard IBM compatible PC using Windows 2000, XP, 2003 Server, Windows 7 or Windows 2008 server and is designed for use in installations ranging from simple two door systems to complex systems covering multiple sites and containing thousands of card readers and tens of thousands of card holders. Remote sites are linked to the system via high-speed networks.

The system can monitor over 1000 networked controller units (NC100/UNC500) with each controller capable of monitoring 8 card readers and 320 input/output points. Remote site monitoring capability is 4,096 readers and 65,535 input/output points. Local site capacity exceeds 8,000 readers and 250,000 input/output points. A minimum configuration consists of a PC, a single controller unit (NC100) and a single reader controller (RC2) or a single Universal controller unit (UNC500) that allows connection of two card readers, eight inputs, and eight outputs.

A standard PC is used for system configuration, set up and maintenance of the cardholder database, and monitoring activity on the system. Once the database is downloaded to the controllers, the PC is not required for system operation. Should the PC be powered down, the NC100/UNC500 Controller will perform all access and other control functions, including logging up to 100,000 events. When the connection is restored, the log is reported to the PC.

The security features of AxiomV™ are extensive and are presented in the familiar Windows NT User Manager format. The system database can be separated into "logical sites" each with full security regarding operator access to system messages, configuration and administration modules, cardholder records and field devices such as controllers, access points etc. Only authorized operators can view events or issue commands for sensitive logical sites.

The open system architecture utilized by AxiomV™ is extremely powerful, flexible, and scalable. New devices developed for the system will be compatible with existing network devices, ensuring extended possibilities for system upgrading and expansion.

AxiomV™ provides extensive programming options for all aspects of system operation and configuration. This is achieved without adding unnecessary complexity to the setup procedure. Less frequently used options are placed in advanced screens. The majority of installations can use the default settings for quick and effective implementation.

AxiomV™ supports networked PC operation with TCP/IP protocol over Ethernet. A networked system is usually required by very large installations where several operators monitor and control the system.

One of the most powerful features of AxiomV™ is *AxiomLinks™*, which allows the operation of the system to be tailored to meet the requirements of a particular installation. *AxiomLinks™* is essentially a mini programming language that provides commands to control system inputs, outputs, and access points. A major application of *AxiomLinks™* is in building management.

AxiomV™ provides extensive elevator control features, allowing control of any building elevator setup. The elevator control board provides fail-safe operation with fire alarm input. Telecommunications interfaces include paging system interface for paging on site security guards or service personnel.

Comprehensive event handling and logging combined with customizable history and system reports making recording and examining system information a simple task. The AxiomV™ system can easily be customized with .wav audio files that sound in association with the logging of system messages and presentation of alarms for operator action. In addition users may customize the icons used to represent field devices and their present status on all map display screens.

AxiomV™ handles all alarm events quickly and presents them to the operator in an informative and easy to understand way. Customizable operator instructions are displayed telling the operator how to handle the alarm and what action to take. Additionally, graphics maps display the exact location of the alarm and an on map icon shows the type of alarm. AxiomV™ provides you with unparalleled power and flexibility, thoughtfully designed into a package that is easy to use for users and installers alike.

This innovative system supports Microsoft SQL Server 2000, 2005, 2008, MSDE 2000 and SQL Server Express 2005 and 2008. The client server database is more powerful than file databases, providing the system with even more flexibility.

Part 2

Chapter 2
Before Installing AxiomV™

This chapter describes considerations that should be addressed before installation of AxiomV™ by an authorized dealer of RBH Access Technologies Inc.

PC Requirements

Before you install AxiomV™, make sure that your computer's configuration meets the following **minimum** requirements:

Server

Requirement	Description
Operating system[1]	Microsoft Windows XP[2], 2003 Server[3], 2008 Server, or Windows 7
Microprocessor	Pentium IV 3.0GHz
Memory	3GB (minimum), 5GB (recommended)
Hard disk space	10Gb (Installation), 100Gb free space (to run)

Client

Requirement	Description
Operating system[1]	Microsoft Windows XP[2], 2003 Server[3], or 2008 Server, or Windows 7
Microprocessor	Pentium IV 1.0GHz
Memory	1GB (minimum), 2GB (recommended)
Hard disk space	5GB(Installation)

LAN Communications

Server to Client

Ensure that the following services have been setup:

[1] No 'Home' versions of operating systems are supported.

[2] Must have service pack 2 or 3 installed.

[3] Must have service pack 2 installed.

- Microsoft's standard networking services under Control Panel / Network.
- Network Card with Microsoft TCP/IP protocol under Network Neighborhood.

Before You Install AxiomV™

Before you install AxiomV™ application software, ensure that you have done the following:

1. You have installed and connected all hardware as described in the AxiomV™ Hardware Installation Manual.
2. Your computer meets the requirements listed in the table in *PC Requirements*.

Installing AxiomV™ on Your Computer

See Technical Bulletin '*TB49_AxiomV Install-Uninstall*' for installation information.

Removing AxiomV™ from Your Computer

See Technical Bulletin '*TB49_AxiomV Install-Uninstall*' for information on removing AxiomV™.

Upgrading AxiomV™

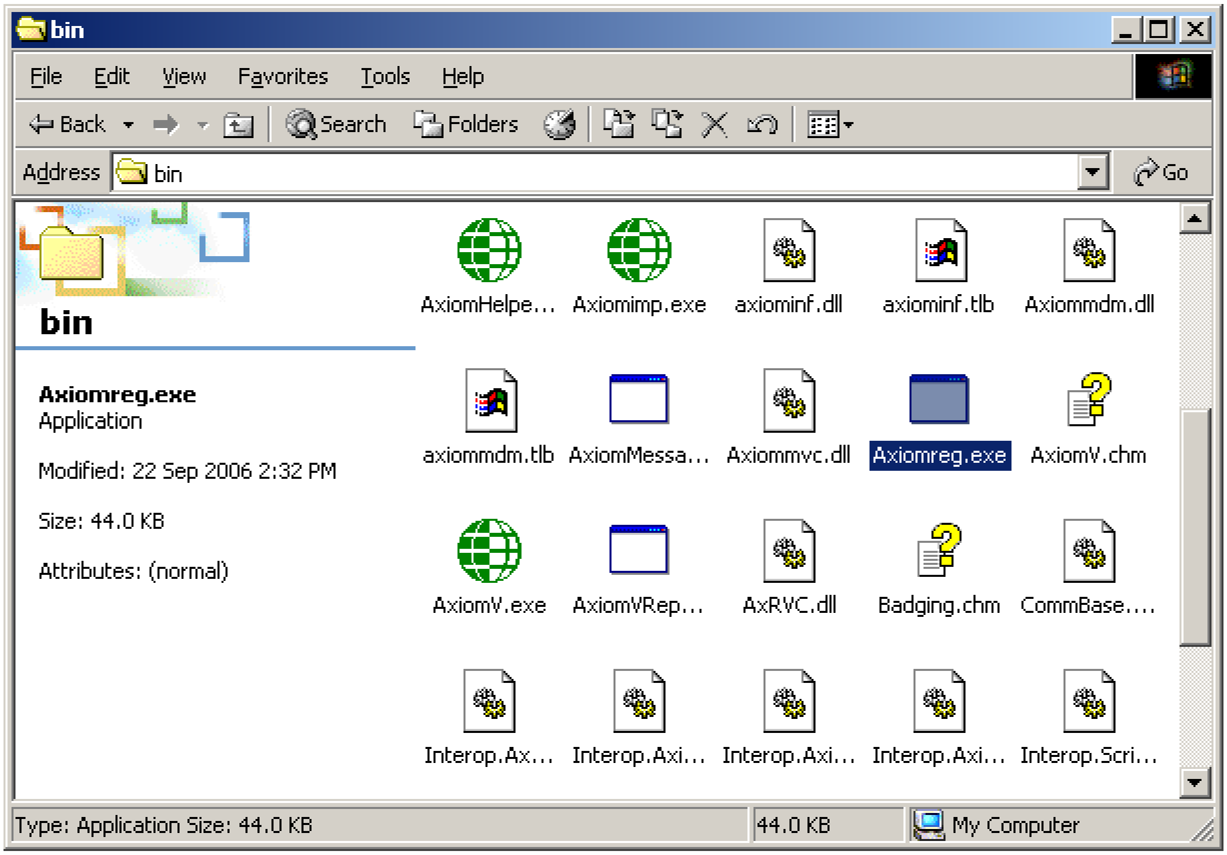
See the Technical Bulletin '*TB37_AxiomVUpgrade38*' for upgrading an *Axiom 3.8* system to *AxiomV*^{TM} and '*TB43_AxiomVUpgrade*' for upgrading AxiomV^{TM} to the latest.

License Registration

There are optional modules for the Axiom™ system that require the purchase and installation of a license for them to work. They are: Alternate Master NC100, Asset Tracking, Visitor Management, Badging, Card Import Utility, Customize Report Designer, Guard Tour, Active directory and History Report Scheduler. To register your license, follow the procedure below.

- Copy the license file [License.Bin] onto your hard drive from the installation CD. It may be a good idea to copy the folder it is in as well.

- From the 'bin' folder of AxiomV™ installation run the executable file Axiomreg.exe.



bin

Axiomreg.exe
Application

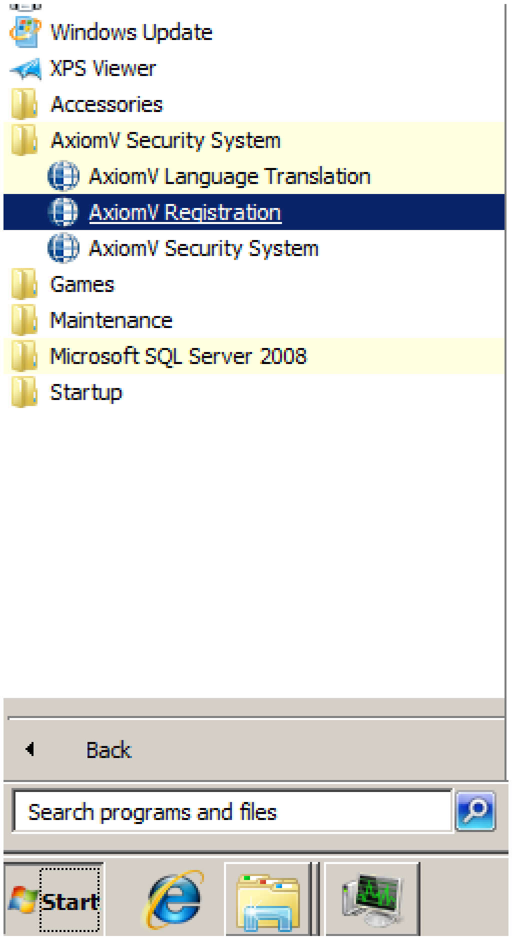
Modified: 22 Sep 2006 2:32 PM

Size: 44.0 KB

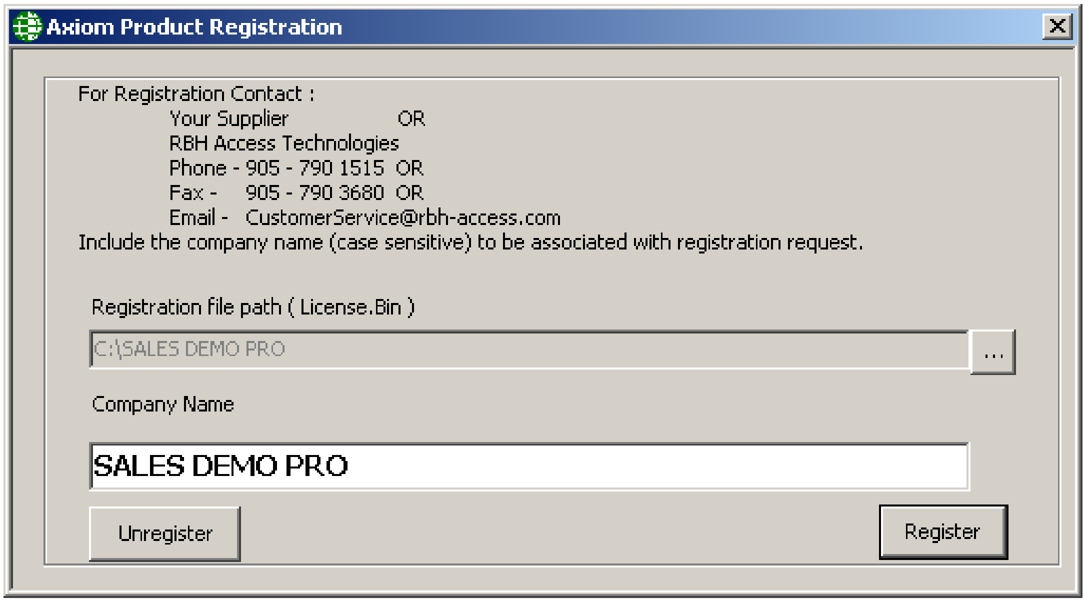
Attributes: (normal)

Type: Application Size: 44.0 KB | 44.0 KB | My Computer

OR



- **For the New SQL express 2008 based Pro CD, click on AxiomV Registration from Start> Programs> AxiomV Security System.**

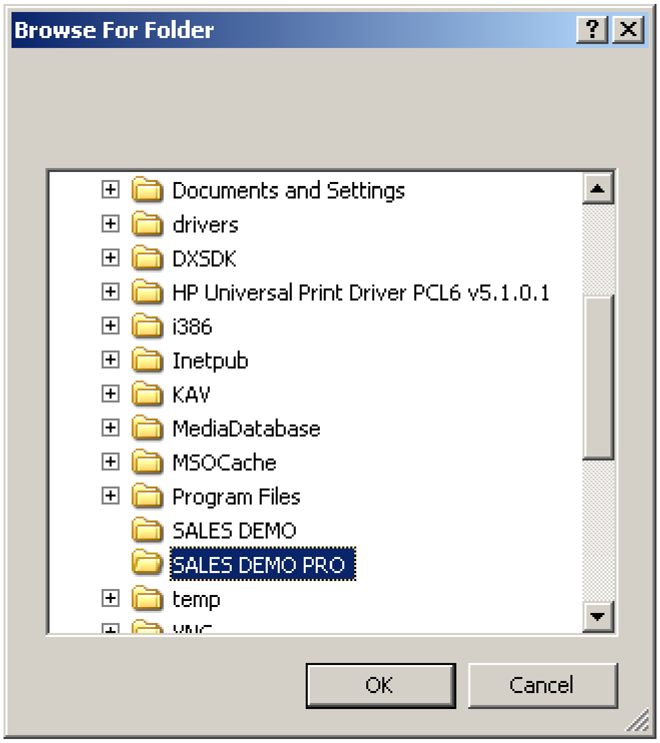


For Registration Contact :
Your Supplier OR
RBH Access Technologies
Phone - 905 - 790 1515 OR
Fax - 905 - 790 3680 OR
Email - CustomerService@rbh-access.com
Include the company name (case sensitive) to be associated with registration request.

Registration file path (License.Bin): C:\SALES DEMO PRO

Company Name: SALES DEMO PRO

- Browse the path to the folder the License.Bin is located in. Click *OK*.



- Type in the '*Company Name*' for the license. (The same name as the folder the License.Bin file is in on the CD). Ensure the name is spelled exactly the same as it is on the CD. The name is case sensitive.

- Click *Register* to complete the registration.

Part 3

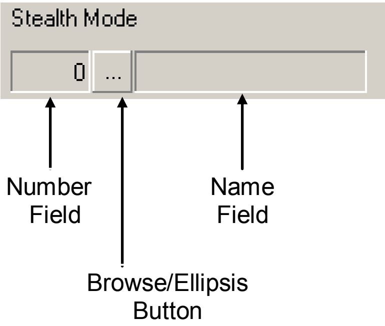
Chapter 3
Getting to Know AxiomV™

AxiomV™ lets you manage and monitor all your security access needs with a standard PC (stand alone or over a network). The client screen is customizable to better suit the user's needs. Therefore AxiomV™ can look different on other client machines, but will have the same capabilities.

Data Entry and Navigation Objects

This section describes Data Entry and Navigation conventions used throughout the AxiomV™ software package. Some of these tools include:

- Number & name object.
- Spin buttons.
- Search object.
- *Search* pop-up window.
- *Check* box.
- *Radio* button.
- Date fields.
- *List* box.
- Time group object.



The *Number & Name* object combines the following three elements, related to a common subject:

Number field

The *Number* field displays the number that identifies the item. The number is system-generated. When you add a new record to the database, the system automatically enters the next available number to identify the device or item.

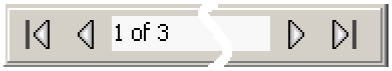
Name field

The *Name* field displays a descriptive name for the item or object you are currently displaying or defining.

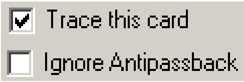
Browse/Ellipsis button

The *Browse/Ellipsis* button lets you display a list of all valid entries for the current field. When you click the *Browse/Ellipsis button* it displays the *Select* pop-up.

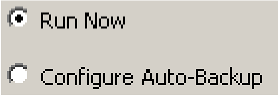
Use *Spin* buttons to increase or decrease the value in the adjoining box.



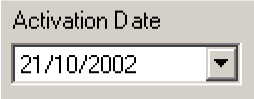
The *Search* object. Use the arrows to locate the first, previous, next, or last record.


☑ Trace this card
□ Ignore Antipassback

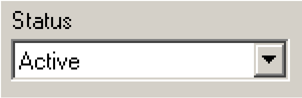
Check box. A *checkbox* that contains a check mark is active; any function associated with the check box is selected. An empty checkbox is inactive.


● Run Now
○ Configure Auto-Backup

Radio button. A *radio* button allows you to select a single option from a group of options. Only one object can be selected at a time. Selecting a second object removes the selection from the previously selected object.


Activation Date: 21/10/2002

Date field. AxiomV™ uses the date format selected in the Windows operating system under *Control Panel – Regional Settings*. Dates can be either typed in or selected from the pull down calendar.

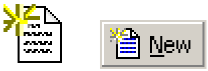

Status: Active

List box. A *list box* provides a selection list where the number of options is small and fixed. An entry can be selected from the list or typed in if the desired entry is not on the list.

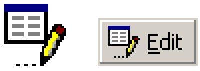
Push buttons. *Push* buttons perform the action named in the button itself, such as open another window or insert a line, etc.

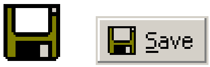
General Screen Operations

Data entry windows in the database have the following controls attached, and operate in a similar manner.



New adds a new record.





Edit allows changes to be made to the current record. When *Edit* is selected, the button changes to *Save*, and should be clicked in order to *Save* the changes.

Cancel

The *Cancel* button exits a window without saving changes or returning a selection.

Delete

Delete or *Remove* the current or selected record. A popup dialog box will request confirmation before deleting the record.

Copy

Copy the selections from the current record, to a new record in the same file. This record may then be renamed, edited and saved. Also see the *Copy Wizard* on page 56 of Chapter 5.

Find

Find a particular record. Opens the search window. (See Search Window for more details.)

View

View will display a report that can be viewed, printed, or exported.

Print

Print will have the currently selected item printed.

Printer Setup

Printer Setup is used to edit the printer's parameters.

Remove

Remove will delete the selected item only.

...

The three dot *Browse/Ellipsis button* will allow you to look for the desired item anywhere you have permission to on the network.

Open will bring up a list of previously saved items to select from and open.

Paste will apply the data previously saved by *Copy*.

OK

Click *OK* to exit and save any changes that were made.

Cancel

Click *Cancel* to exit and not save any changes that were made.

Apply

Click *Apply* to save any changes that were made.

Next >>

Click *Next>>* to go on to the next screen.

<< Back

Click <<*Back* to go back to the previous screen.

1 of 6776

Number of records will show the number of the record currently being viewed and total number of records available.

▷| *Last* will go to the last record.

▷ *Next* will go to the next record.

◁ *Previous* will go to the previous record.

|◁ *First* will go to the first record.

> Select Highlighted Items.

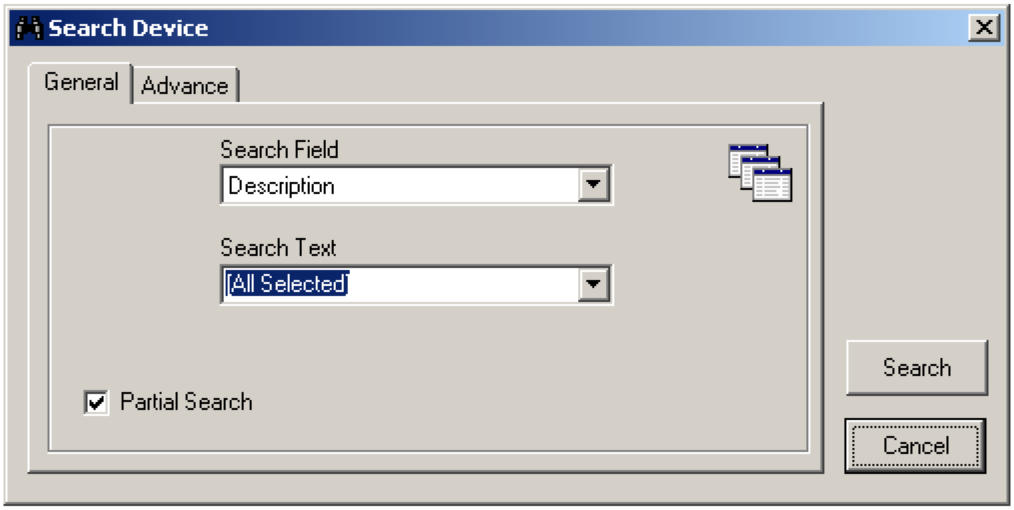
< Remove Highlighted Items.

>> Select All Items.

<< Remove All Items.

Search Window

General



Search Device

General | Advance

Search Field: Description

Search Text: [All Selected]

☑ Partial Search

Search Field

Select the field to be searched. The choices will vary depending on where the search was initiated. Searching under networks will have different fields then searching under access points.

Search Text

Either select from the provided pull down list or enter in your own criteria for the search.

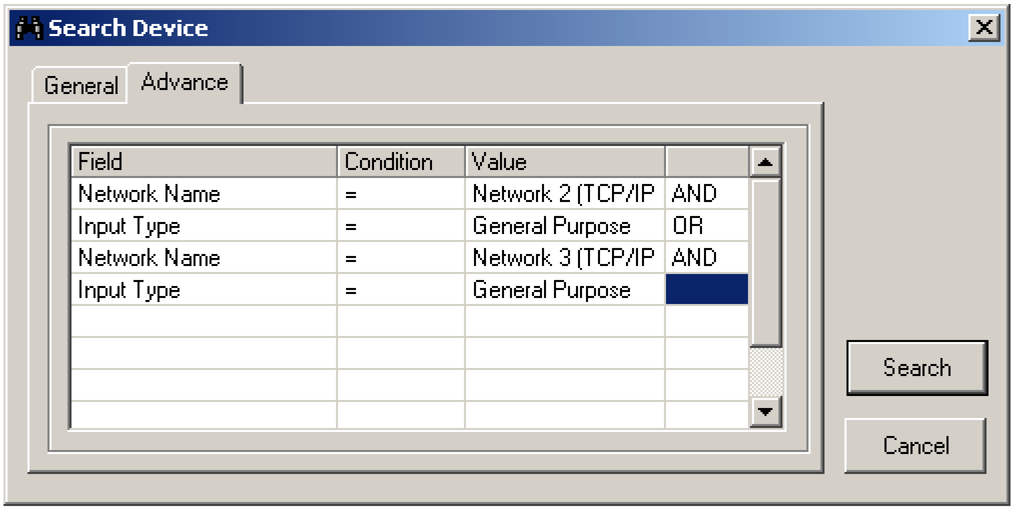
Partial Search

A partial search will look for the text anywhere within the field (e.g. "net" will find "direct network"). For an exact search uncheck *Partial Search*.

Search

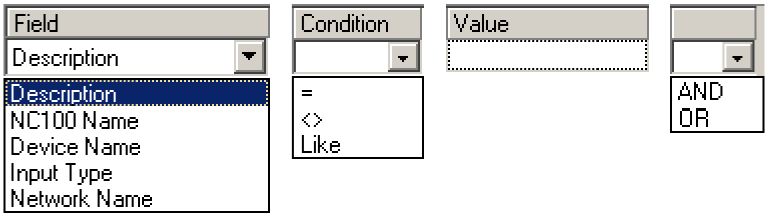
Click the *Search* button to execute a search based on the parameters set in *Search Field* and *Search Text*.

Advanced



Field	Condition	Value	
Network Name	=	Network 2 (TCP/IP	AND
Input Type	=	General Purpose	OR
Network Name	=	Network 3 (TCP/IP	AND
Input Type	=	General Purpose	

The *Advanced* search tab is used to create custom searches. Choose the parameters for each *Field* to customize the search for your individual needs.



Commands

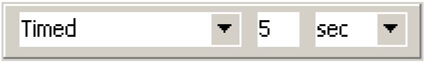
Commands can be issued by the operator (user) or by the system itself (links, schedules). There are three types of commands, Permanent, Semi-Permanent, and Timed.

Permanent

Permanent Commands are commands that can only be overridden by operator commands or by other permanent commands. These commands are usually used when it is important that the command is not countermanded by a schedule or a link.

Semi-permanent

Semi-Permanent Commands are the most common command type. Any other command issued after a *Semi-Permanent Commands* is valid regardless of the type or source.



Timed 5 sec

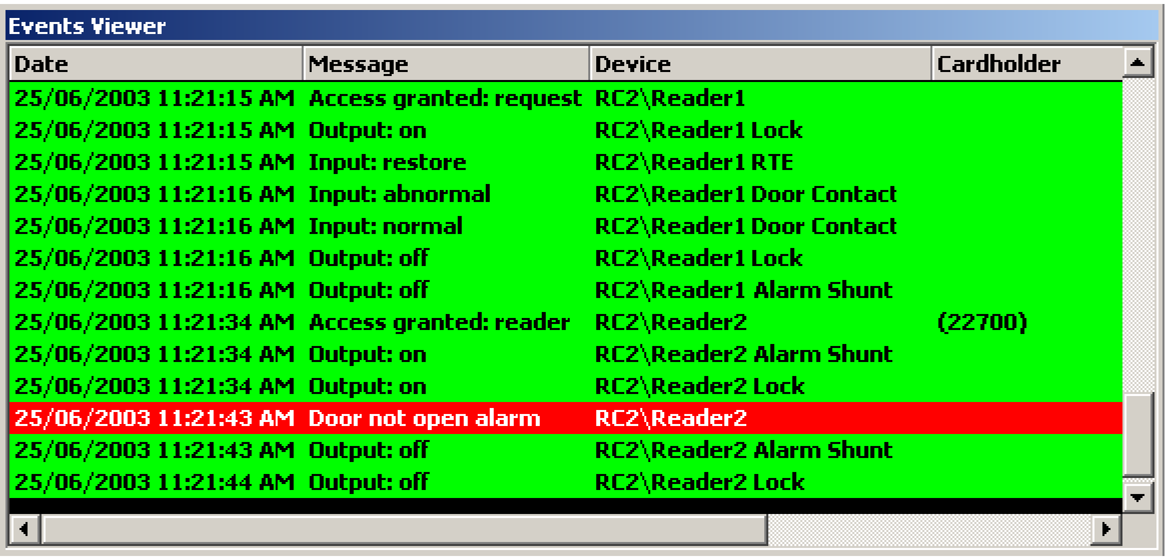
Timed Commands are executed like *Semi-Permanent Commands* except for the timer. The timer starts at the same time the command is issued. When the timer expires the system checks the item's schedule to verify what the item's status should be, and sets the item to that status.

Example: An access point has an unlock schedule of 9:00 a.m. to 5:00 p.m. Monday to Friday. At 4:55 p.m. the access point is given a timed command to lock for ten minutes. The access point locks immediately and the timer run for ten minutes. When the timer expires at 5:05 p.m. the door remains locked since the unlock schedule has turned off.

Event Viewer and System Status Displays

Events Viewer

Clicking on a header will cause the messages in the viewer to be sorted by that header. Consecutive clicks will toggle the sort between ascending and descending. A selected header will be indicated by a triangle (▲ ▼) that will show the direction of the sort.

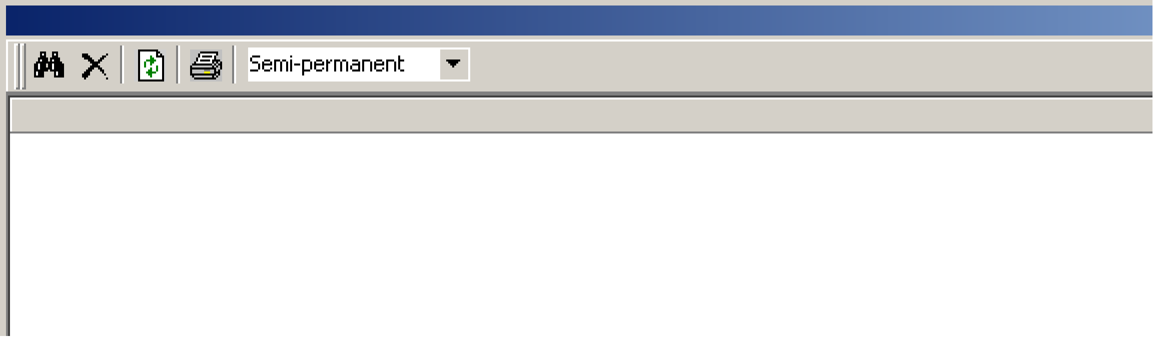


Events Viewer

Date	Message	Device	Cardholder
25/06/2003 11:21:15 AM	Access granted: request	RC2\Reader1	
25/06/2003 11:21:15 AM	Output: on	RC2\Reader1 Lock	
25/06/2003 11:21:15 AM	Input: restore	RC2\Reader1 RTE	
25/06/2003 11:21:16 AM	Input: abnormal	RC2\Reader1 Door Contact	
25/06/2003 11:21:16 AM	Input: normal	RC2\Reader1 Door Contact	
25/06/2003 11:21:16 AM	Output: off	RC2\Reader1 Lock	
25/06/2003 11:21:16 AM	Output: off	RC2\Reader1 Alarm Shunt	
25/06/2003 11:21:34 AM	Access granted: reader	RC2\Reader2	(22700)
25/06/2003 11:21:34 AM	Output: on	RC2\Reader2 Alarm Shunt	
25/06/2003 11:21:34 AM	Output: on	RC2\Reader2 Lock	
25/06/2003 11:21:43 AM	Door not open alarm	RC2\Reader2	
25/06/2003 11:21:43 AM	Output: off	RC2\Reader2 Alarm Shunt	
25/06/2003 11:21:44 AM	Output: off	RC2\Reader2 Lock	

System Status Display

Clicking and dragging a header can change the order of columns to suit the operator. The header names will change depending on the data being displayed.



This is the end of the overview for AxiomV™ Monitor. Once you have read and become familiar with the general features and environment of AxiomV™, proceed to:

Part 4 for information on how to monitor security access with AxiomV™ Monitor and System Status.

Part 5 for information on how to use and set up the AxiomV™ Database.

Chapter 4 Concepts

This chapter describes many security access concepts used in AxiomV™.

Access Control

A method of controlling entry and exit to protected areas.

Access Level

Each cardholder is assigned an access level that determines where the cardholder is allowed access and when the access is allowed. For example, an access level assigned to cardholders working in the warehouse would only allow access to the warehouse area form Monday to Friday and from 8 a.m. to 5 p.m.

Access Point

An access point is a point of entry or exit, such as a door, whose access is controlled and monitored by AxiomV™.

Antipassback (APB)

Antipassback is an access control feature that prevents cardholder misuse, by putting certain restrictions on the use of their cards. When the Antipassback feature is enabled, cardholders are restrictions from re-entering an Area until they have exited that Area.

Each AxiomV™ cardholder record in the database has two fields for area tracking – one for the last APB Area entered, and one for the Current Area, which may or may not be an APB area. If the last reader that a cardholder used was an APB reader, then both fields will contain the entering area of that Access Point record. If the last reader was not an APB reader, but had an entering area assigned, then the Current Area field will contain the entering area for that Access Point and the APB Area will contain the entering area from the last APB reader used.

Hard and Soft Antipassback

Hard Antipassback does not allow access to be granted if the antipassback criterion is violated. *Soft Antipassback* does allow access if the antipassback criteria is violated but posts the message "*Access Granted APB Reader*" to signify that a violation has occurred. Generally *Soft Antipassback* is only used during a training period before *Hard Antipassback* is enabled.

Timed Antipassback

Timed Antipassback resets the area of the cardholder after a specified time delay. This is used in applications where the cardholder reads their card to get in but uses a Request-to-Exit device to get out. The time delay is settable for each access point from 1 to 127 seconds or minutes.

Reader Antipassback

For *Reader APB*, the reader's *Entering Area* in the *Access Point* configuration record is compared with the *Current Area* of the cardholder as recorded in the AxiomV™ database. If they match, a *Reader APB* violation exists. In short, *Reader APB* is only concerned with the area the cardholder is moving into, and restricts the cardholder from re-entering the area without first reading into another area.

Area Antipassback

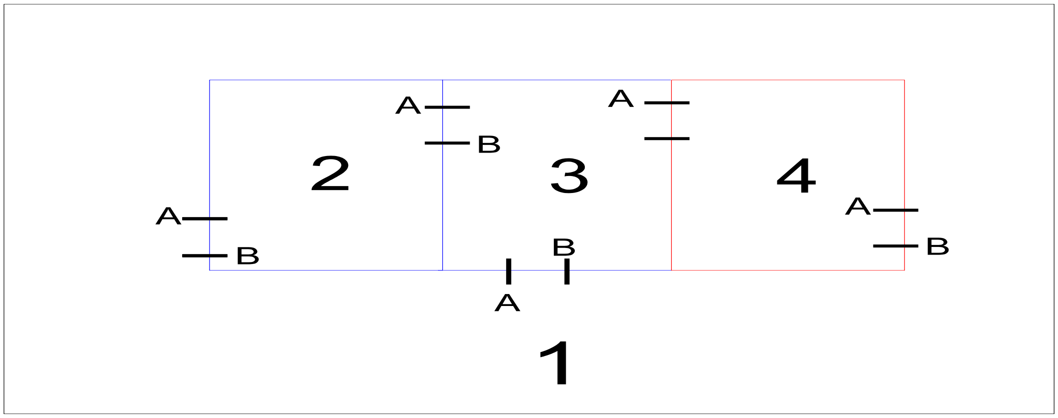
Area APB is more restrictive then Reader APB. In addition to the Reader APB check outlined above, the system also performs a check on the exiting area in the Access Point configuration record. First the system checks that the *Entering Area* and the *Current Area* **are not** the same. Then the system checks to see that the *Exiting Area* and the *Current Area* **are** the same. Antipassback is violated if either check fails. Area Antipassback not only checks to see if the cardholder is trying to enter the Area that they are already in, but also checks to see if the cardholder is trying to leave an Area that they are not in. This higher level of antipassback is mostly used in applications with Areas inside of other Areas.

Global Antipassback

When antipassback is enabled it functions within a network since networks don't communicate to each other while panels within a network do. Checking 'Required PC Decision' with antipassback enabled means that the AxiomV™ software will control antipassback for the site and that antipassback can function across networks. This will be true as long as the AxiomV™ server is running.

Example

In the diagram below, there are four areas numbered 1 to 4, programmed as antipassback areas. Each door to each area has two card readers: A and B. All readers are set for hard antipassback, and each access point has both its entering area and its exiting area defined. This establishes the cardholder flow for area to area.



Let's say John enters Area 2 from Area 1. Once John is in Area 2, his card allows him to:

Exit Area 2 to Area 1.

Exit Area 2 to Area 3.

While in Area 2, if John were to pass his card back to someone in Area 1, the card does not allow access to Area 2 because the cardholder location has been recorded as Area 2, and therefore Area 2 cannot be re-entered. In addition, if John were to follow someone into Area 3 without presenting his card, he could not gain access to Area 4 because his cardholder location has been recorded as Area 2, which is not connected to Area 4. He would not be exiting Area 2 when trying to enter Area 4.

Area

A predefined physical location such as warehouse or office, with entry and exit through *access points* controlled and monitored by AxiomV™.

C-NET Controller Network

The C-Net is the communications network that links NC100/UNC500 controllers together. Each C-Net can support up to fifteen NC100/UNC500 controllers.

Connection Types

Direct connection – the controller network (C-NET) is connected directly to the PC serial port via RS232 or RS485 (applicable only for *UNC, Universal network controller*).

Ethernet connection – the controller network (C-NET) is connected directly to a 10 Base-T Ethernet network running Windows on the server.

D-NET Device Network

The D-Net is the communications network that links card reader controllers (RC2) and input/output controllers (IOC16) to the NC100/UNC500 controllers**.** Up to four RC2s and sixteen IOC16s can be connected to a single NC100 controller (UNC500 has one inbuilt RC).

Holidays

The operation of the scheduler can be programmed to take special action on holidays. The system supports two different holiday types for added flexibility.

On a holiday, *Time Groups* follow the time schedule assigned to the holiday and ignore the normal day of the week time group parameters. All time groups have a nine-day schedule, with the eighth and ninth day designated as the *H1* (holiday type 1) and *H2* (holiday type 2) days.

IOC16 Input/Output Controller

The IOC16 supports sixteen points, each of which is programmable as an input or a relay output.

NC100 Network Controller

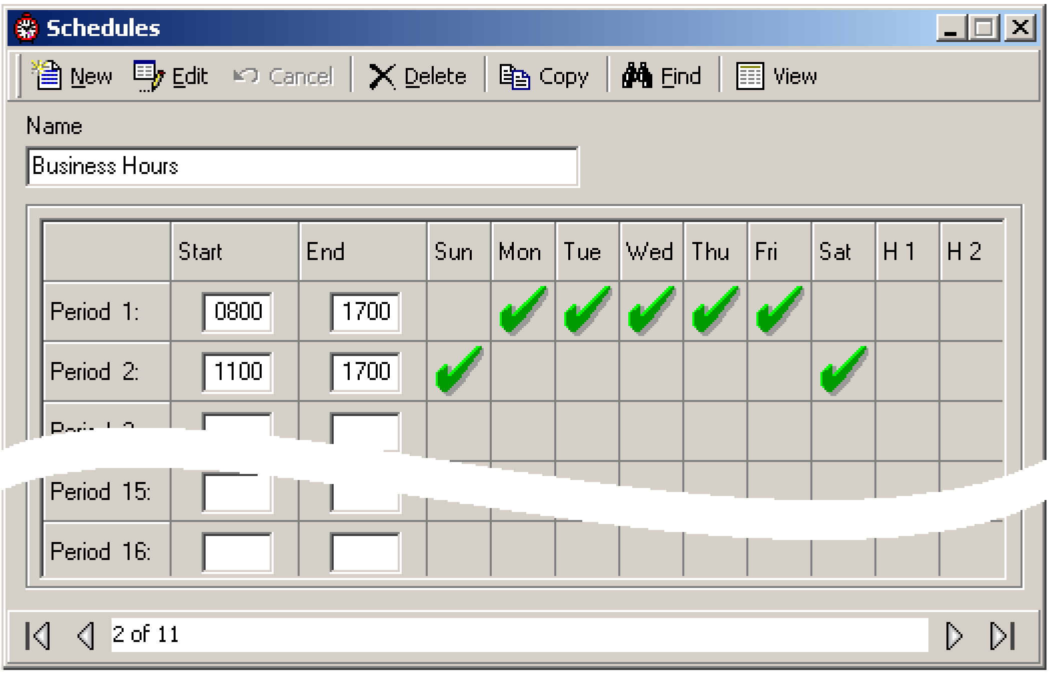
The NC100/UNC500 is the main controller in the system and stores all information required for local access control functions. Each NC100/UNC500 is capable of monitoring eight readers (four - RC2 controllers) and sixteen IOC16 input/output controllers over its D-Net.

RC2 Reader Controller

The RC2 connects to the NC100/UNC500 (UNC500 has one inbuilt RC2) on the D-Net and supports two readers (PIN pad and/or card reader) as well as eight inputs and eight outputs.

Schedules

Most functions in an access system are affected by Time, which may be the time of day, the day of the week, or the day of the month. A *Schedule* (e.g., Business Hours) is a window during which specific activity occurs in predefined time and day combinations. As an example you want to define Business Hours during 8:00 a.m. to 5:00 p.m. Monday through Friday, plus 11:00 a.m. to 5:00 p.m. Saturday and Sunday, excluding Holidays. This predefined window is a schedule.



Name: Business Hours

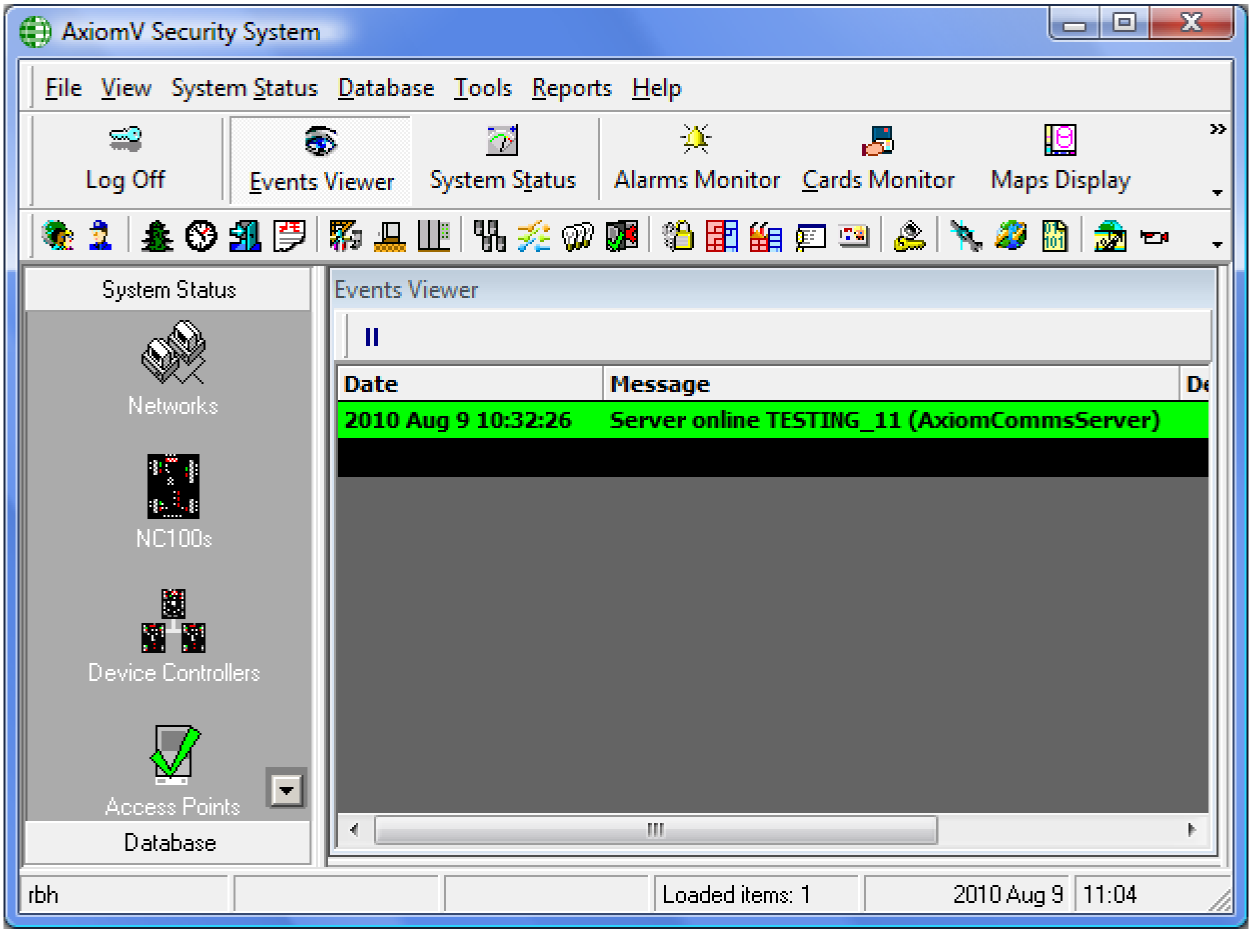
	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H 1	H 2
Period 1:	0800	1700		✓	✓	✓	✓	✓			
Period 2:	1100	1700	✓						✓		
Period 15:											
Period 16:											

Schedules may be used to control access point operation, input arming/disarming, output switching, and other system functions.

Part 4

Chapter 5
Monitoring Security Access

This chapter describes the operation of the AxiomV™ client screen. All functions of the system can be performed from the client screen (as long as the operator has permission). The client screen can be customized so that frequently used functions are easily accessed.



Date	Message
2010 Aug 9 10:32:26	Server online TESTING_11 (AxiomCommsServer)

rbh | Loaded items: 1 | 2010 Aug 9 | 11:04

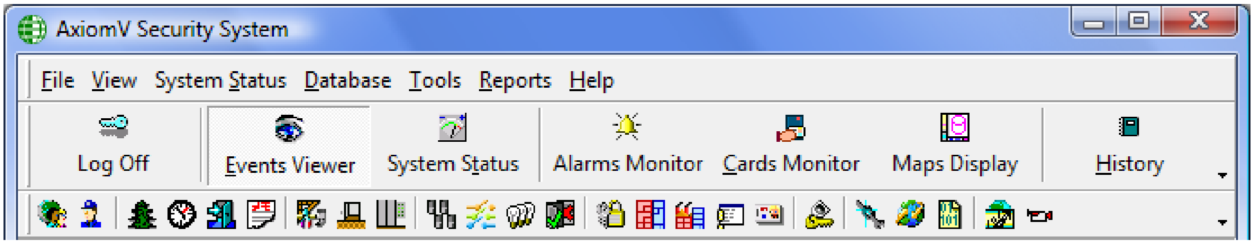
Client Screen

The client screen can be broken down into five separate areas:

1. The Menus and Toolbars.
2. The Module Selector.
3. The Status Bar.
4. The Events Viewer.
5. The System Status Pane.

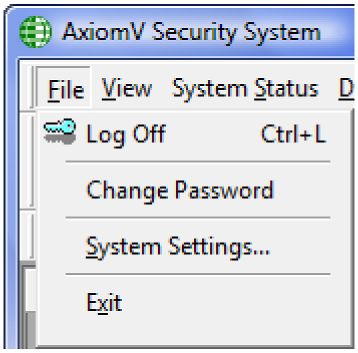
The Alarm Monitor is an additional area that can be called up as required.

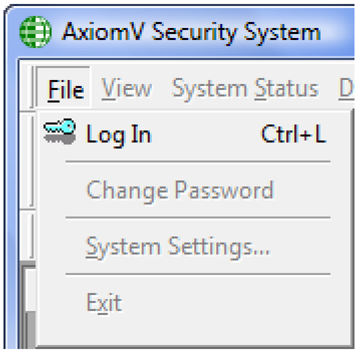
Menus and Toolbars



Menus

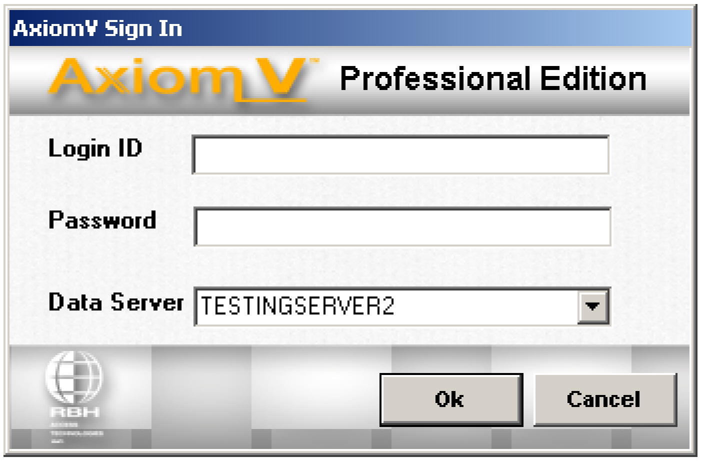
File





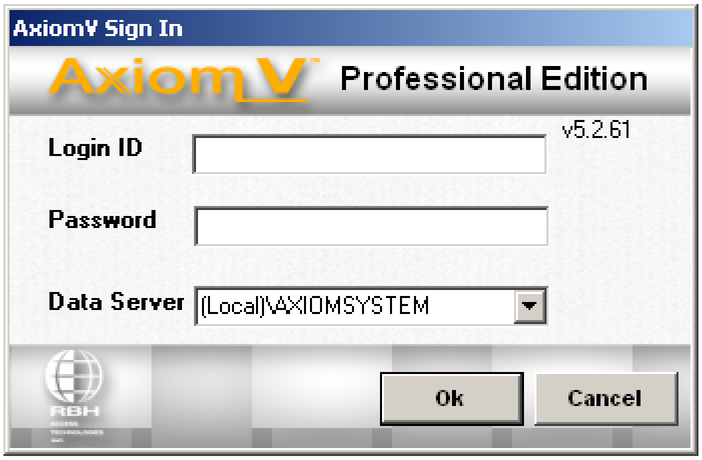
Log In (Ctrl+L)

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



Data Server TESTINGSERVER2

OR



Data Server (Local)\AXIOMSYSTEM

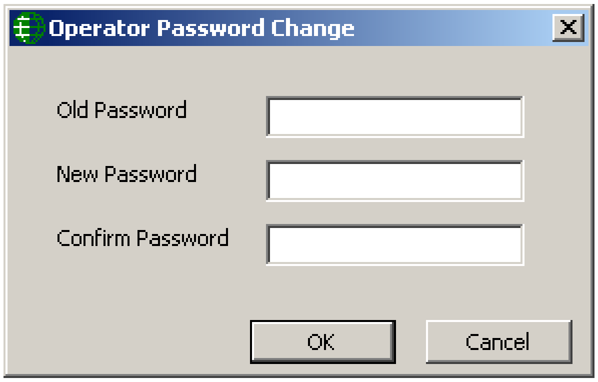
To log in, enter your user name and password. Although the "*Login Name*" is not case sensitive the "*Password*" is.

The default operator name is 'rbh' and the default password is 'password'. After you have the system up and running it is recommended that you change the default Operator ID and Password.

Log Off (Ctrl+L)

An operator should log out when leaving the computer unattended or when finished his/her shift. To log off, simply click the appropriate button or press **Ctrl+L**. A keyboard timeout can also be set, to automatically log out the user if there isn't any keyboard or mouse activity for the preset amount of time. Logging off protects the system against unauthorized access. AxiomV™ has a built-in *Default Account,* which activates whenever an operator logs out and it will capture and display events on the monitor screen. These messages will be available to the next operator that logs in.

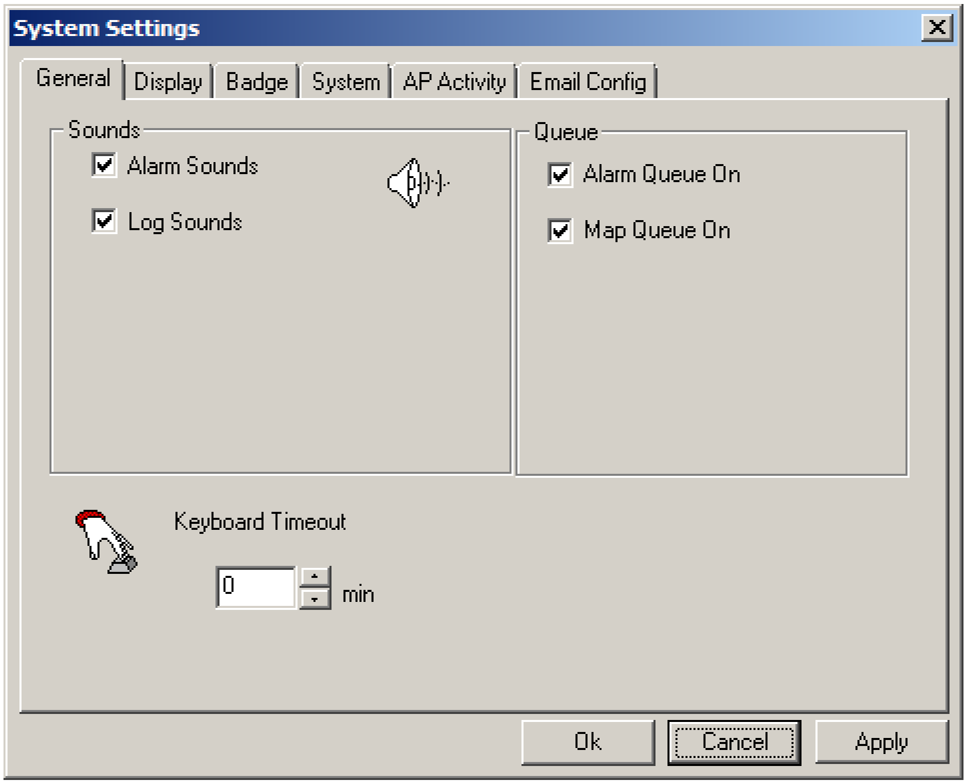
Change Password



Change Password allows an operator to change their password without them have to access *Operators* or *Operator Profiles* in the database. The current operator simply enters their existing password under *Old Password* then they enter a new password under both *New Password* and *Confirm Password*. Click *OK* to *save* the change.

System Settings…

General



Sounds

☑ Alarm Sounds

☑ Log Sounds

Queue

☑ Alarm Queue On

☑ Map Queue On

Keyboard Timeout

0 min

Sounds:

☑ Alarm Sounds

☑ Log Sounds

Alarm, Log, and System sounds can be activated or deactivated as required. Alarm sounds will come from the PC speaker if there isn't a sound card installed in the machine. Log and System sounds are only played through the sound card and are used to help recognize particular messages as they come in.

Queue:

☑ Alarm Queue On

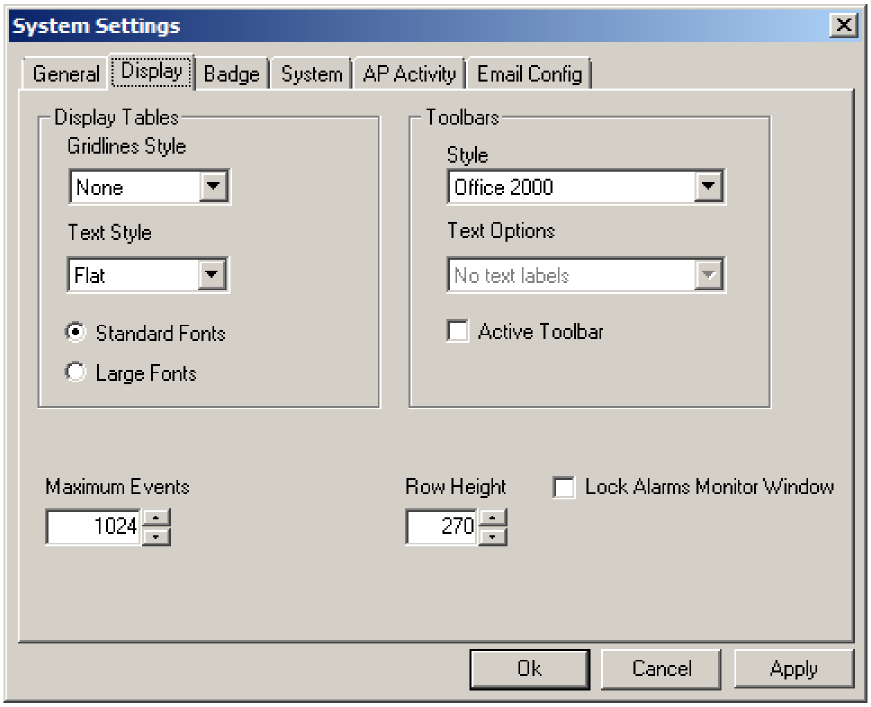
☑ Map Queue On

When the alarm queue is turned on the Alarm Monitor screen will be brought up whenever a new alarm comes in. The map queue will do the same for a specified map associated with the alarm.

Keyboard Timeout

Keyboard timeout is set in minutes and can either be typed in or scrolled to. The operator will be logged out at the end of the set time if there is no mouse or keyboard activity.

Display



Display Tables
Gridlines Style: None
Text Style: Flat
● Standard Fonts
○ Large Fonts

Toolbars
Style: Office 2000
Text Options: No text labels
□ Active Toolbar

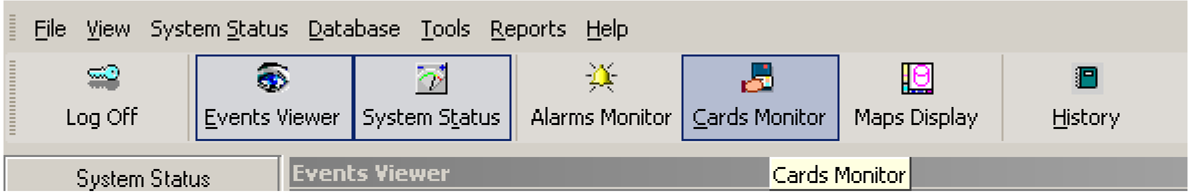
Maximum Events: 1024
Row Height: 270
□ Lock Alarms Monitor Window

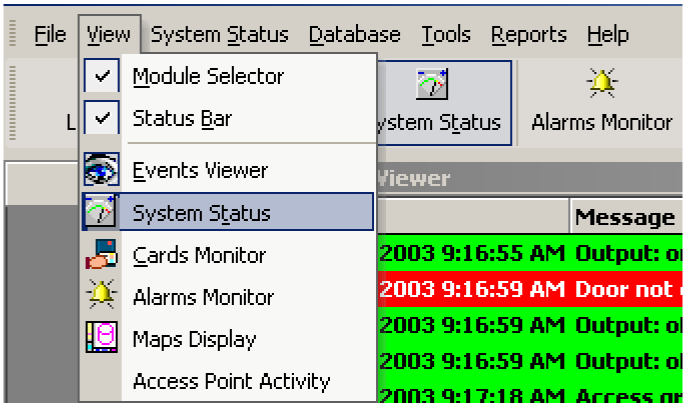
Display Table:

Aesthetic setting for the tables are chosen here. Gridline Styles can be chosen as Raised, Inset, Flat, or None. Text Style can be Inset Light, Raised Light, Inset, Raised, or Flat. Font size can be either standard or large.

Toolbars:

The style of the toolbars can be Office97™ style, Office2000™ style, or OfficeXP™ style. All other examples in this manual are in Office2000 style. The examples below here are in OfficeXP™ style.

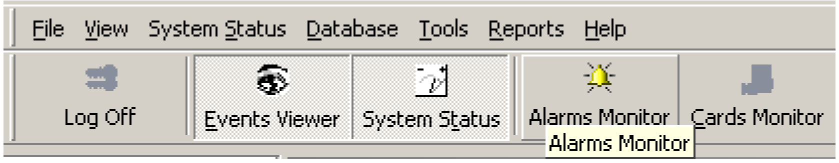




2003 9:16:55 AM Output: o
2003 9:16:59 AM Door not
2003 9:16:59 AM Output: o
2003 9:16:59 AM Output: o
2003 9:17:18 AM Access gr

Text Options – This feature is not supported at this time.

☑ When *Active Toolbar* is selected the buttons on the toolbar are grayed out until the cursor is moved over them.



☑ Gridlines in all Selection boxes.

Select if all *Selection* boxes are to have gridlines.

Maximum Events

How many lines of events are to be buffered for immediate viewing is set under Maximum Events. Type in or scroll to the desired value.

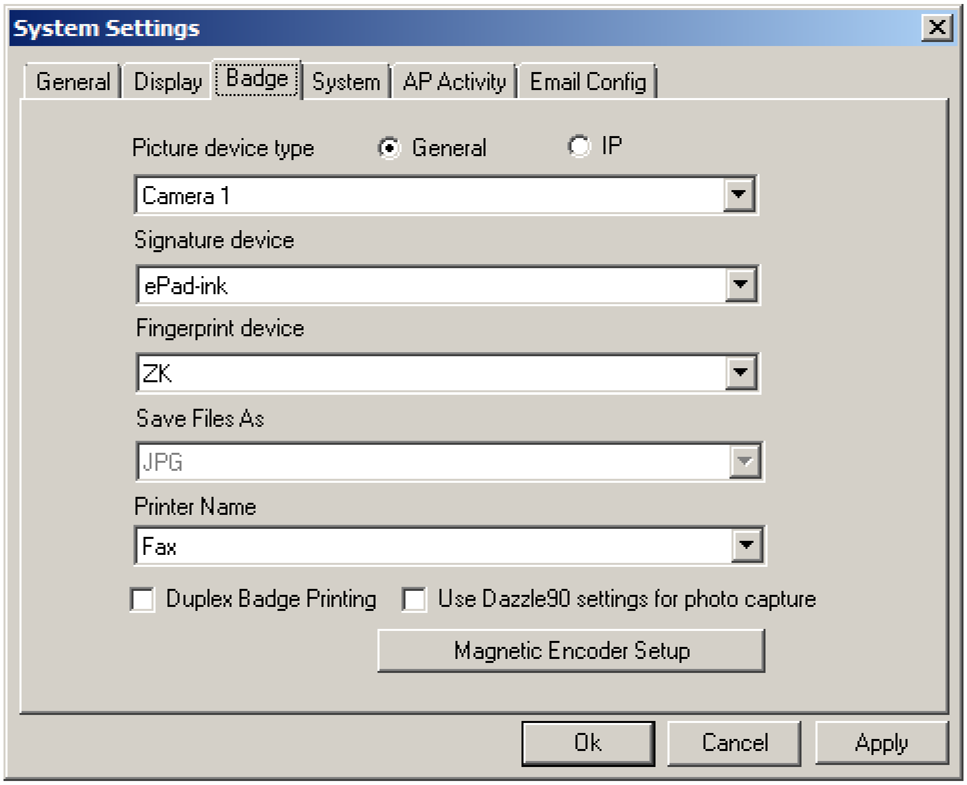
Row Height

Changes in Row Height will reflect in the Event Log, the Status Screen, and the message portion of the Access Point Activity Screen. Font size will also affect the same areas.

Lock Alarms Monitor Window

☑ The *Alarm Monitor Window* is a separate display that pops-up as required; selecting this feature will include it in the main screen.

Badge



Picture device type ● General ○ IP

Camera 1

Signature device

ePad-ink

Fingerprint device

ZK

Save Files As

JPG

Printer Name

Fax

□ Duplex Badge Printing □ Use Dazzle90 settings for photo capture

Devices associated with creating badges are selected under the *Badge* Tab. Cameras (or picture device) for acquiring the cardholder's picture are selected here. Devices for acquiring the cardholder's signature and/or fingerprint, picture format as well as which Printer to use is also selected here. Check boxes are provided for selecting Duplex Badge Printing (printing on both sides of the card) and for users of the Dazzle90 photo capture device. Magnetic strip encoding can be set under the *Magnetic Encoder Setup*.

Magnetic Encoder Setup

Printer Name

Allows you to select the printer that will be encoding the card.

Field Name

Select the fields form the database that the data will come from. More than one field may be selected.

Length

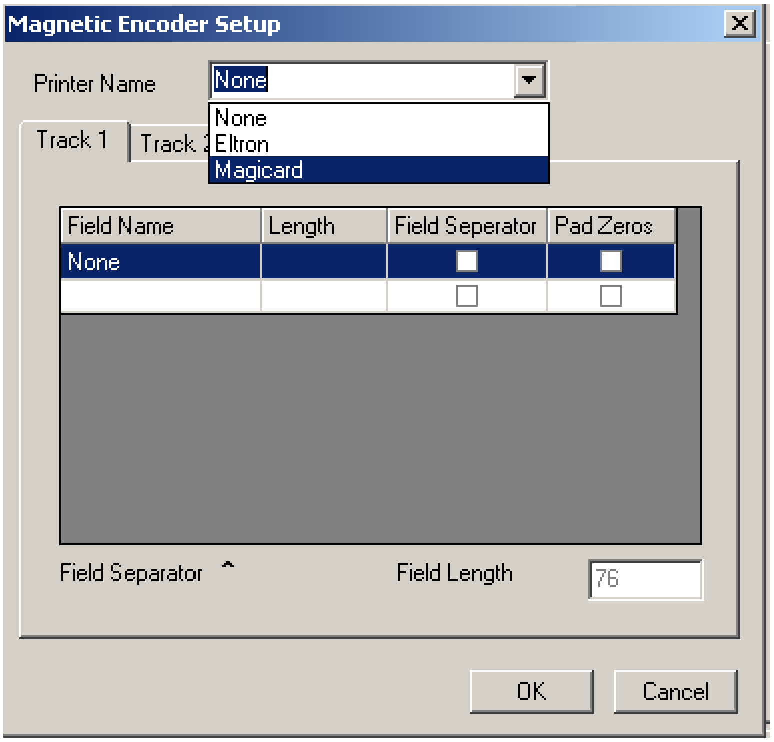
The number of characters allotted for the data of the field named.

Field Separator

Check here to add a field separator character before this field (not applicable if only one field is selected).

Pad Zeros Check here to add leading zero character to numeric data to fill the field to its full length.

Field Length The *Field Length* is the total number of character that may be encoded on the track. The sum of the *Lengths* plus one character for each separator is not to exceed this value



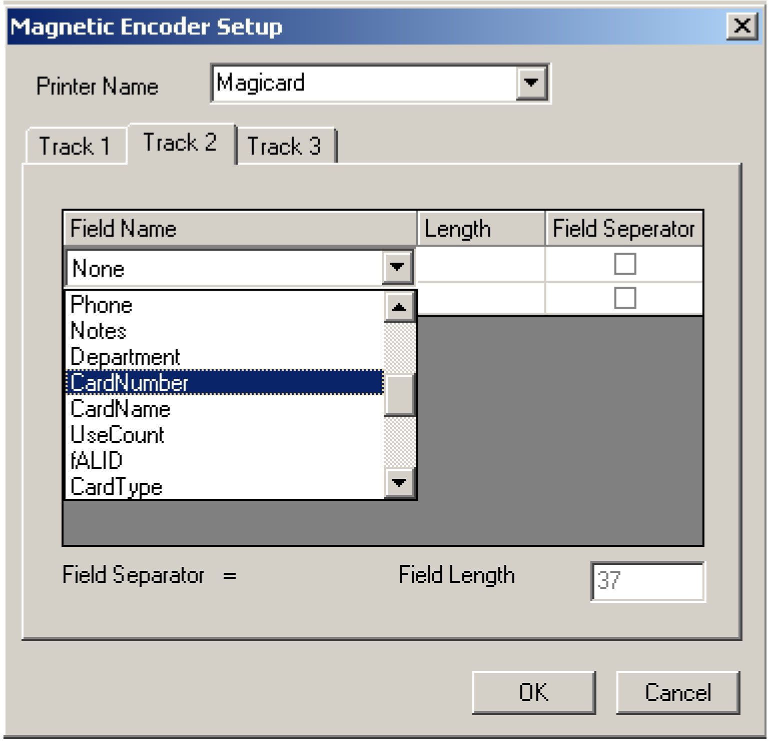
Printer Name: None

Field Name	Length	Field Seperator	Pad Zeros
None		☐	☐
		☐	☐

Field Separator ^

Field Length 76

Select the *Printer Name* used for encoding (*Eltron* and *Magicard* Encoders supported currently), select the track and rest of the information to encode.



Magnetic Encoder Setup

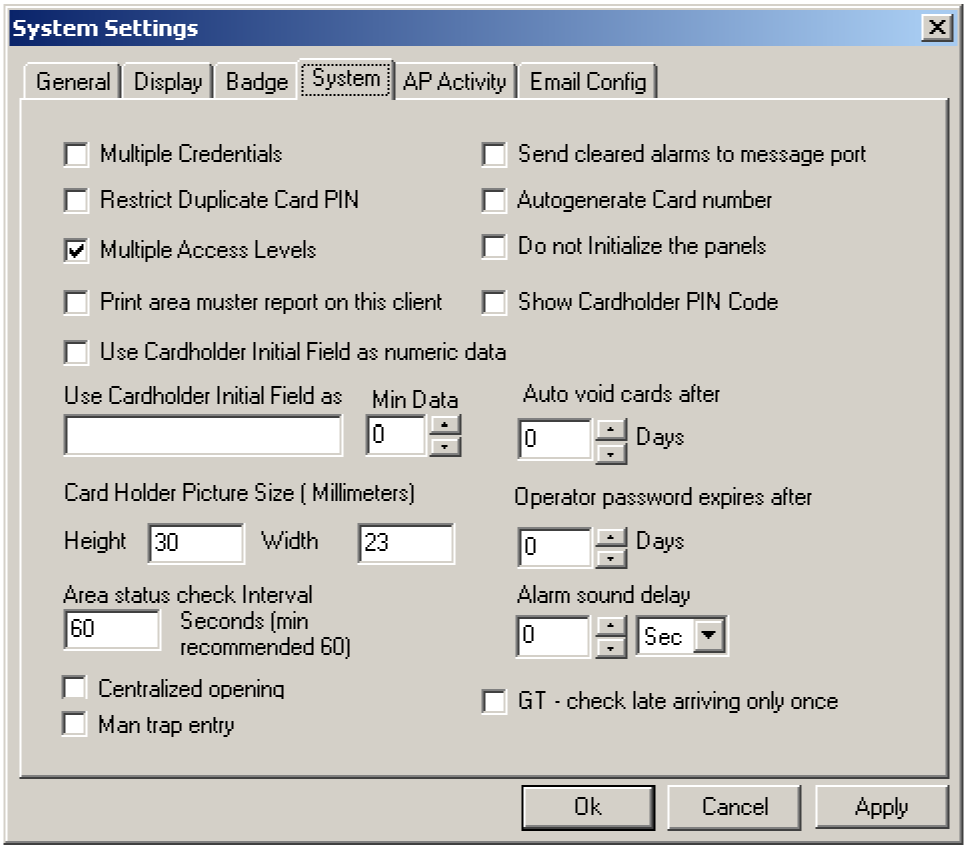
Printer Name: Magicard

Field Name	Length	Field Seperator
None		□
		□

Field Separator =

Field Length 37

System



□ Multiple Credentials

□ Restrict Duplicate Card PIN

☑ Multiple Access Levels

□ Print area muster report on this client

□ Use Cardholder Initial Field as numeric data

Use Cardholder Initial Field as

Min Data: 0

Card Holder Picture Size (Millimeters)

Height: 30 Width: 23

Area status check Interval: 60 Seconds (min recommended 60)

□ Centralized opening

□ Man trap entry

□ Send cleared alarms to message port

□ Autogenerate Card number

□ Do not Initialize the panels

□ Show Cardholder PIN Code

Auto void cards after: 0 Days

Operator password expires after: 0 Days

Alarm sound delay: 0 Sec

□ GT - check late arriving only once

☑ Multiple Credentials:

This feature allows a cardholder to have more than one card number. Look for the *Browse/Ellipsis button* beside the card number box in the cardholder screen when this feature is checked

☑ Restrict Duplicate Card PIN:

When checked this feature prevents cardholders from having the same PIN code. If it is left unchecked then multiple cardholders will be allowed to use the same PIN code.

☑ Multiple Access Levels:

When checked this feature it activates Multiple Access Levels along with special Access Levels Special Access Levels allows you to customize the access of each cardholder while Multiple Access Levels allows you to give each cardholder one standard Access Level and up to ten multiple Access Levels (see *Access Levels* - General (Multiple Access Levels for information on creating access levels).

☑ Print Area Muster Report on This Client:

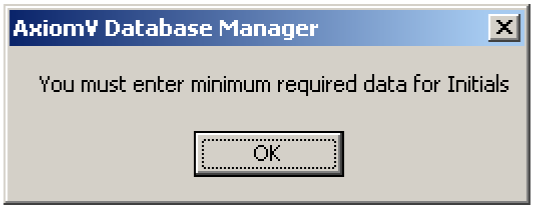
When checked this feature will print area muster reports on the client machine instead of at the server. These reports are generated by tripping a specified input for the area (see Areas).

☑ Use Cardholder Initials Field as Numeric Data:

When checked this feature will allow to enter only numeric data in initial field in cardholder screen. This field can be combined with *Min Data*

Min Data:

Maximum allowed is 10. If anything selected between 1 and 10, it will not allow saving a cardholder until initial field have selected number of required data.



You must enter minimum required data for Initials

☑ Use Cardholder Initials Field as:

Enter (type) a new label for the Initial Field in the cardholder screen to use this field for a different purpose.

☑ Send cleared alarms to message port:

Check this feature to send the alarm's ASCII message with the addition of "alarm cleared" to the alarm's message port.

☑ Autogenerate Card Number:

When checked this feature will automatically enter a card number whenever a new cardholder is created. The number generated will be the next card number in sequence higher than the highest card number in the system.

☑ Do not initialize the panels:

With this feature selected the operator will not be asked if they want the panels initialized or not, the panels will not be initialized. When the feature isn't selected the operator will be asked whether or not to initialize the panels.

☑ Show Cardholder Pin Code

With this feature selected the operator will be able to see the Pin Code assigned to cardholder in edit mode, otherwise, it always shows as asterisks.

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.

Card Holder Picture Size (Millimeters):

Type in here the desired Height and Width for the cardholder picture. This size is applicable for the cardholder screen only and does not apply to the card template at all.

Operator password expires after

Set the number of days here, after which the operator's password will expire, if the value is zero the password will never expire. Users will be given chance to change their password when logging in, if the expired password is not changed then AxiomV™ will not start for that user. The new password cannot match the previous password.

Area Status Check Interval

Server checks every 60 seconds (recommended settings) if any Area is empty (Set up done in Area Configuration). User can change this value if required.

Alarm Sound Delay

This setting is per workstation for Alarm sounds. If Alarm sounds are selected in General tab, alarms will start the sound after the specified delay in that workstation.

☑ Centralized Opening:

Centralized Opening is a system option where operator controls the access as per cardholder requests after verifying the person at door requesting to access. This option is integrated with some DVRs

☑ Mantrap Entry

Mantrap Entry is another system option where operator controls the access as per cardholder requests after verifying the person at door requesting to access. The operator has power to control whichever door he wants to provide the access first, if more than one user's request the access at the same time at various access points. This option is also integrated with some DVRs (For detailed information read TB68_AxiomV Mantrap Entry.pdf)

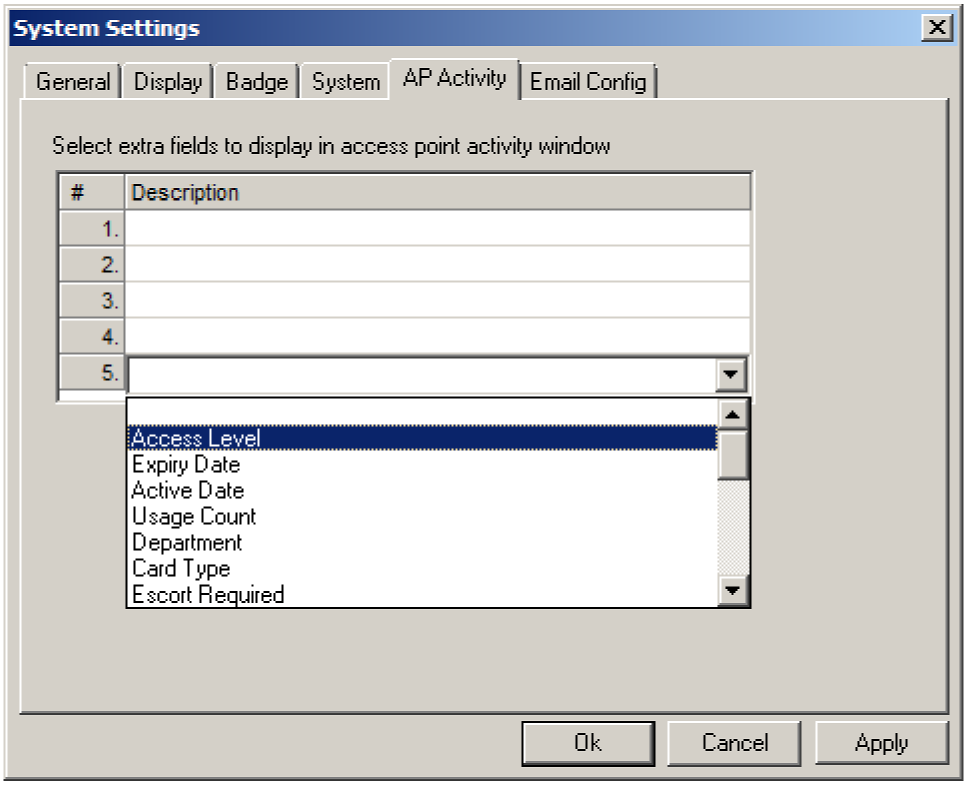
The user can select only one of the two options: Centralized Opening or Mantrap Entry. Both the options have similar functionalities where operator controls the access

to doors after verifying person at door, but different video integration windows. Mantrap Entry option is per workstation

☑ GT-Check late arriving only once

With this option selected the system will receive late arriving alarms for Guard tour only once.

AP Activity



Select extra fields to display in access point activity window

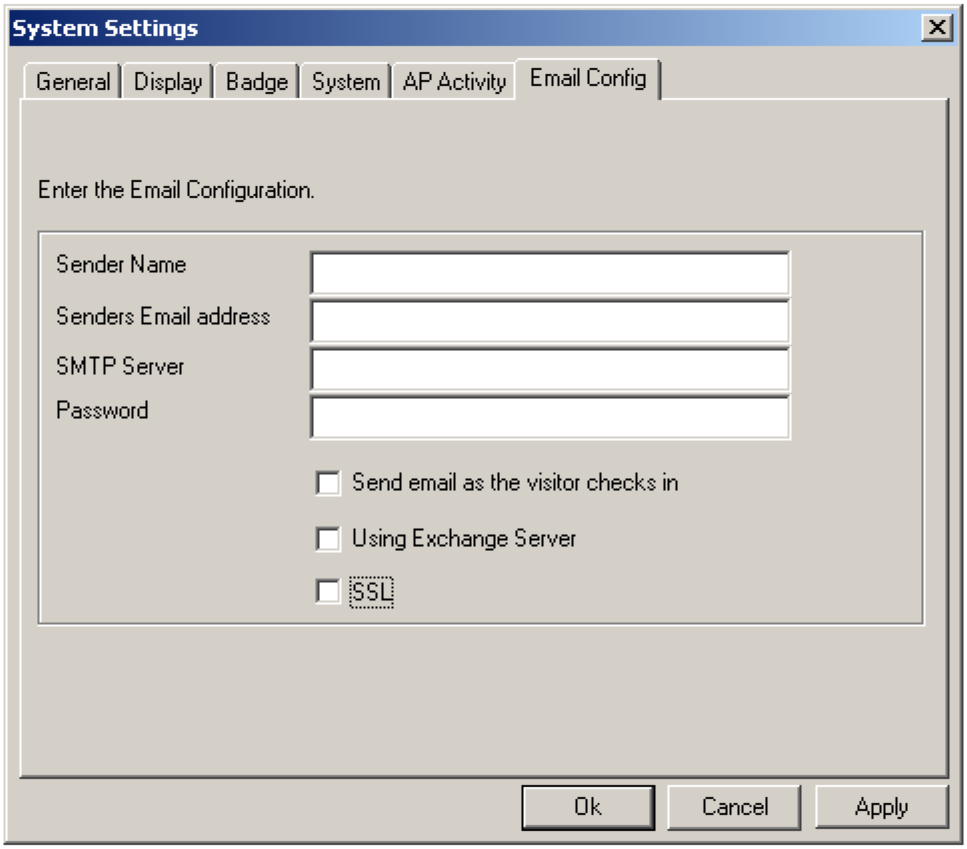
#	Description
1.	
2.	
3.	
4.	
5.	

Along with the Name of the Reader, the Name of the Cardholder, the Card Number, the Picture of the Cardholder, and the Access Point event message, you can select five fields of data that will be displayed on the Access Point Activity window. (See page 43 for more information on AP Activity,)

EMail Config

In *Visitor Management*, (see page 300 for more information on Visitor Management) email notification can be sent to the visiting cardholder. For this to work the senders email information must be configured in *eMail Config* under System settings.

These settings are also required for *Report server* to email the reports, if *email reports* option is selected under report server settings



Enter the Email Configuration.

Sender Name

Senders Email address

SMTP Server

Password

□ Send email as the visitor checks in

□ Using Exchange Server

□ SSL

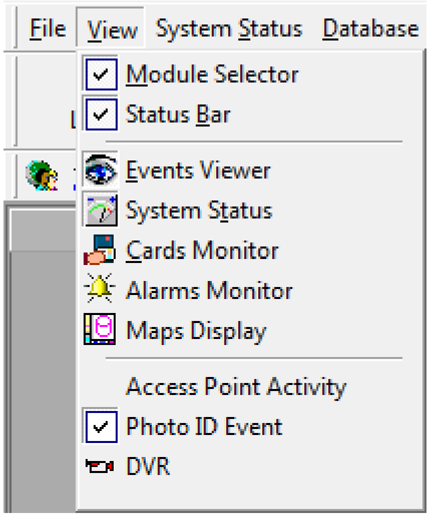
Fill in the required information as per your email settings.

Check the box **Send email as the visitor is checked in** to automatically send an email to the cardholder being visited as the visitor checks in. The being visited cardholder’s *Personal Tab* also must have an email address.

Exit

Click here to end the AxiomV™ session. The operator must be logged on in order to exit the system.

View



Module Selector

When the Module Selector is active the user may chose (by clicking) a database module or a System Status module. The database modules will open up a window for viewing or programming of the appropriate section of the database. The System Status modules will bring up a search window for item selection. These items will be displayed in the Status pane. (See page 138 for more information on *Module Selector*.)

Status Bar

The *Status Bar* at the bottom of the *Client* screen is used to display alarm counts, number of devices loaded for a specific search in system status. The name of the currently logged on operator is displayed here as well.

Events Viewer

The Event Viewer displays system and device messages. Which messages are displayed will depend on the policy of the logged in operator. The number of messages buffered for immediate recall can be set under the *Display* tab of *System Settings*. (See page 139 for more information on *Event Viewer*.)

System Status Pane

The System Status Pane will display the current status of the selected items. Right clicking on an item will bring up a menu. From this menu the operator could choose a command to execute or possibly they could make a programming selection. (See page 148 for more information on *System Status Pane*.)

Cards Monitor

The *Cards Monitor* window is used to display a list of cardholders and the area they are logged into. Operators can choose between displaying selected cardholders (and what area they are in) or selected areas (and which cardholders are in them). (See page 157 for more information on *Cards Monitor*.)

Alarms Monitor

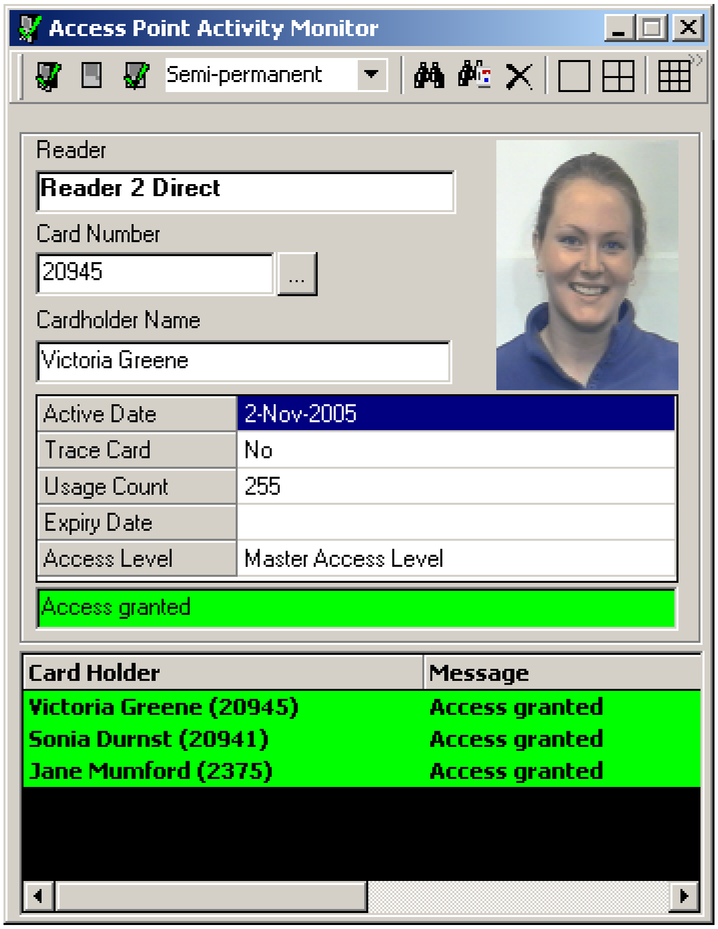
The Alarm Monitor window is used to acknowledge and clear alarms. The operator can also get instructions on what to do about the alarm and enter what was actually done for each alarm event. (See page 158 for more information on *Alarms Monitor*.)

☞ **Only the operator that acknowledged the alarm can clear the alarm.**

Maps Display

Maps Display will provide a list of maps to choose from. These maps can display the status of different types of items (like inputs, outputs, and access points) at the same time. Maps are created in the *MapMaker* module (see page 61 for more information on *MapMaker*).

Access Point Activity



Reader: Reader 2 Direct

Card Number: 20945

Cardholder Name: Victoria Greene

Active Date	2-Nov-2005
Trace Card	No
Usage Count	255
Expiry Date	
Access Level	Master Access Level

Access granted

Card Holder	Message
Victoria Greene (20945)	Access granted
Sonia Durnst (20941)	Access granted
Jane Mumford (2375)	Access granted

Single View

The *Access Point Activity Monitor* is used to monitor one, four, or nine access points. All activity on the selected access point(s) will be shown on this screen, including the cardholder's name, card number, and picture. Five additional fields of data can also be displayed (Selected in AP Activity tab of system settings as explained on Page 39); as well the last ten access point events will be displayed. Once selected, this screen can be minimized. It will automatically 'pop-up' when an event occurs on a selected access point.

Grant Access

Click on this icon to grant access to the selected access point (highlighted).

Lock & Unlock

Use these icons to either lock or unlock the selected access point. These commands will be affected by the *permanent*, *semi-permanent*, or *timed* selection immediately to the right.

Search

Use the *Search* icon to look for the access points to be monitored.

Card Search

An operator that doesn't have access to the cardholders in the database can use the Card Search icon to bring up information on a card number. Guards who don't have access to the cardholder database could use this to verify personnel by calling up the cardholder's information (including their picture) with a relatively quick search.

Clear

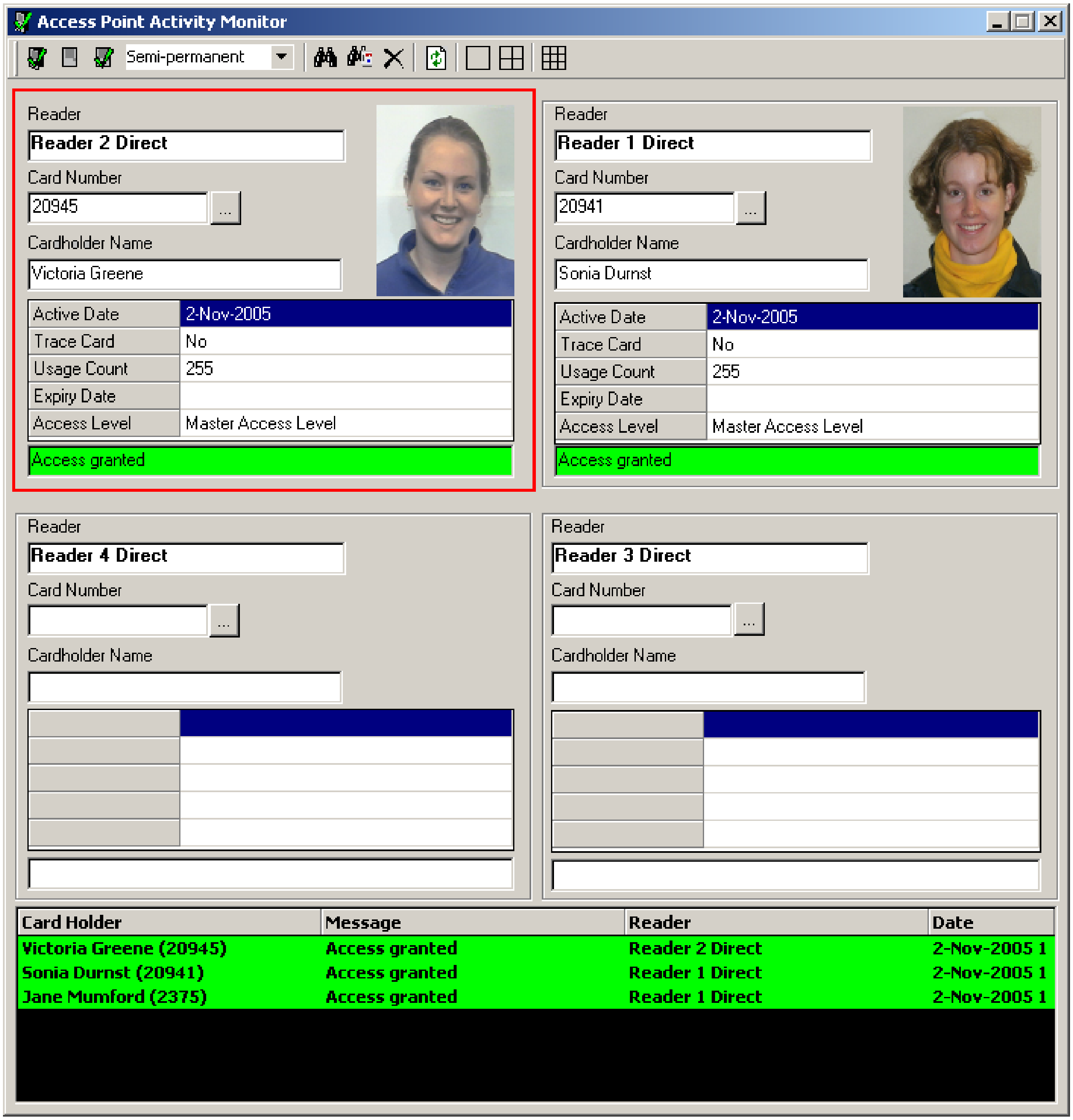
Clear will remove an access point that is no longer needed.

Refresh

Refresh will update the status of the selected access point.

View Single, Quad, or Nine

Select to view nine, four, or just one access point. You do not have to choose access points for all sections in the nine or quad view; some sections may be left unused.



Reader	Reader 2 Direct
Card Number	20945
Cardholder Name	Victoria Greene
Active Date	2-Nov-2005
Trace Card	No
Usage Count	255
Expiry Date	
Access Level	Master Access Level

Access granted

Reader	Reader 1 Direct
Card Number	20941
Cardholder Name	Sonia Durnst
Active Date	2-Nov-2005
Trace Card	No
Usage Count	255
Expiry Date	
Access Level	Master Access Level

Access granted

Reader
Reader 4 Direct
Card Number
Cardholder Name

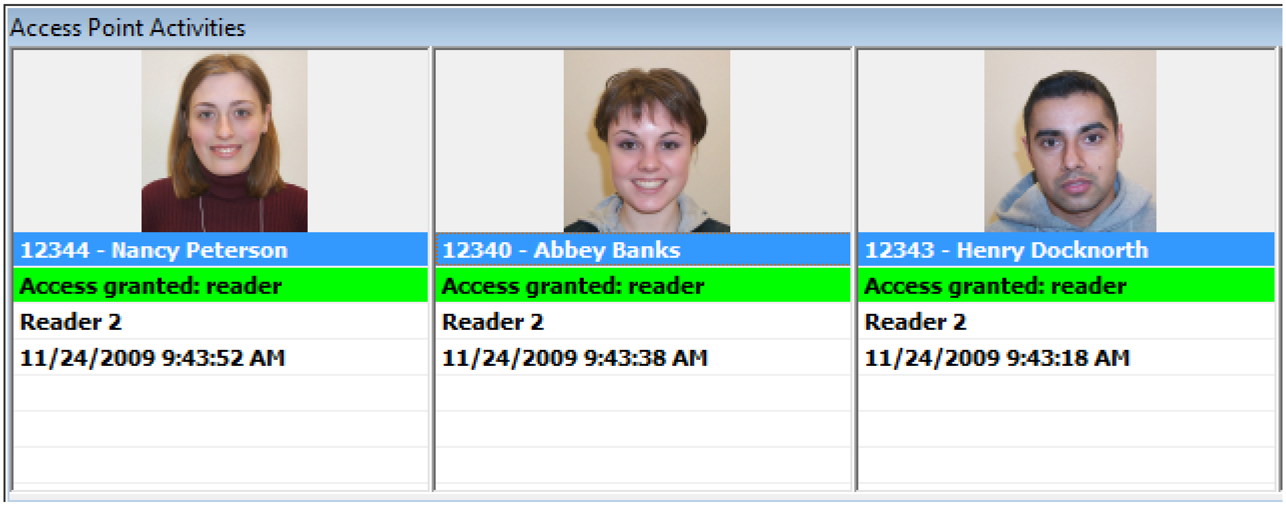
Reader
Reader 3 Direct
Card Number
Cardholder Name

Card Holder	Message	Reader	Date
Victoria Greene (20945)	Access granted	Reader 2 Direct	2-Nov-2005 1
Sonia Durnst (20941)	Access granted	Reader 1 Direct	2-Nov-2005 1
Jane Mumford (2375)	Access granted	Reader 1 Direct	2-Nov-2005 1

Quad View

Photo ID Event

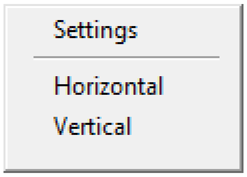
Photo ID Event is similar to *Access Point Activity*. Both provide about the same information. *Access Point Activity* is a floating window that can be moved around the screen while *Photo ID Event* is fixed at the bottom of the screen.



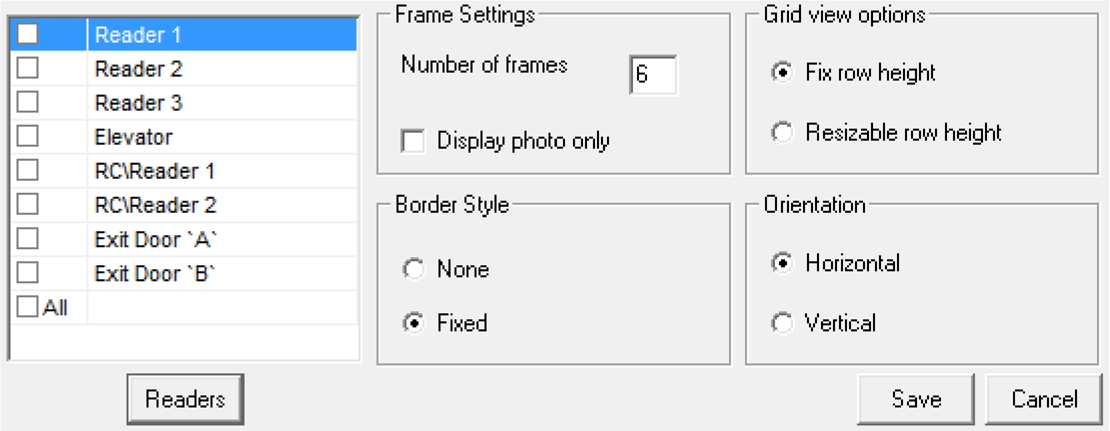
Access Point Activities

12344 - Nancy Peterson	12340 - Abbey Banks	12343 - Henry Docknorth
Access granted: reader	Access granted: reader	Access granted: reader
Reader 2	Reader 2	Reader 2
11/24/2009 9:43:52 AM	11/24/2009 9:43:38 AM	11/24/2009 9:43:18 AM

Entries shift to the right (or down) as new entries come in.



Right click in the activities area to get the menu selection.



□	Reader 1
□	Reader 2
□	Reader 3
□	Elevator
□	RC\Reader 1
□	RC\Reader 2
□	Exit Door `A`
□	Exit Door `B`
□ All	

Frame Settings
Number of frames 6
□ Display photo only

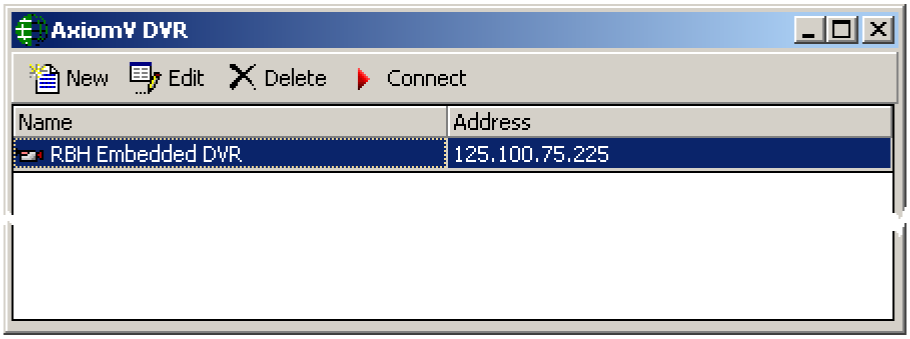
Grid view options
● Fix row height
○ Resizable row height

Border Style
○ None
● Fixed

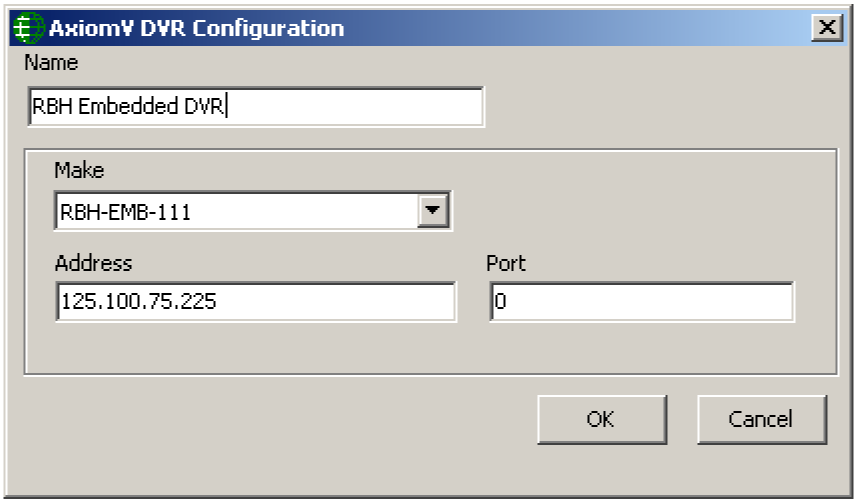
Orientation
● Horizontal
○ Vertical

Click on *Readers* and check the reader you want displayed in the activities area. Select the *Number of frames* required (the amount of traffic will likely determine how many frames you will want). The *Grid View Options* allows for the text *row heights* to be *Fixed* or *Resizable*, and therefore the text font to remain constant or adjust with the size of the activities area. *Border Style* selects either *Fixed* (border) or *None* (no border). *Orientation* will put the activities area either at the bottom of the screen under *System Status* (*Horizontal*) or on the right of *Event viewer* screen (*Vertical*).

DVR



Name	Address
RBH Embedded DVR	125.100.75.225



Name: RBH Embedded DVR

Make: RBH-EMB-111

Address: 125.100.75.225

Port: 0

New

Click *New* to configure a new DVR connection. Select a make from the pull down list and enter a name, the address, and a port number for this DVR.

Edit

Clicking *Edit* will open the DVR configuration window to make changes or to just view the DVR configuration.

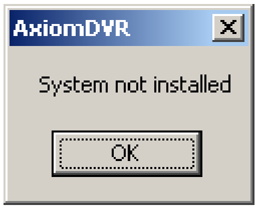
Delete

Use *Delete* to remove the highlighted DVR configuration record.

Connect

Click *Connect* to open a connection to the selected DVR.

If you get the message below then you have not yet installed the necessary driver/integration file for that manufacturer's DVR.

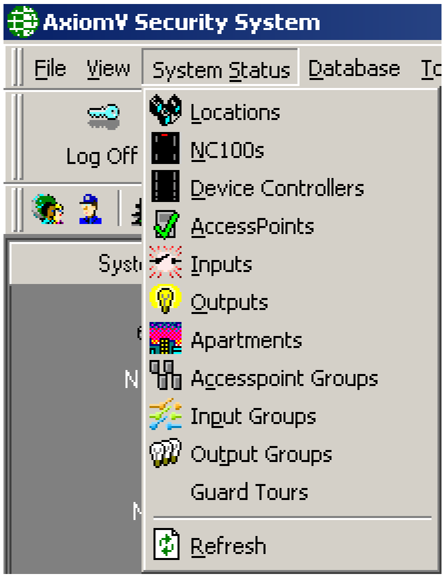


AxiomDVR

System not installed

For more information on the Axiom DVR integration; please refer to the document DVR Manual (AxiomV™).

System Status



Choices made here will have the same effect as choices made from the *Module Selector*.

Locations

Locations will display the selected Networks. (For more information see page 166.)

NC100s

NC100s will display the selected NC100/UNC500 panels. (For more information see page 168.)

Device Controllers

Device Controllers will display the selected RCs, IOC16s and Keypads. (For more information see page 174.)

Access Points

Access Points will display the selected Access Points. (For more information see page 178.)

Inputs

Inputs will display the selected Inputs. (For more information see page 181.)

Outputs

Outputs will display the selected Outputs. (For more information see page 183.)

Apartments

Apartments will display the selected SafeSuite™ apartments. (For more information see page 185.)

Access Point Groups

Access Point Groups will display the selected Access Point Groups. (For more information see page 189.)

Input Groups

Input Groups will display the selected Input Groups. (For more information see page 190.)

Output Groups

Output Groups will display the selected Output Groups. (For more information see page 192.)

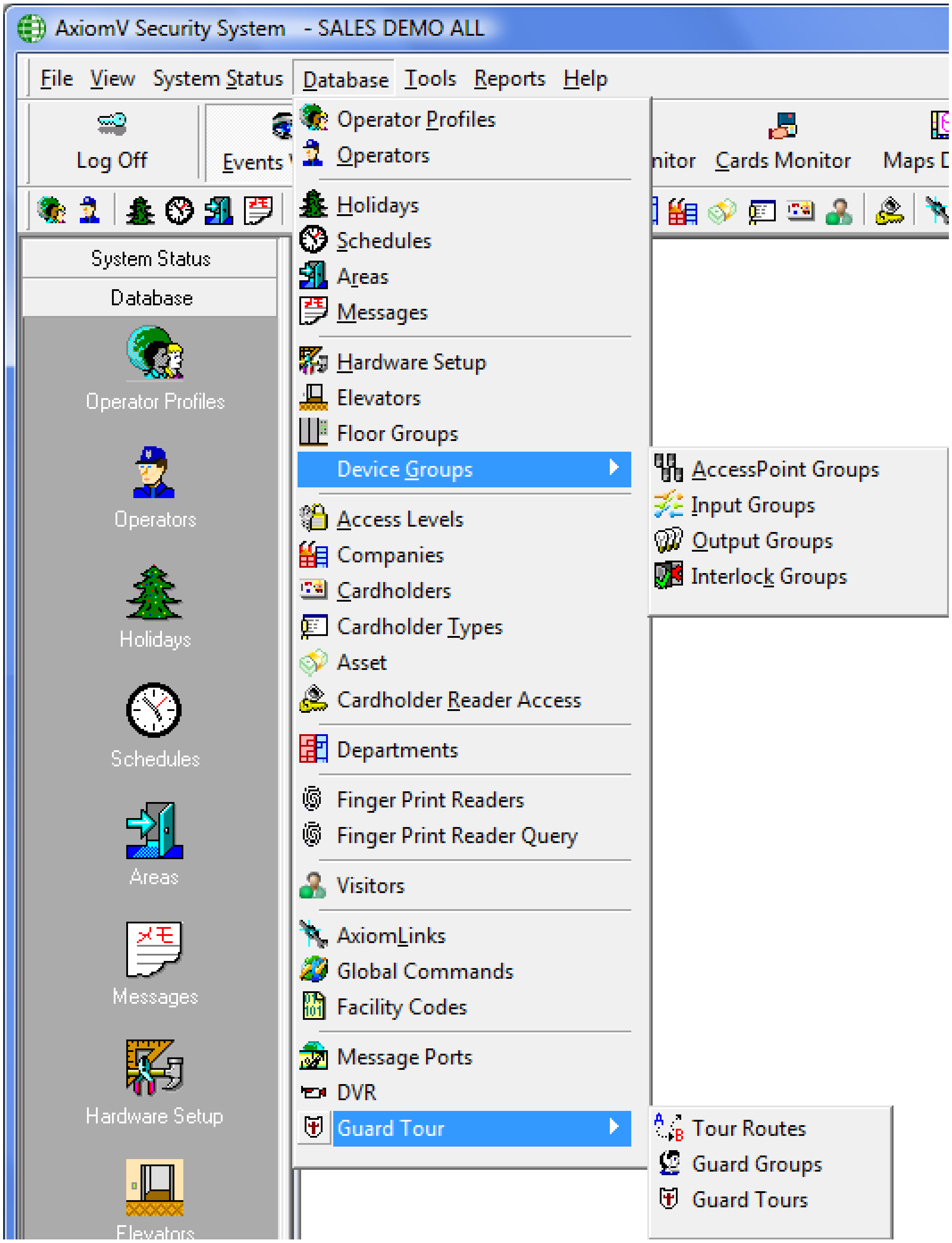
Guard Tours

Guard Tours will display the selected Guard Tours. (For more information see page 193.)

Refresh

Refresh will query the selected items to update their status.

Database



Choices made here will have the same effect as choices made from the *Module Selector*.

Operator Profiles

Operator Profiles opens the *Operator Security Profiles* window for the management of the security profiles, for the operators. The abilities of the default or “Master Profile” cannot be changed although the name can be. (For more information on creating *Operator Profiles* see page 198.)

Operators

Operators will open the Operators window to enter new operators, change the profiles of existing operators, or view the profiles of existing operators. The default operator (rbh) will always have the default operator profile. Although the login ID, name, and language of the default operator may be changed it will always have full privileges. (For more information on creating see page 204.)

Holidays

Holidays will open the *Holidays* window to create new holidays, edit the existing holidays, or view existing holidays. (For more information on creating *Holidays* see page 206.)

Schedules

Schedules will open the *Schedules* window to create new schedules, edit the existing schedules, or view the time groups of existing schedules. (For more information on creating *Schedules* see page 208.)

Areas

Areas will open the *Areas* window to create new areas, edit the existing areas, or view the properties of existing areas. (For more information on creating *Areas* see page 213.)

Messages

Messages will open the *Messages* window to create new messages, edit the existing messages, or view the properties of existing messages. (For more information on creating *Messages* see page 214.)

Hardware Setup

Hardware Setup will bring up the *Hardware Setup* tree view window. In this tree view the operator can manage the system’s hardware. Networks, NC100s, RC2s, IOC16s, Access Points, Inputs, and Outputs can be added, deleted, or edited as required by the system's configuration. (For more information on *Hardware Setup* see page 217.)

Elevators

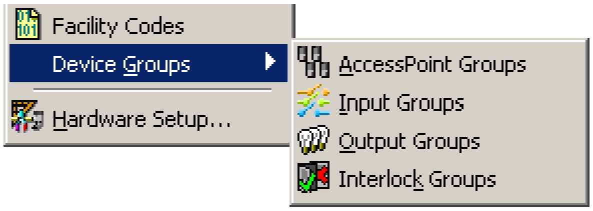
Click *Elevators* to create and/or assign floor outputs to an elevator reader for the purpose of controlling access to those floors. (For more information on *Elevators* see page 252.)

Floor Groups

Floor Groups will open the Elevator Floor Groups window so that combinations of elevator floor can be created for access control purposes. (For more information on *Floor Groups* see page 254.)

Device Groups

Device Groups allows the operator to create groups of like devices (access points, input and outputs). These groups can be used with operator commands or they can be used in links. Grouping like devices will make it easier to issue the same command to multiple devices. (For more information on creating, *Access Point Groups* see page 255, *Input Groups* see page 256, *Output Groups* see page 257.)



Interlock Groups are groups of access points grouped for a different purpose such as Mantrap. If any door contact of a member access point of an *Interlock Group* is in violation, then no other member of that group will grant access. I.e. **if any door of an *Interlock Group* is open then no other door, of that group, can be opened.** (For more information on creating *Interlock Groups* see page 258)

Access Levels

Access Levels will open the Access Level window to create new access levels, edit existing access levels, or view the properties of existing access levels. (For more information on creating *Access Levels* see page 259.)

Companies

Companies will open a window to create Cardholder groups/companies, edit or view existing companies. Cardholder Groups (or *Companies*) are only used in *Operator Profiles*. They are used to segregate cardholder, and limit operators in their availability to cardholders. (For more information on creating *Companies* see page 267.)

Cardholders

Cardholders will open the Cardholder screen to add cardholders, edit existing cardholders, or view cardholder properties. (For more information on creating *Cardholders* see page 271.)

Cardholder Types

Cardholder Types will open the Cardholder Type configuration screen to add, edit, or view Cardholder Types. (For more information on *Cardholder Types* see page 294.)

Assets

Assets will open the Asset configuration screen to add, edit, or view assets. (For more information on *Assets* see page 294.)

Cardholder Reader Access

Cardholder Reader Access will open the *Cardholder Reader Access Update* window to create special access for cardholders. (For more information on creating *Reader Access* see page 298.)

Departments

Departments will open the *Departments* window. *Departments* are used to fill the *Department 1* and *Department 2* fields in the *Cardholder* screen. (For more information on creating *Departments* see page 266.)

Finger Print Readers

Finger Print Readers will open the *Finger Print Readers*. (For more information on creating *Finger Print Readers* see page 263)

Finger Print Reader Query

Finger Print Reader Query will open the *Finger Print Reader Query* window. (For more information on creating *Finger Print Reader Query* see page 265.)

Visitors

Visitors will open the *Visitors* window. (For more information on *Visitors* see page 301.)

AxiomLinks

AxiomLinks™ will open the *AxiomLinks*™ window to create new links, edit the existing links, or view the properties of existing links. (For more information on creating *AxiomLinks*™ see page 311.)

Global Commands

Global Commands are the same as *AxiomLinks*™ except that the *CommsServer* executes them instead of the NC-100/UNC500. Therefore (unlike *AxiomLinks*™) *Global Commands* can bridge networks. A command triggered on one network can be executed on another network. (For more information on creating *Global Commands* see page 317.)

Facility Codes

Facility Codes will open the *Facility Codes* window to enter new facility codes, edit the existing facility codes, or view existing facility codes. (For more information on creating *Facility Codes* see page 318.)

Message Ports

Message Ports will open the *Message Port* window to configure your ASCII message ports. You can setup new message ports, edit existing ports, or delete ports that are no longer required. (For more information on *Message Ports* see page 320.)

DVR

The database selection *DVR* will call up the same connection/configuration window as the *View DVR* menu selection. (See *View DVR* on page 47 for more information.)

Guard Tour[4]*Error! Bookmark not defined.*

Tour Routes

[4] This selection is only available if the optional license for the Guard Tour Software has been purchased and installed.

Tour Route will open the configuration window for tour route as described on page 326.

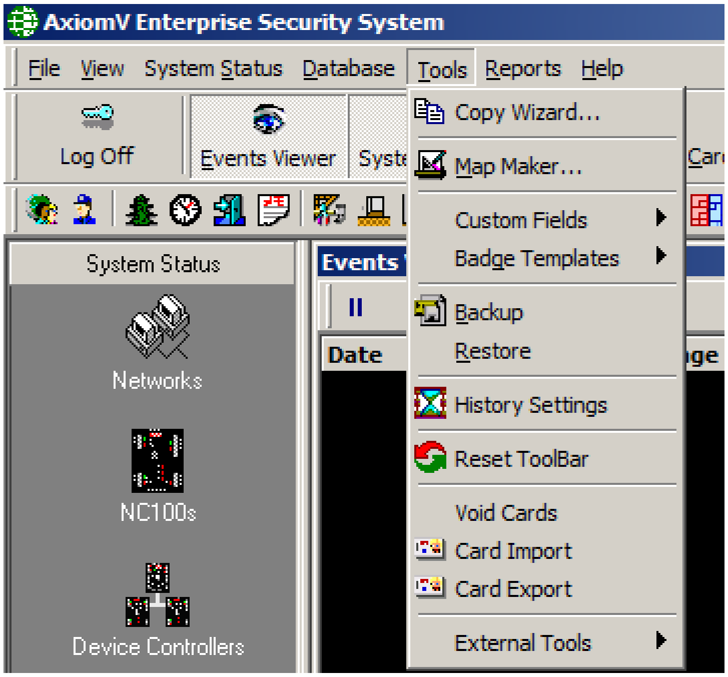
Guard Groups

Guard Groups will open the configuration window for guard group as described on page 328.

Guard Tours

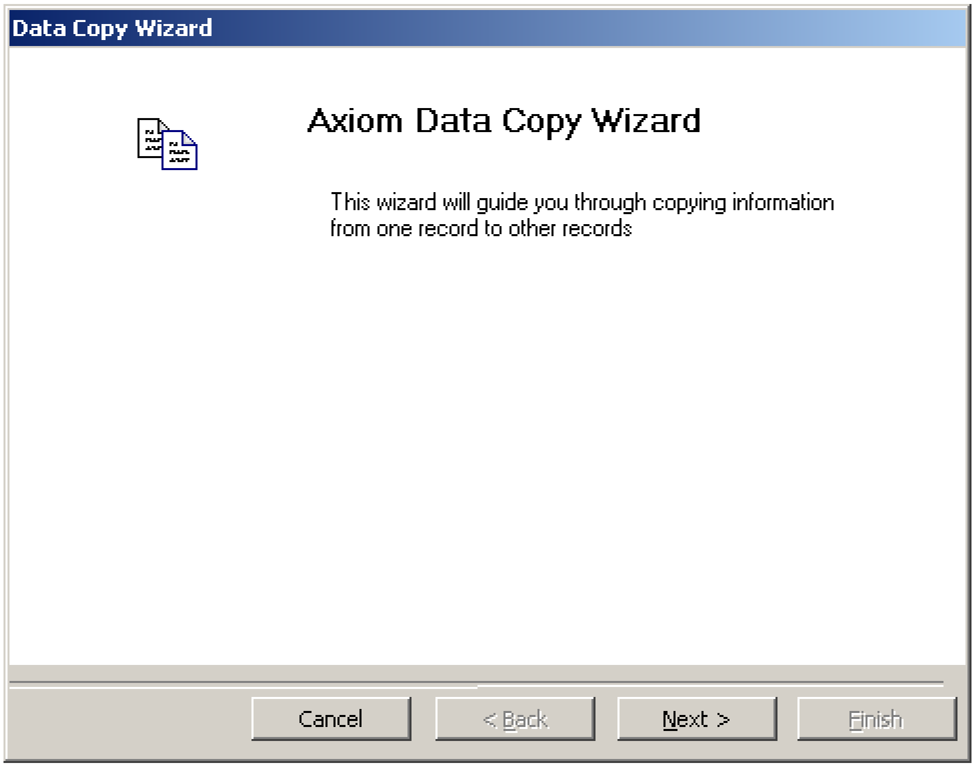
Guard Tours will open the configuration window for guard tours as described on page 329.

Tools



Copy Wizard…

Copy Wizard will open the *AxiomV™ Data Copy Wizard*. Through the *Copy Wizard* the operator can copy selected data from one item to multiple like items.



Data Copy Wizard

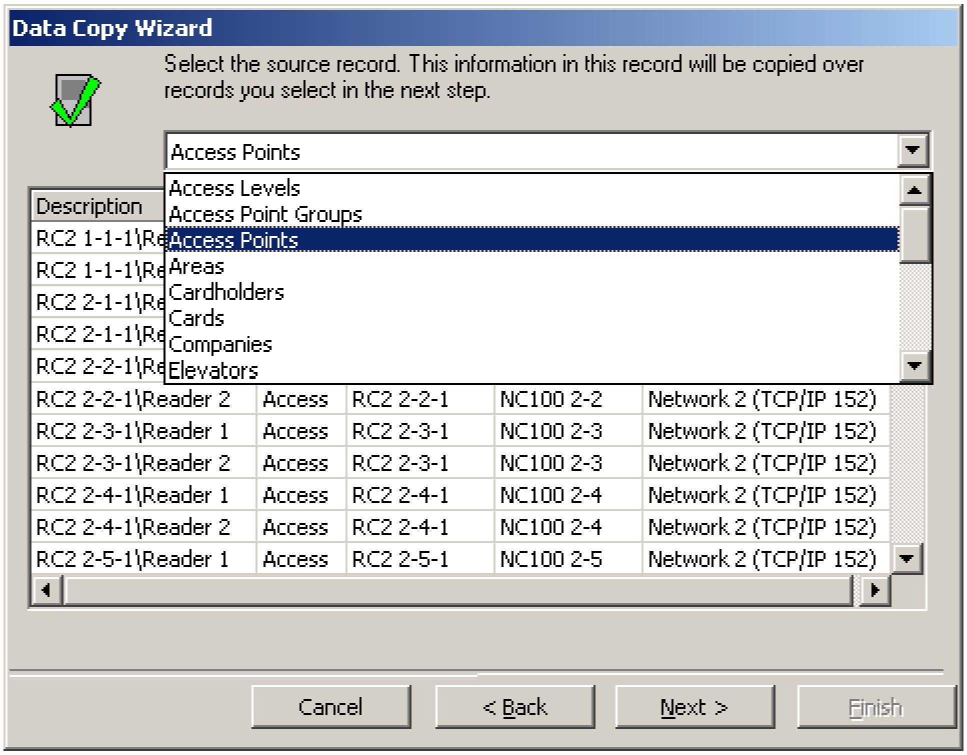
Axiom Data Copy Wizard

This wizard will guide you through copying information from one record to other records

The *Copy Wizard* is a very versatile and quick way to program the AxiomV™ system. After programming one item, that item can be used as a template to program all of the other items of the same type. For example if one access point was programmed then all the other access points could be programmed from that one.

➢ To copy data from one item to another start the *Copy Wizard* and click *Next*. Then follow the steps on the following pages.

1. First select a category from the pull down list.



Data Copy Wizard

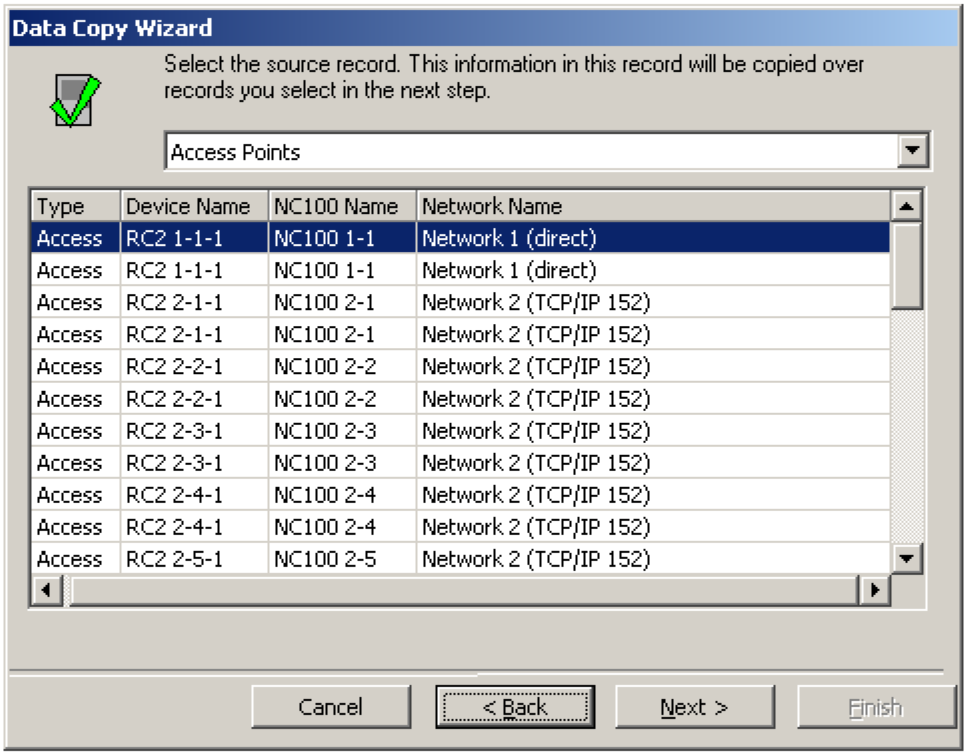
Select the source record. This information in this record will be copied over records you select in the next step.

Access Points

- Access Levels
- Access Point Groups
- Access Points
- Areas
- Cardholders
- Cards
- Companies
- Elevators

Description				
RC2 1-1-1\Re				
RC2 1-1-1\Re				
RC2 2-1-1\Re				
RC2 2-1-1\Re				
RC2 2-2-1\Re				
RC2 2-2-1\Reader 2	Access	RC2 2-2-1	NC100 2-2	Network 2 (TCP/IP 152)
RC2 2-3-1\Reader 1	Access	RC2 2-3-1	NC100 2-3	Network 2 (TCP/IP 152)
RC2 2-3-1\Reader 2	Access	RC2 2-3-1	NC100 2-3	Network 2 (TCP/IP 152)
RC2 2-4-1\Reader 1	Access	RC2 2-4-1	NC100 2-4	Network 2 (TCP/IP 152)
RC2 2-4-1\Reader 2	Access	RC2 2-4-1	NC100 2-4	Network 2 (TCP/IP 152)
RC2 2-5-1\Reader 1	Access	RC2 2-5-1	NC100 2-5	Network 2 (TCP/IP 152)

2. Then choose the source record to be copied from.



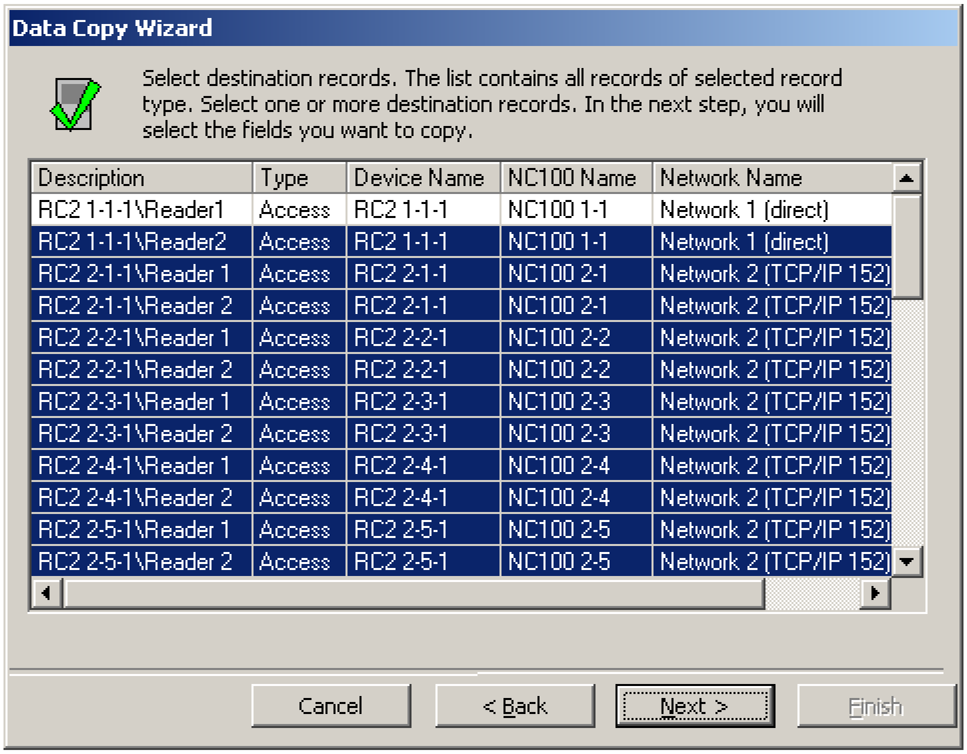
Data Copy Wizard

Select the source record. This information in this record will be copied over records you select in the next step.

Access Points

Type	Device Name	NC100 Name	Network Name
Access	RC2 1-1-1	NC100 1-1	Network 1 (direct)
Access	RC2 1-1-1	NC100 1-1	Network 1 (direct)
Access	RC2 2-1-1	NC100 2-1	Network 2 (TCP/IP 152)
Access	RC2 2-1-1	NC100 2-1	Network 2 (TCP/IP 152)
Access	RC2 2-2-1	NC100 2-2	Network 2 (TCP/IP 152)
Access	RC2 2-2-1	NC100 2-2	Network 2 (TCP/IP 152)
Access	RC2 2-3-1	NC100 2-3	Network 2 (TCP/IP 152)
Access	RC2 2-3-1	NC100 2-3	Network 2 (TCP/IP 152)
Access	RC2 2-4-1	NC100 2-4	Network 2 (TCP/IP 152)
Access	RC2 2-4-1	NC100 2-4	Network 2 (TCP/IP 152)
Access	RC2 2-5-1	NC100 2-5	Network 2 (TCP/IP 152)

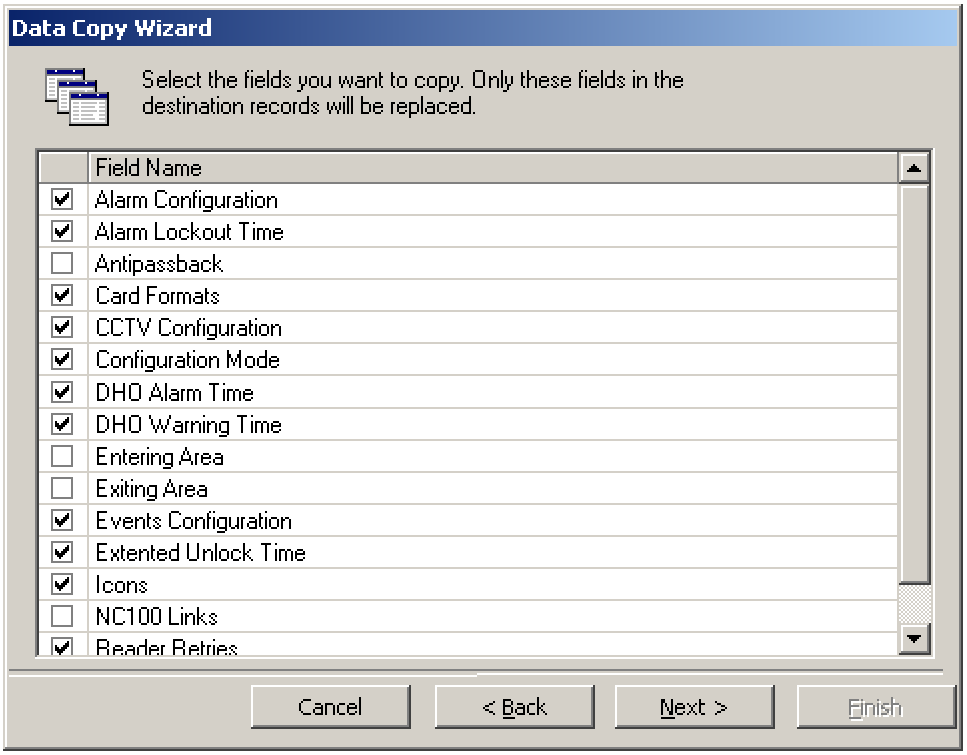
3. Now select all of the destination records that are to be programmed.



Select destination records. The list contains all records of selected record type. Select one or more destination records. In the next step, you will select the fields you want to copy.

Description	Type	Device Name	NC100 Name	Network Name
RC2 1-1-1\Reader1	Access	RC2 1-1-1	NC100 1-1	Network 1 (direct)
RC2 1-1-1\Reader2	Access	RC2 1-1-1	NC100 1-1	Network 1 (direct)
RC2 2-1-1\Reader 1	Access	RC2 2-1-1	NC100 2-1	Network 2 (TCP/IP 152)
RC2 2-1-1\Reader 2	Access	RC2 2-1-1	NC100 2-1	Network 2 (TCP/IP 152)
RC2 2-2-1\Reader 1	Access	RC2 2-2-1	NC100 2-2	Network 2 (TCP/IP 152)
RC2 2-2-1\Reader 2	Access	RC2 2-2-1	NC100 2-2	Network 2 (TCP/IP 152)
RC2 2-3-1\Reader 1	Access	RC2 2-3-1	NC100 2-3	Network 2 (TCP/IP 152)
RC2 2-3-1\Reader 2	Access	RC2 2-3-1	NC100 2-3	Network 2 (TCP/IP 152)
RC2 2-4-1\Reader 1	Access	RC2 2-4-1	NC100 2-4	Network 2 (TCP/IP 152)
RC2 2-4-1\Reader 2	Access	RC2 2-4-1	NC100 2-4	Network 2 (TCP/IP 152)
RC2 2-5-1\Reader 1	Access	RC2 2-5-1	NC100 2-5	Network 2 (TCP/IP 152)
RC2 2-5-1\Reader 2	Access	RC2 2-5-1	NC100 2-5	Network 2 (TCP/IP 152)

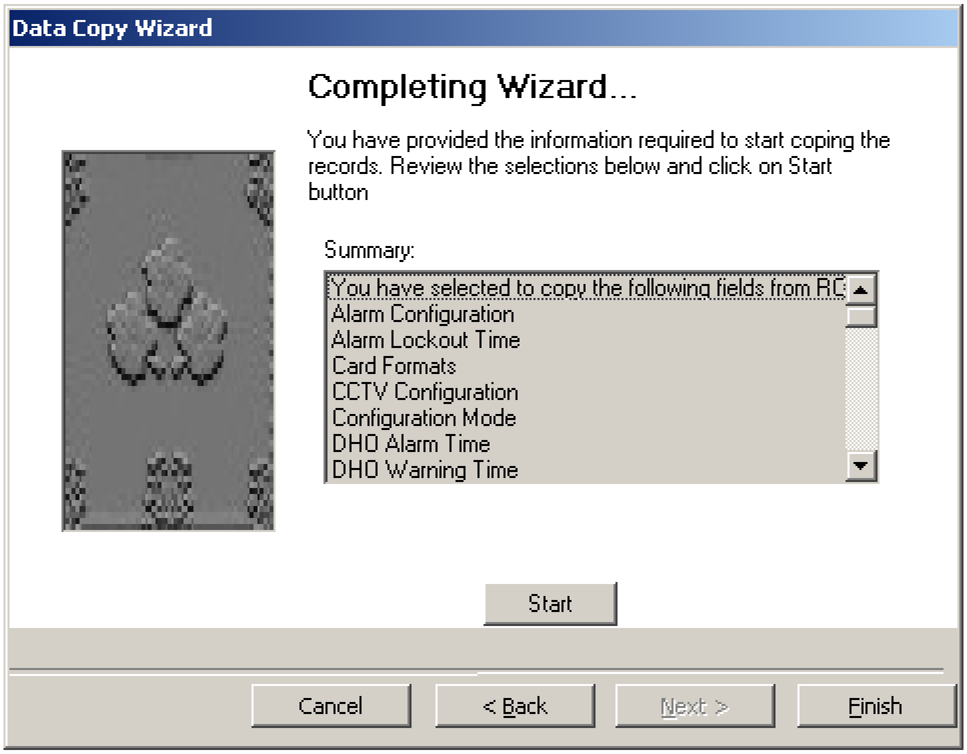
4. At this point the fields to be copied are selected (choose from the list).



Data Copy Wizard

Select the fields you want to copy. Only these fields in the destination records will be replaced.

	Field Name
☑	Alarm Configuration
☑	Alarm Lockout Time
□	Antipassback
☑	Card Formats
☑	CCTV Configuration
☑	Configuration Mode
☑	DHO Alarm Time
☑	DHO Warning Time
□	Entering Area
□	Exiting Area
☑	Events Configuration
☑	Extented Unlock Time
☑	Icons
□	NC100 Links
☑	Reader Retries



Data Copy Wizard

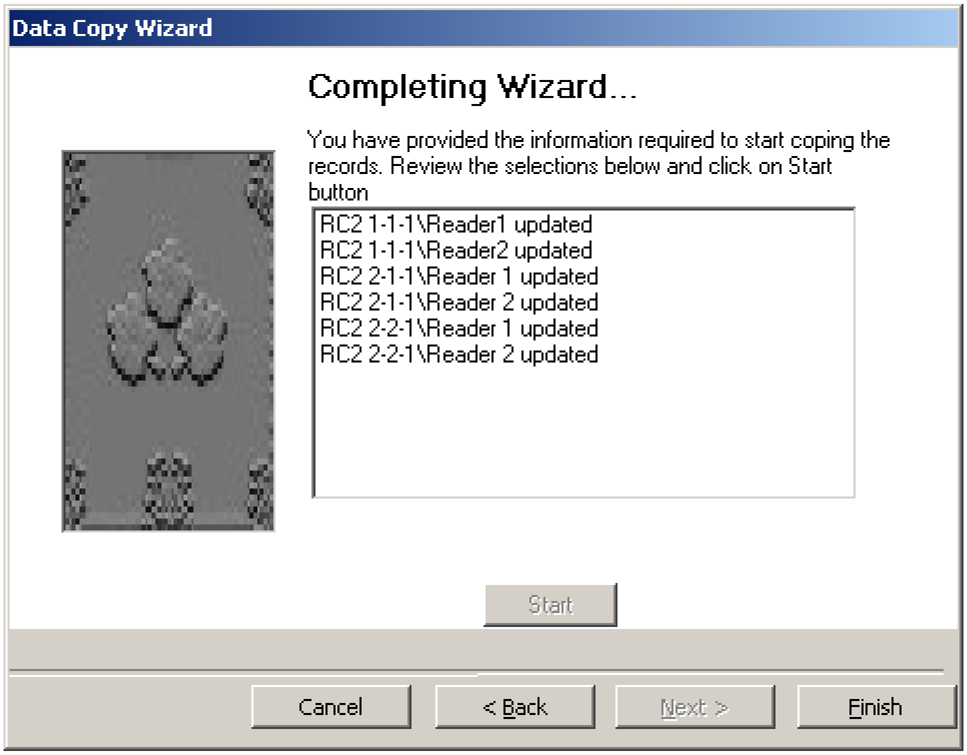
Completing Wizard...

You have provided the information required to start coping the records. Review the selections below and click on Start button

Summary:

You have selected to copy the following fields from RC
Alarm Configuration
Alarm Lockout Time
Card Formats
CCTV Configuration
Configuration Mode
DHO Alarm Time
DHO Warning Time

5. The final screen will allow you to review your selection before continuing. Click *Start* to execute the copy. As each item is updated it will be listed on the screen. You can go *Back* to do another copy or exit by clicking *Finish* or *Cancel*.



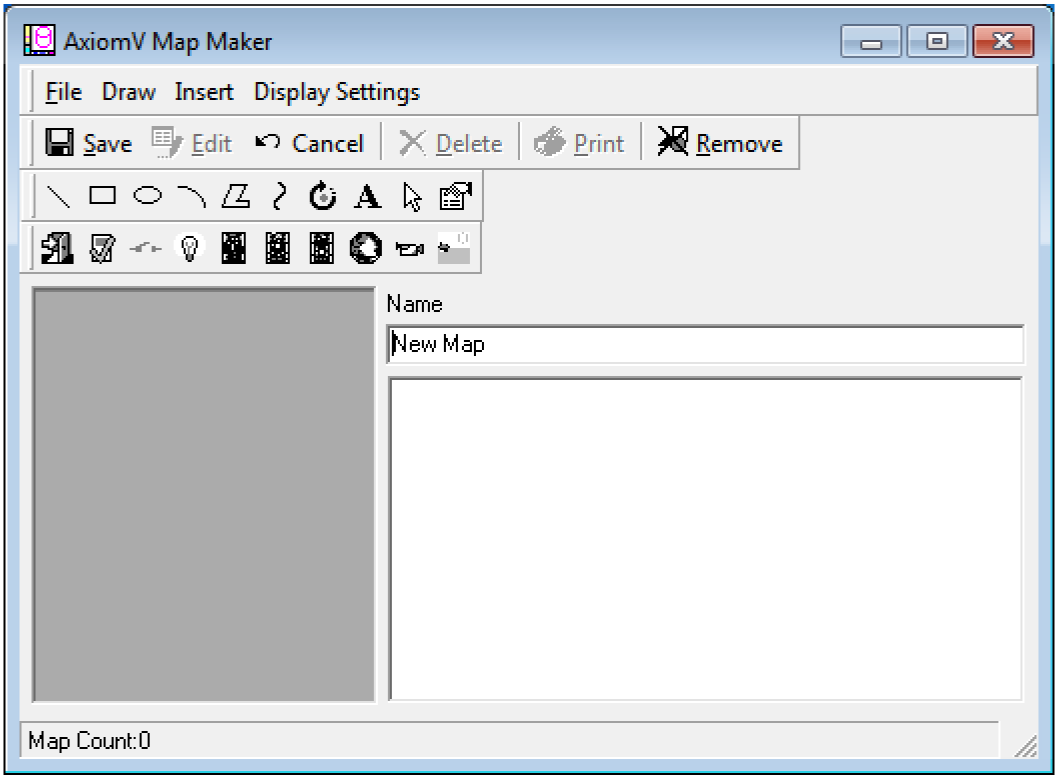
Completing Wizard...

You have provided the information required to start coping the records. Review the selections below and click on Start button

RC2 1-1-1\Reader1 updated
RC2 1-1-1\Reader2 updated
RC2 2-1-1\Reader 1 updated
RC2 2-1-1\Reader 2 updated
RC2 2-2-1\Reader 1 updated
RC2 2-2-1\Reader 2 updated

Map Maker…

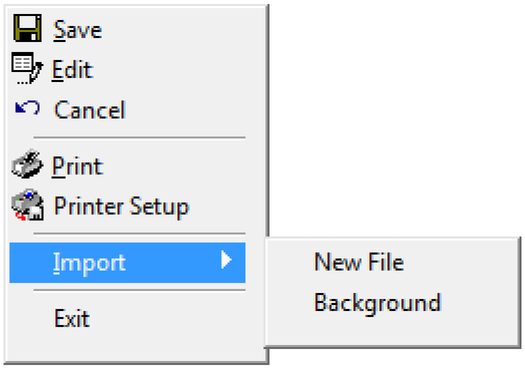
Map Maker is a module used to create maps (graphic displays) of a location. Devices and other items (like links to other maps) can be added to these maps. These maps can then be used to display the current status of the equipment in the chosen area. The *Status Bar* of this screen will display the number of maps already created.


AxiomV Map Maker
File Draw Insert Display Settings
Save Edit Cancel Delete Print Remove
Name

Name: New Map

Map Count:0

File



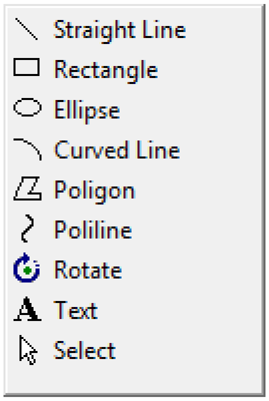
Import

Use *Import* to enter a pre-created graphic as a background for the map.

New File will import a graphics file as the background to a new map.

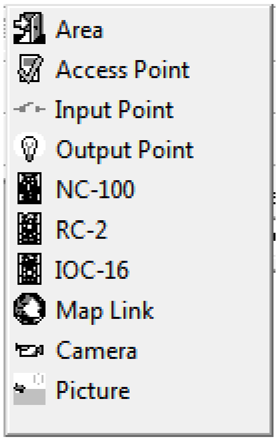
Background will import a graphics file as the background to an existing map.

Draw



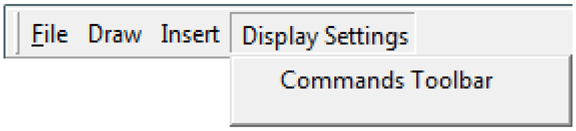
Use the *Draw* tools to enhance the map. Lines and shapes can be added to emphasize aspects of the map. Text can be added to label portions of the map for clarity.

Insert



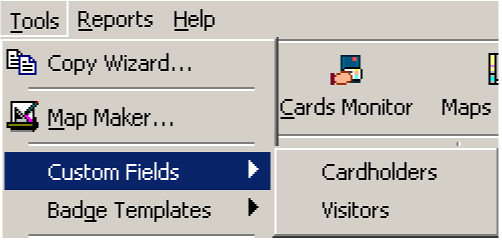
Use the *Insert* tools to add device icons to the map. These icons (*Access Points, Inputs, Outputs* etc.) will show the status of the devices when the map is displayed. The *Map Link* icon can be used to call up another map to be displayed.

Display Settings

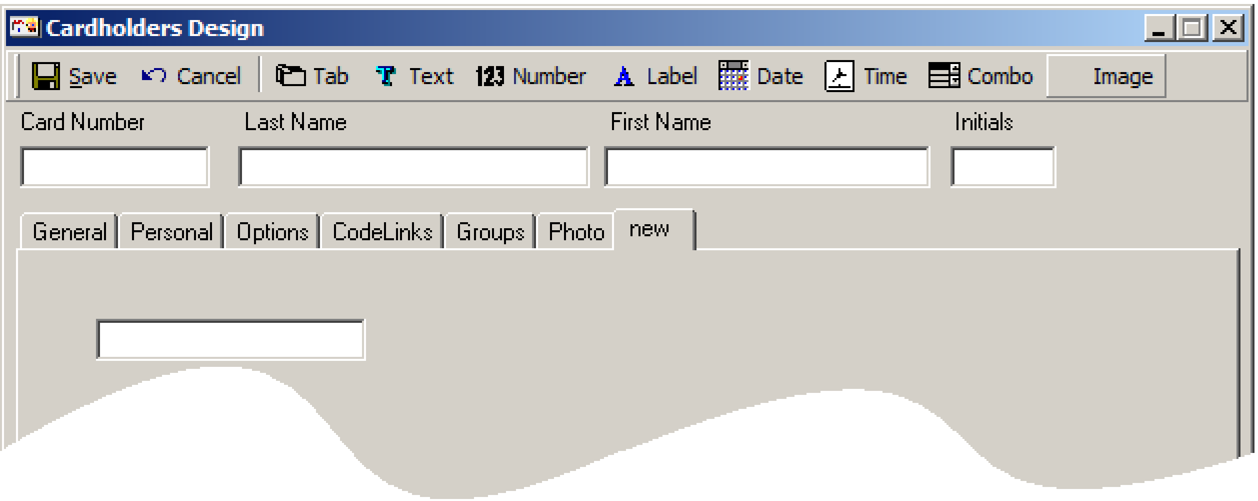


Commands Toolbar is a toolbar on the *Maps Display* that provides the commands for the last selected icon. If this feature is not selected, the operator needs to **right-click** on the selected icon to get a command list. This feature was developed to make it easier for operators using touch-screens to execute commands like *Grant Access* for selected *access point* from a map.

Custom Fields



This section allows additional user-defined cardholder and/or visitor fields to be setup and given a field name. Additional fields might include emergency contact number, car license plate number, parking spot number, hiring date, tax codes, or any other information that is required for the cardholder.



Tab

Click on *Tab* to create a new tab. Just enter a new name for the tab and click *OK*.

Text

Click on *Text* to insert a text box on to the current tab. *Text* boxes can contain both alpha and numeric characters.

Number

Click on *Number* to insert a number box on to the current tab. *Number* boxes can only contain numeric characters.

Label

Click on *Label* to create a label to describe a box or a group of boxes.

Date

Click on *Date* to insert a date box on to the current tab. *Date* boxes only contain valid calendars dates. You can pull down a calendar to scroll through and select a date or you can simply type over the day/month/year to change them.

Time

Click on *Time* to insert a time box on to the current tab. *Time* boxes only contain valid clock times. You can select hours, minutes, seconds, or AM/PM and use the up/down buttons to change the time or simply type over the current entry.

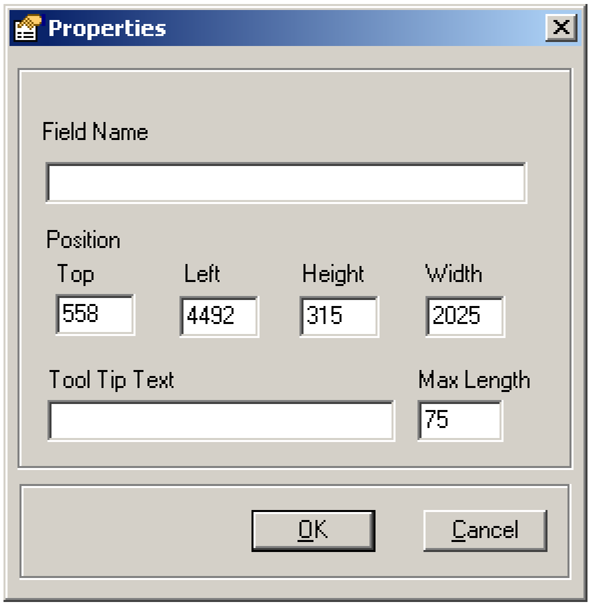
Combo

Click on *Combo* to insert a combo box on to the current tab. *Combo* boxes provide a pull down list of all the different entries already entered into the box. You can either select an entry from the list or type in a new one.

Image

Click on *Image* to insert a combo box on to the current tab. *Image* boxes are combo boxes that provide a pull down list of images. Image files are entered here or selected from the list if they were entered previously. These images are stored in the RBH Image folder along with cardholder pictures, and can be added to a Badging Template so that the picture appears on the cardholder's badge.

Field Properties



Field Name

Position

Top	Left	Height	Width
558	4492	315	2025

Tool Tip Text

Max Length: 75

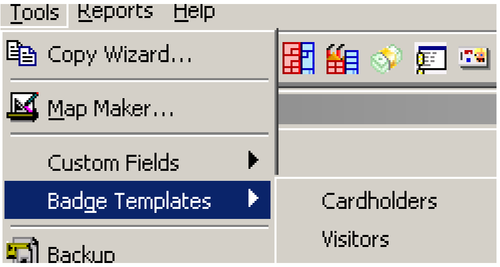
Creating a new box will pop-up the properties window for that field. Enter the name of the field to be added to the database (it will be a searchable field). You may also enter your own 'Tool Tip' for this box; as well you may determine the maximum length of the field. The box can be repositioned on the tab by dragging it to the desired location. In the properties window its position can be set precisely (numerically).

Label properties have only *Caption* (instead of *Field* name) and *Position*, no *Tool Tip* or *Max Length*.

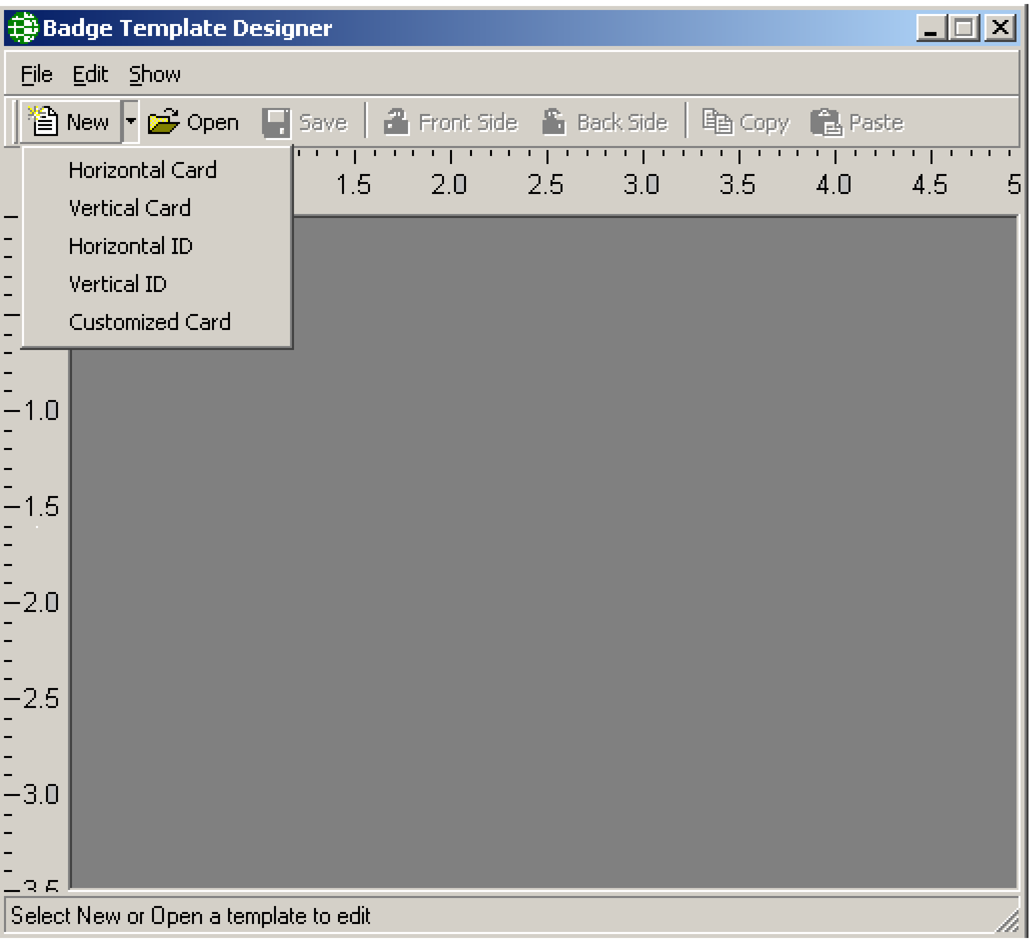
Right click on a box to delete the box or edit its properties.

Badge Templates[5]

This section allows designing Badge templates for Cardholders and/or Visitors



Badge Template Designer



Select New or Open a template to edit

[5] This selection is only available if the optional license for the Badging Software has been purchased and installed.

New Template

Click on the down arrow to choose from the menu the size and orientation of the card template to be created.

1. Horizontal Card (Width 3.36", Height 2.18")
2. Vertical Card (Width 2.18", Height 3.36")
3. Horizontal ID (Width 3.50", Height 2.11")
4. Vertical ID (Width 2.11", Height 3.50")
5. Customized Card(Size set by user)

Open

To edit or view an existing template, click on *Open*.

Save

To save the current template, click on *Save*.

Front Side

Clicking on *Card Front* will switch the card view to show the front of the card.

Back Side

Clicking on *Card Back* will switch the card view to show the back of the card.

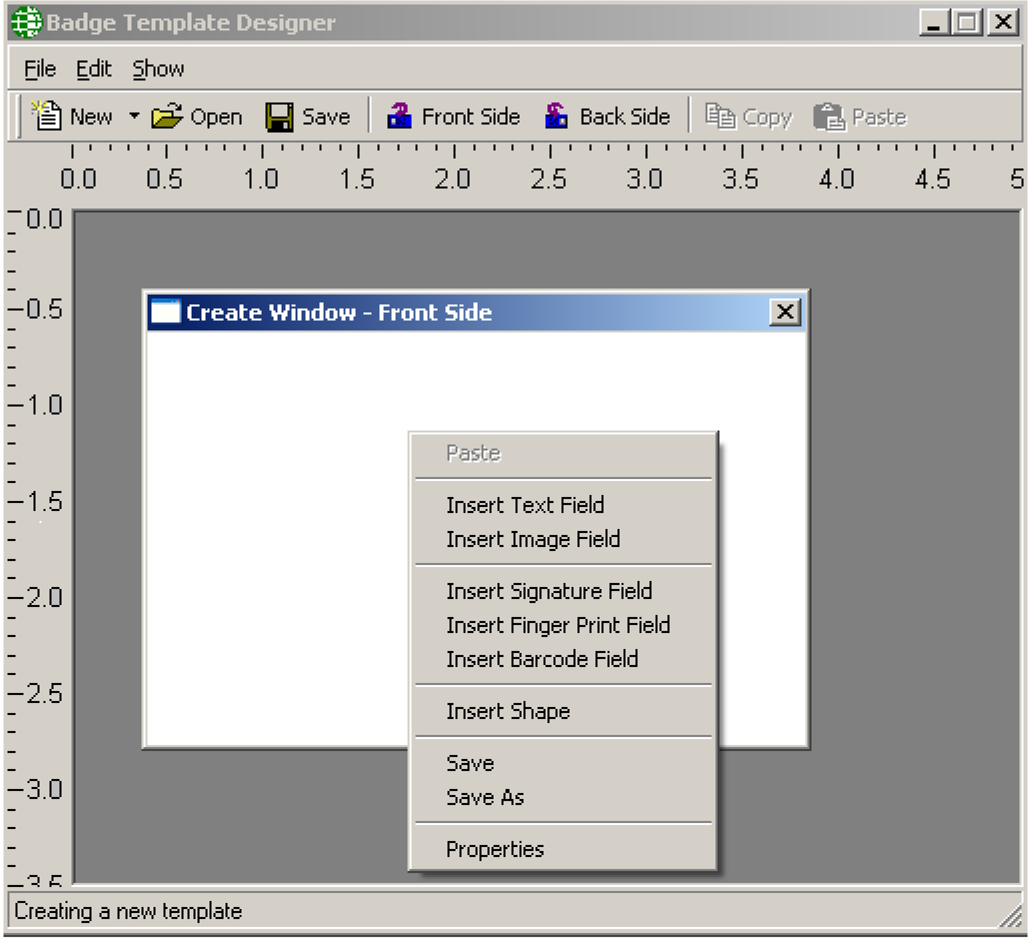
Copy

Copy is used to create duplicate boxes on a card. If you need two *Text* boxes the same size, you can make a copy of the one you created to create the other. You can then edit box to have different data entered into each box.

Paste

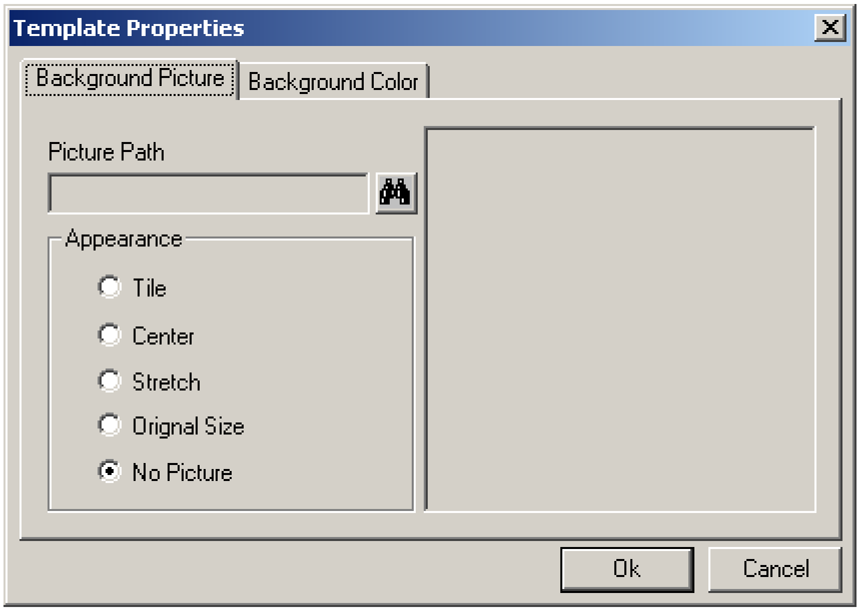
Clicking *Paste* will actually create the copy.

Create a Badge



➢ **To create a badge template**:

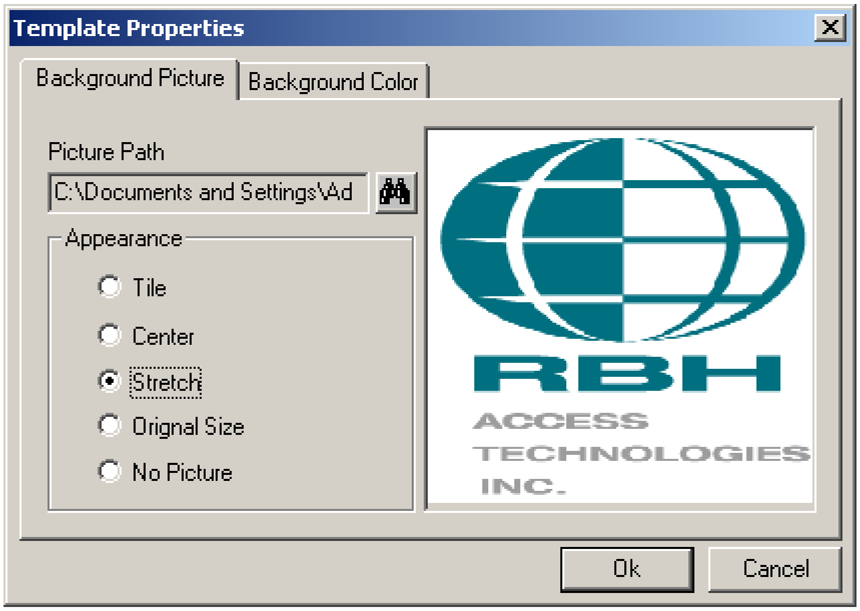
- Select the size and the orientation for the template.
- Right click on the card image to pop-up a menu where you can select *Properties* to choose a background picture or a background color for the card template.



Picture Path:

Appearance:
○ Tile
○ Center
○ Stretch
○ Orignal Size
● No Picture

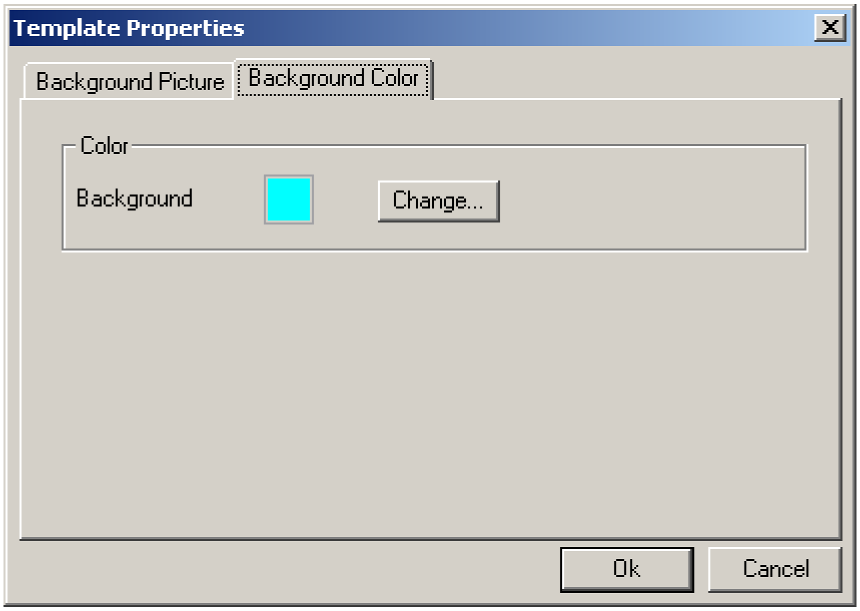
The *Background Picture* tab allows you to add a background picture to the card template. Use the *Find* button [🔍] to browse for a picture and set its appearance as *Tile*, *Center*, *Original Size*, or *Stretch*. *No Picture* is used to remove a previously chosen picture. This feature can be appropriately used to select the company logo, picture of the company building and such similar images as the background picture for the card template.



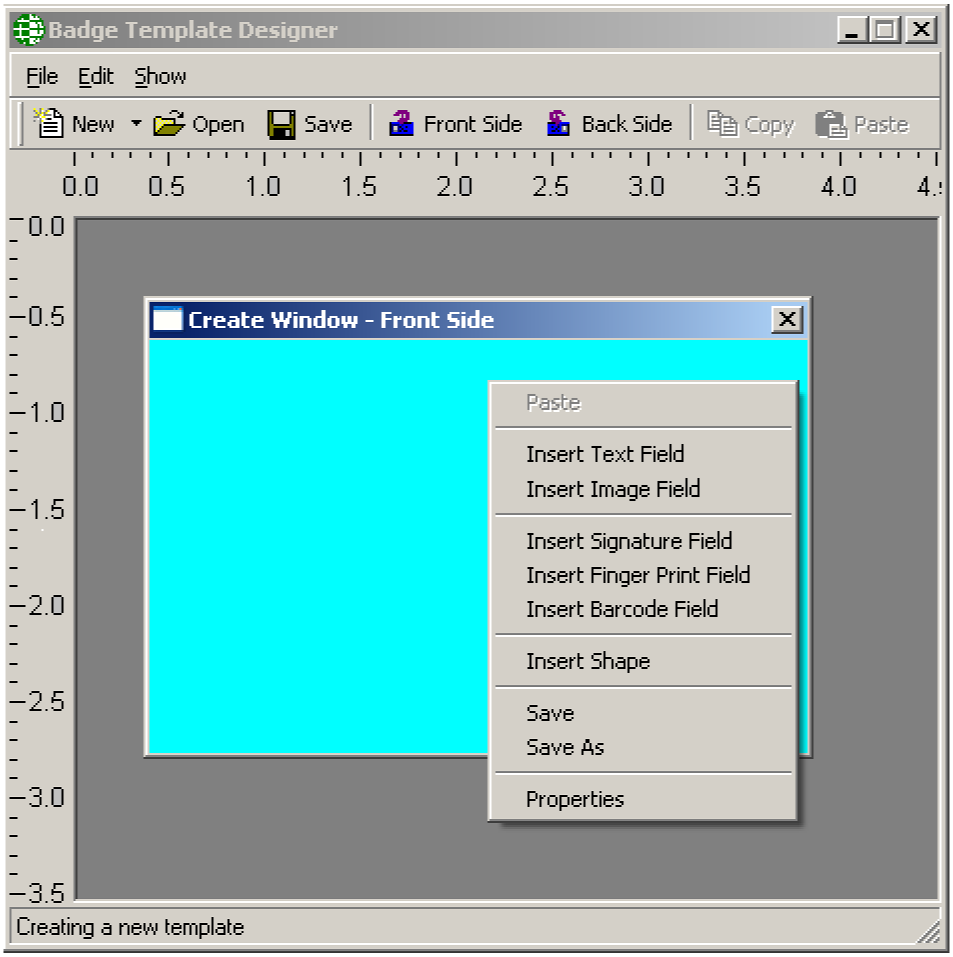
Picture Path: C:\Documents and Settings\Ad

Appearance:
○ Tile
○ Center
● Stretch
○ Orignal Size
○ No Picture

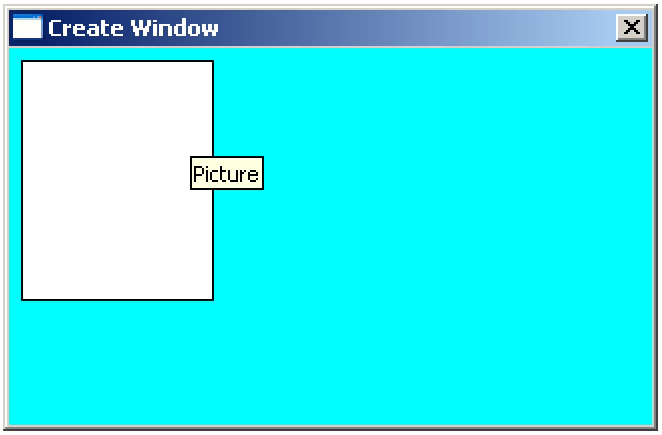
The *Background Color* tab will allow you to add a solid color to the background of your card. Choose a color by clicking on the *Change* button.



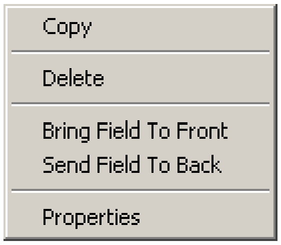
- After setting up the card's background, right click on the card template again to insert one of the fields available.



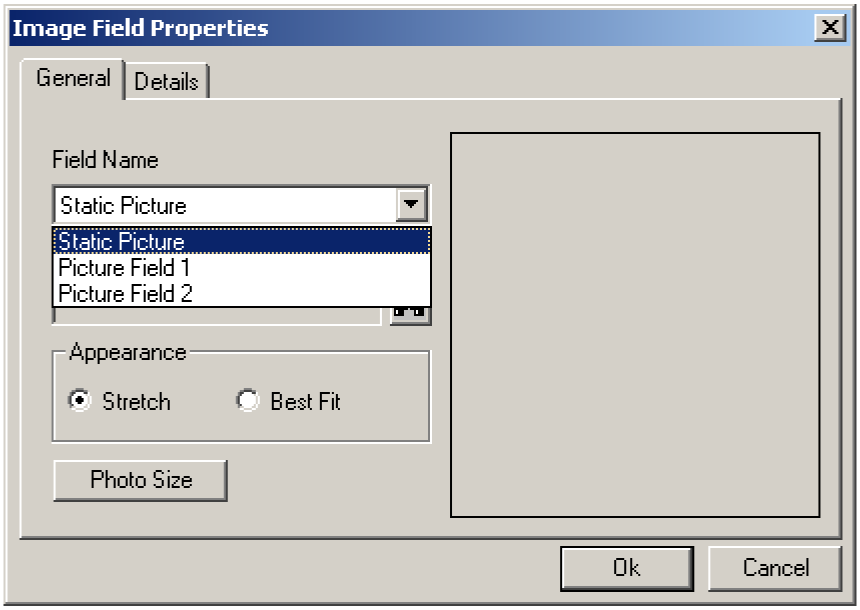
- Select *Insert Image Field* to insert a picture field in the card template.



- Right click on the *Picture* box and select *Properties*.



***You can arrange overlapping boxes on your card template with* Bring Field to Front *and* Send Field to Back.**

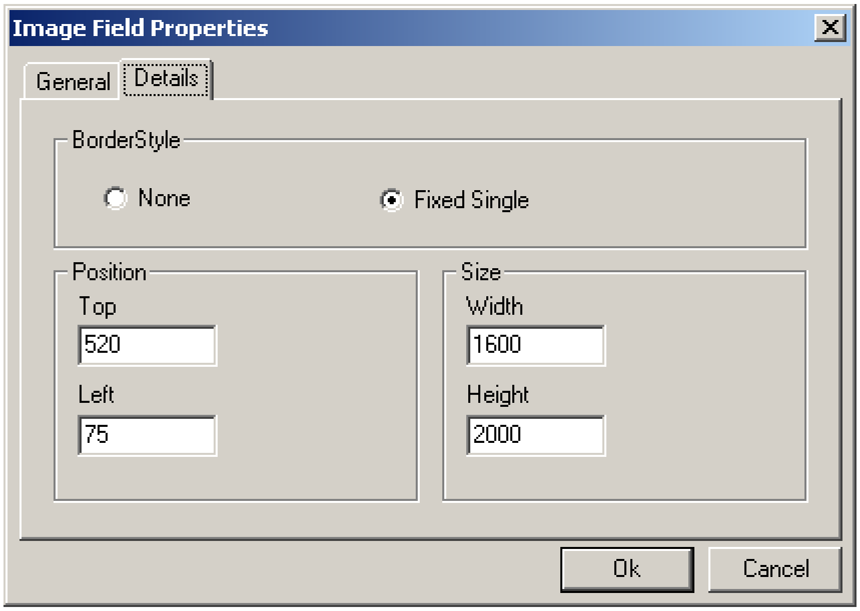


Field Name: Static Picture

Static Picture
Picture Field 1
Picture Field 2

Appearance: ● Stretch ○ Best Fit

A *Static Picture* is usually something like a company logo, (use the *Find* button [🔍] to browse for the required picture) while *Picture Field* will insert the cardholder's picture. *Best Fit* will display the picture in its actual size and S*tretch* will fill the available space completely with the picture. The default picture box size is 1440 by 1800 (that's a standard portrait ratio of 1:1¼). The *Photo Size* button changes the box size to 1600 by 2000.



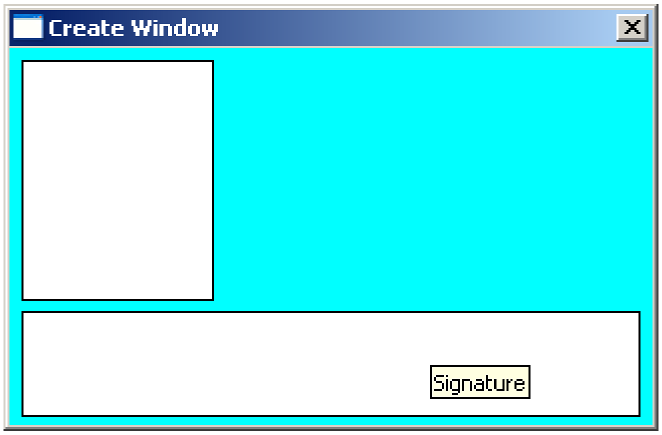
BorderStyle
○ None
● Fixed Single

Position
Top: 520
Left: 75

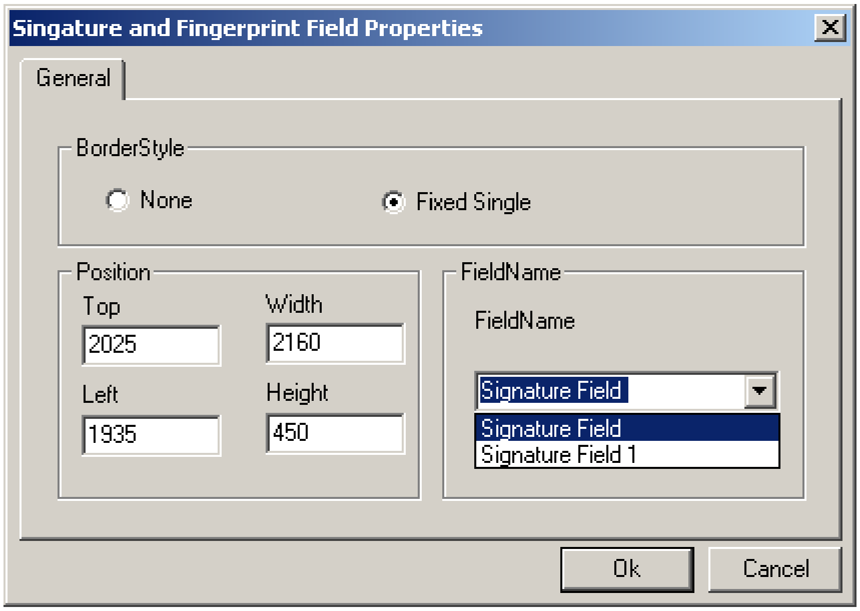
Size
Width: 1600
Height: 2000

Under the Details tab you can choose to have a border around the picture box. You can adjust the size and position of the box as well.

Next add a *Signature/fingerprint* box the same way you added the picture box.



Right click on the *Signature* box and set the properties for signature box as you did for the picture box. *Signature* and *Fingerprint* boxes only have one tab in their properties. You can set the size & position of signature/fingerprint box either by stretching and moving the box in the card template itself or by setting its position in the properties window.



Singature and Fingerprint Field Properties

General

BorderStyle

○ None ● Fixed Single

Position

Top: 2025

Width: 2160

Left: 1935

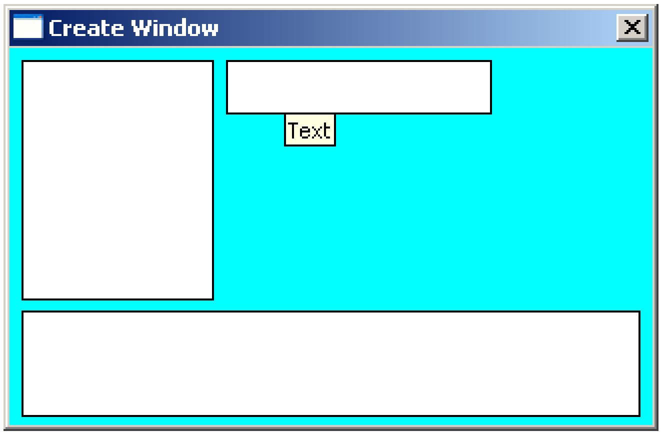
Height: 450

FieldName

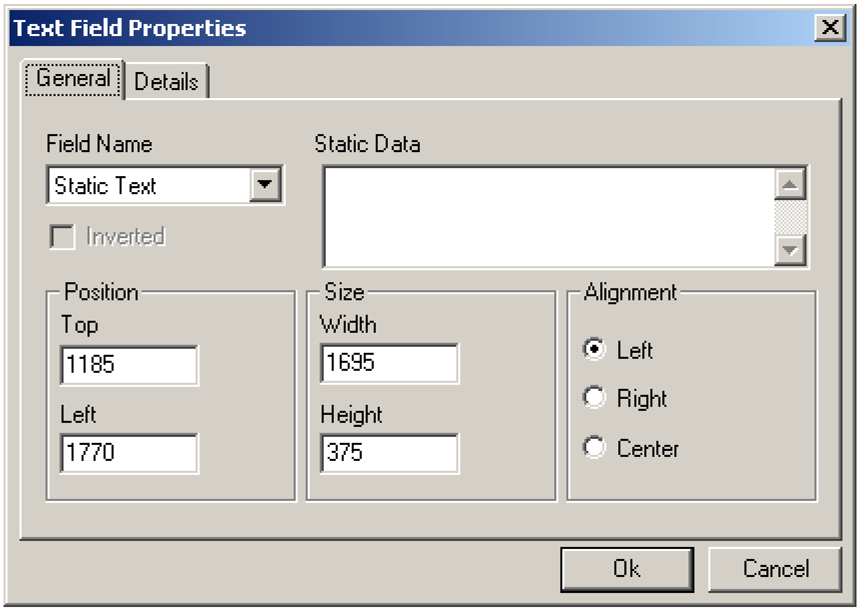
FieldName: Signature Field

- Signature Field
- Signature Field 1

Add *Text* boxes the same way that you've added the *Picture* and *Signature* boxes.



A *Text* box like *Picture* boxes can have fields inserted from the Cardholders Database, or it can have static (or fixed) text.



Field Name: Static Text

Static Data

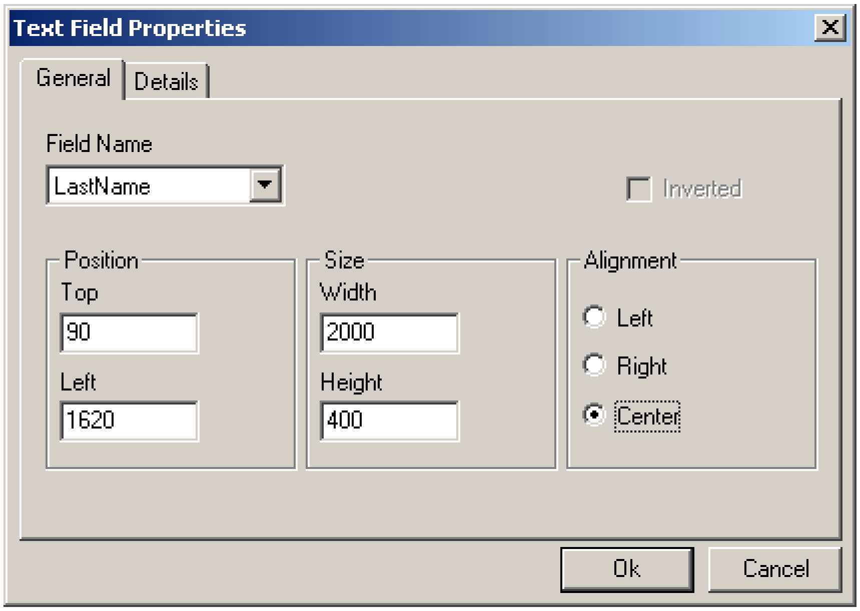
□ Inverted

Position
Top: 1185
Left: 1770

Size
Width: 1695
Height: 375

Alignment
● Left
○ Right
○ Center

Size and *Position* can be set exactly and *Alignment* can be configured.



Field Name: LastName

□ Inverted

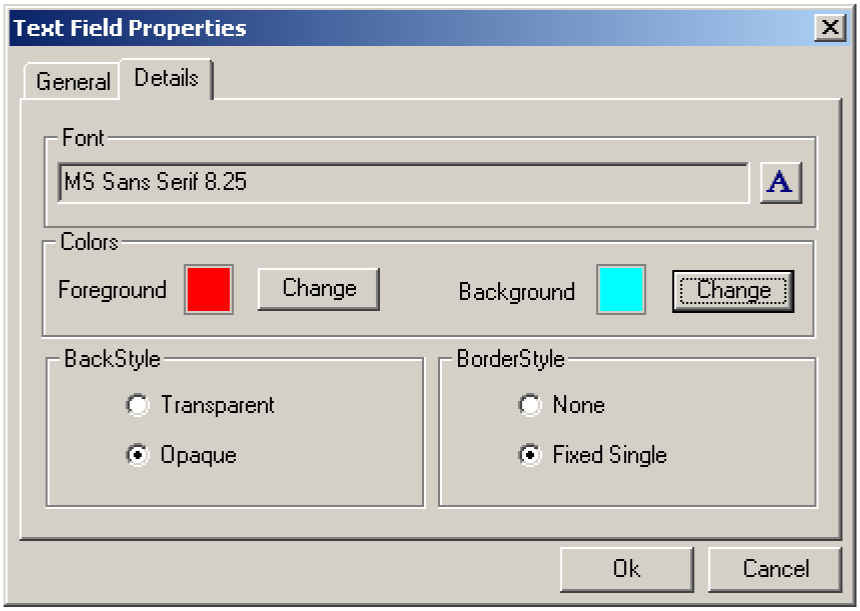
Position
Top: 90
Left: 1620

Size
Width: 2000
Height: 400

Alignment
○ Left
○ Right
● Center

Text Details tab is where the font for the text can be changed. *Foreground* color will change the color of the text itself, while *Background* color will change the background in the text box only. A pure white background will not be printed; therefore the card background will show around the text. To print a white background change the color to something that is close but not pure white.

If you have selected a background color for the card template, you would probably like to have the same color selected as the background for the text box.



Text Field Properties

General | Details

Font: MS Sans Serif 8.25

Colors: Foreground 🟥 Change — Background 🟦 Change

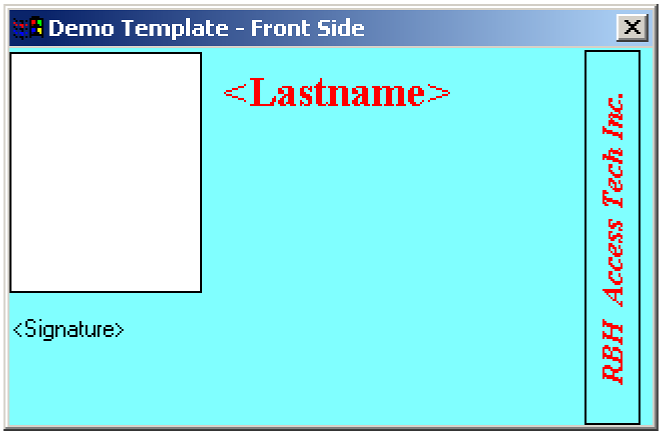
BackStyle: ○ Transparent ● Opaque

BorderStyle: ○ None ● Fixed Single

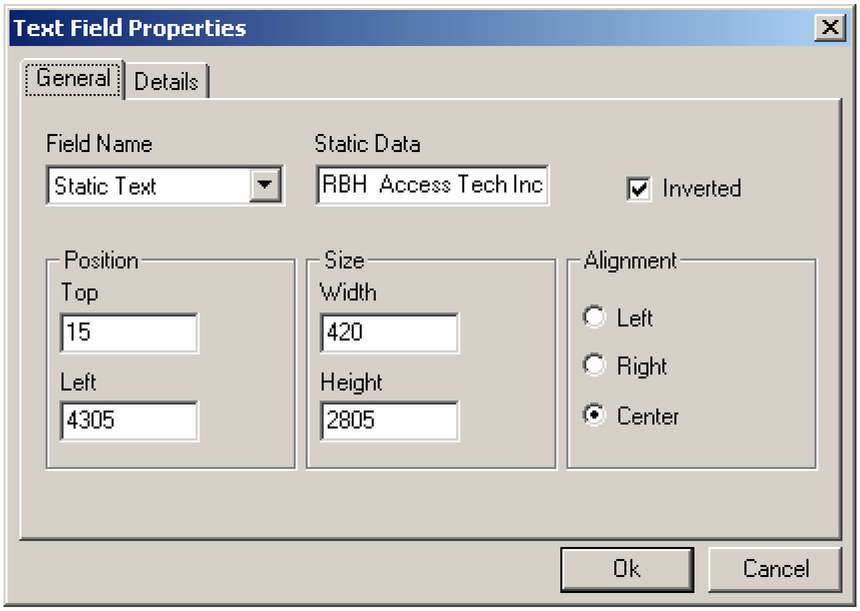
Ok | Cancel

RBH Badging Module also supports what is called *Vertical Text.*

In *Text* boxes that are taller than they are wide (and have a TrueType font selected) the text will be rotated 90º (or 270º if the *Inverted* box is checked).



☞ **Only TrueType fonts can be rotated.**



Text Field Properties

General | Details

Field Name: Static Text

Static Data: RBH Access Tech Inc

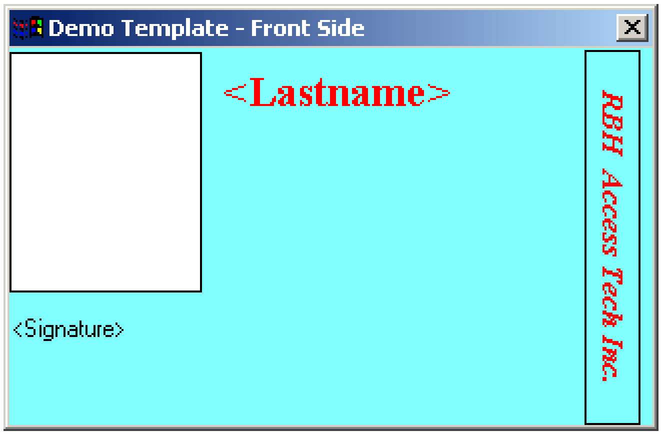
☑ Inverted

Position
Top: 15
Left: 4305

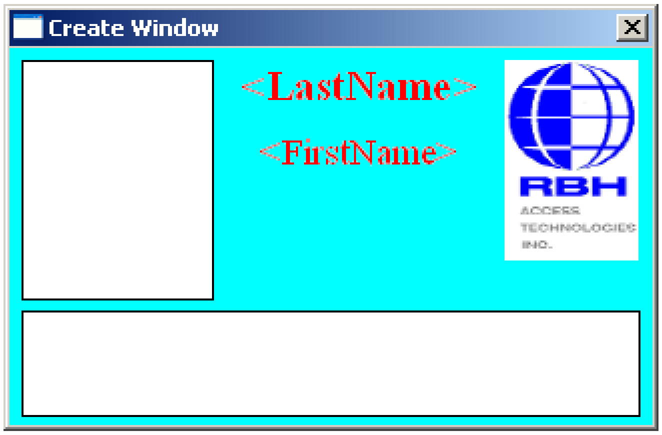
Size
Width: 420
Height: 2805

Alignment
○ Left
○ Right
● Center

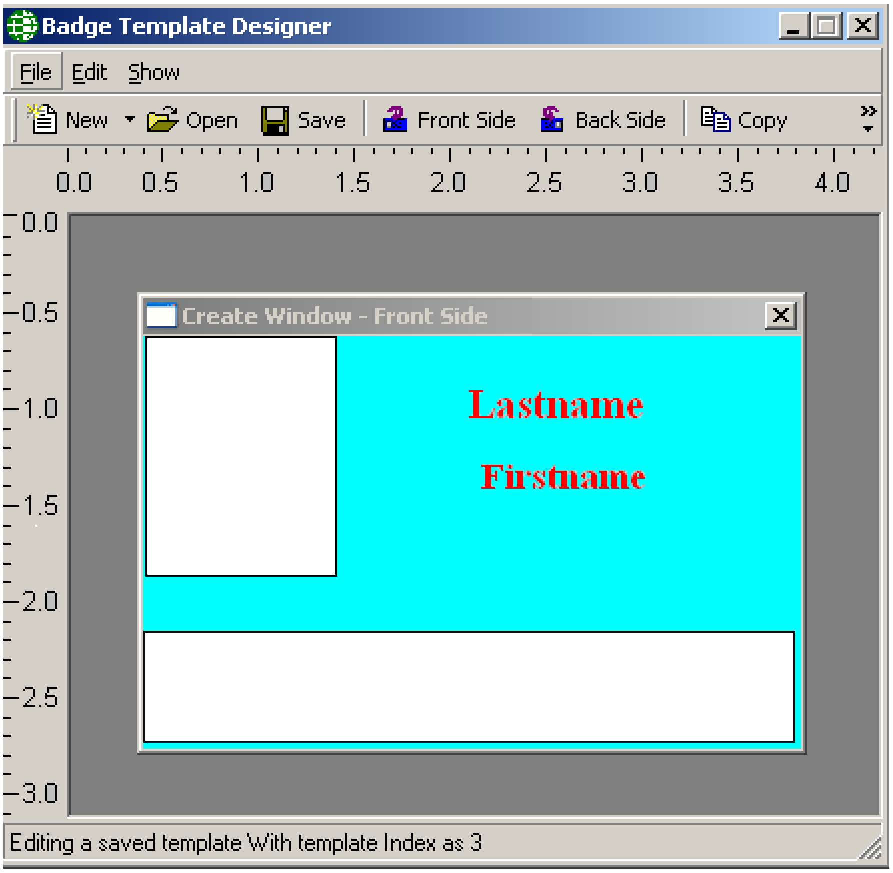
The same text can be rotated 270º if the *Inverted* Box is checked in the *Text Field Properties* Window.



☞ **The inverted Box is visible only if the text selected is vertical.**



When you are finished with the front of your card flip it over by clicking on the backside button in *Badge Template Designer* window and design the backside.

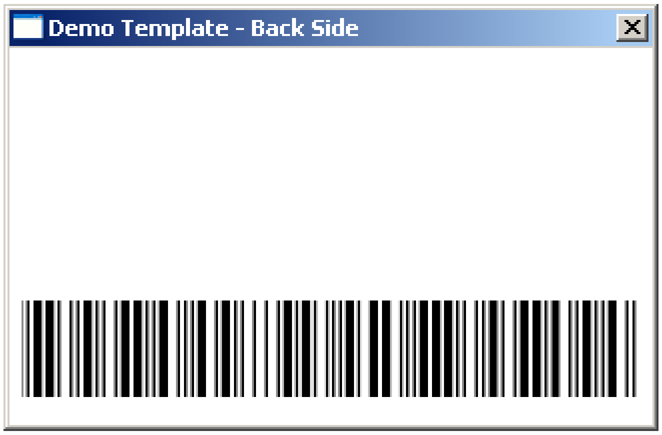


Editing a saved template With template Index as 3

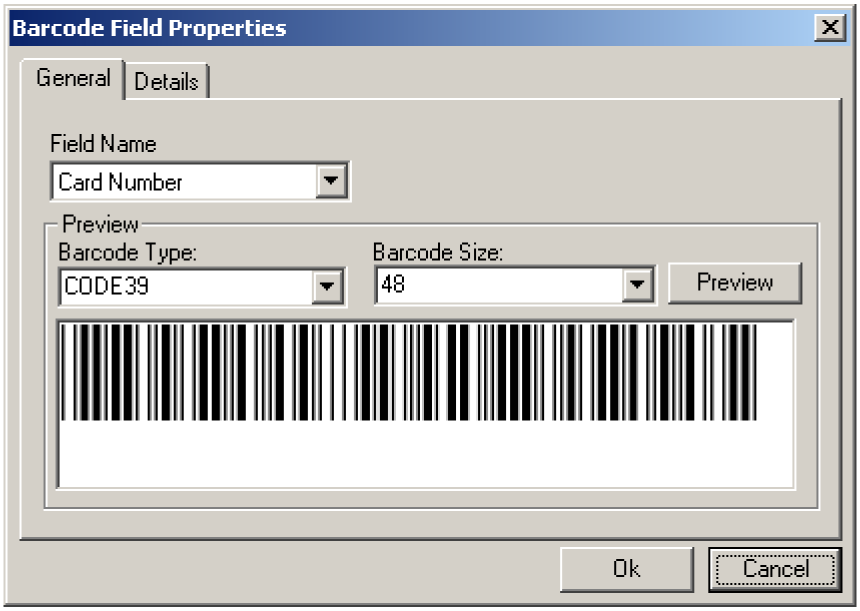
You will have to save your template before flipping to the backside of the template.

The same procedures apply to the back that applied to the front.

Add *Bar Code* field the same way that you've added the *Text*, *Picture* and *Signature* boxes



To add a barcode you will need to install the required *barcode fonts* (available in *Resources* folder on the CD). Select from the list under *Barcode Type* and choose a *Barcode Size*. Select under *Field Name* the source of the data for the barcode. You have the option to select *Static Text* or one of the Cardholder's fields, as the field for *Barcode,* same as in case of *Text Field*. *Preview* will show you how the barcode will appear.

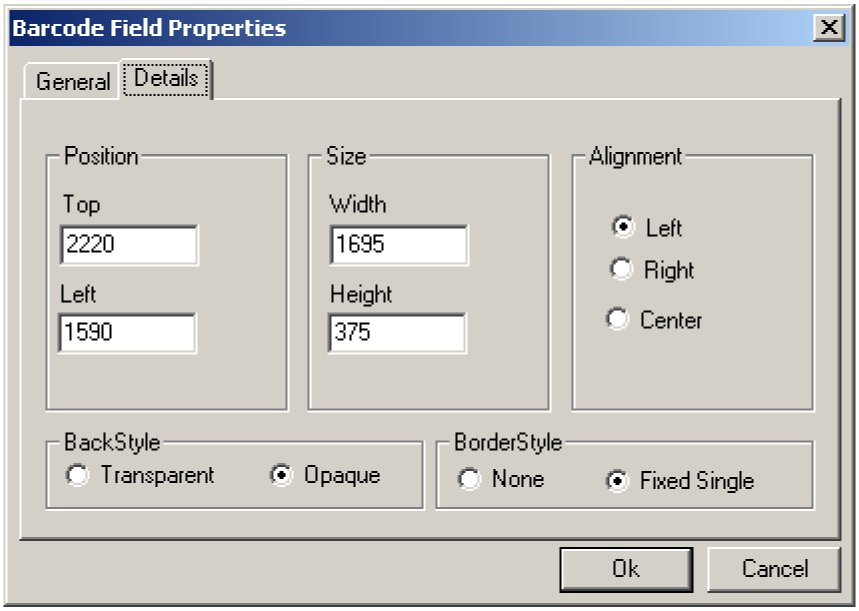


Field Name: Card Number

Barcode Type: CODE39

Barcode Size: 48

The *Details* tab allows you set the *Size*, *Position*, and *Alignment* for the Barcode box. Border or no border and the back style for the Barcode is also selected here.



Barcode Field Properties

Position
Top: 2220
Left: 1590

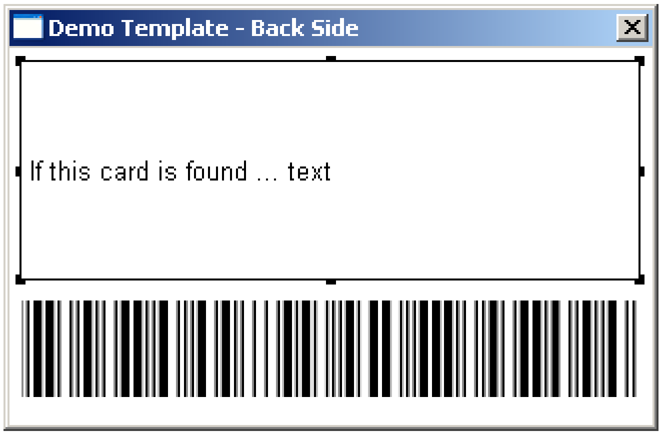
Size
Width: 1695
Height: 375

Alignment
● Left
○ Right
○ Center

BackStyle
○ Transparent ● Opaque

BorderStyle
○ None ● Fixed Single

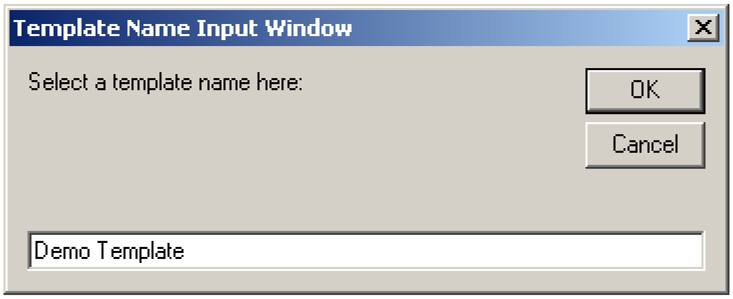
You can add extra text in a *Text* box one line at a time, or you could create a bitmap with multiple lines and add it as a picture.



Demo Template - Back Side

If this card is found ... text

When you have completed your design; save it. It can then be used with RBH database to display cardholders and print cards.



Template Name Input Window

Select a template name here:

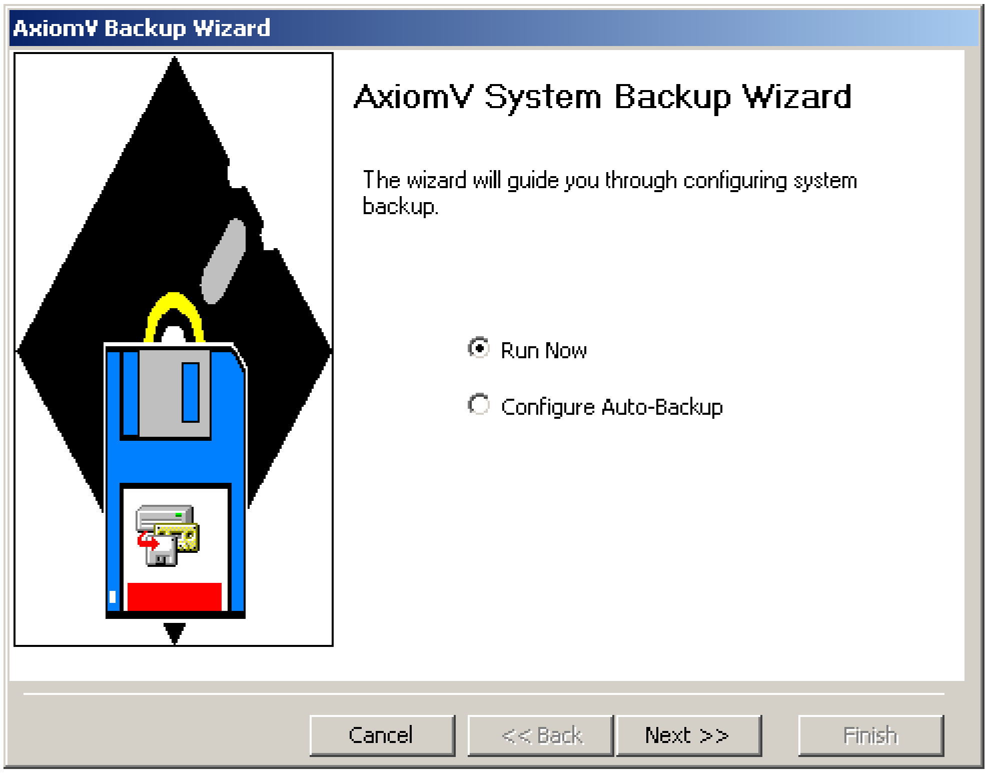
Demo Template

Saved templates can be viewed with the cardholder data under the *Photo* tab in the cardholder\visitor screen.

Backup…

Backup will open the AxiomV™ System Backup Wizard. Through the Backup Wizard the operator can either run a backup immediately or configure the backup to run automatically.

Run Now



AxiomV Backup Wizard

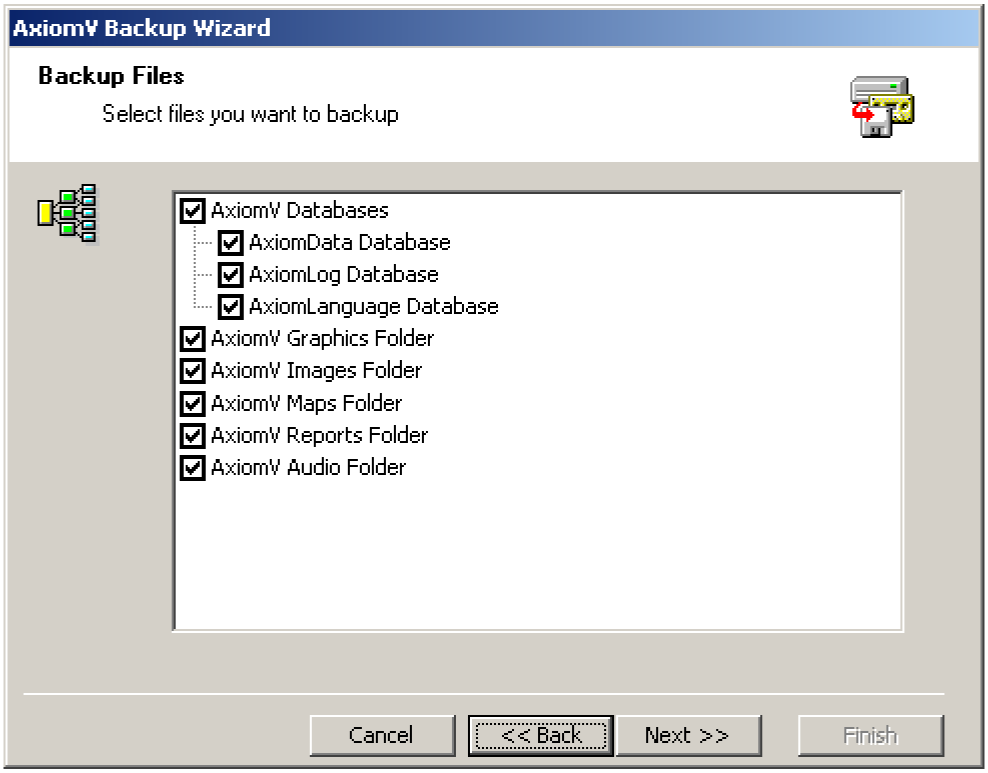
AxiomV System Backup Wizard

The wizard will guide you through configuring system backup.

● Run Now

○ Configure Auto-Backup

- ➢ To run the backup immediately, select '*Run Now*' and click *Next*.



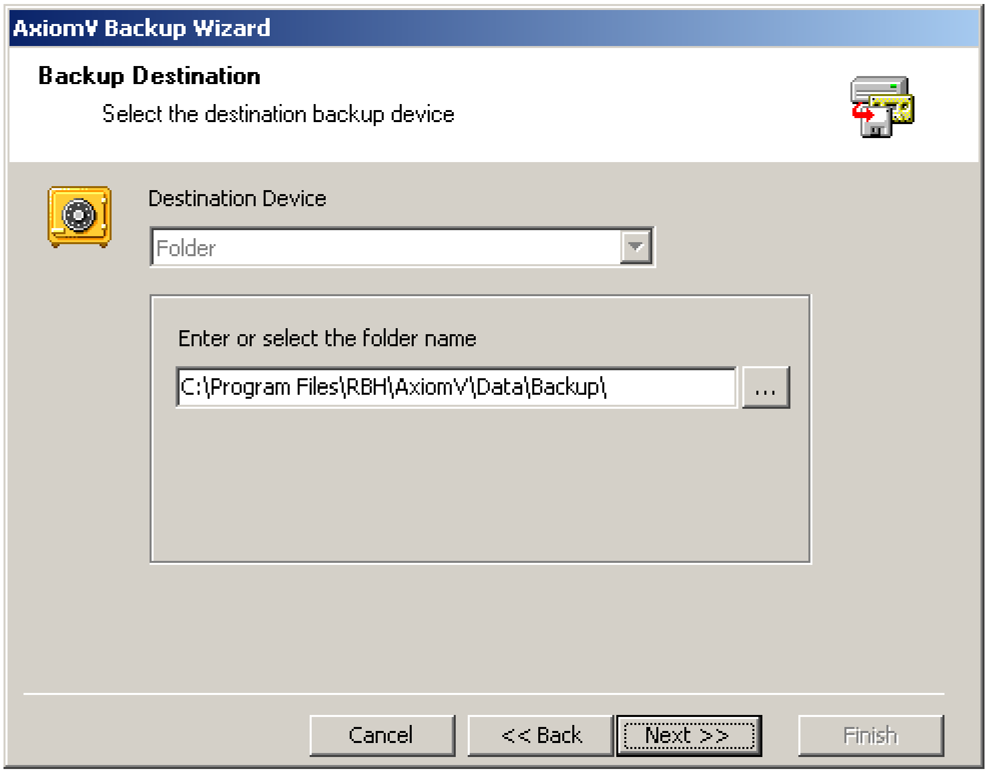
AxiomV Backup Wizard

Backup Files

Select files you want to backup

- ☑ AxiomV Databases
  - ☑ AxiomData Database
  - ☑ AxiomLog Database
  - ☑ AxiomLanguage Database
- ☑ AxiomV Graphics Folder
- ☑ AxiomV Images Folder
- ☑ AxiomV Maps Folder
- ☑ AxiomV Reports Folder
- ☑ AxiomV Audio Folder

1. Select the items to be backed up by clicking in the box to check or uncheck the selection.



AxiomV Backup Wizard

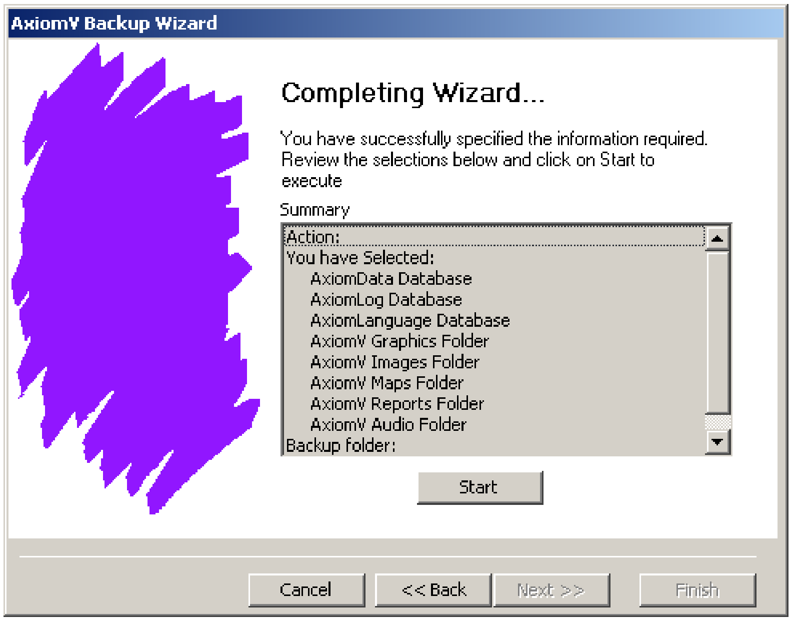
Backup Destination

Select the destination backup device

Destination Device: Folder

Enter or select the folder name: C:\Program Files\RBH\AxiomV\Data\Backup\

2. Enter or select the folder the backup files will be sent to.



Completing Wizard...

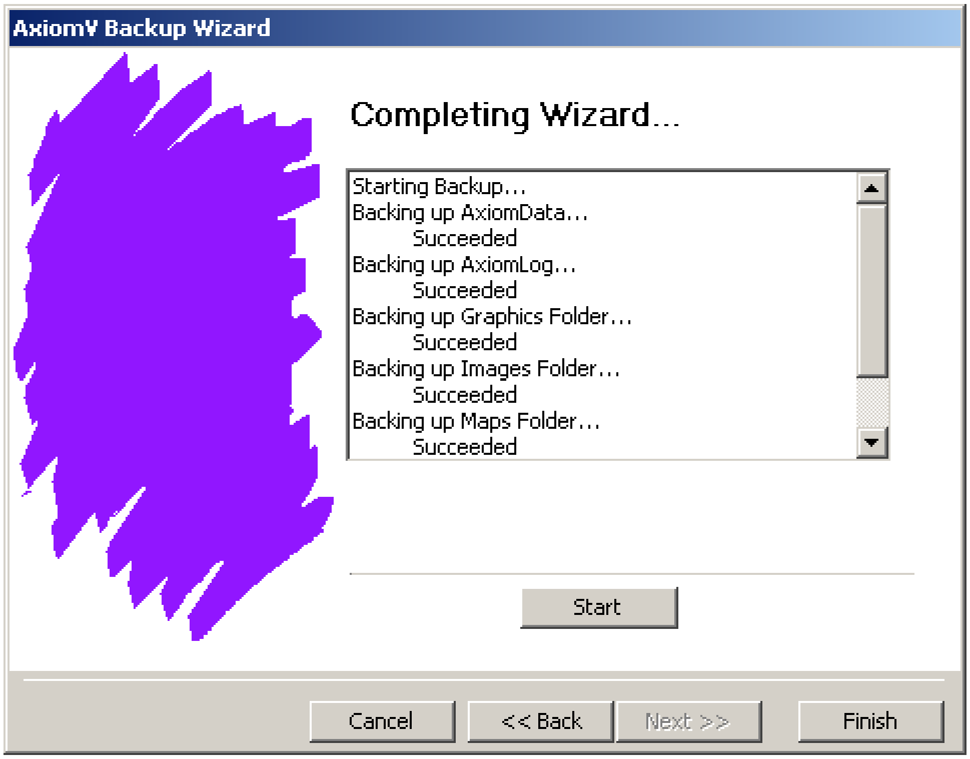
You have successfully specified the information required. Review the selections below and click on Start to execute

Summary

```
Action:
You have Selected:
    AxiomData Database
    AxiomLog Database
    AxiomLanguage Database
    AxiomV Graphics Folder
    AxiomV Images Folder
    AxiomV Maps Folder
    AxiomV Reports Folder
    AxiomV Audio Folder
Backup folder:
```

3. Verify your backup parameters by reviewing the summary, then click *Start* to execute the backup.

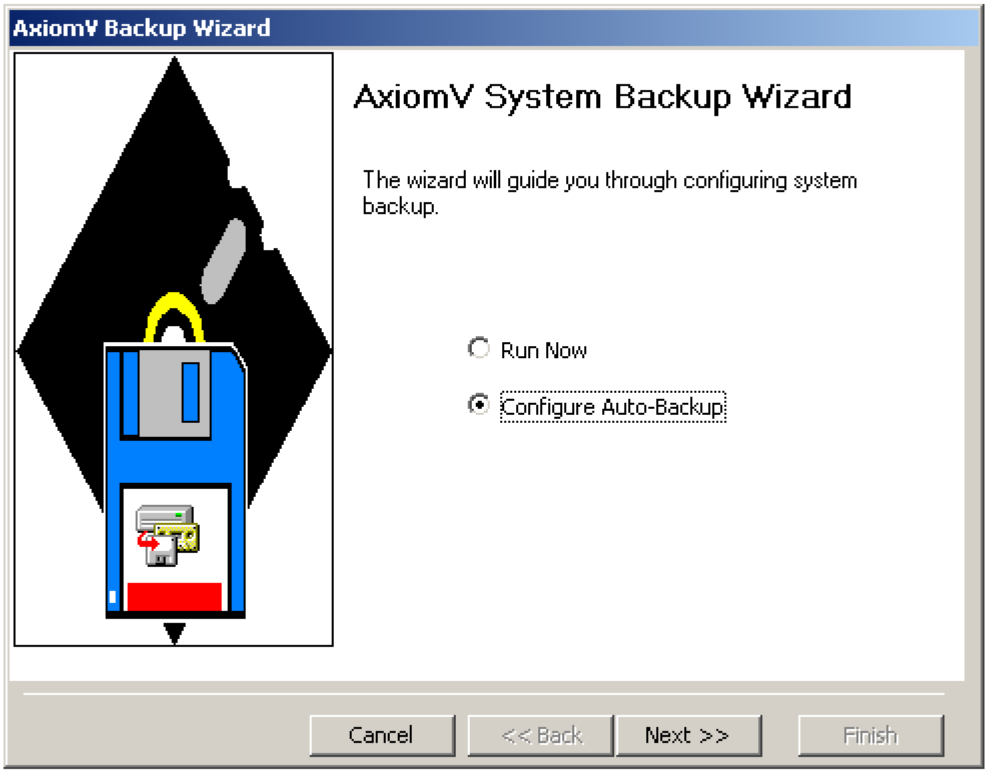
   A progress bar will appear and each file will be listed as it is backed up. You can click *Stop* during the procedure to cancel the backup. Click *Finish* to exit.



Completing Wizard...

```
Starting Backup...
Backing up AxiomData...
        Succeeded
Backing up AxiomLog...
        Succeeded
Backing up Graphics Folder...
        Succeeded
Backing up Images Folder...
        Succeeded
Backing up Maps Folder...
        Succeeded
```

Auto Backup



AxiomV Backup Wizard

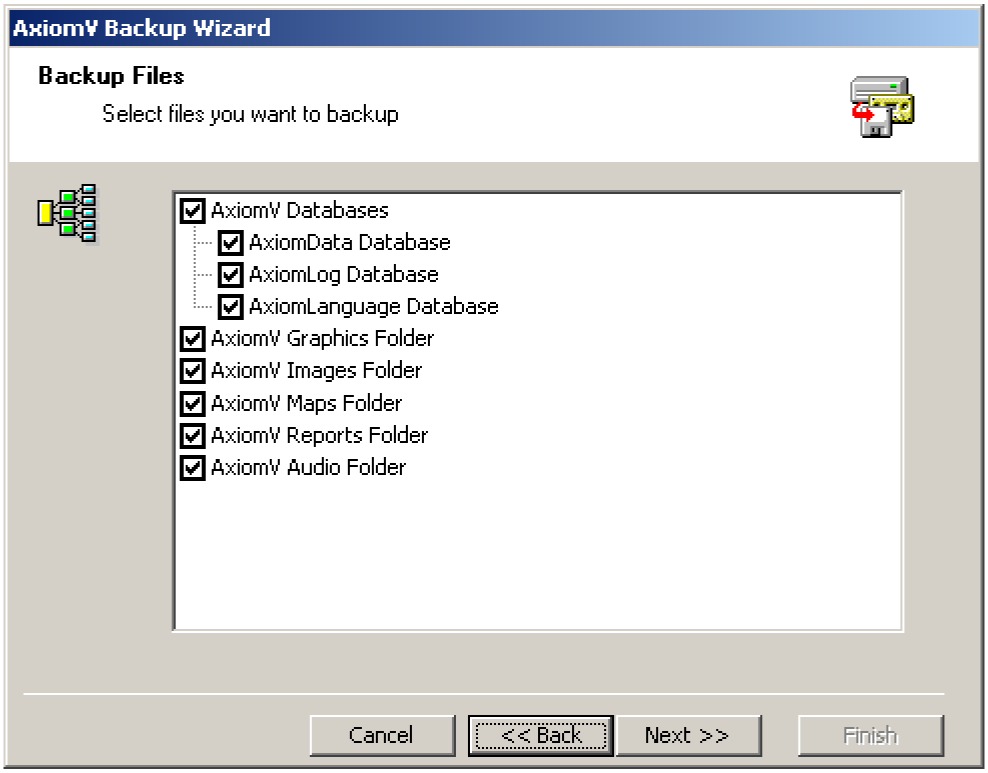
AxiomV System Backup Wizard

The wizard will guide you through configuring system backup.

○ Run Now

● Configure Auto-Backup

- Click on *Configure Auto-Backup* to set the parameters for a scheduled backup.



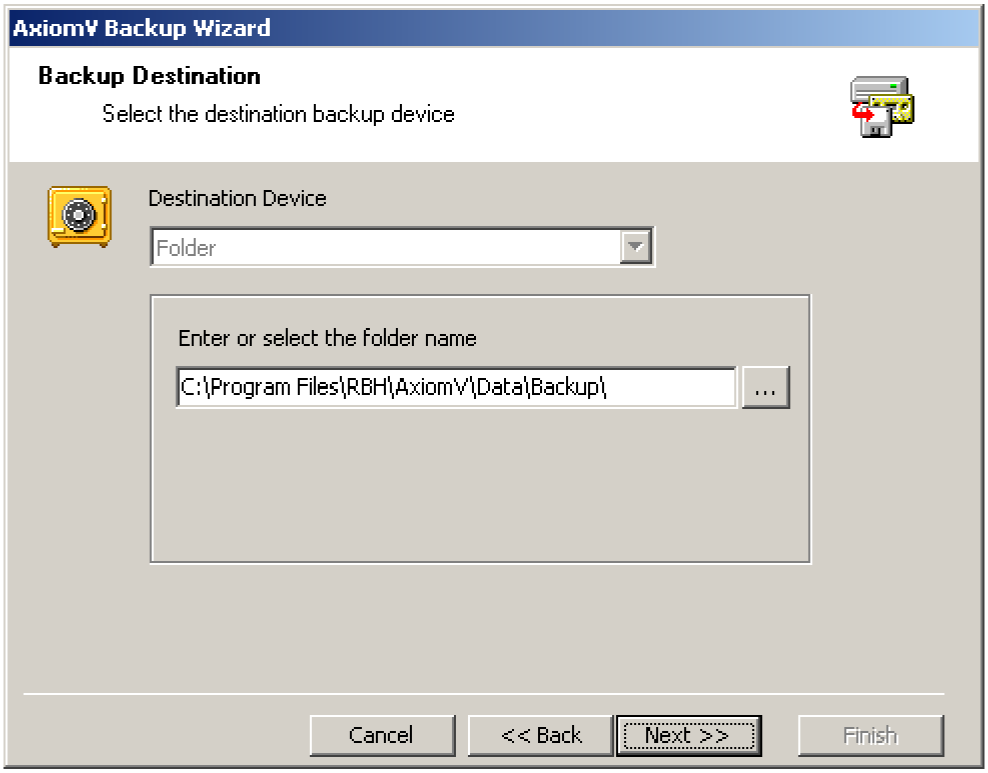
AxiomV Backup Wizard

Backup Files

Select files you want to backup

☑ AxiomV Databases
  ☑ AxiomData Database
  ☑ AxiomLog Database
  ☑ AxiomLanguage Database
☑ AxiomV Graphics Folder
☑ AxiomV Images Folder
☑ AxiomV Maps Folder
☑ AxiomV Reports Folder
☑ AxiomV Audio Folder

1. Select the items to be backed up by clicking in the box to check or uncheck the selection.



AxiomV Backup Wizard

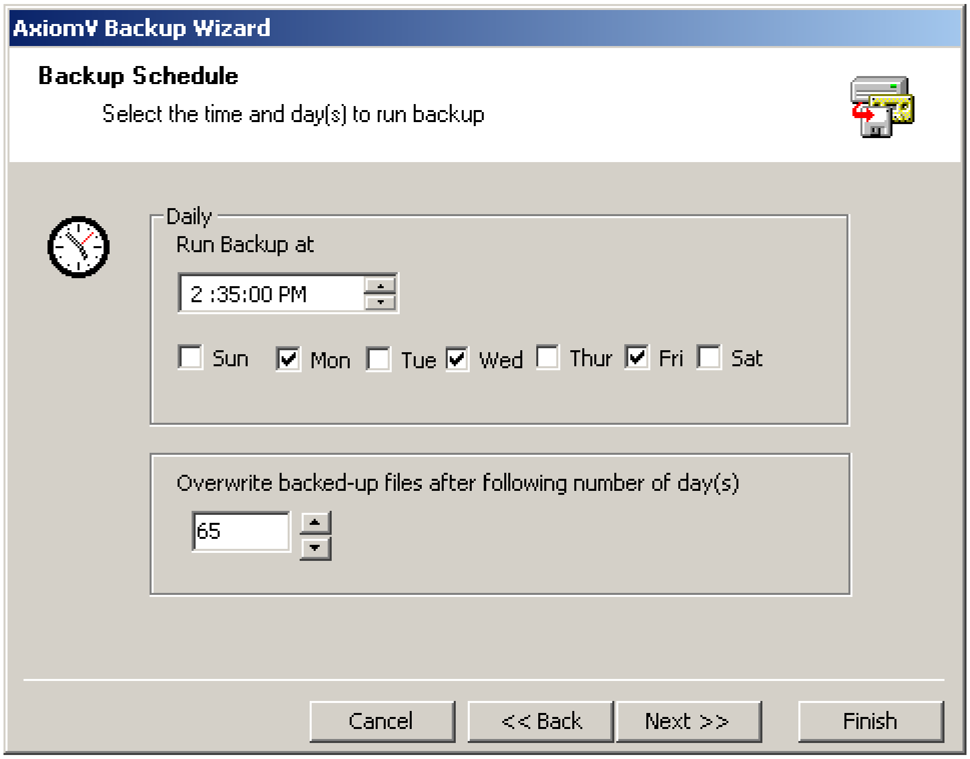
Backup Destination

Select the destination backup device

Destination Device: Folder

Enter or select the folder name: C:\Program Files\RBH\AxiomV\Data\Backup\

2. Enter or select the folder the backup files will be sent to.



AxiomV Backup Wizard

Backup Schedule

Select the time and day(s) to run backup

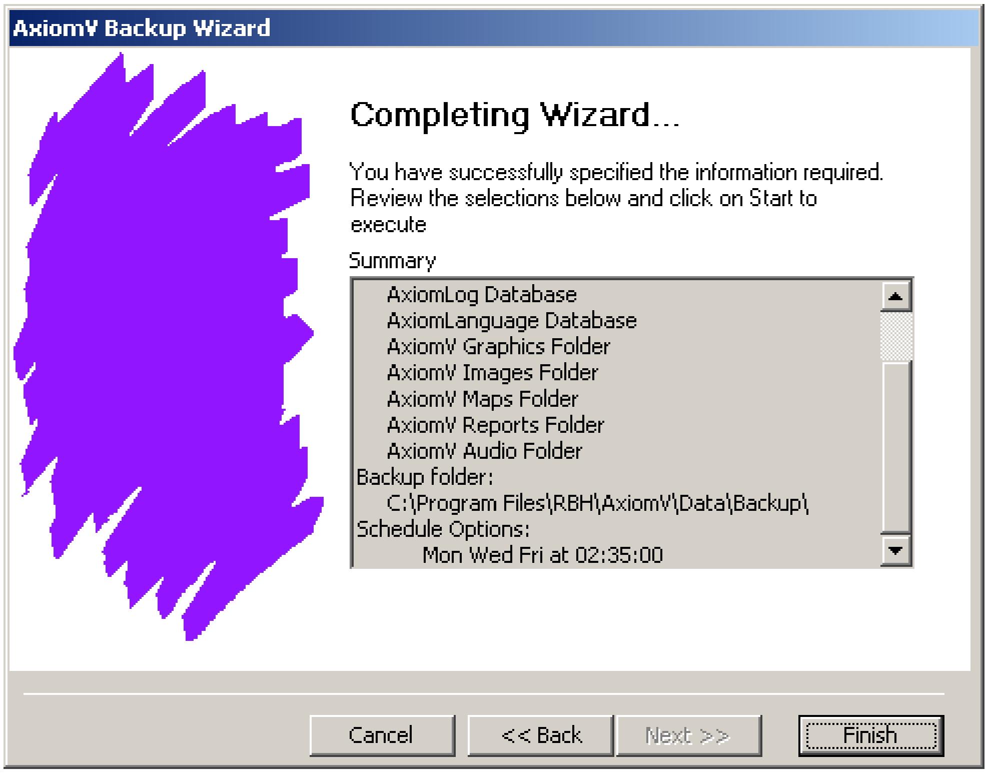
Daily

Run Backup at: 2 :35:00 PM

□ Sun ☑ Mon □ Tue ☑ Wed □ Thur ☑ Fri □ Sat

Overwrite backed-up files after following number of day(s): 65

3. Choose the time of day and the days of the week the backup is to be executed. Also select number of days old backup files are to be kept before overwriting them.



Completing Wizard...

You have successfully specified the information required.
Review the selections below and click on Start to execute

Summary

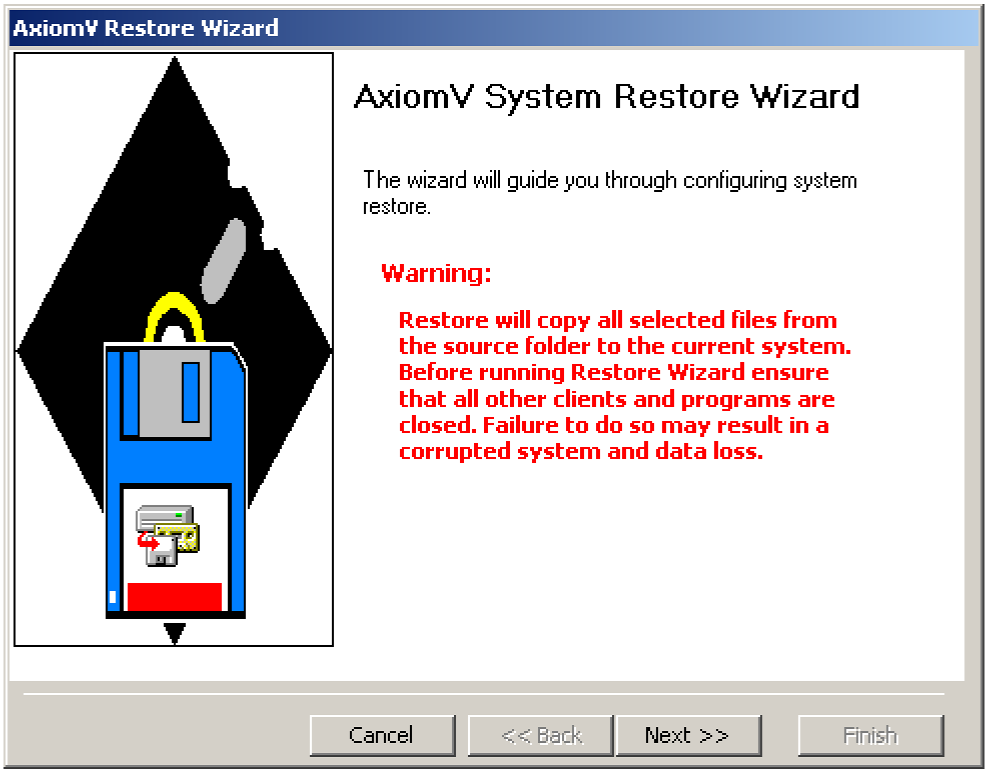
```
    AxiomLog Database
    AxiomLanguage Database
    AxiomV Graphics Folder
    AxiomV Images Folder
    AxiomV Maps Folder
    AxiomV Reports Folder
    AxiomV Audio Folder
Backup folder:
    C:\Program Files\RBH\AxiomV\Data\Backup\
Schedule Options:
        Mon Wed Fri at 02:35:00
```

4. Verify your parameter choices and select *Finish* to complete the setup.

Archived Log databases cannot be backed up through above Backup Module. To backup those databases, user needs to copy both.mdf and .ldf files of archived log databases (AxiomLog1, 2, 3---- and so on). For better understanding of Archived log databases, call RBH Technical Support)

Restore

Restore will open the *AxiomV™ System Restore Wizard*. Through the *Restore Wizard* the operator can run a restore to replace existing data with previously backed up data.


AxiomV Restore Wizard

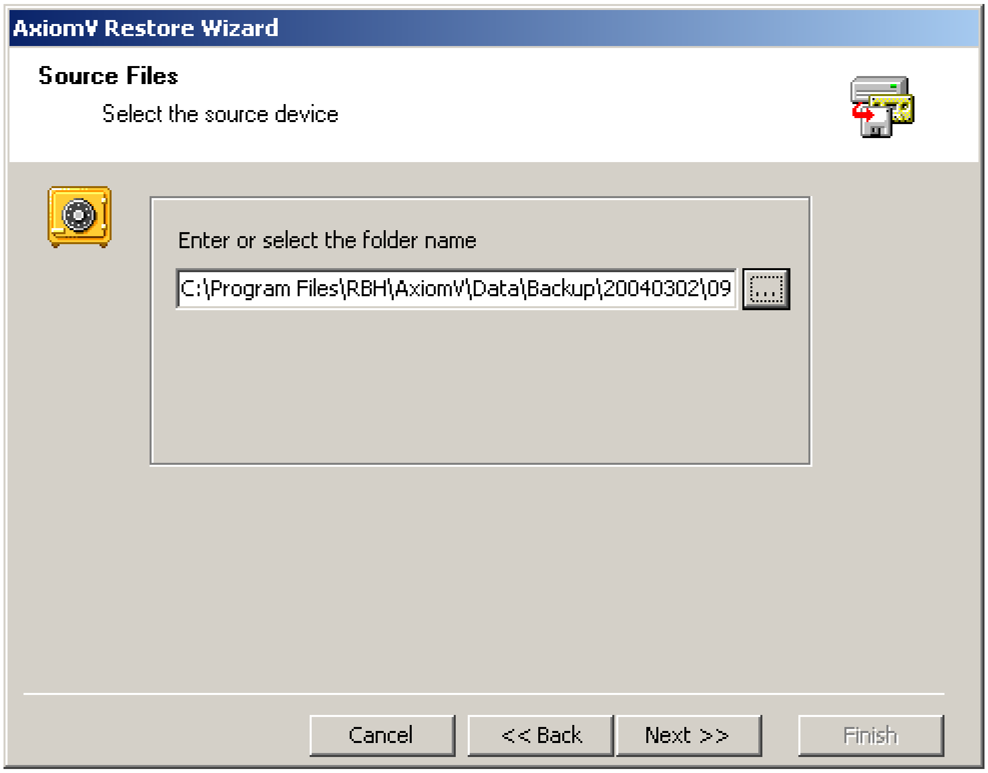
AxiomV System Restore Wizard

The wizard will guide you through configuring system restore.

Warning:

Restore will copy all selected files from the source folder to the current system. Before running Restore Wizard ensure that all other clients and programs are closed. Failure to do so may result in a corrupted system and data loss.

- ➢ Click on *Next* to set the parameters and continue with the *Restore*



AxiomV Restore Wizard

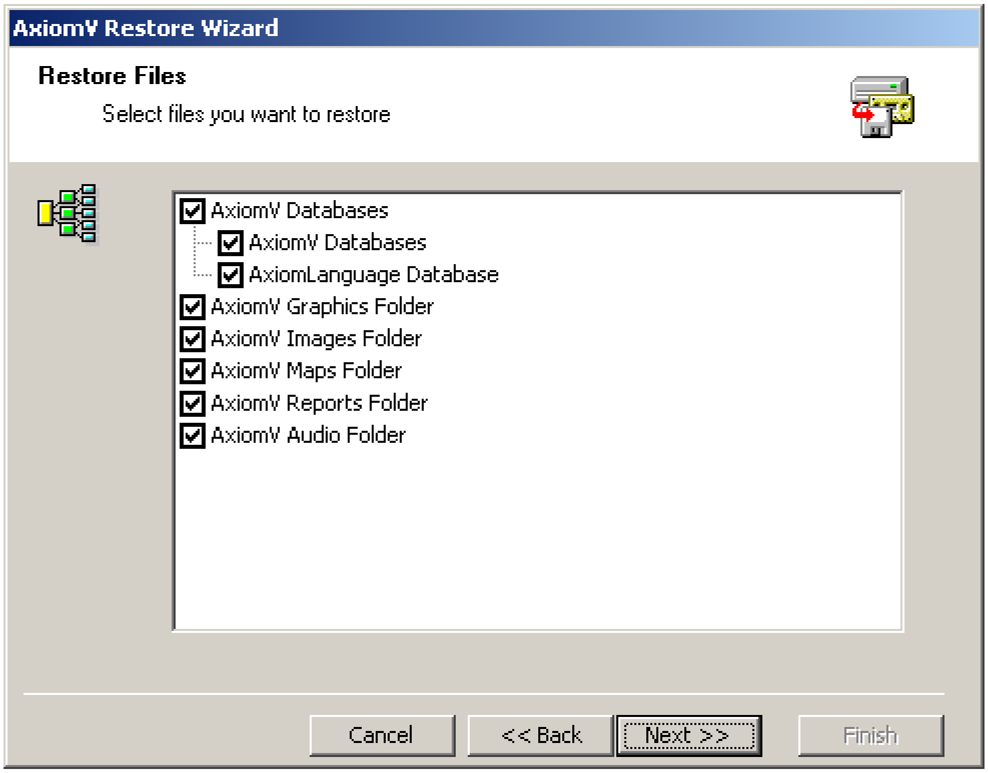
Source Files

Select the source device

Enter or select the folder name

C:\Program Files\RBH\AxiomV\Data\Backup\20040302\09

1. Enter or select the folder from which the backup is to retrieve the files from.



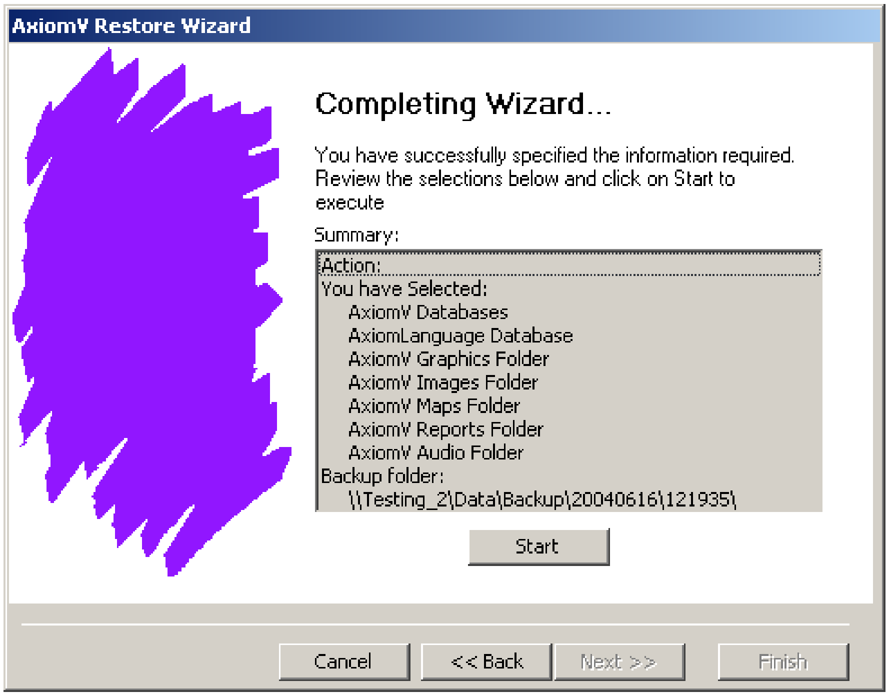
AxiomV Restore Wizard

Restore Files

Select files you want to restore

- ☑ AxiomV Databases
  - ☑ AxiomV Databases
  - ☑ AxiomLanguage Database
- ☑ AxiomV Graphics Folder
- ☑ AxiomV Images Folder
- ☑ AxiomV Maps Folder
- ☑ AxiomV Reports Folder
- ☑ AxiomV Audio Folder

2. Select the items to be restored up by clicking in the box to check or uncheck the selection.



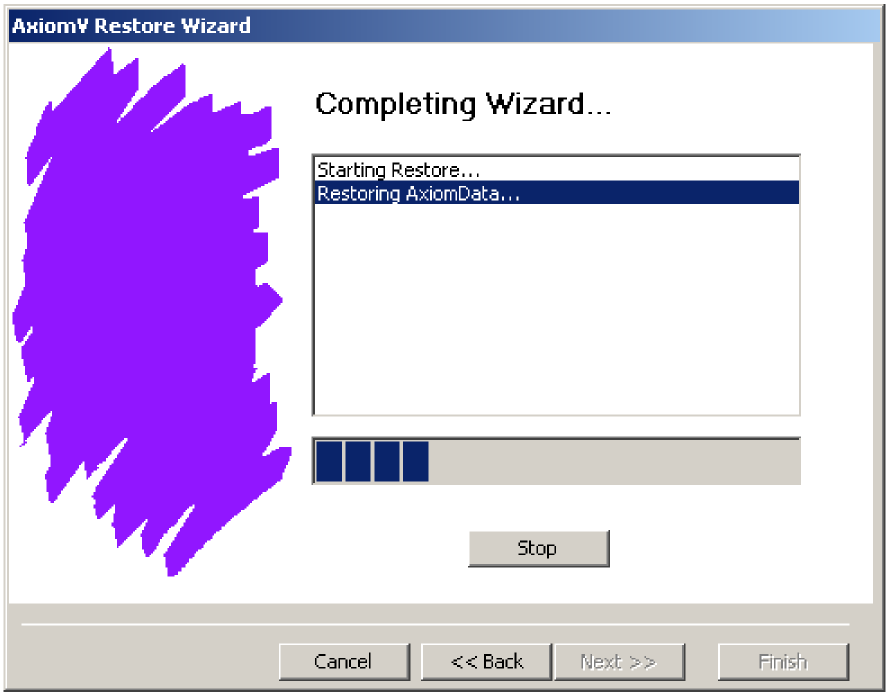
Completing Wizard...

You have successfully specified the information required. Review the selections below and click on Start to execute

Summary:

```
Action:
You have Selected:
    AxiomV Databases
    AxiomLanguage Database
    AxiomV Graphics Folder
    AxiomV Images Folder
    AxiomV Maps Folder
    AxiomV Reports Folder
    AxiomV Audio Folder
Backup folder:
    \\Testing_2\Data\Backup\20040616\121935\
```

3. Click *Start* to execute the restore. Restored files will be listed as they are restored. Clicking *Finish* will exit the *Restore Wizard*.

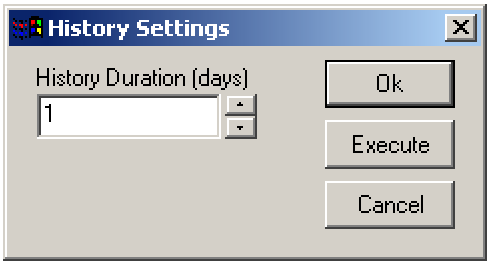


Completing Wizard...

```
Starting Restore...
Restoring AxiomData...
```

AxiomLog and Archived Log databases cannot be restored through above *Restore* Module. To restore these databases, call RBH Technical Support.

History Settings



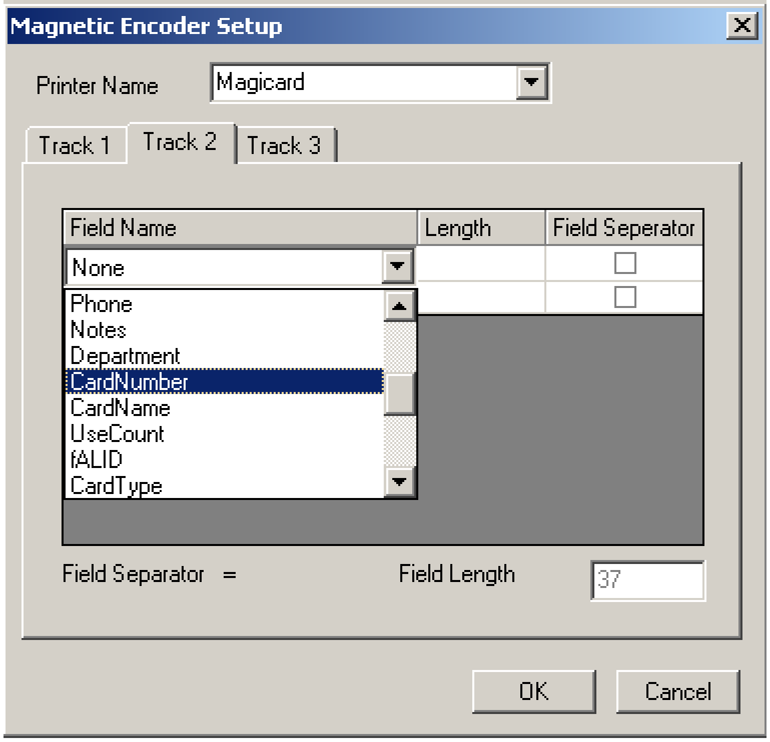
History Duration (days) is used to set the number of days of history that are to be kept. Any records beyond this duration are deleted. Clicking *OK* will accept any changes made and exit the window. The change will take effect during the next *History Purge*. If *Execute* is clicked then the change is applied immediately. Reducing the number could mean the deletion of some files. *Cancel* will exit the window without saving any changes that were made.

Reset Toolbar

Reset Toolbar will return the Toolbar to its default settings. These settings though will be subject to the current user's *Operator Profile*. Selecting that part of the Toolbar's default setting will not be shown if the current user does not have access to these items.

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 the System tab in *File* - *System Settings*.



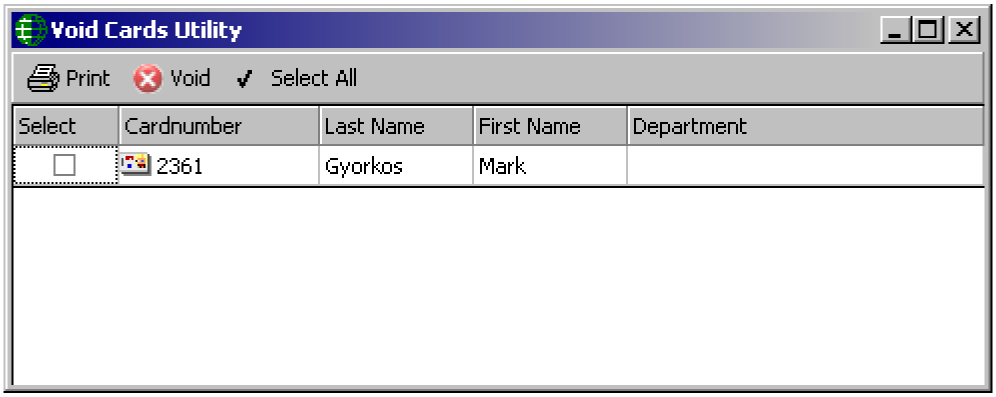
Magnetic Encoder Setup

Printer Name: Magicard

Field Name	Length	Field Seperator
None		☐
		☐

Field Separator =

Field Length: 37



Void Cards Utility

Select	Cardnumber	Last Name	First Name	Department
☐	2361	Gyorkos	Mark	

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

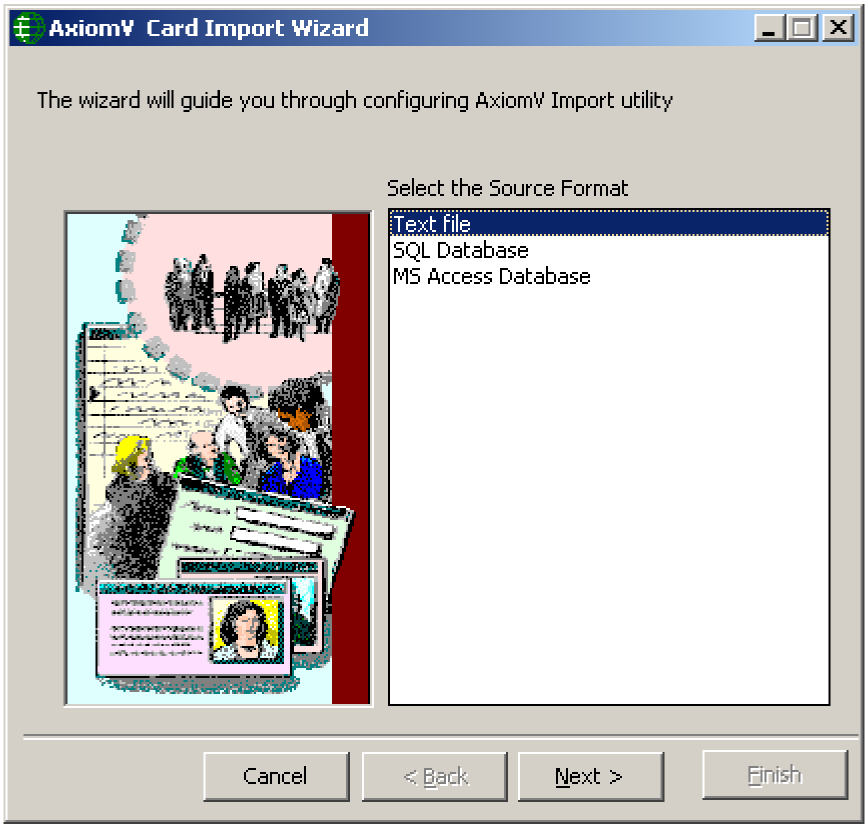
Void will immediately deactivate all selected cards.

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

Import

Selecting *Import* will start the Card Import utility.

- **AxiomV™ Card Import Wizard** is used to import cardholder information from other sources into AxiomV™.



AxiomV Card Import Wizard

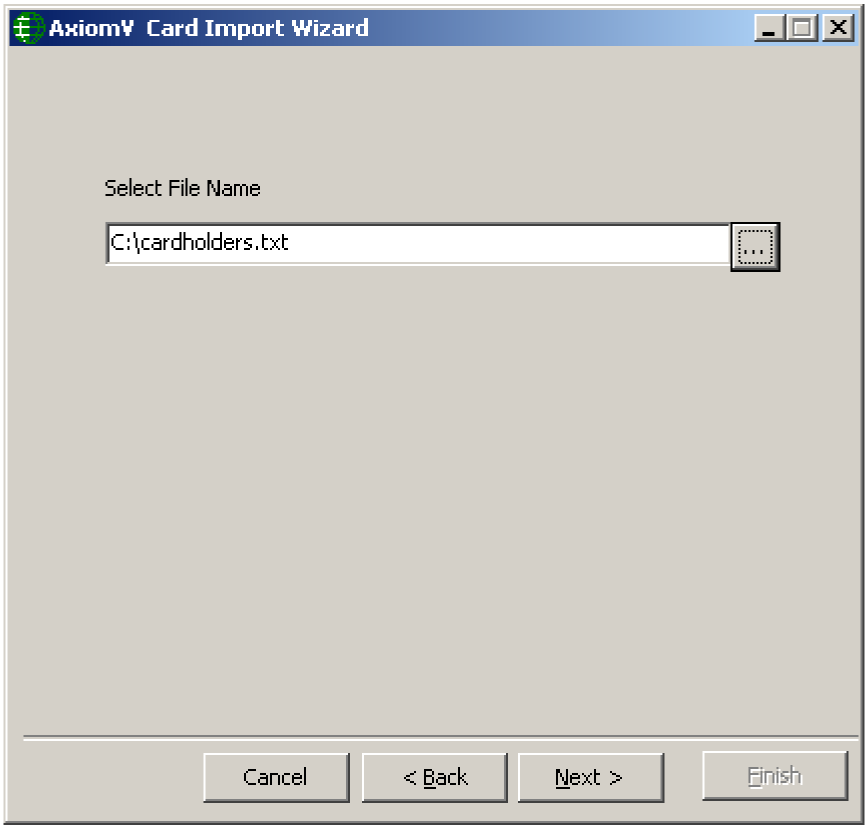
The wizard will guide you through configuring AxiomV Import utility

Select the Source Format

Text file
SQL Database
MS Access Database

- Select one of the three available *Source Formats* of the file to be imported (the file with the cardholder data) and then click the *Next* button.

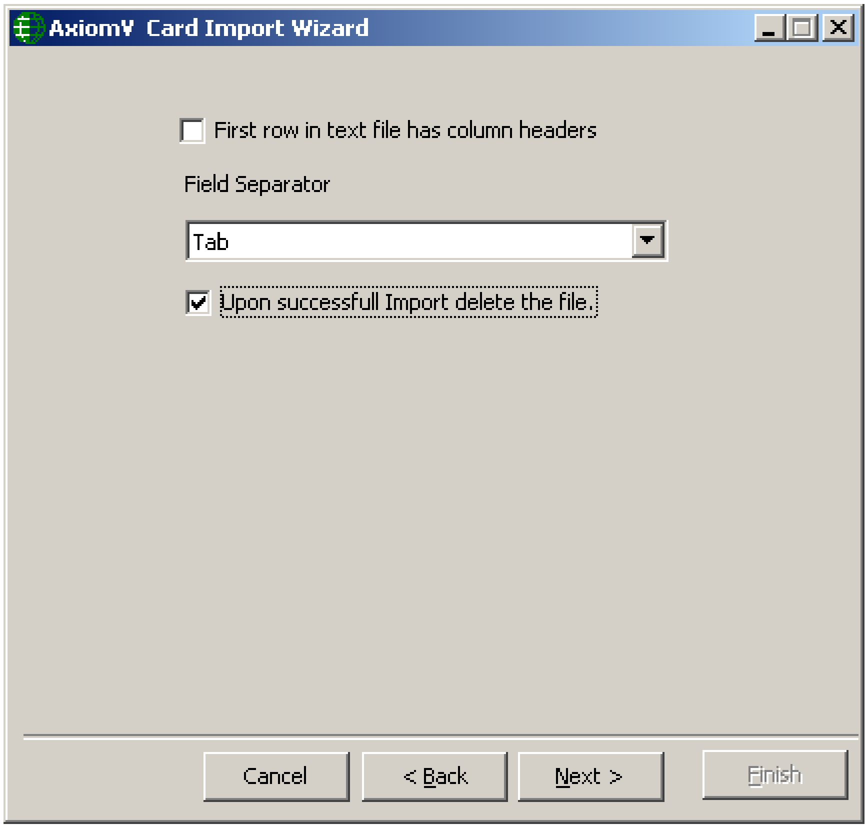
Text Format



Select File Name

C:\cardholders.txt

- If you selected *Text File* as the *Source Format*, select the file to be imported from and click the *Next* button. You can use the Browse/Ellipsis button (…) to search for the path to the required file.



AxiomV Card Import Wizard

☐ First row in text file has column headers

Field Separator: Tab

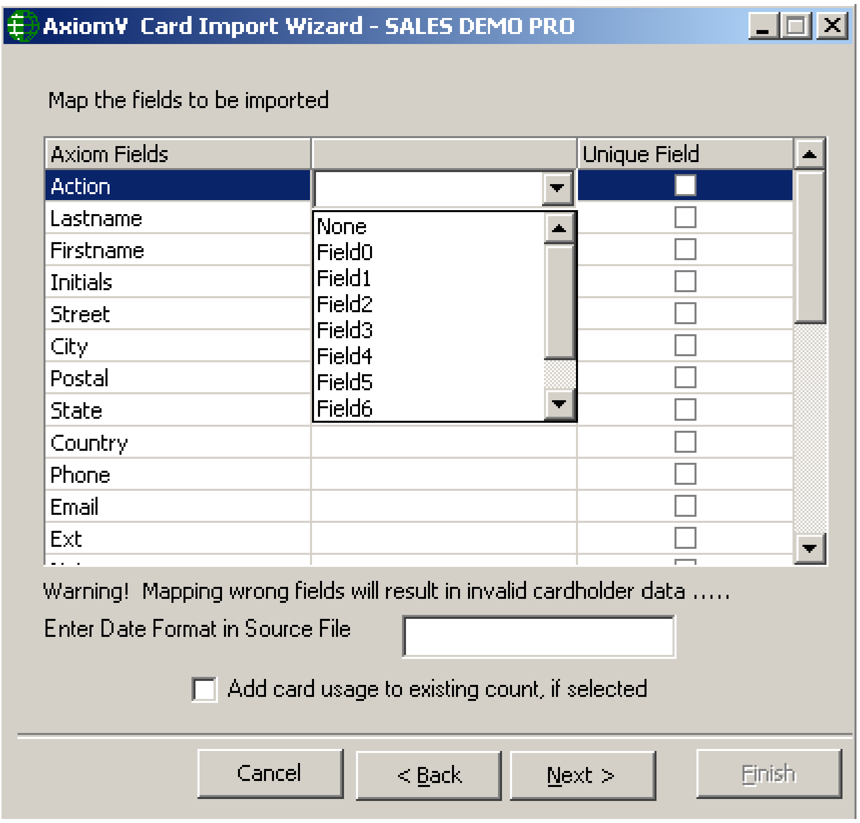
☑ Upon successfull Import delete the file.

- Select the type of *Field Separator* used in the source file and click the *Next* button.

  Separators can be:

  Tab
  Comma (,)
  Semicolon (;)
  Pipeline (|)
  Colon (:)

- Check 'First row in text file has column headers' if it is applicable.
- Check 'Upon successful Import delete the file' if you want the text file deleted after the data has been imported.



AxiomV Card Import Wizard - SALES DEMO PRO

Map the fields to be imported

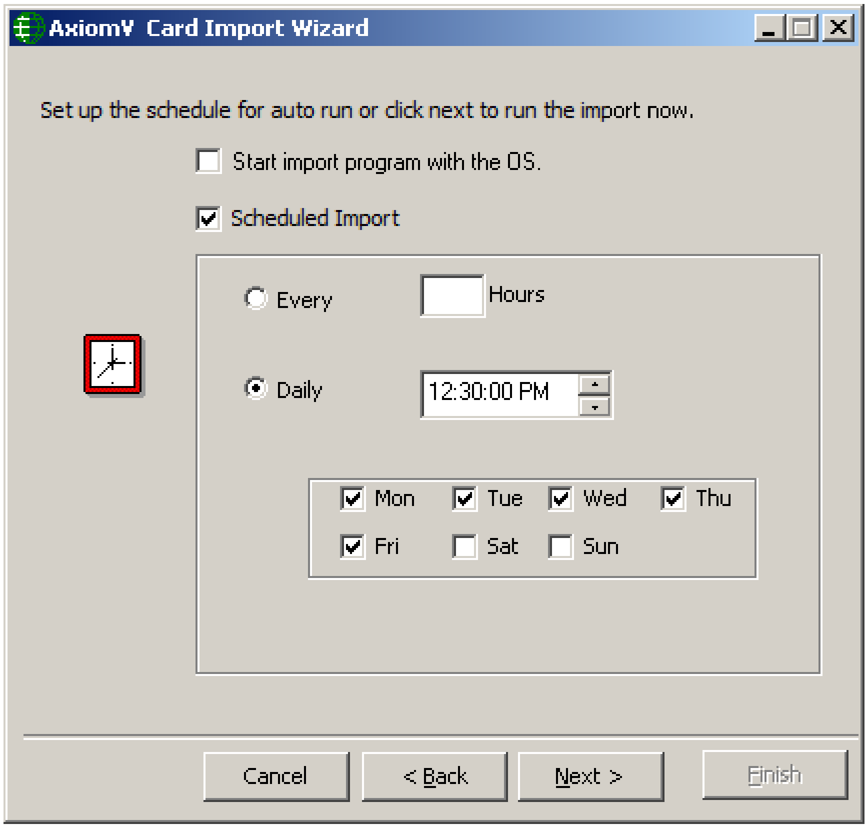
Axiom Fields		Unique Field
Action		☐
Lastname		☐
Firstname		☐
Initials		☐
Street		☐
City		☐
Postal		☐
State		☐
Country		☐
Phone		☐
Email		☐
Ext		☐

Warning! Mapping wrong fields will result in invalid cardholder data .....

Enter Date Format in Source File

☐ Add card usage to existing count, if selected

- Map the source fields to AxiomV™ cardholder fields. Mapping the wrong fields may result in invalid cardholder data. Enter the Date Format of the source file if you are importing date fields as well. Card usage count can be increased by the inputted number instead of being set to that number by checking the box. Check the appropriate box for any Unique Fields. If nothing is checked, then Card Number is taken to be the unique field by default. Click *Next* to launch the window to schedule the import.



AxiomV Card Import Wizard

Set up the schedule for auto run or click next to run the import now.

□ Start import program with the OS.

☑ Scheduled Import

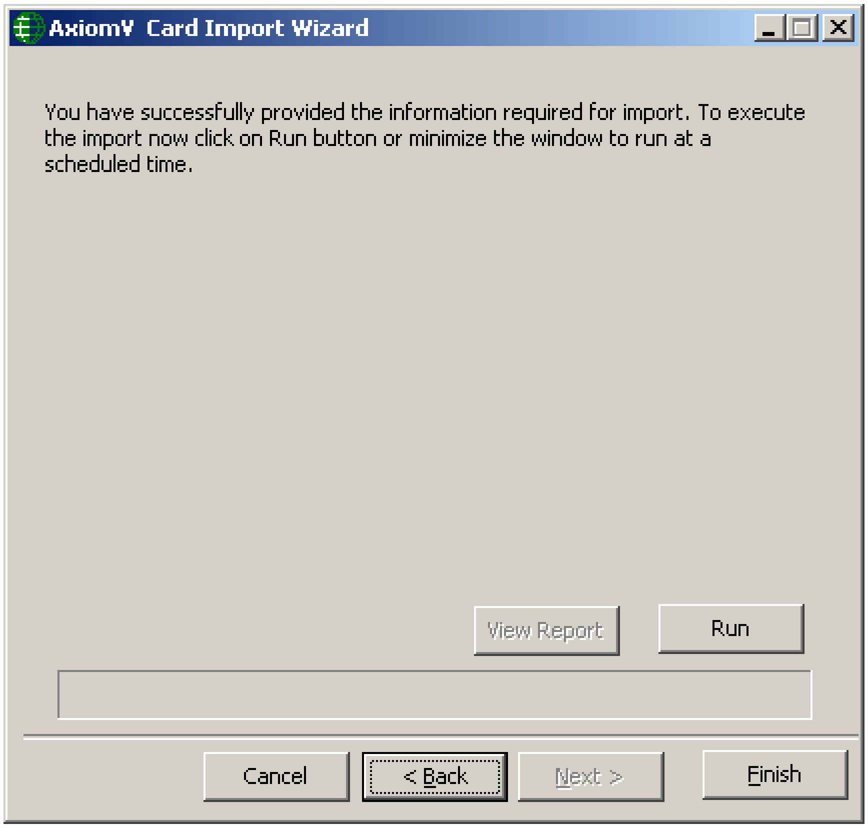
○ Every Hours

● Daily 12:30:00 PM

☑ Mon ☑ Tue ☑ Wed ☑ Thu

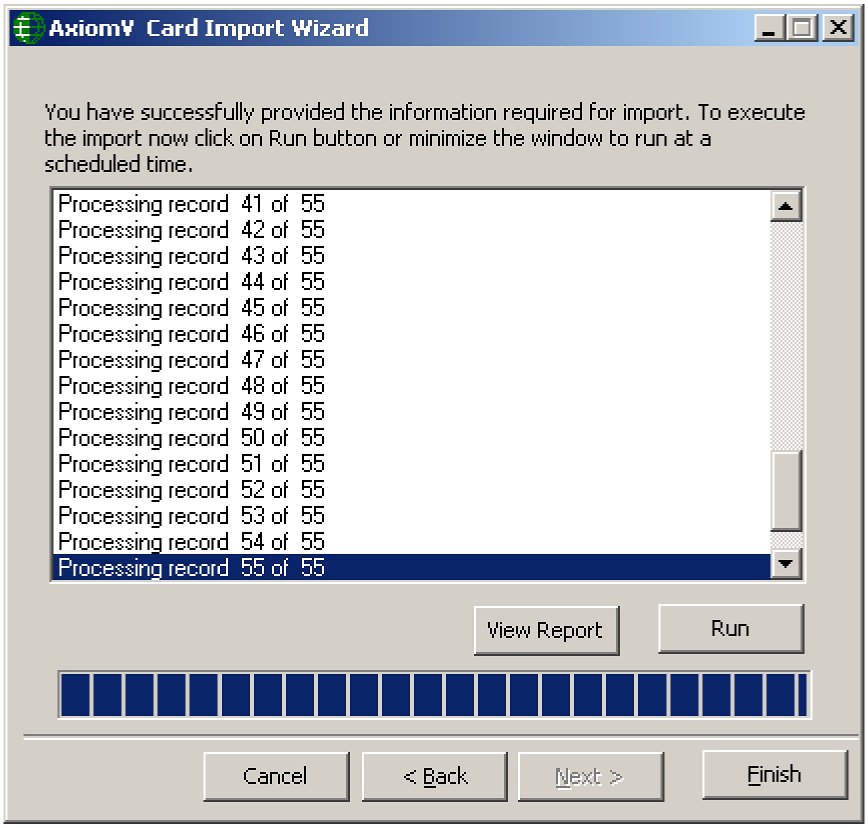
☑ Fri □ Sat □ Sun

- Configure the *Schedule* for importing cardholders' information. Click the *Next* button to have the option of selecting *Run* (to import the selected information right away) or minimize the Wizard to auto run the import at the scheduled time. The utility can also be set to start up when the Operating System starts.
- The import utility can be set to run at an interval set in hours (e.g. every two hours or every five), or it can be set to run on specific days at a specific time (e.g. 12:30pm).



You have successfully provided the information required for import. To execute the import now click on Run button or minimize the window to run at a scheduled time.

- Click on *Run* button to start importing the selected fields from the source file to AxiomV™ cardholder.

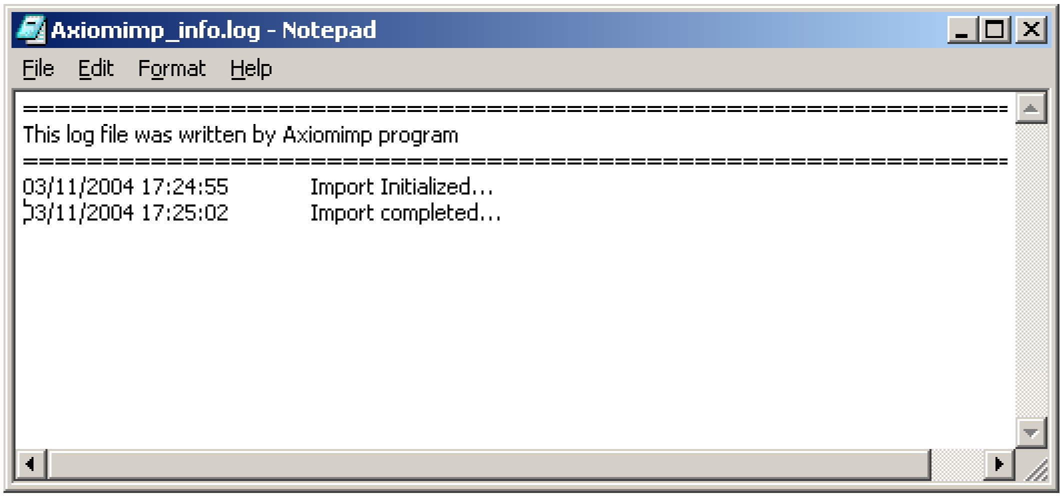


You have successfully provided the information required for import. To execute the import now click on Run button or minimize the window to run at a scheduled time.

```
Processing record  41 of  55
Processing record  42 of  55
Processing record  43 of  55
Processing record  44 of  55
Processing record  45 of  55
Processing record  46 of  55
Processing record  47 of  55
Processing record  48 of  55
Processing record  49 of  55
Processing record  50 of  55
Processing record  51 of  55
Processing record  52 of  55
Processing record  53 of  55
Processing record  54 of  55
Processing record  55 of  55
```

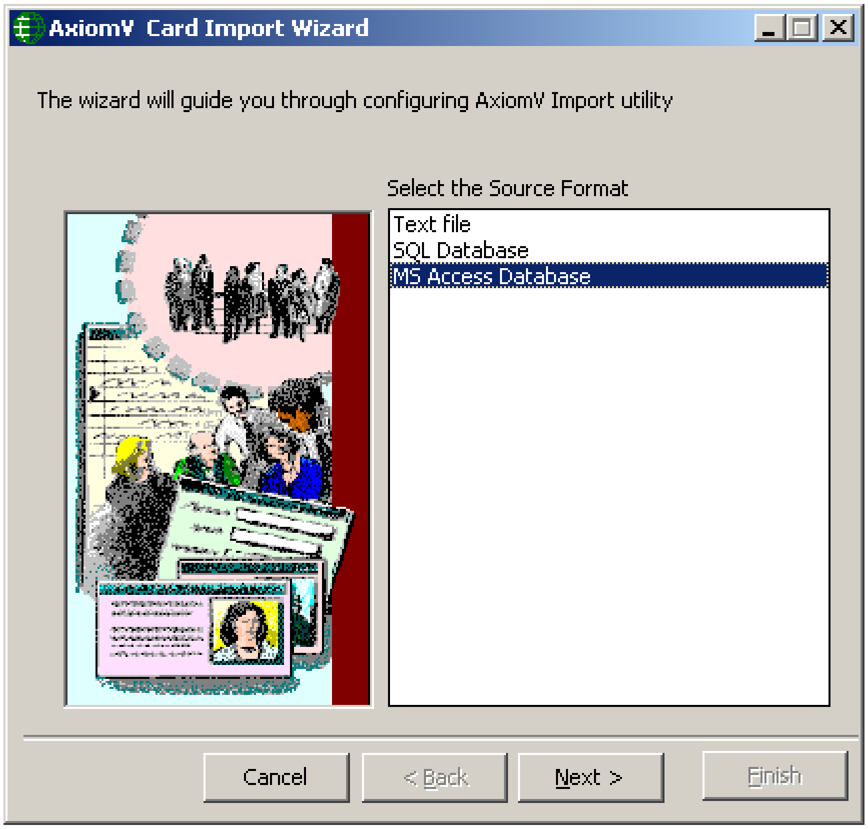
- Minimize the Import Wizard to have in auto run mode. Clicking on the *Finish* button will shut down the AxiomV™ Card Import Utility.

- Click on *View Report* button to view Axiom Import Log information once the cardholder information is imported to AxiomV™ cardholder.



```
=================================================================
This log file was written by Axiomimp program
=================================================================
03/11/2004 17:24:55          Import Initialized...
03/11/2004 17:25:02          Import completed...
```

MS Access Database Format

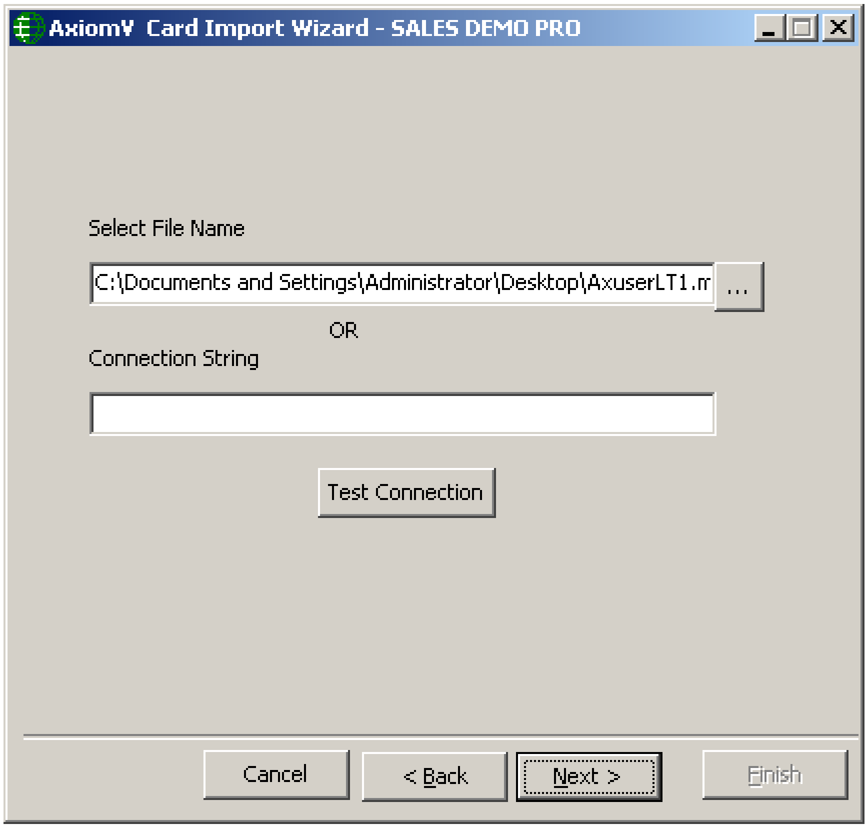


The wizard will guide you through configuring AxiomV Import utility

Select the Source Format

Text file
SQL Database
MS Access Database

- Select the *Source format* as *MS Access Database* and click on *Next* button.



AxiomV Card Import Wizard - SALES DEMO PRO

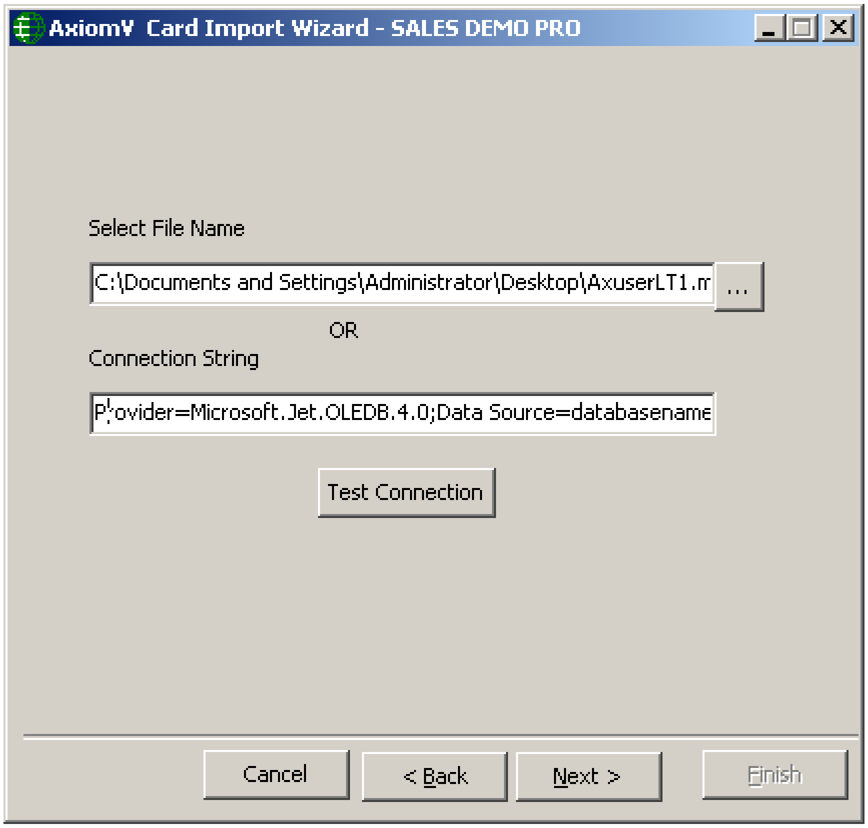
Select File Name

C:\Documents and Settings\Administrator\Desktop\AxuserLT1.m

OR

Connection String

- Select the *File Name* or write in the *Connection String*, whichever way the source file from where the cardholder information to be imported, is available.



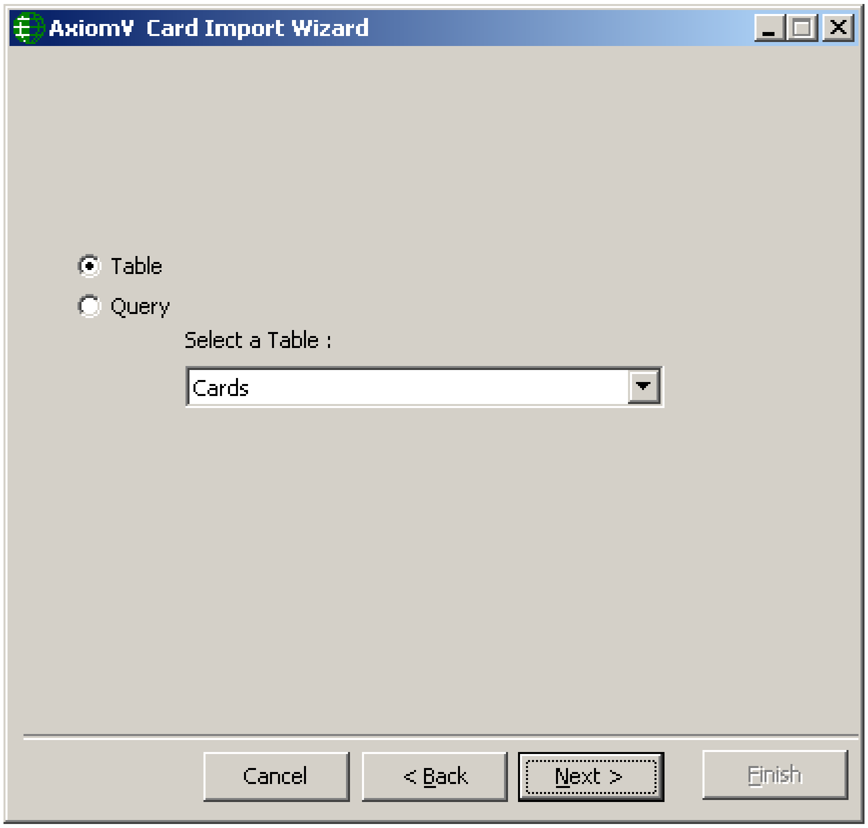
Select File Name

C:\Documents and Settings\Administrator\Desktop\AxuserLT1.m

Connection String

Provider=Microsoft.Jet.OLEDB.4.0;Data Source=databasename

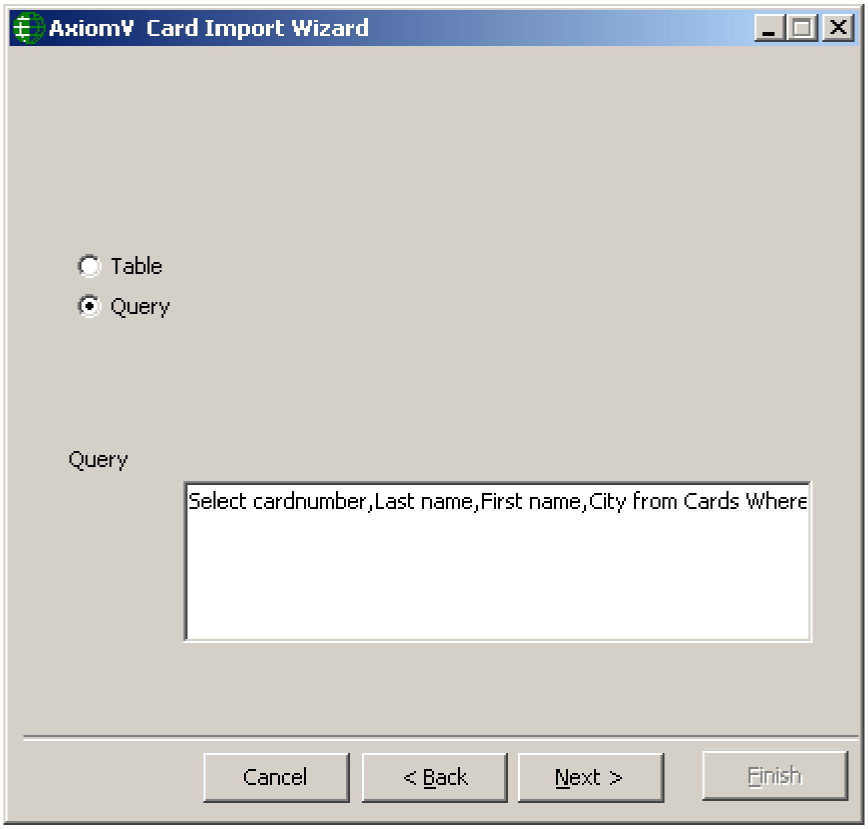
- Select *Table* or *Query* for importing Cardholder information.



● Table
○ Query

Select a Table : Cards

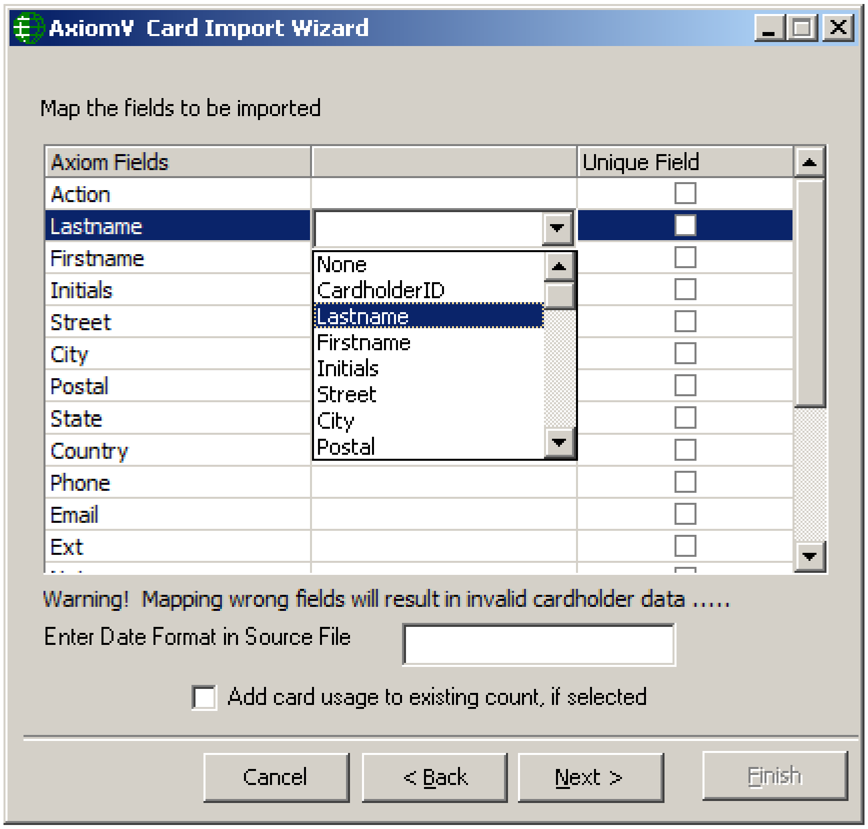
Or



○ Table
● Query

Query: Select cardnumber,Last name,First name,City from Cards Where

- Click on *Next* button to Map the fields to be imported.



AxiomV Card Import Wizard

Map the fields to be imported

Axiom Fields		Unique Field
Action		□
Lastname		□
Firstname		□
Initials		□
Street		□
City		□
Postal		□
State		□
Country		□
Phone		□
Email		□
Ext		□

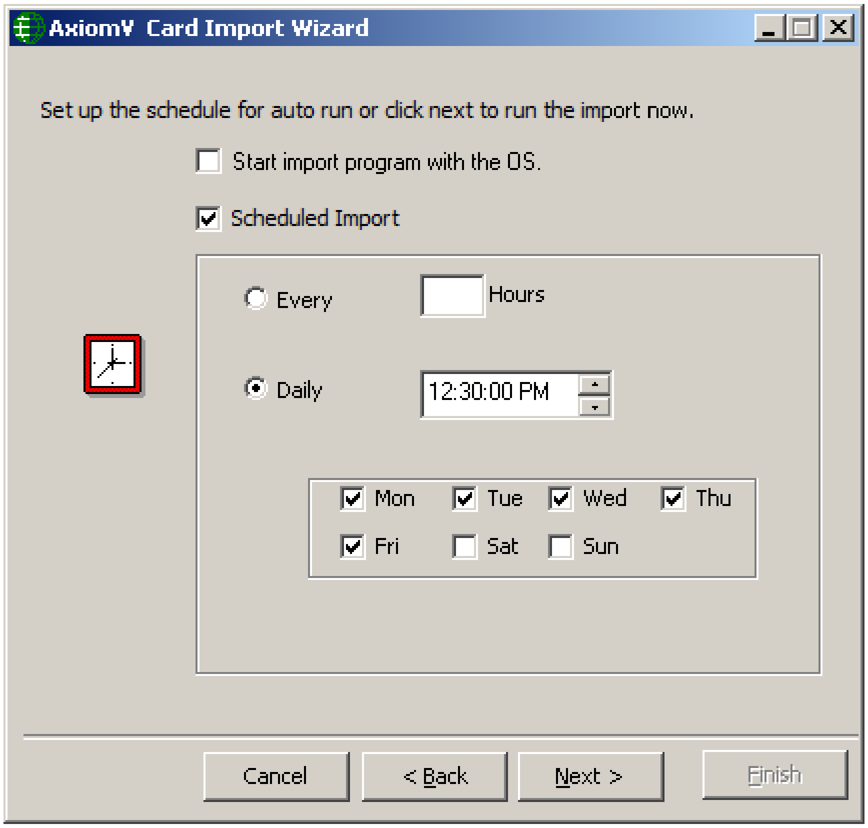
None
CardholderID
Lastname
Firstname
Initials
Street
City
Postal

Warning! Mapping wrong fields will result in invalid cardholder data .....

Enter Date Format in Source File

□ Add card usage to existing count, if selected

- Map the source fields to AxiomV™ cardholder fields. Mapping the wrong fields may result in invalid cardholder data. Enter Date Format of the source file if you are importing date fields as well. Card usage count can be increased by the inputted number instead of being set to that number by checking the box. Check in the Unique Field. If nothing is checked, then Card number is taken to be the unique field by default. Click *Next* to launch the window to schedule the import.



Set up the schedule for auto run or click next to run the import now.

□ Start import program with the OS.

☑ Scheduled Import

○ Every [ ] Hours

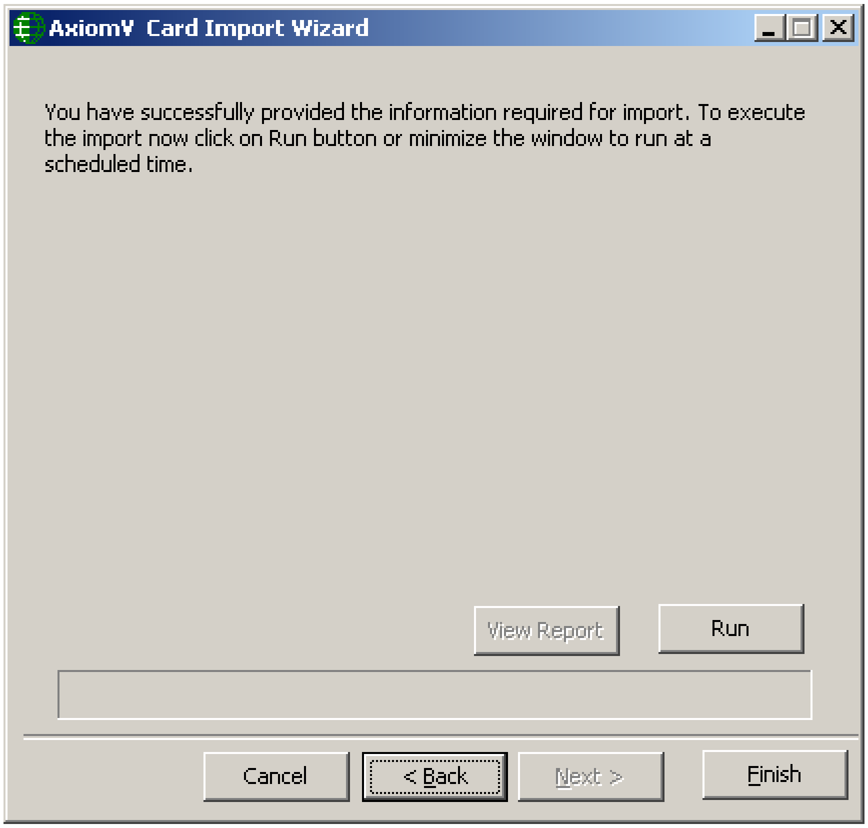
● Daily 12:30:00 PM

☑ Mon ☑ Tue ☑ Wed ☑ Thu

☑ Fri □ Sat □ Sun

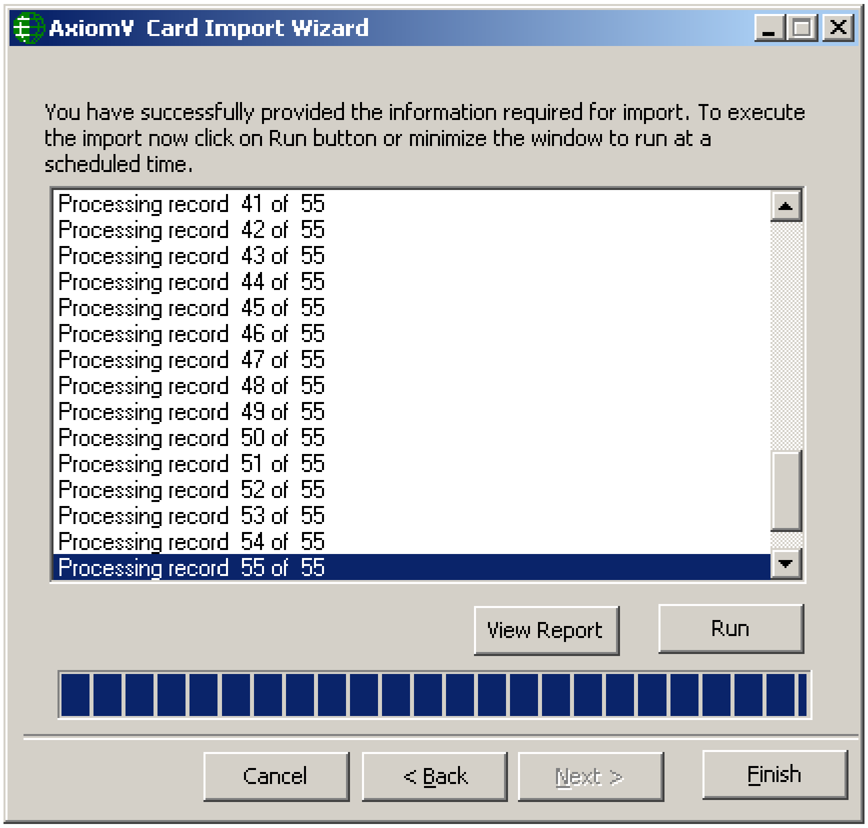
- Configure the *Schedule* for importing cardholders' information. Click the *Next* button to have the option of selecting *Run* (to import the selected information right away) or minimize the Wizard to auto run the import at the scheduled time. The utility can also be set to start up when the Operating System starts.

- The import utility can be set to run at an interval set in hours (e.g. every two hours or every five), or it can be set to run every day at a specific time (e.g. 12:55 p.m.).



You have successfully provided the information required for import. To execute the import now click on Run button or minimize the window to run at a scheduled time.

- Click on *Run* button to start importing the selected fields from the source file to AxiomV™ cardholder.

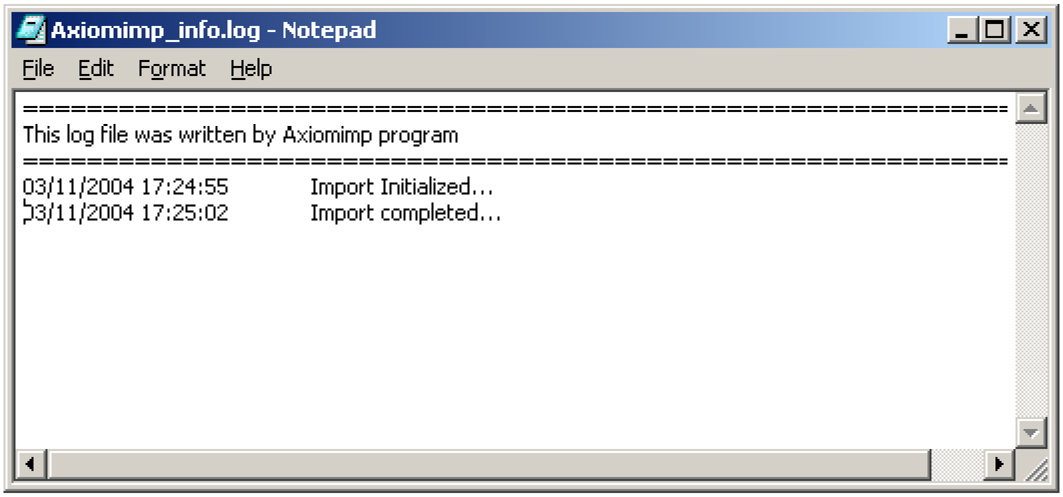


You have successfully provided the information required for import. To execute the import now click on Run button or minimize the window to run at a scheduled time.

```
Processing record  41 of  55
Processing record  42 of  55
Processing record  43 of  55
Processing record  44 of  55
Processing record  45 of  55
Processing record  46 of  55
Processing record  47 of  55
Processing record  48 of  55
Processing record  49 of  55
Processing record  50 of  55
Processing record  51 of  55
Processing record  52 of  55
Processing record  53 of  55
Processing record  54 of  55
Processing record  55 of  55
```

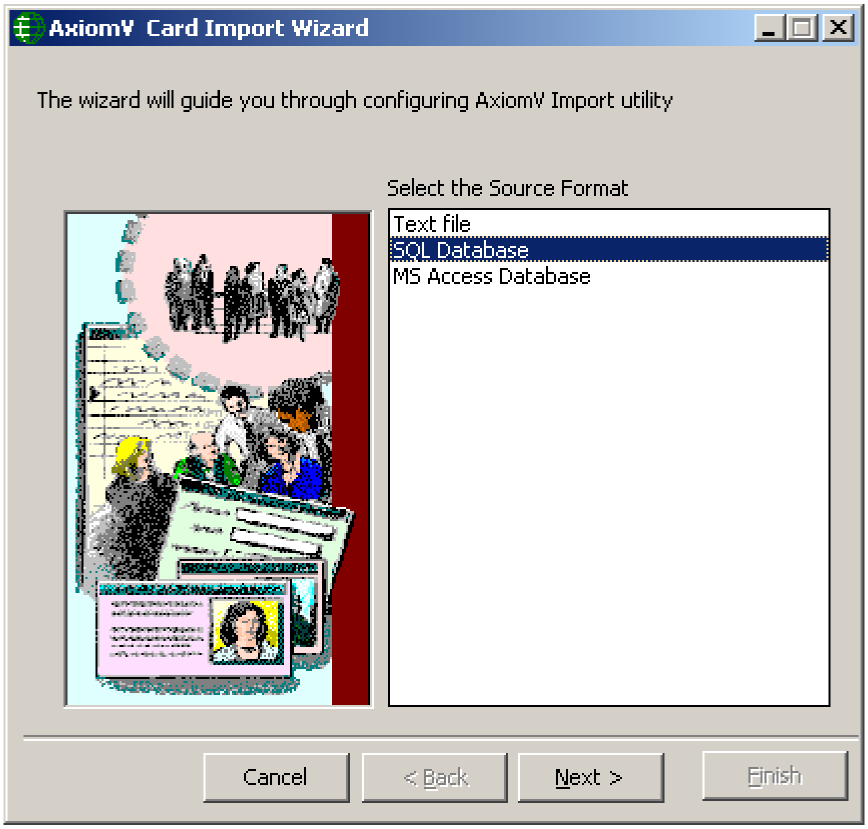
- Minimize the Import Wizard to have in auto run mode. Clicking on the *Finish* button will shut down the AxiomV™ Card Import Utility.

- Click on *View Report* button to view Axiom Import Log information once the cardholder information is imported to AxiomV™ cardholder.



```
==================================================================
This log file was written by Axiomimp program
==================================================================
03/11/2004 17:24:55          Import Initialized...
03/11/2004 17:25:02          Import completed...
```

SQL Database Format



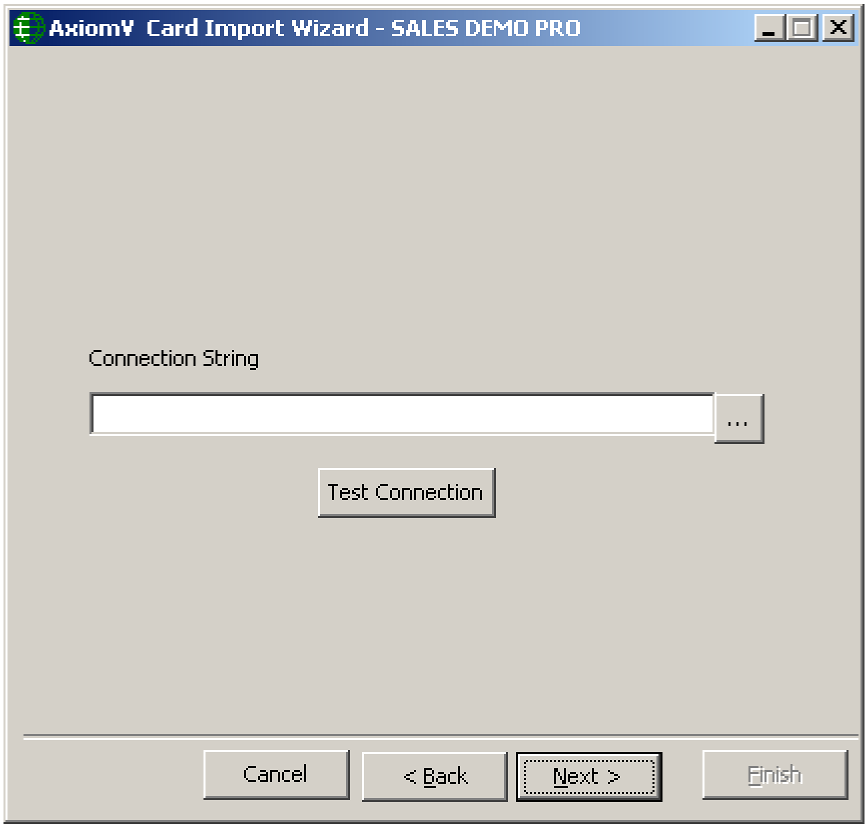
AxiomV Card Import Wizard

The wizard will guide you through configuring AxiomV Import utility

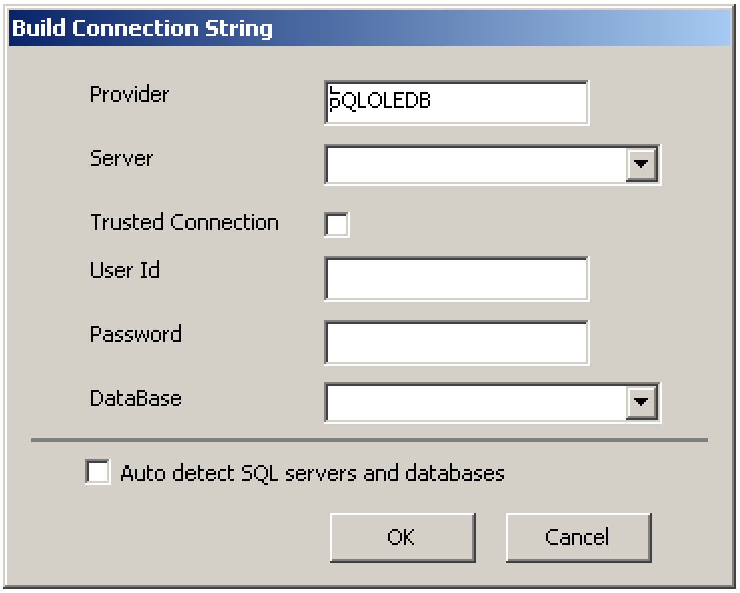
Select the Source Format

- Text file
- SQL Database
- MS Access Database

- Select the *Source format* as *SQL Database* and click on *Next* button.



- Click on *Browse/Ellipsis* Button to provide the information about the connection string for the SQL database from where the cardholders' information is to be imported.



Provider: SQLOLEDB

Server:

□ Trusted Connection

User Id:

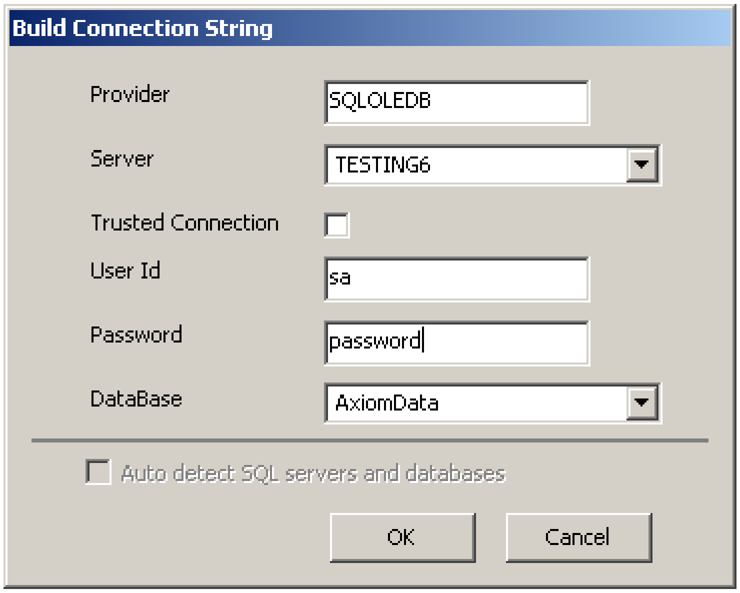
Password:

DataBase:

□ Auto detect SQL servers and databases

- Provide the above information to build a valid connection string. Use ‘sa’ as the ‘User Id’ and ‘password’ for the ‘password’ if you haven’t changed them.

- Select *Auto detect SQL servers and databases* option, if import utility is opened from an AxiomV server machine. If an Axiom client connection cannot detect other SQL installation on the same network, it will allow to put in the SQL information manually and will disable this option

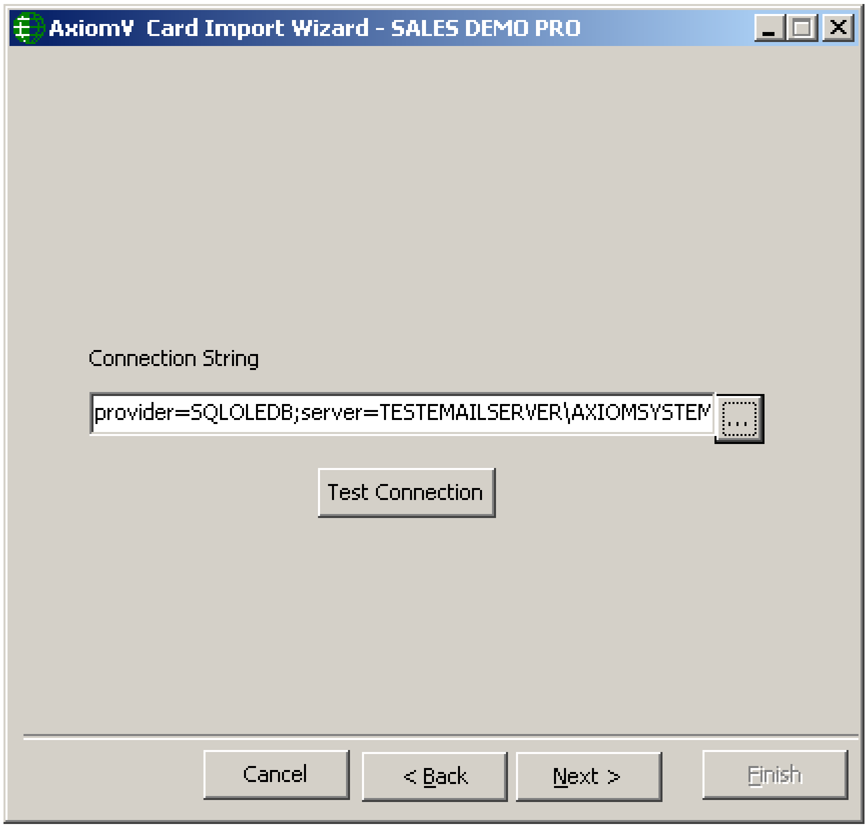


Build Connection String

Provider: SQLOLEDB
Server: TESTING6
Trusted Connection: □
User Id: sa
Password: password
DataBase: AxiomData

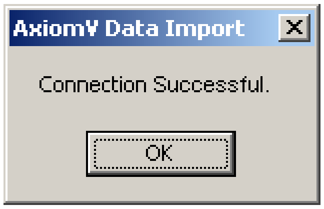
□ Auto detect SQL servers and databases

- Click *OK* to get back to connection string window.



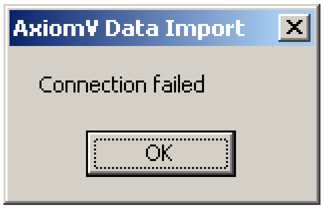
provider=SQLOLEDB;server=TESTEMAILSERVER\AXIOMSYSTEM

- Click on *Test Connection* button to verify a valid connection string.



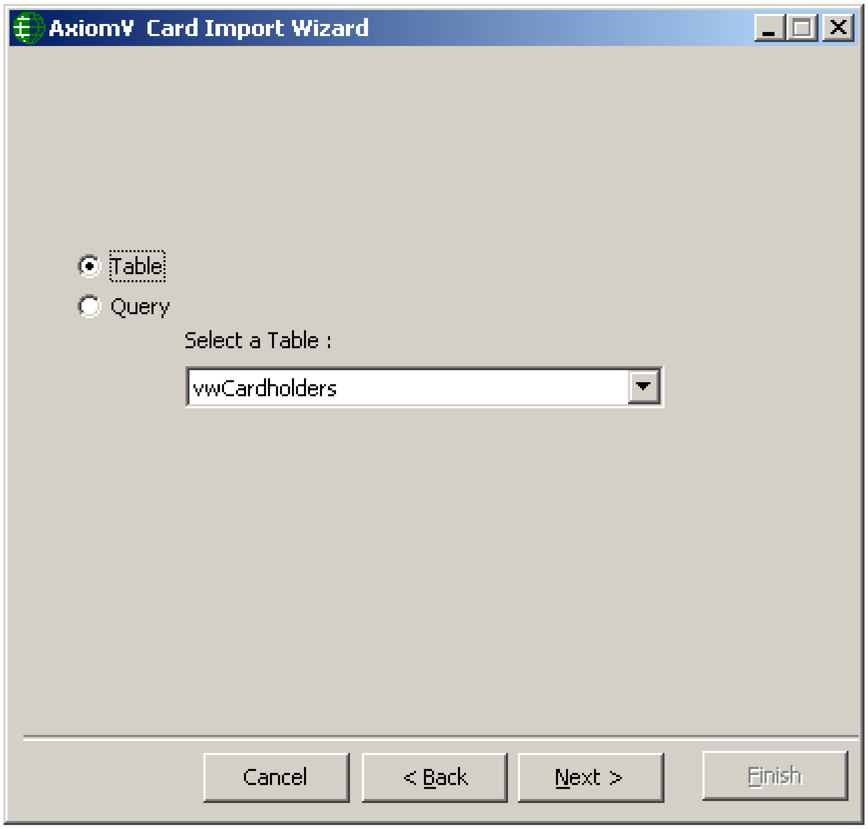
Connection Successful.

- If the information provided is correct, you will get the message ‘Connection Successful’, otherwise



Connection failed

- Click on *Next* button after providing a successful connection for importing cardholder SQL database.



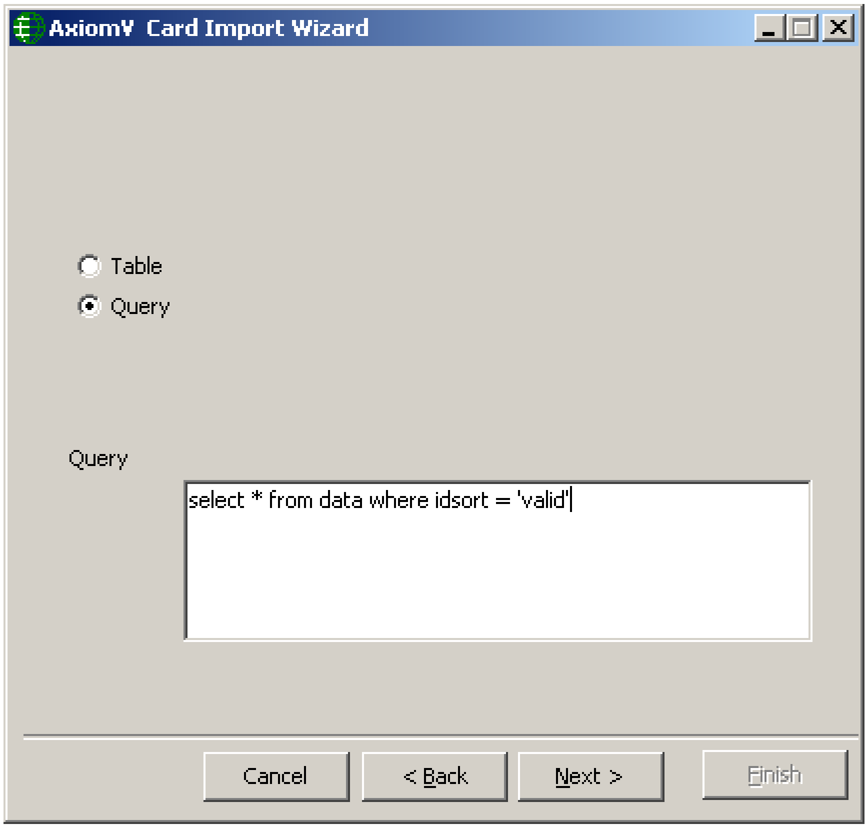
AxiomV Card Import Wizard

● Table

○ Query

Select a Table : vwCardholders

- Select *Table* or *Query* for importing Cardholder information. Select the name of the table if 'Table' option is selected or write the query if 'Query' option is selected.

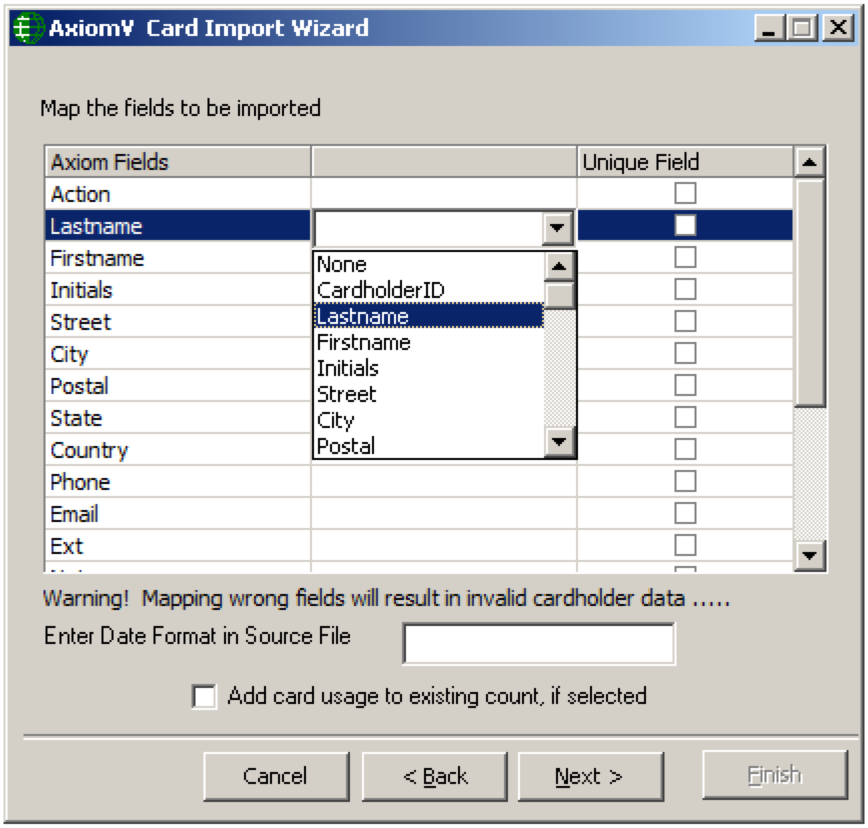


○ Table
● Query

Query

select * from data where idsort = 'valid'

- Click on *Next* button to Map the fields to be imported.



AxiomV Card Import Wizard

Map the fields to be imported

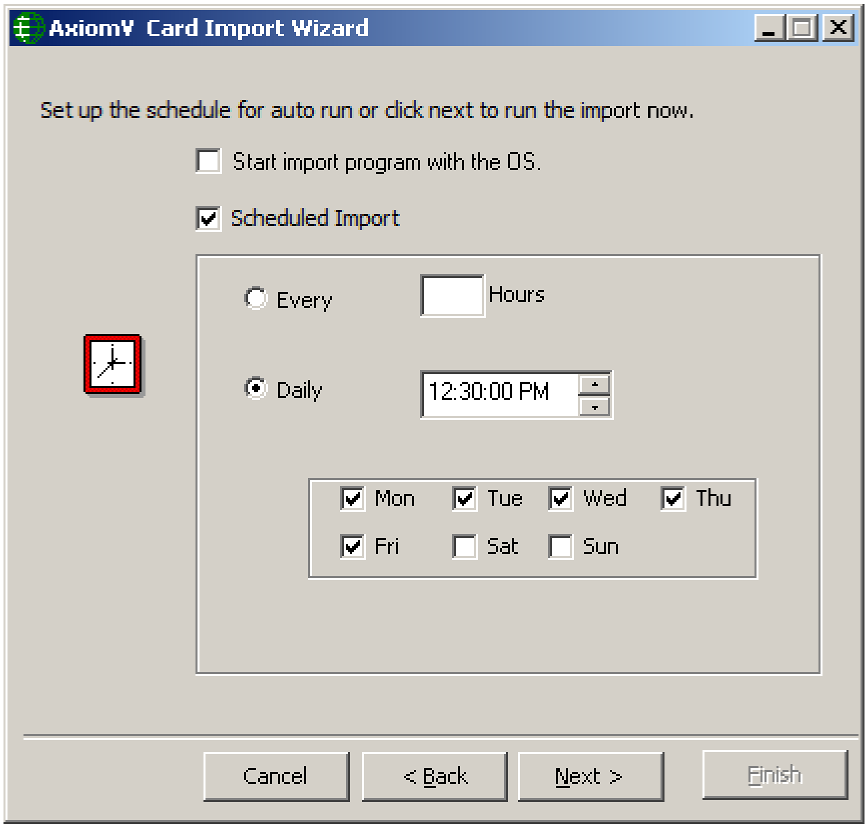
Axiom Fields		Unique Field
Action		□
Lastname		□
Firstname		□
Initials		□
Street		□
City		□
Postal		□
State		□
Country		□
Phone		□
Email		□
Ext		□

Warning! Mapping wrong fields will result in invalid cardholder data .....

Enter Date Format in Source File

□ Add card usage to existing count, if selected

- Map the source fields to AxiomV™ cardholder fields. Mapping the wrong fields may result in invalid cardholder data. Enter Date Format of the source file if you are importing date fields as well. Card usage count can be increased by the inputted number instead of being set to that number by checking the box. Check in the Unique Field. If nothing is checked, then Card number is taken to be the unique field by default. Click *Next* to launch the window to schedule the import.



AxiomV Card Import Wizard

Set up the schedule for auto run or click next to run the import now.

□ Start import program with the OS.

☑ Scheduled Import

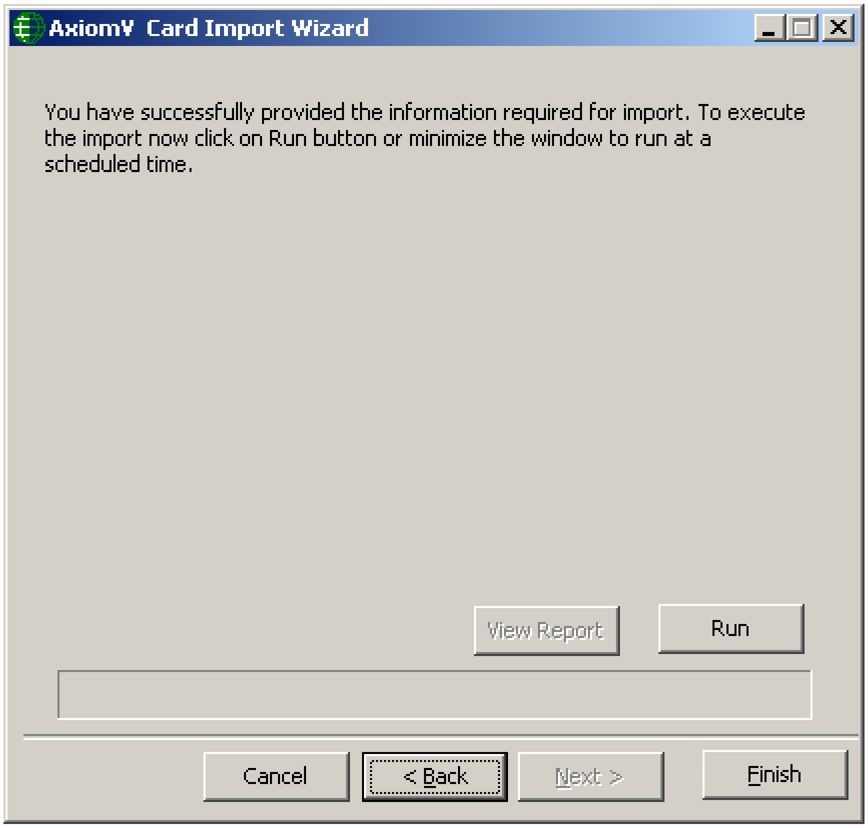
○ Every Hours

● Daily 12:30:00 PM

☑ Mon ☑ Tue ☑ Wed ☑ Thu
☑ Fri □ Sat □ Sun

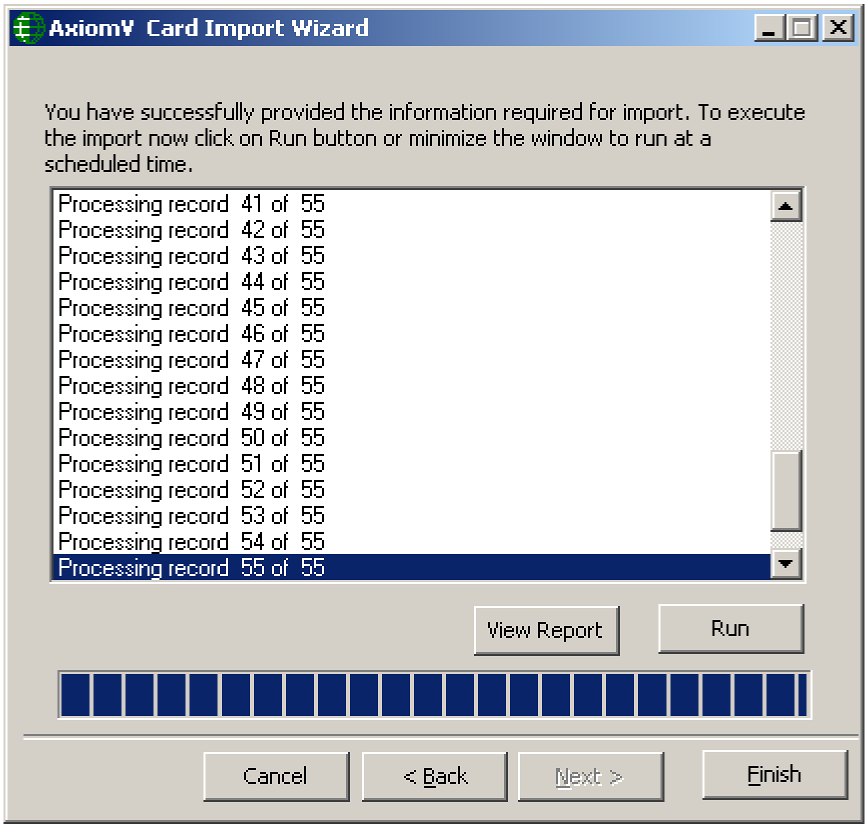
- Configure the *Schedule* for importing cardholders' information. Click the *Next* button to have the option of selecting *Run* (to import the selected information right away) or minimize the Wizard to auto run the import at the scheduled time. The utility can also be set to start up when the Operating System starts.

- The import utility can be set to run at an interval set in hours (e.g. every two hours or every five), or it can be set to run every day at a specific time (e.g. 12:55 p.m.).



You have successfully provided the information required for import. To execute the import now click on Run button or minimize the window to run at a scheduled time.

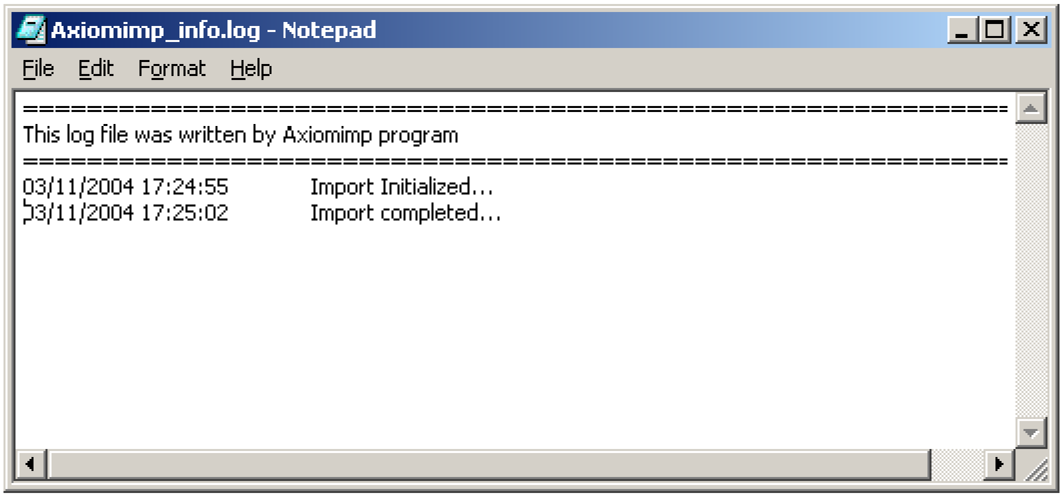
- Click on *Run* button to start the import.



You have successfully provided the information required for import. To execute the import now click on Run button or minimize the window to run at a scheduled time.

```
Processing record  41 of  55
Processing record  42 of  55
Processing record  43 of  55
Processing record  44 of  55
Processing record  45 of  55
Processing record  46 of  55
Processing record  47 of  55
Processing record  48 of  55
Processing record  49 of  55
Processing record  50 of  55
Processing record  51 of  55
Processing record  52 of  55
Processing record  53 of  55
Processing record  54 of  55
Processing record  55 of  55
```

- Minimize the Import Wizard to have in auto run mode. Clicking on the *Finish* button will shut down the AxiomV™ Card Import Utility.
- Click on *View Report* button to view *Axiomimp_info.log* file to check the error messages for import, if any.



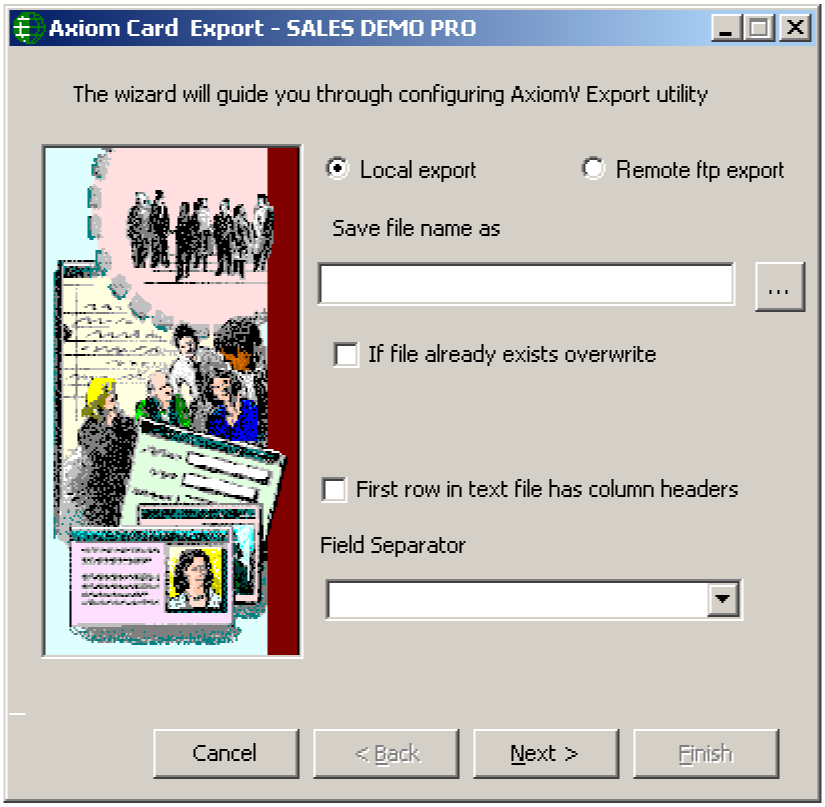
```
=================================================================
This log file was written by Axiomimp program
=================================================================
03/11/2004 17:24:55          Import Initialized...
03/11/2004 17:25:02          Import completed...
```

Export[6]

Selecting *Export* will start the Card Export utility.

- Export module has two options to select from: *Local export*, and *Remote ftp export*

Local export



Axiom Card Export - SALES DEMO PRO

The wizard will guide you through configuring AxiomV Export utility

● Local export ○ Remote ftp export

Save file name as

□ If file already exists overwrite

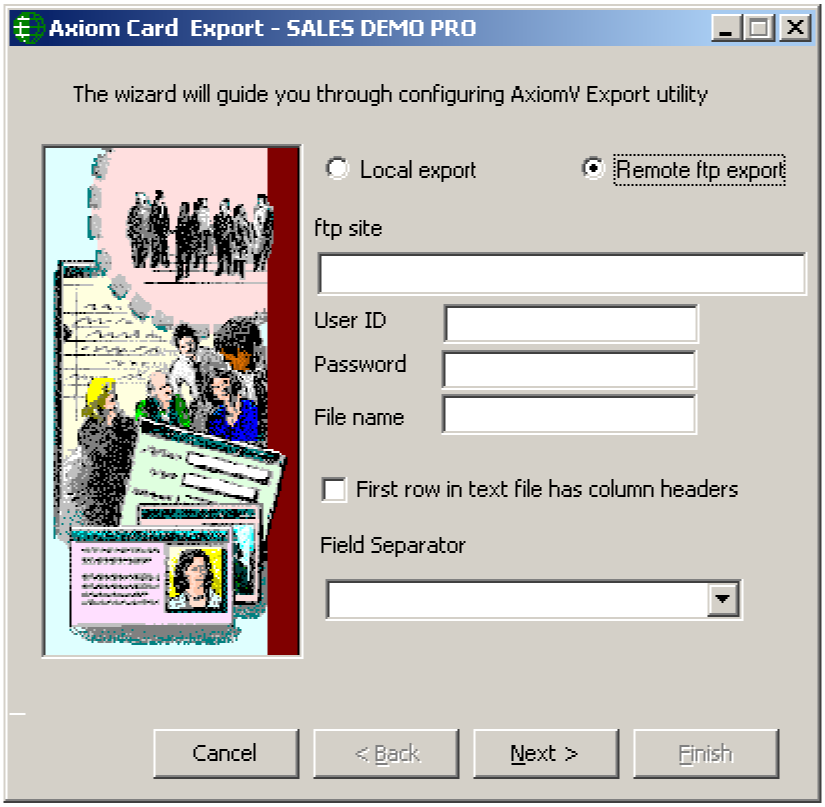
□ First row in text file has column headers

Field Separator

- Browse or type the name of the file to be saved. Check the box if you wish to overwrite an existing file of that name.

[6] This selection is only available if the optional license for the Import & Export Utilities has been purchased and installed.

Remote ftp export



Axiom Card Export - SALES DEMO PRO

The wizard will guide you through configuring AxiomV Export utility

○ Local export ● Remote ftp export

ftp site

User ID

Password

File name

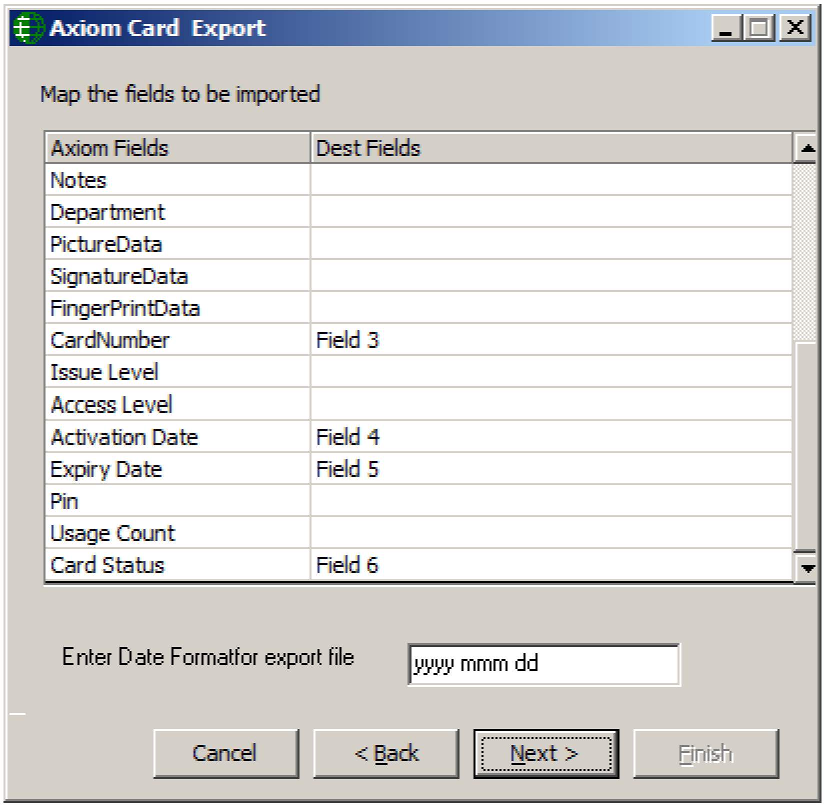
□ First row in text file has column headers

Field Separator

- Fill in the required ftp information

- Check the second box if you wish to include column headers in the text file.

- Select the Field Separator to be used and then click *Next*.



Axiom Card Export

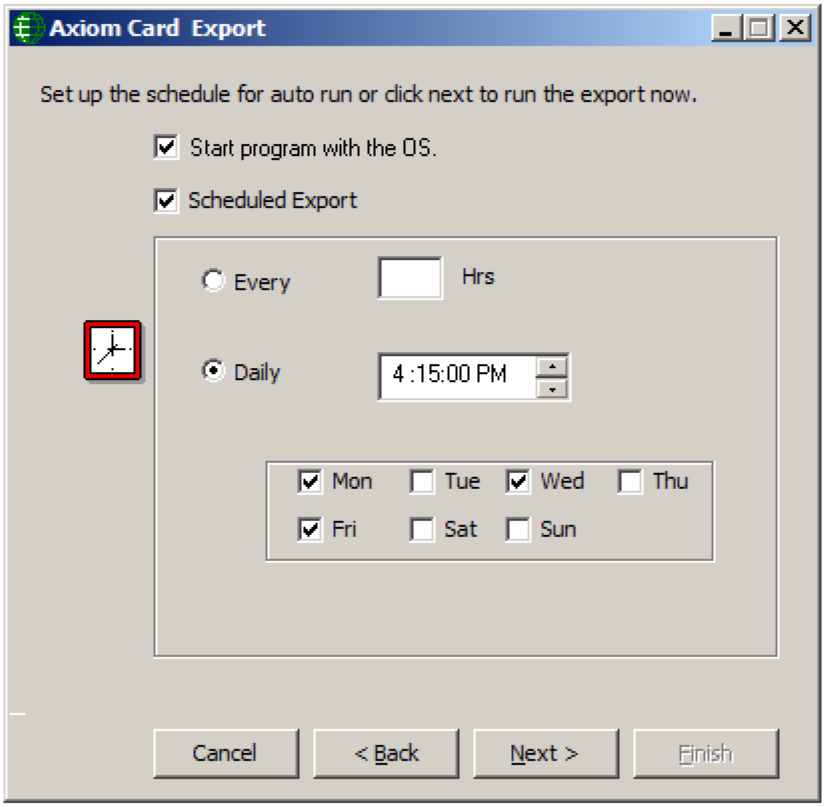
Map the fields to be imported

Axiom Fields	Dest Fields
Notes	
Department	
PictureData	
SignatureData	
FingerPrintData	
CardNumber	Field 3
Issue Level	
Access Level	
Activation Date	Field 4
Expiry Date	Field 5
Pin	
Usage Count	
Card Status	Field 6

Enter Date Formatfor export file: yyyy mmm dd

- Select which *AxiomV*™ fields are to be saved and to which destination fields.

- If a date field is being saved enter the desired date format to be used.



Set up the schedule for auto run or click next to run the export now.

☑ Start program with the OS.

☑ Scheduled Export

○ Every □ Hrs

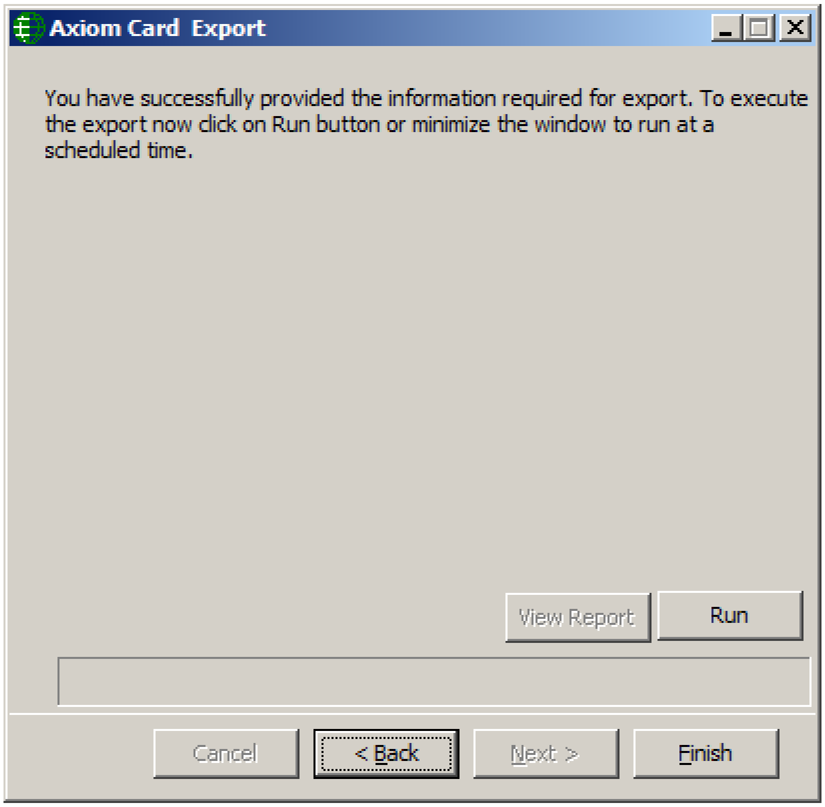
● Daily 4 :15:00 PM

☑ Mon □ Tue ☑ Wed □ Thu
☑ Fri □ Sat □ Sun

- If you want the *Export* utility to start very time the computer starts then check the top box.

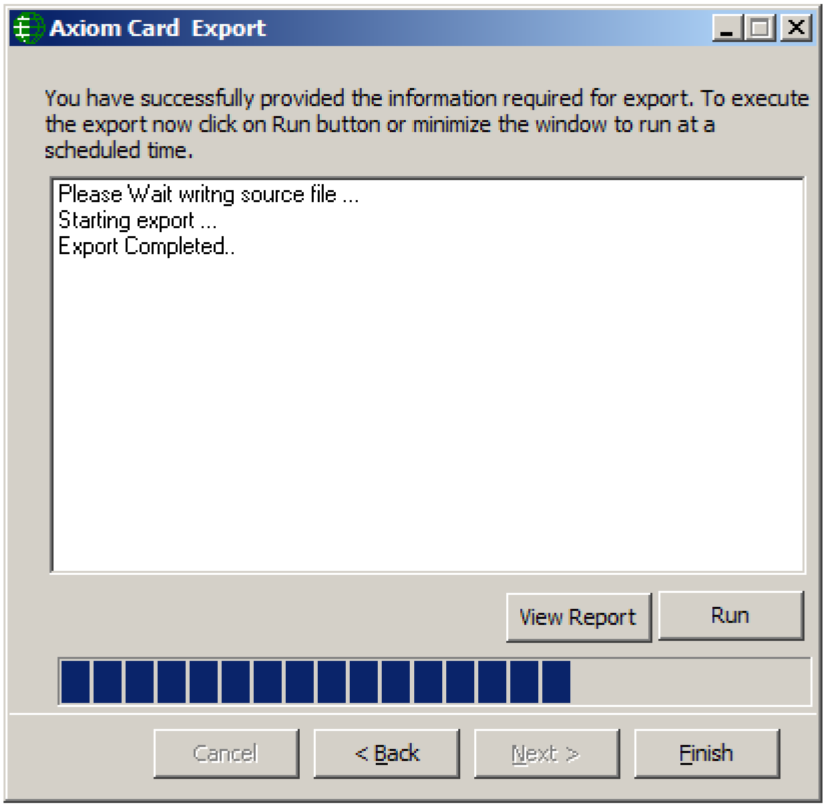
- Check the second box to configure a schedule for periodic exports, every ***x*** number of hours (up to twenty-four), or on specified days at a specified time.

- Click *Next* to go on to the next screen.



You have successfully provided the information required for export. To execute the export now click on Run button or minimize the window to run at a scheduled time.

After setting up the export you can either Run it now, minimize the screen to run in the background, or shut it down by clicking on Finish.

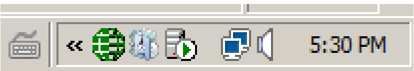


Axiom Card Export

You have successfully provided the information required for export. To execute the export now click on Run button or minimize the window to run at a scheduled time.

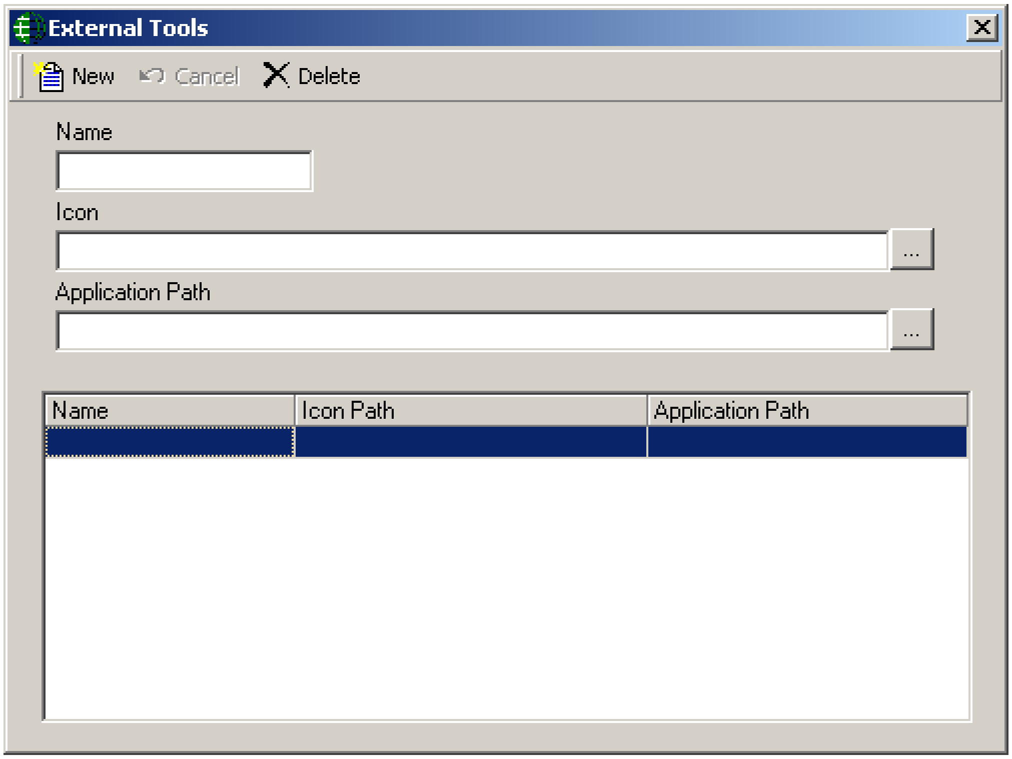
```
Please Wait writng source file ...
Starting export ...
Export Completed..
```

The green RBH globe icon can be found in the bottom right corner of your computer screen when the Export utility is running in the background.



External Tools

External Tools allows the user to access programs, utilities, and tools that are not part of the AxiomV™ system.



Name

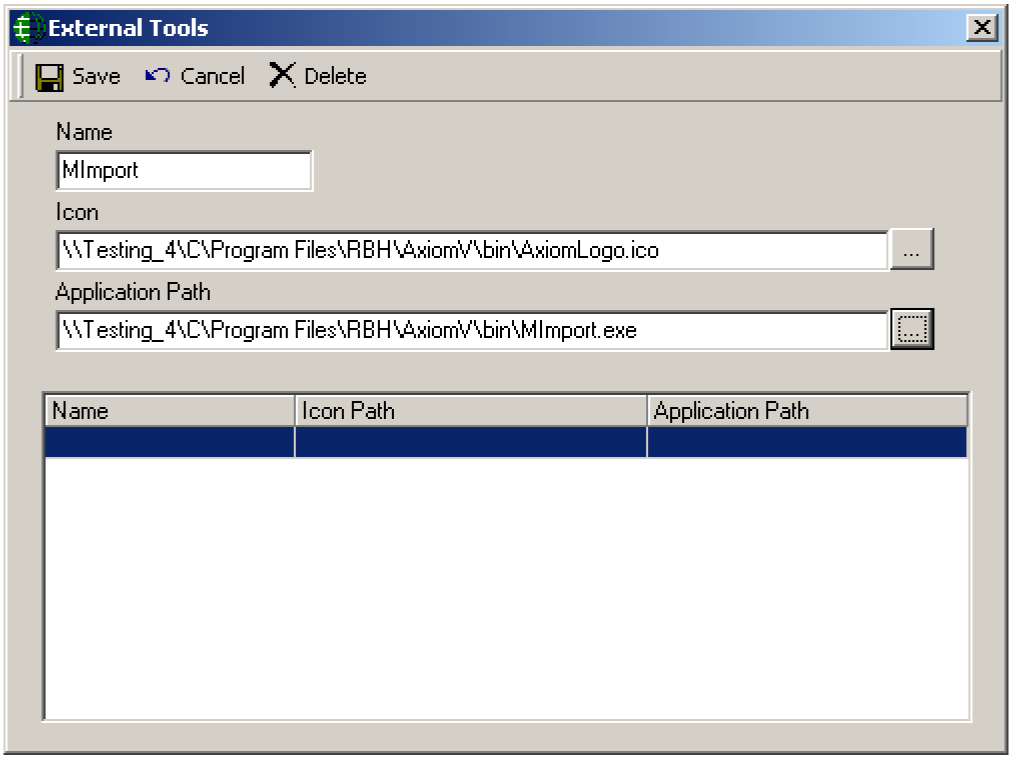
Enter the name (description) of the desired program (utility or tool) as you would like it displayed in the menu.

Icon

Browse or enter the path to the icon that is to be displayed in the menu (optional).

Application Path

Browse or enter the path to the desired program (utility or tool).



Name

MImport

Icon

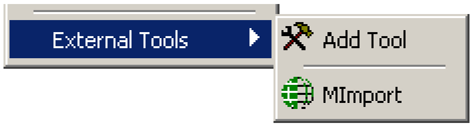
\\Testing_4\C\Program Files\RBH\AxiomV\bin\AxiomLogo.ico

Application Path

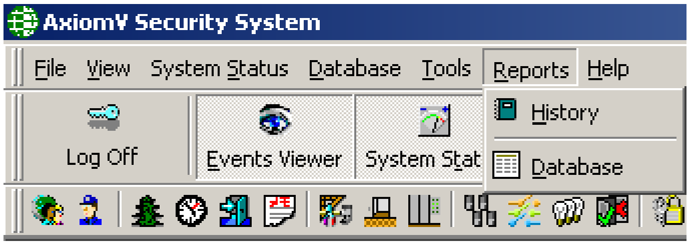
\\Testing_4\C\Program Files\RBH\AxiomV\bin\MImport.exe

Name	Icon Path	Application Path

Save the entry and it will be added to the External Tools menu.



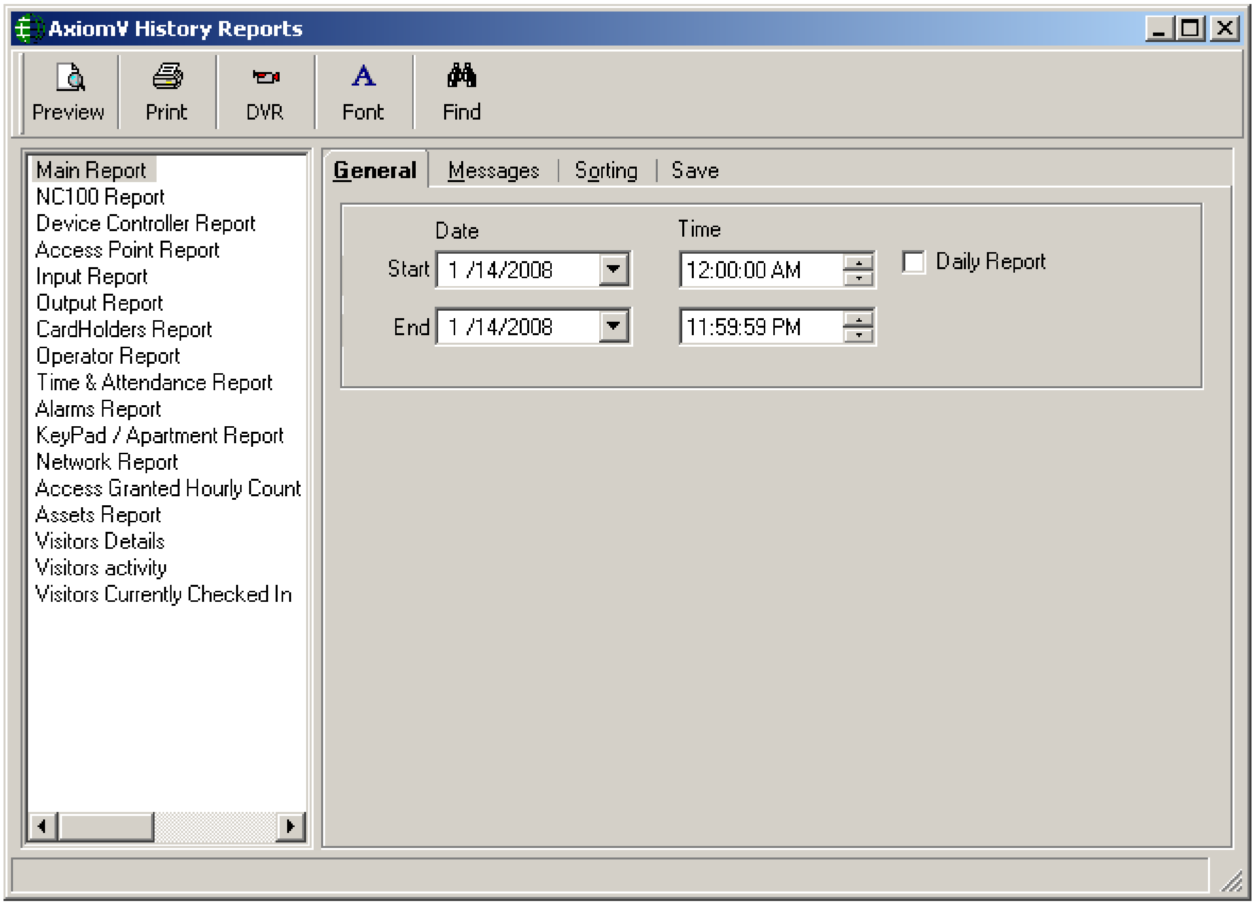
Reports



History Reports

History Report will open the *AxiomV™ History Report* window. The operator can generate reports from the history files, filtered and sorted as needed.

Main. Operator and *Alarms History Report* is shown only under *Master Profile*



	Date	Time
Start	1 /14/2008	12:00:00 AM
End	1 /14/2008	11:59:59 PM

☐ Daily Report

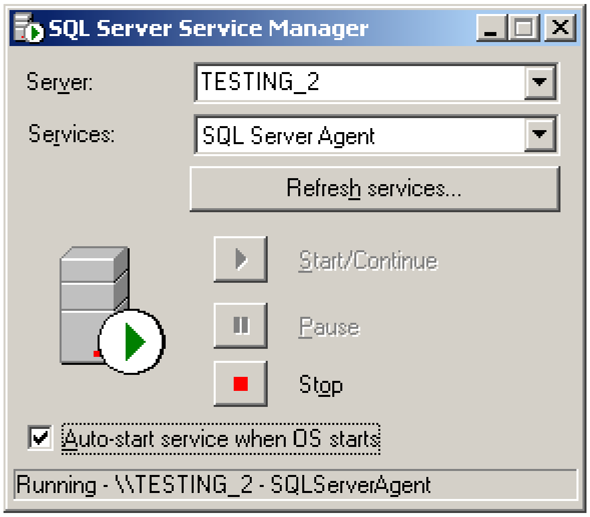
Information on how to create Event History Reports is given on page 330 of Chapter 8.

Maintaining History Files (Archive Log database)

SQL Server Agent

To maintain your Event History, SQL Server Agent must be running

To confirm that SQL Server Agent is running double click the SQL Server Service Manager icon (found on the right-side of the Task Manager, near the clock display).



Server: TESTING_2

Services: SQL Server Agent

☑ Auto-start service when OS starts

Running - \\TESTING_2 - SQLServerAgent

SQL Server Agent maintains the AxiomLog files. Additional history files will be created (e.g. AxiomLog1, AxiomLog2) as the amount of history data increases. After a history data file surpasses 1.5 GB a new file is created.

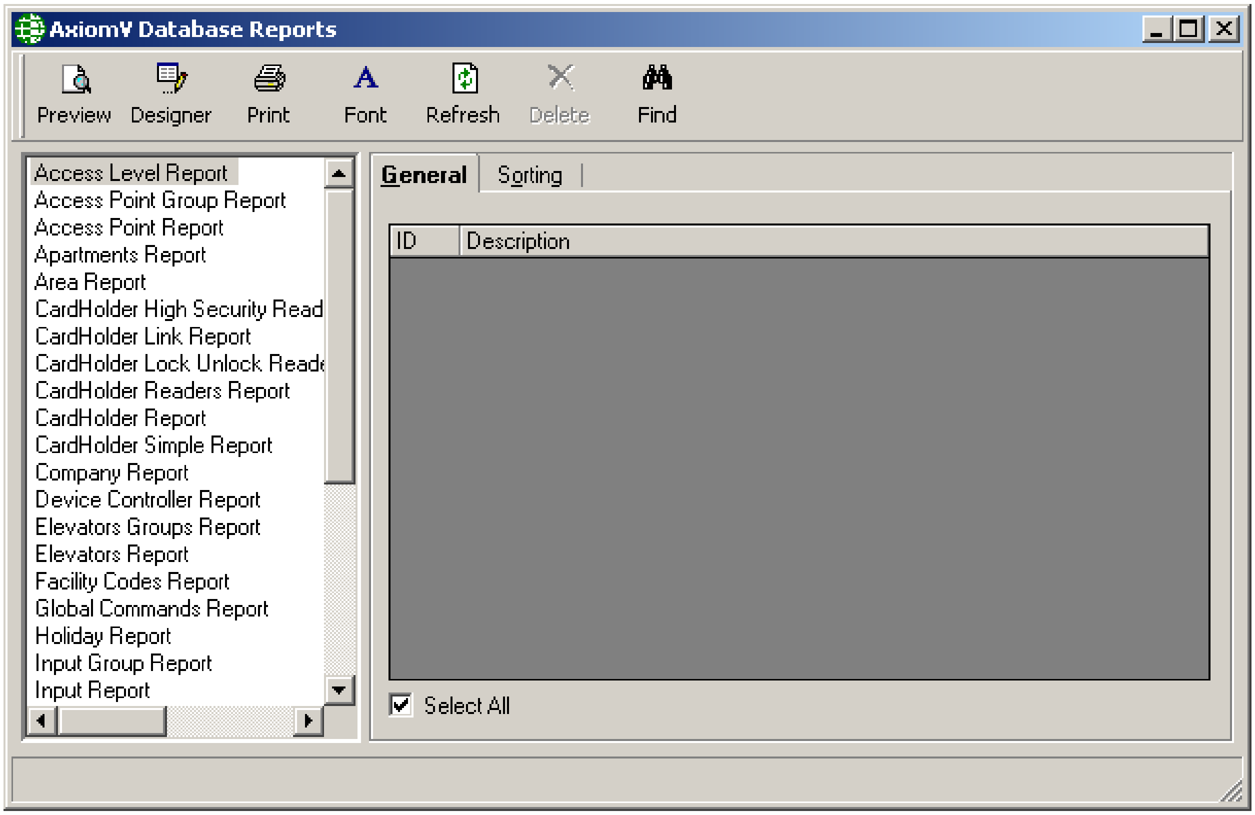
This option is available for all supported SQL server and /or MSDE 2000 based systems only.

For SQL Express 2005 and 2008 based system SQL Server Agent is disabled and history data file is maintained through a program within AxiomV™ system

If your history data file (AxiomLog.mdf) grows beyond 1.6 GB contact RBH Support for assistance. You will likely lose history if your history data file reaches 2048Mb.

Database Reports

Database Report will open the available *AxiomV™ Database Reports and Database Report Designer*[7] window. This window will allow the operator to generate reports from the database files, designed as needed by the operator.



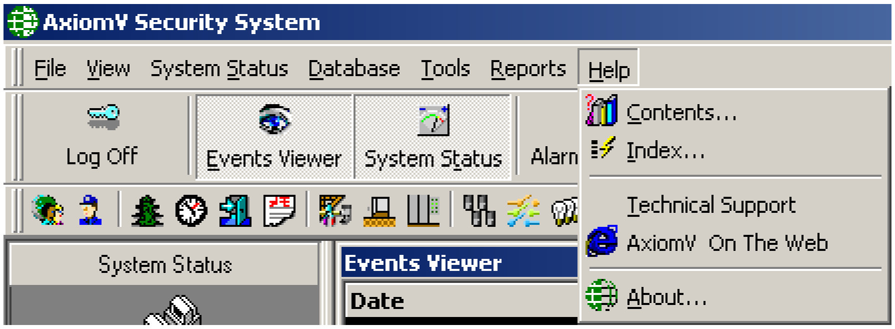
- Access Level Report
- Access Point Group Report
- Access Point Report
- Apartments Report
- Area Report
- CardHolder High Security Read
- CardHolder Link Report
- CardHolder Lock Unlock Reade
- CardHolder Readers Report
- CardHolder Report
- CardHolder Simple Report
- Company Report
- Device Controller Report
- Elevators Groups Report
- Elevators Report
- Facility Codes Report
- Global Commands Report
- Holiday Report
- Input Group Report
- Input Report

☑ Select All

Information on how to create Custom Database Reports is given on page 341 of Chapter 8.

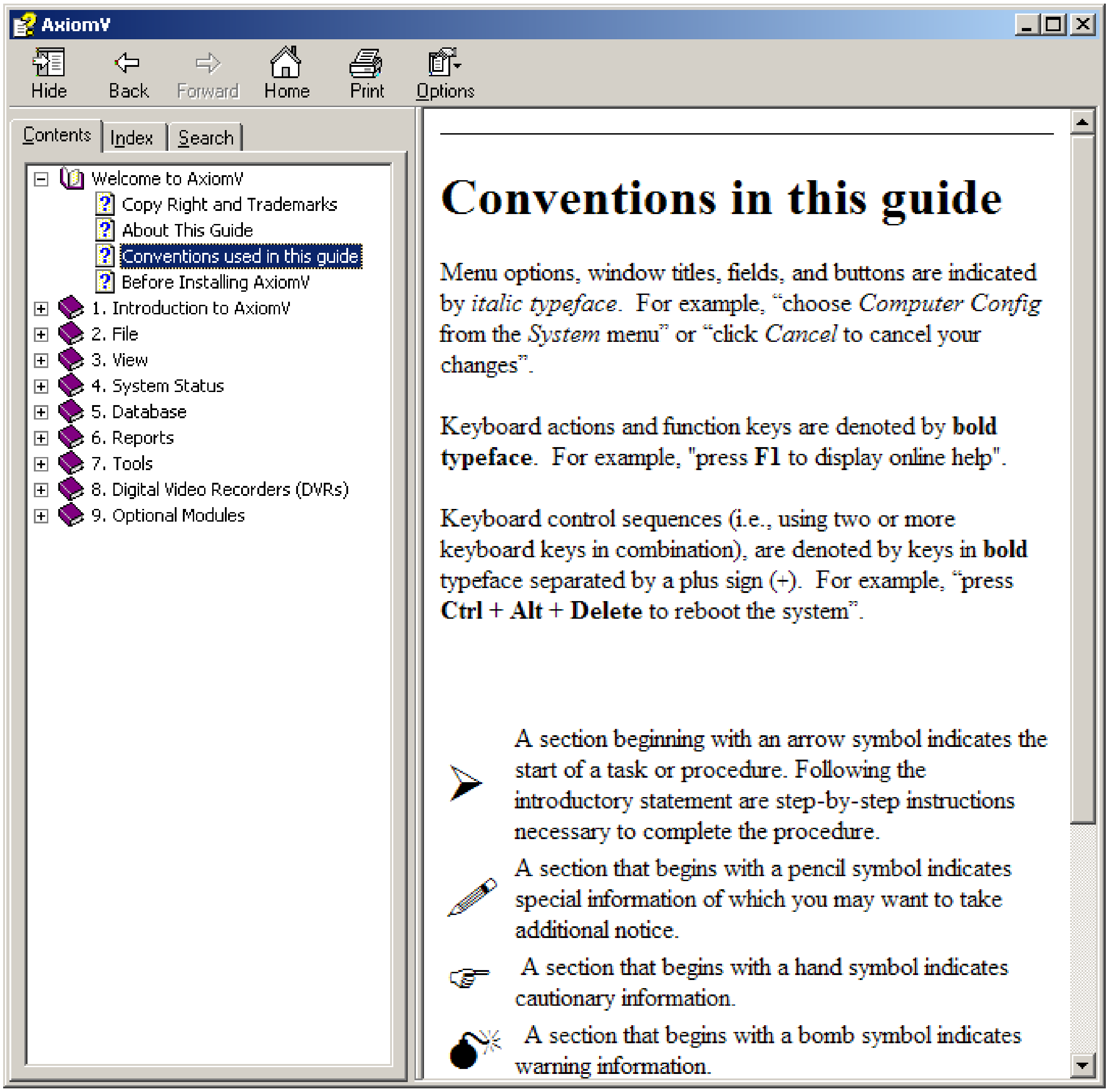
[7] Licence is required for enabling Designer in Database Reports

Help



Pressing **F1** while in the program will bring up a portion of the Help Utility relating to the current screen.

Contents…



Conventions in this guide

Menu options, window titles, fields, and buttons are indicated by *italic typeface*. For example, "choose *Computer Config* from the *System* 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".

➢ A section beginning with an arrow symbol indicates the start of a task or procedure. Following the introductory statement are step-by-step instructions necessary to complete the procedure.

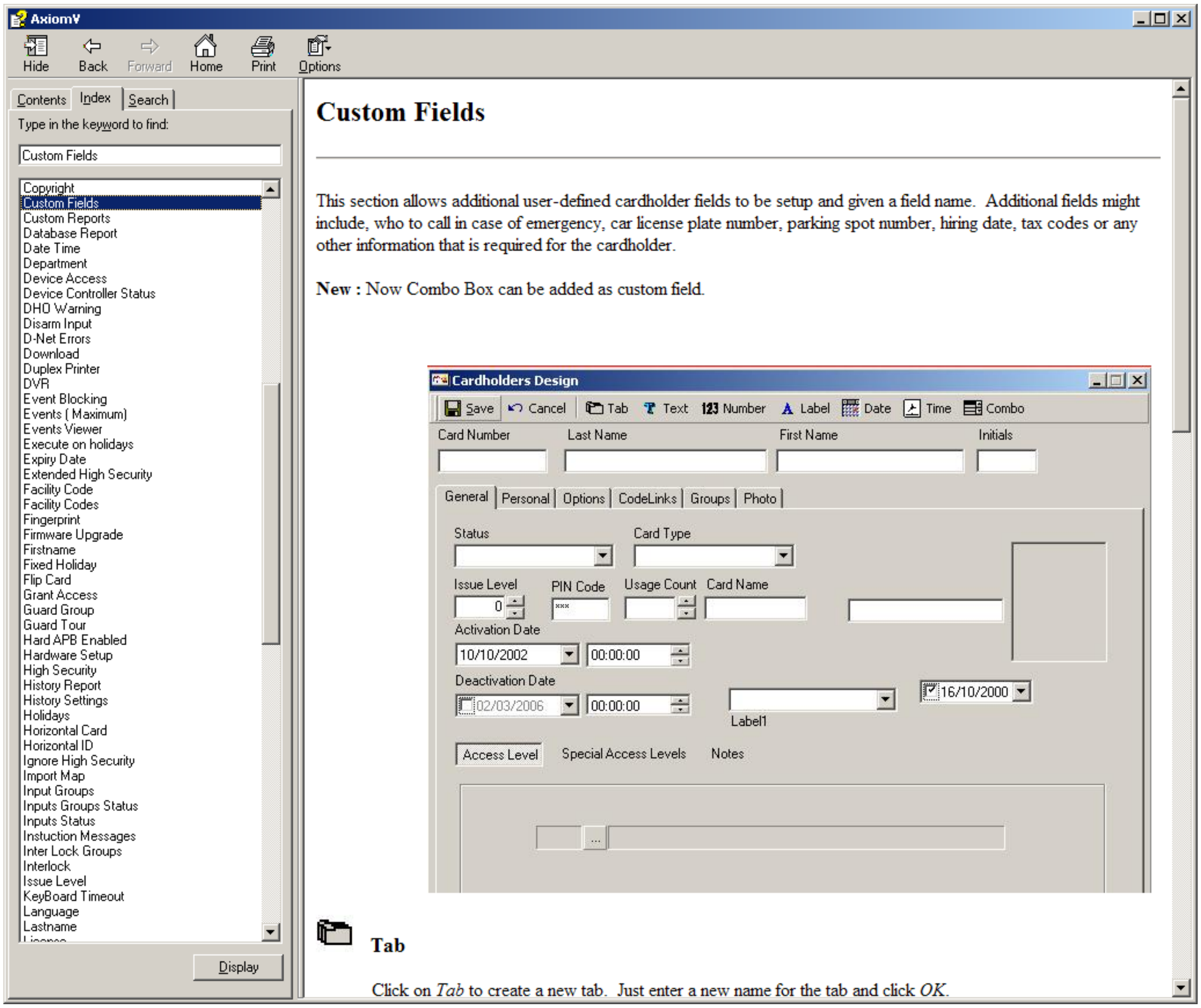
✎ A section that begins with a pencil symbol indicates special information of which you may want to take additional notice.

☞ A section that begins with a hand symbol indicates cautionary information.

💣 A section that begins with a bomb symbol indicates warning information.

Contents will take you into the online help.

Index…



Type in the keyword to find:

Custom Fields

Copyright
Custom Fields
Custom Reports
Database Report
Date Time
Department
Device Access
Device Controller Status
DHO Warning
Disarm Input
D-Net Errors
Download
Duplex Printer
DVR
Event Blocking
Events (Maximum)
Events Viewer
Execute on holidays
Expiry Date
Extended High Security
Facility Code
Facility Codes
Fingerprint
Firmware Upgrade
Firstname
Fixed Holiday
Flip Card
Grant Access
Guard Group
Guard Tour
Hard APB Enabled
Hardware Setup
High Security
History Report
History Settings
Holidays
Horizontal Card
Horizontal ID
Ignore High Security
Import Map
Input Groups
Inputs Groups Status
Inputs Status
Instuction Messages
Inter Lock Groups
Interlock
Issue Level
KeyBoard Timeout
Language
Lastname

Custom Fields

This section allows additional user-defined cardholder fields to be setup and given a field name. Additional fields might include, who to call in case of emergency, car license plate number, parking spot number, hiring date, tax codes or any other information that is required for the cardholder.

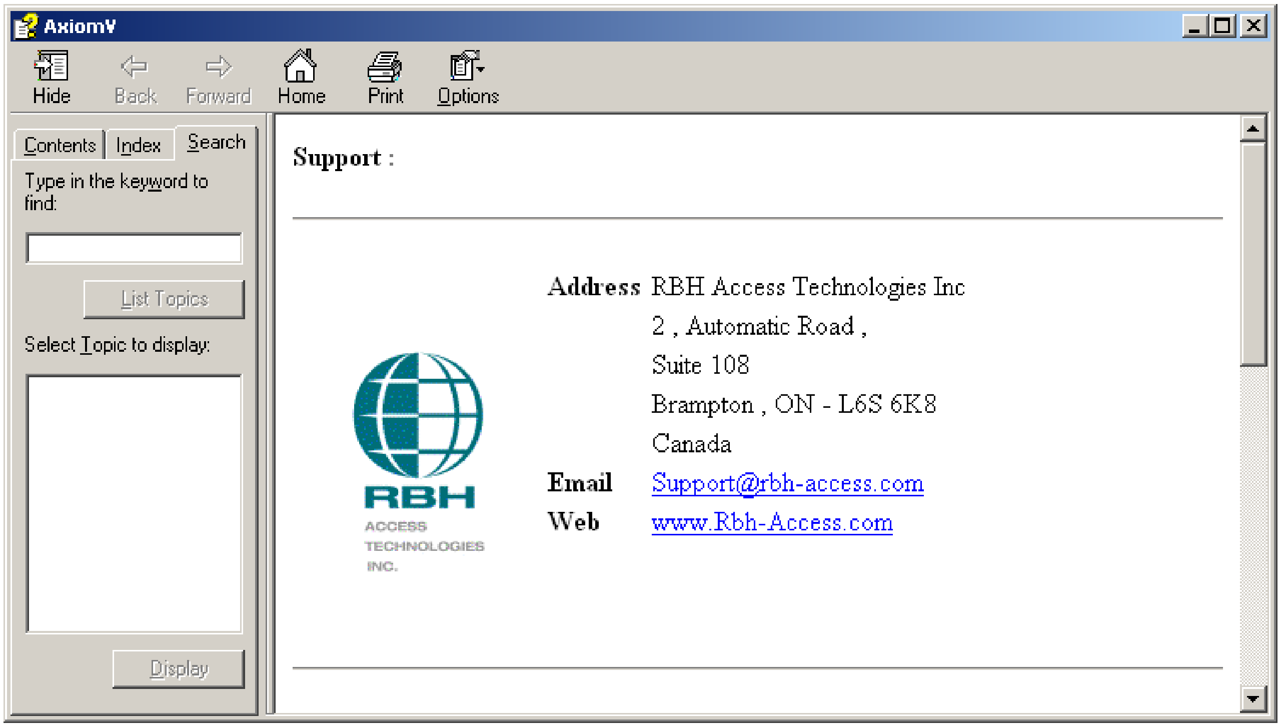
New : Now Combo Box can be added as custom field.

Tab

Click on *Tab* to create a new tab. Just enter a new name for the tab and click *OK*.

Index will take you into the online help.

Technical Support



Support :

Address RBH Access Technologies Inc
2 , Automatic Road ,
Suite 108
Brampton , ON - L6S 6K8
Canada

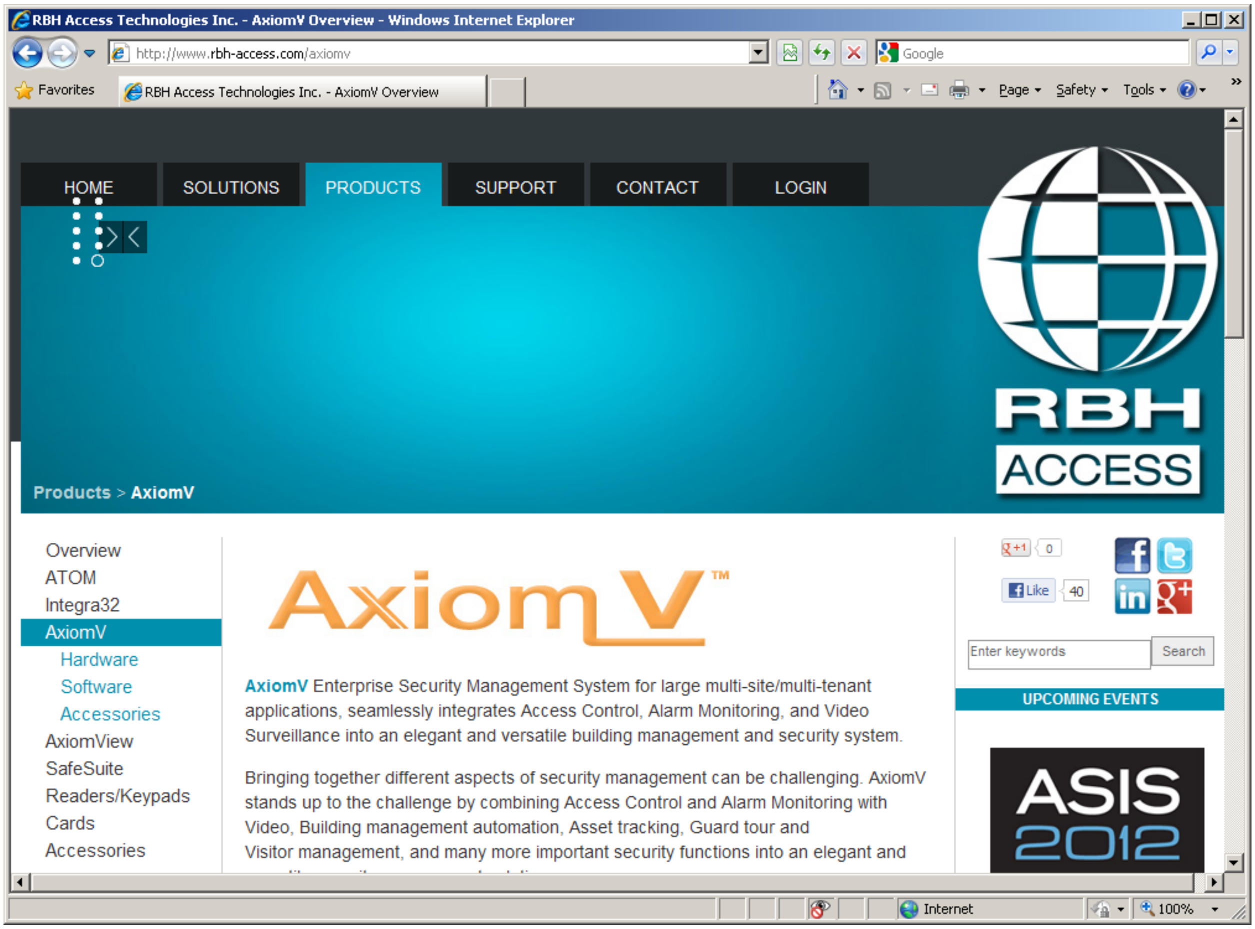
Email Support@rbh-access.com

Web www.Rbh-Access.com

Clicking support brings up a window that has information on how to contact RBH for technical support.

AxiomV™ on the Web

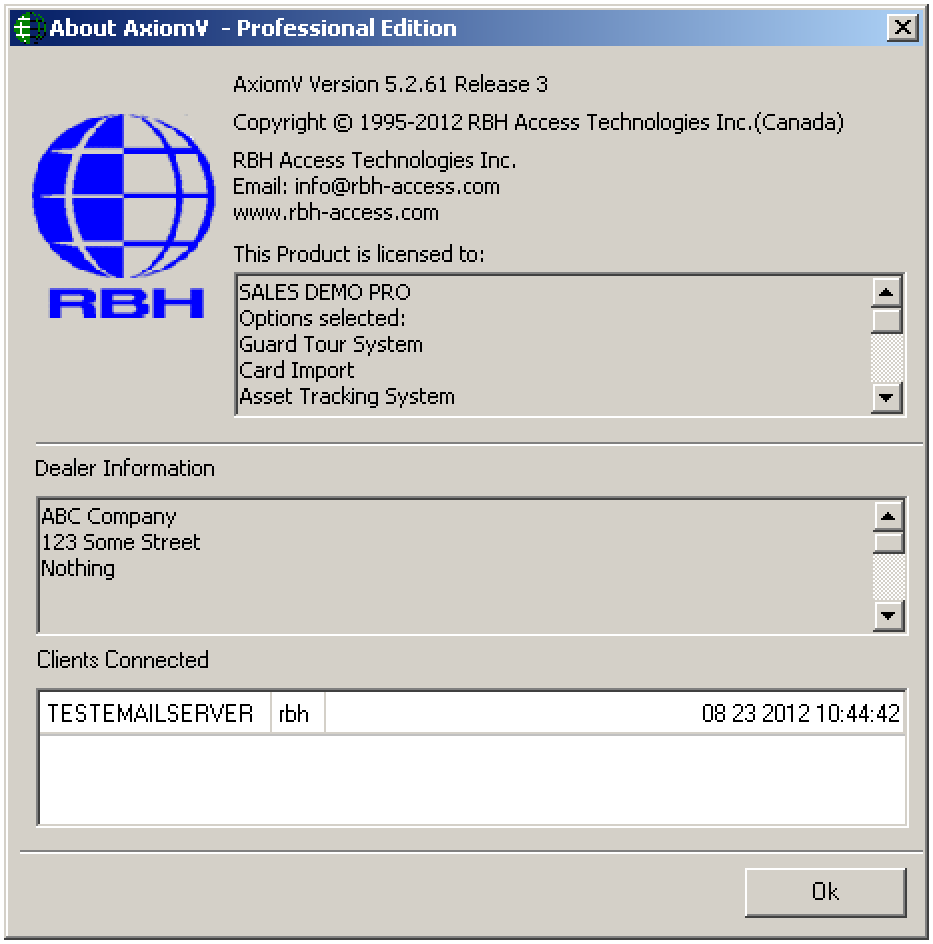
Clicking here will launch the Internet Explorer and take you to the RBH web site.



AxiomV Enterprise Security Management System for large multi-site/multi-tenant applications, seamlessly integrates Access Control, Alarm Monitoring, and Video Surveillance into an elegant and versatile building management and security system.

Bringing together different aspects of security management can be challenging. AxiomV stands up to the challenge by combining Access Control and Alarm Monitoring with Video, Building management automation, Asset tracking, Guard tour and Visitor management, and many more important security functions into an elegant and

About…



AxiomV Version 5.2.61 Release 3

Copyright © 1995-2012 RBH Access Technologies Inc.(Canada)

RBH Access Technologies Inc.
Email: info@rbh-access.com
www.rbh-access.com

This Product is licensed to:

SALES DEMO PRO
Options selected:
Guard Tour System
Card Import
Asset Tracking System

Dealer Information

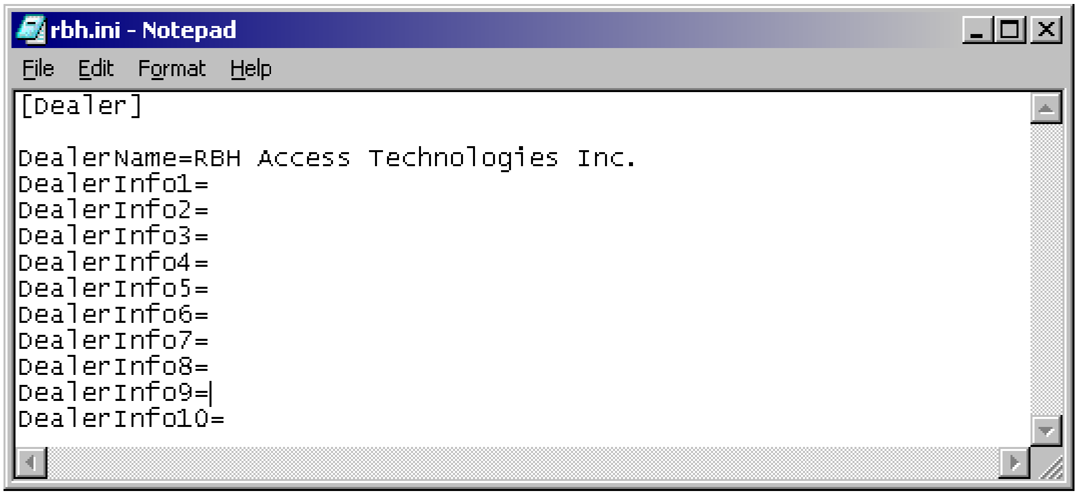
ABC Company
123 Some Street
Nothing

Clients Connected

TESTEMAILSERVER	rbh	08 23 2012 10:44:42

This window will display the current version of the software.

To input information into the 'Dealer Information' box create a notepad file called "rbh.ini" **<u>as shown below</u>** **and save it in the 'bin' folder under AxiomV™. (*Enter your company's name in place of "RBH Access Technologies Inc."*). You can also add an additional ten lines to your dealer information.**



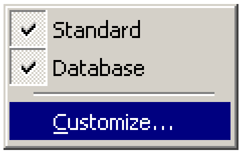
```
[Dealer]

DealerName=RBH Access Technologies Inc.
DealerInfo1=
DealerInfo2=
DealerInfo3=
DealerInfo4=
DealerInfo5=
DealerInfo6=
DealerInfo7=
DealerInfo8=
DealerInfo9=
DealerInfo10=
```

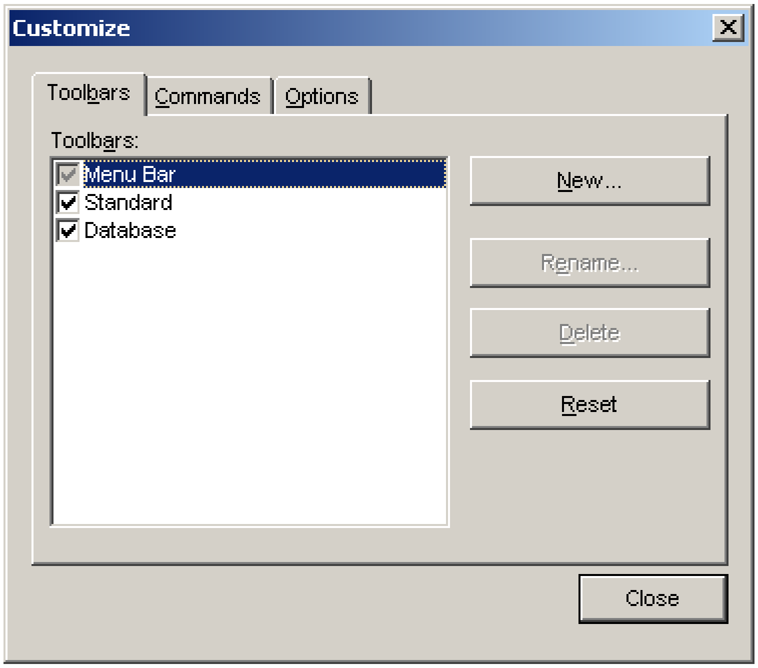
The bottom part of the screen provides information about all the axiom clients connected at that time and also the time client logged on and connected to the server.

Toolbars

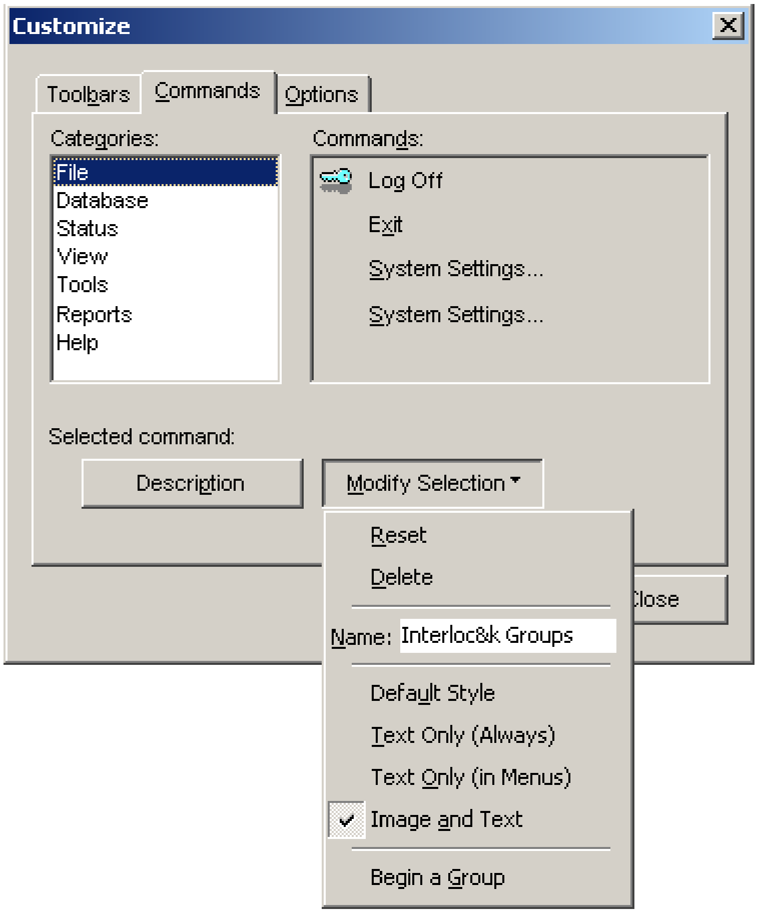
AxiomV™ has customizable toolbars. Items can be added to or removed from the standard toolbar. As well additional toolbars can be added. Any selection from any menus can be added to any toolbar.



Right click in an open space of the menu or toolbar and a menu will pop up. Click to uncheck or check the availability of the listed toolbars. Click *Customize…* to open the customization window.

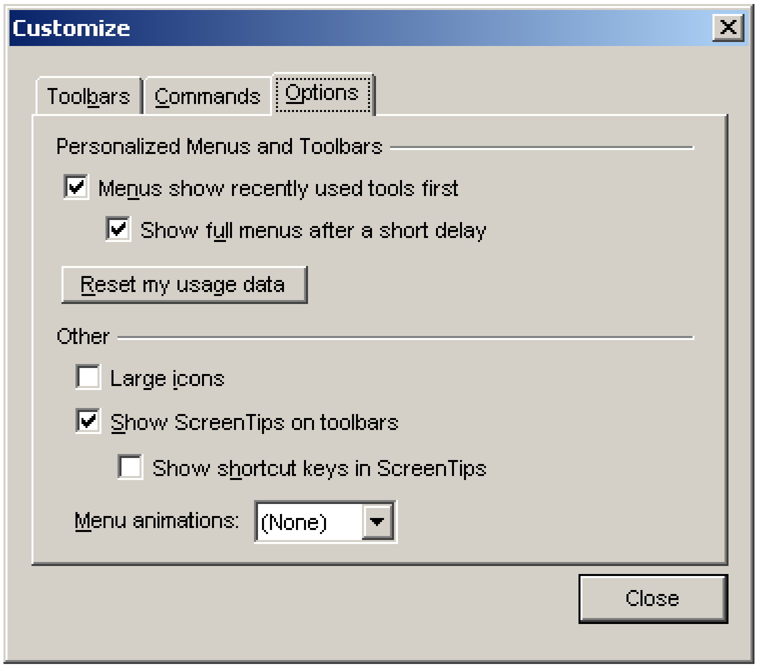


The *Customize* window has three tabs. The *Toolbars* tab is where new toolbars can be added, existing toolbars can be renamed or reset to their default settings, or non-required toolbars can be deleted.



From the *Commands* tab items can be added to the toolbars. Make a selection from the *Categories* on the left, *Commands* will be shown on the right. Simply click and drag the appropriate command to its desired location on a toolbar.

Select a button on a toolbar and click *Modify Selection* or you can right click on the button. The menu revealed is used to modify the button itself. You can choose from image only (*Default Style*), text only, or both (*Image and Text*). *Reset* will change the button's setting back to their default values, and *Delete* will remove the button from the toolbar. Dragging a button off of a toolbar will also remove it. *Name* will give you the true name of the button while *Description* will show the displayed name. *Begin a Group* inserts a separator to the left of the button.



Customize

Toolbars | Commands | Options

Personalized Menus and Toolbars

☑ Menus show recently used tools first

☑ Show full menus after a short delay

Reset my usage data

Other

☐ Large icons

☑ Show ScreenTips on toolbars

☐ Show shortcut keys in ScreenTips

Menu animations: (None)

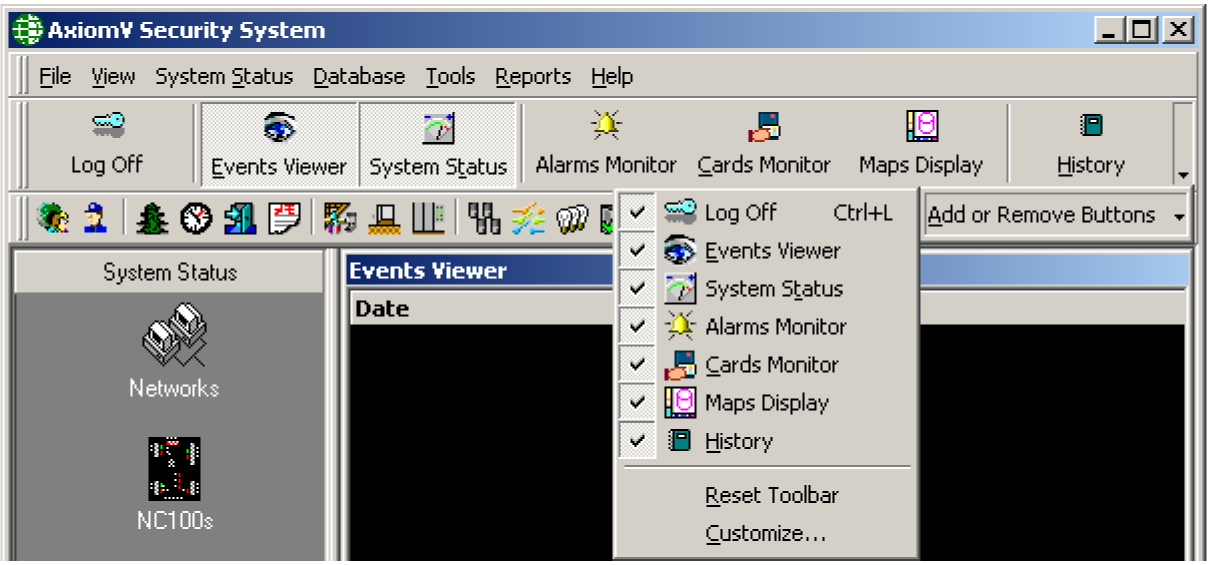
Close

Select from:

- ☑ Menus show recently used tools first.
  - ☑ Show full menus after a short time.
- ☑ Large Icons.
- ☑ Show Screen Tips on toolbars.
  - ☑ Show shortcut keys in Screen Tips.

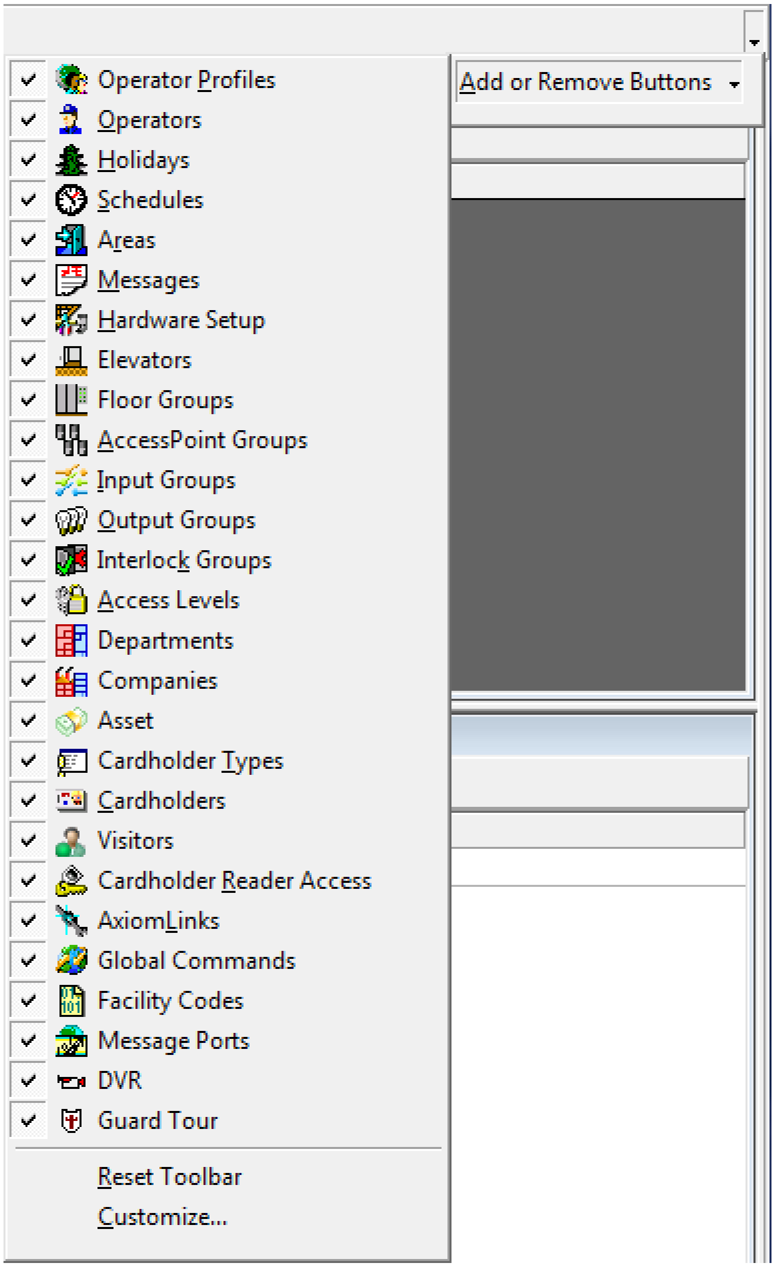
Menu animation can be set as None, Random, Unfold, Slide, Explode, or FadeIn.

Add or Remove Buttons



Only the two default toolbars will have the feature to add or remove buttons. There is a pull-down indicator (▾) at the end of the standard or database toolbars, click on it. Move your cursor over the *Add or Remove Buttons* selection to open a list of buttons that can be easily added or removed. Simply click to check or uncheck selections. Buttons added under *Customize* will show on the list but will be grayed-out to show that they can only be changed under *Customize*.

Customize will open the same window as show above on page 134. *Reset Toolbar* will restore the selected toolbar back to default settings the same as the *Reset* selection under *Customize* does.

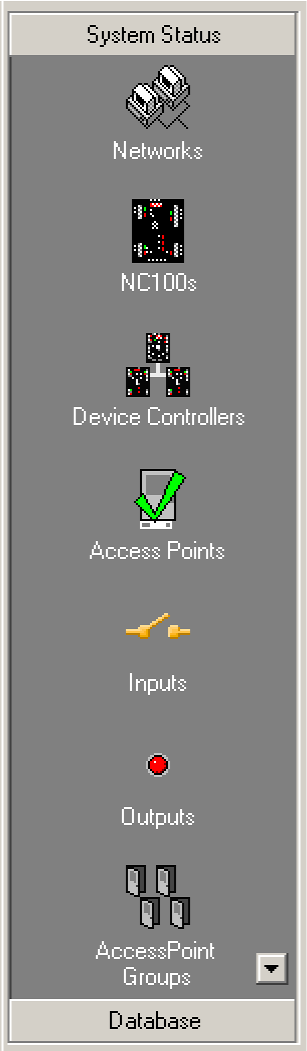


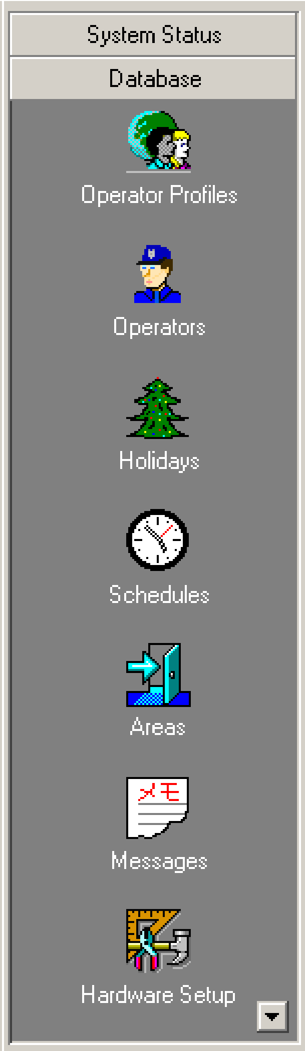
Module Selector

The Module Selector has two tabs, *System Status* and *Database*. Under *System Status* the operator can select which category of items to display in the *System Status Pane*. The list of choices is the same as the list in the *System Status* menu: Networks, NC100s, Device Controllers, Access Points, Inputs, Outputs, Access Point Groups, Input Groups, and Output Groups.

The Database tab gives the operator access to all the database modules available from the Database menu. These include, Cardholders, Access Levels, Operators, Database Profiles, Schedules, Holidays, Areas, Messages, AxiomLinks™, Facility Codes, Access Point Groups, Input Groups, Output Groups, and Hardware Setup.

To switch from *System Status* items to *Database* items click the 'Database' box at the bottom of the *Module Selector*. The *Database* box will move up and the database items will be displayed. To switch back to *System Status* items from *Database* items click the 'System Status' box at the top of the *Module Selector*. The *Database* box will move down and the system status items will be displayed.



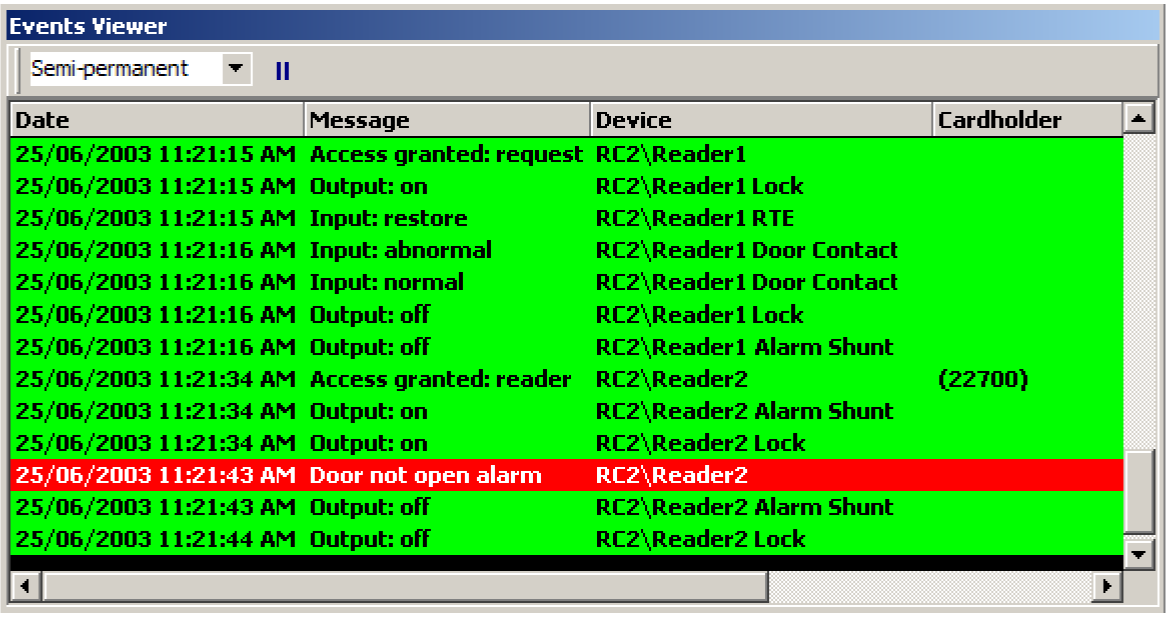


▲ ▼ The scroll up and down buttons will reveal more selections if there isn't enough room to display all of the choices on the screen.

Status Bar

The *Status Bar* will display the name of the logged on operator. It also displays alarms count, total items loaded on system status pane and current date and time.

Events Viewer

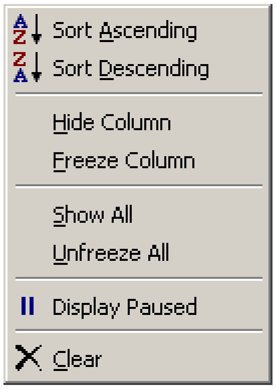


Date	Message	Device	Cardholder
25/06/2003 11:21:15 AM	Access granted: request	RC2\Reader1	
25/06/2003 11:21:15 AM	Output: on	RC2\Reader1 Lock	
25/06/2003 11:21:15 AM	Input: restore	RC2\Reader1 RTE	
25/06/2003 11:21:16 AM	Input: abnormal	RC2\Reader1 Door Contact	
25/06/2003 11:21:16 AM	Input: normal	RC2\Reader1 Door Contact	
25/06/2003 11:21:16 AM	Output: off	RC2\Reader1 Lock	
25/06/2003 11:21:16 AM	Output: off	RC2\Reader1 Alarm Shunt	
25/06/2003 11:21:34 AM	Access granted: reader	RC2\Reader2	(22700)
25/06/2003 11:21:34 AM	Output: on	RC2\Reader2 Alarm Shunt	
25/06/2003 11:21:34 AM	Output: on	RC2\Reader2 Lock	
25/06/2003 11:21:43 AM	Door not open alarm	RC2\Reader2	
25/06/2003 11:21:43 AM	Output: off	RC2\Reader2 Alarm Shunt	
25/06/2003 11:21:44 AM	Output: off	RC2\Reader2 Lock	

The *Event Viewer* displays the messages of events as they happen. These events are also logged to history for later retrieval. Which messages are displayed can be set for each operator.

The top messages can be locked so that scrolling up and down will not affect them. Move your curser to the line between the headers and the top message. When the curser changes (to╪), click and hold the left mouse button. Then drag the line down to include all the lines to be locked (all messages above the line will not move during scrolling). To remove the lock drag the dividing line back up above the top message.

Right click a header in the event window to bring out the pop-up menu as shown below. Other pop-up menus will appear when you right click on a specific message. The menu items will correspond to the device in the selected message.



Sort Ascending

Click on *Sort Ascending* to sort the selected header ascending. Events in the monitor screen now appear sorted with the lowest value at the top.

Sort Descending

Click on *Sort Descending* to sort the selected header descending. Events in the monitor screen now appear sorted with the highest value at the top.

Hide Column

Use *Hide Column* to hide the selected column from view, so that unnecessary information does not take up space on the monitor screen. Hidden columns can be brought back when their data becomes relevant again.

Freeze Column

Freeze Column is used to lock columns. These columns include the selected column and any columns to its left. Locked columns will not shift with left and right scrolling. The line separating the locked and non-locked columns can be shifted. Just click and drag the line to move it. Look for the curser to change (to) indicating the ability to move the dividing line.

Show All

To display all hidden columns, click on *Show All*. Showing only some columns is not directly possible. To achieve the same end result, unhide all columns and hide again the columns not required.

Unfreeze All

Unfreeze All will shift the column lock dividing line all the way to the left, thereby unlocking all columns.

Pause Display

New messages are always added to the bottom of the log display, and the log display is moved to show these messages as they come in. Select this option to hold the display on the desired messages and not automatically move to show the new messages just added.

Clear

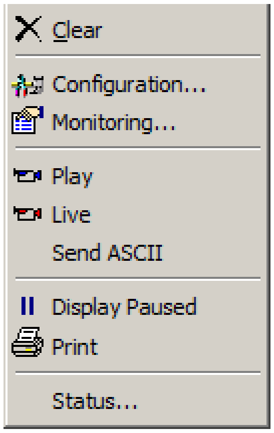
Click here to permanently clear all events from the monitor screen, and to begin accumulating new events. Once events have been cleared, they will only be accessible through history reports.

Event Viewer Commands

Pop-up menus will appear when you right click on a specific event message. The menu items will correspond to the device in the selected message.

Standard Commands

Standard Commands are commands that are common to all items, although some commands are only available if the option has been configured. Where applicable commands can be executed as permanent, semi-permanent, or timed.



Clear

Click here to permanently clear all events from the event viewer screen. Once events have been cleared, they will only be accessible through history reports.

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information is given in Chapter 7 Database.

Monitoring…

In *Monitoring*, alarms can be set to trigger, messages can be blocked and/or sent out as ASCII messages, and the status icons for the item can be changed.

Play

Selecting *Play* will start DVR playback for the selected item starting from the time stamp of the selected event. DVR and cameras must be configured for this command to function.

Live

Selecting *Live* will start live play of a camera configured for the selected item.

Send ASCII

Send ASCII will activate the message module for the selected item. This option must be configured for the item for the command to appear in the menu.

Pause Display

New messages are always added to the bottom of the log display, and the log display is moved to show these messages as they come in. Select this option to hold the display on the desired messages and not automatically move to show the new messages just added.

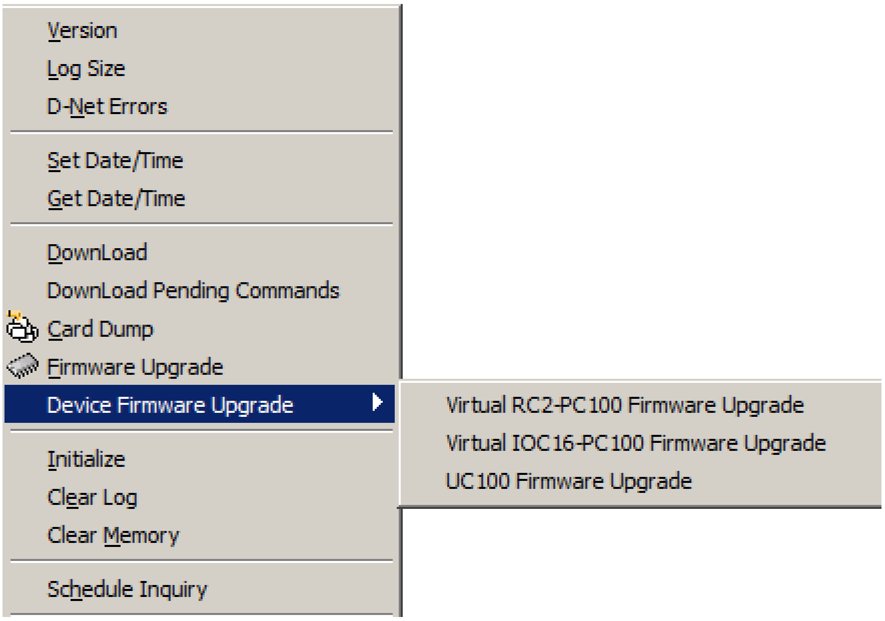
Print

Use *Print* to produce a printout of the current status of all selected items.

Status…

Status will bring up a status window as shown in System Status AccessPoints, see page 179.

NC-100 Commands



Version

Version will return the firmware version of the selected NC100/UNC500.

Log Size

Log Size will return the amount of memory the selected NC100/UNC500 has to store event messages when it is not connected to the PC.

D-Net Errors

D-Net Errors will return the error count window for that NC100/UNC500.

Set Date/Time

Set Date/Time is used to set the date and time for the selected NC100/UNC500.

Get Date/Time

Get Date/Time: will return the current date and time in the selected NC100/UNC500.

Download

Download: will download all the files on the selected NC100/UNC500. Download server service should be started for download to work.

Download Pending Commands

Download Pending Commands: will execute the pending commands immediately on the selected, NC100/UNC500, otherwise system takes care of them at 1:30AM. Download server service should be started for this functionality to work.

Card Dump

Card Dump: is functionality available just for the first NC100/UNC500 on the network. This utility shows all the binary information about the card read on any reader connected on the devices of first NC100/UNC500.

Firmware Upgrade

Firmware Upgrade: is used to upgrade firmware on selected NC100/UNC500

Device Firmware Upgrade

Device Firmware Upgrade: is used to upgrade firmware on the devices connected on D-Net of the selected NC100/UNC500

Initialize

Initialize will initialize the microprocessor of the selected NC100/UNC500.

Clear Log

Clear Log will delete all messages from the selected NC100/UNC500's log buffer.

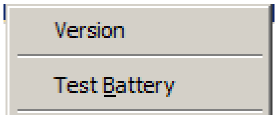
Clear Memory

Clear Memory will remove all data in the selected NC100/UNC500's RAM. This will include all database files and log messages.

Schedule Inquiry

Schedule Inquiry will return the status of all schedules for the selected NC100/UNC500.

RC-2 / IOC-16 /Keypad Commands



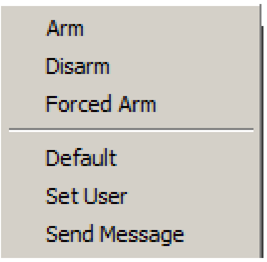
Version

Version will return the firmware version of the selected device RC2/IOC16/Keypad.

Test Battery

Test Battery is used to immediately have the battery tested on the selected device. This command is available only for RC2 and IOC16.

SafeSuite™ Commands



Arm

Arm will arm the keypad of the selected apartment.

Disarm

Disarm will disarm the keypad of the selected apartment.

Forced Arm

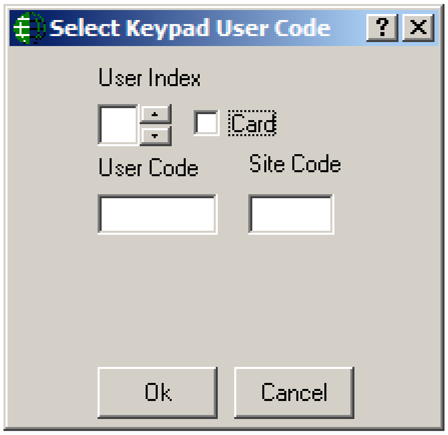
Forced Arm will arm the keypad of the selected apartment even though one or more zones are in violation.

Default

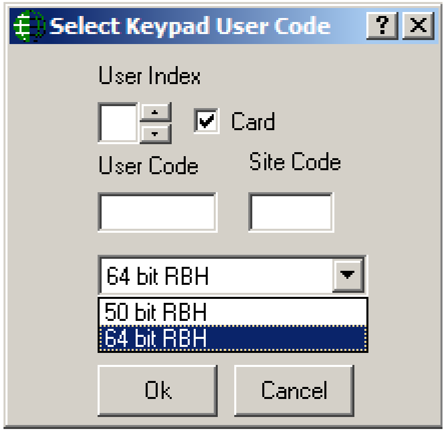
This selection will reset the user codes of the panel back to default. User 1 is reset back to 1234 and the other seven are cleared.

Set User

The user codes can be set up for the keypad of the selected apartment.

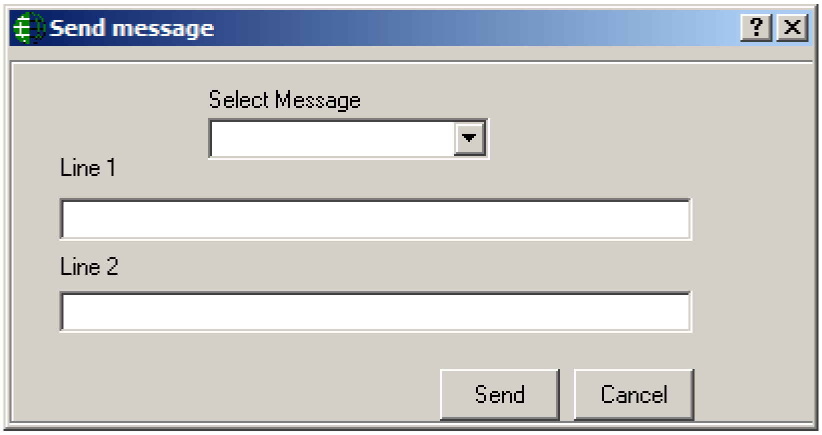


Cards for the specific formats can also be setup on the keypad of the selected apartment.

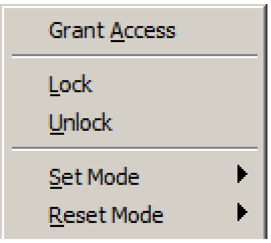


Send Message

This button will pop up a small screen so that you can enter a text message to be sent to the Liquid Crystal Display of the panel. (See Send Message in *Apartments* for more details.)



Access Points Commands



Grant Access

Grant Access will grant access at all selected access points.

Lock

Lock will lock at all selected access points.

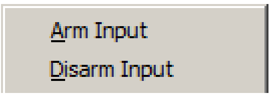
Unlock

Unlock will unlock at all selected access points.

Set Mode and Reset Mode

Set Mode and Reset Mode are used to turn on or off different modes (High Security, Two Person, Door Held Open, Interlock, Request to Exit Disabled, Hard Antipassback Enabled, and Facility Code) on the selected access points.

Input Commands



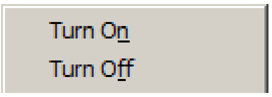
Arm Input

Arm Input is used to arm the selected input.

Disarm Input

Disarm Input is used to disarm the selected input.

Outputs Commands



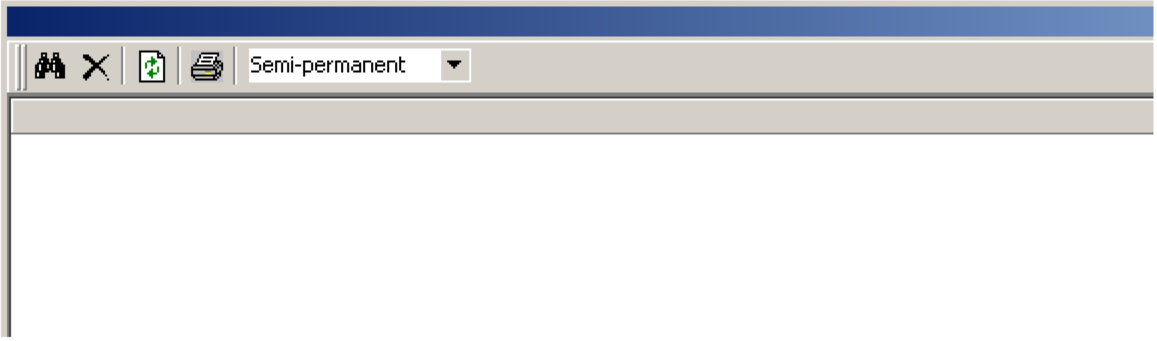
Turn On

Turn On will turn all selected outputs on.

Turn Off

Turn Off will turn all selected outputs off.

System Status Pane



The *System Status Pane* will display the current status of items from a selected group (inputs, outputs, access points, etc.). Operators can also send commands to the items displayed here as well as edit their configuration and monitoring parameters. Commands can be sent to a single item or a group of items. Highlight the desired items then right click on one of them to bring up the command menu. Clicking on a command will cause it to be executed for all highlighted items.

Use *Search* to display the required items.

Use *Clear* to remove any highlighted items that are no longer required.

Use *Refresh* to update the status of highlighted items.

Use *Print* to produce a printout of the status of all highlighted items.

System Status Commands Menus

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. This is where the properties of the item can be changed. Detailed information on the properties windows is given in Chapter 7 starting on page 196.

Monitoring…

Monitoring is where alarms and ASCII messages are configured. Status icon for the item can be changed here as well. More information on *Monitoring* is provided below.

Status…

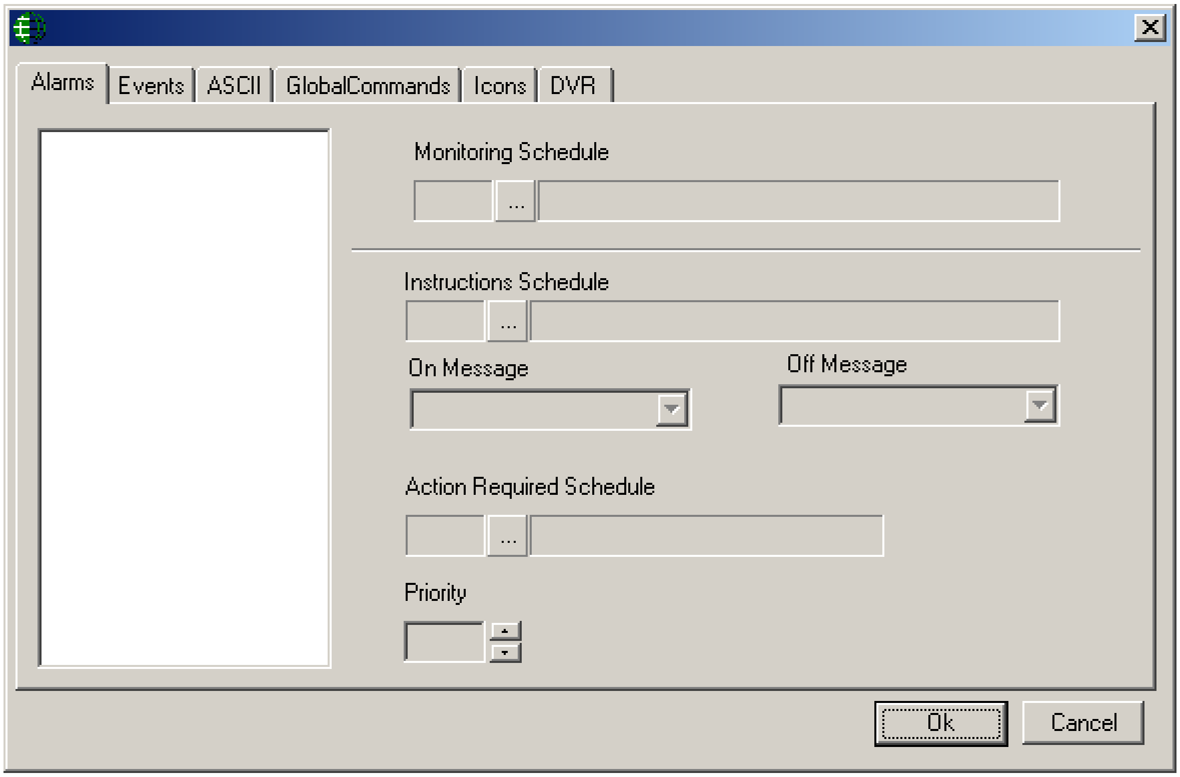
The Status selection will bring up a detail status window for the selected item. More information is given on the detail windows in Chapter 6 starting on page 165.

Other menu selections for each item will be detailed in Chapter 6.

Monitoring

Each item has its own list of events. From this list each item can be selected and have the following parameters set.

Please note that not all tabs will be applicable for every item. Only the applicable tabs for the item will be provided, and all tabs are shown here for reference purposes.



Alarms

Monitoring Schedule

Use the *Browse/Ellipsis button* to select the *Schedule* during which this event is added to the *Alarm Queue*.

Instruction Schedule

Use the *Browse/Ellipsis button* to select the *Schedule* during which this event will display an instruction message in the *Alarm Detail Window* of this event.

On Message

Select from the pull down list an instruction message to be displayed when the schedule is on.

Off Message

Select from the pull down list an instruction message to be displayed when the schedule is off.

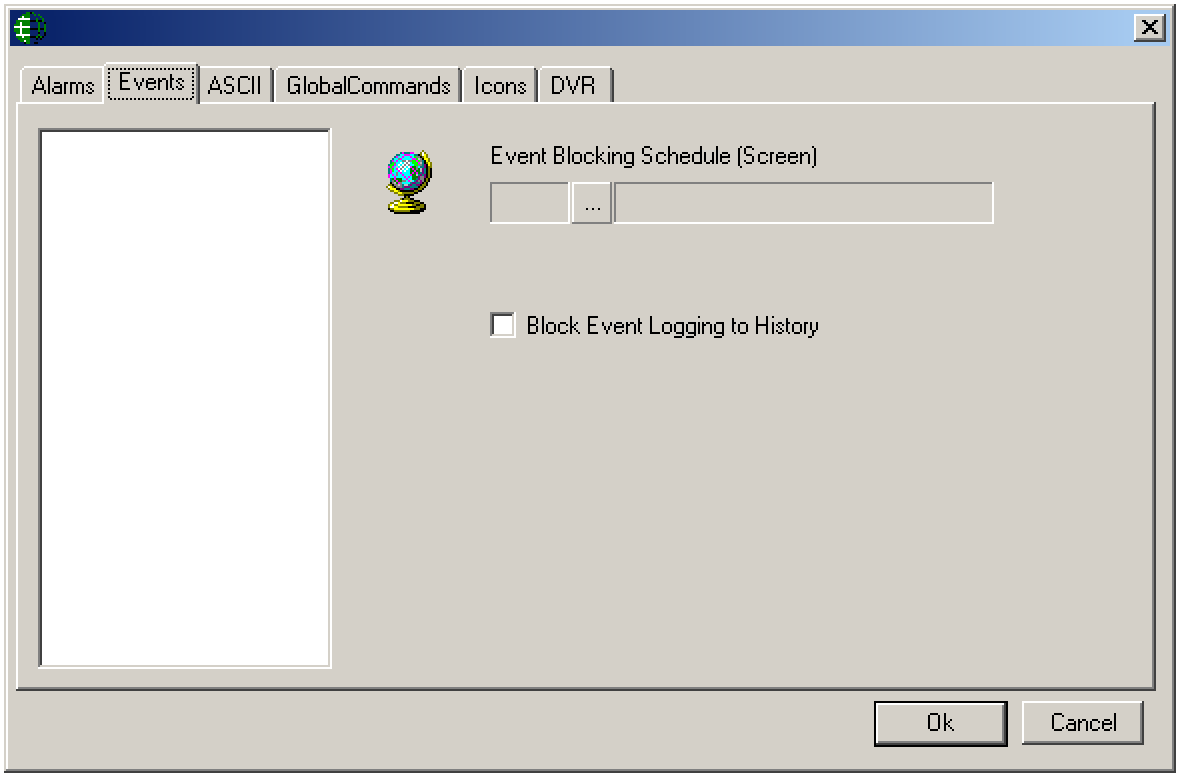
Action Required Schedule

Use the *Browse/Ellipsis button* to select the *Schedule* during which this *Alarm Event* can only be cleared if data has been entered into its *Action* box.

Priority

Give this *Alarm Event* a priority from 1 to 99.

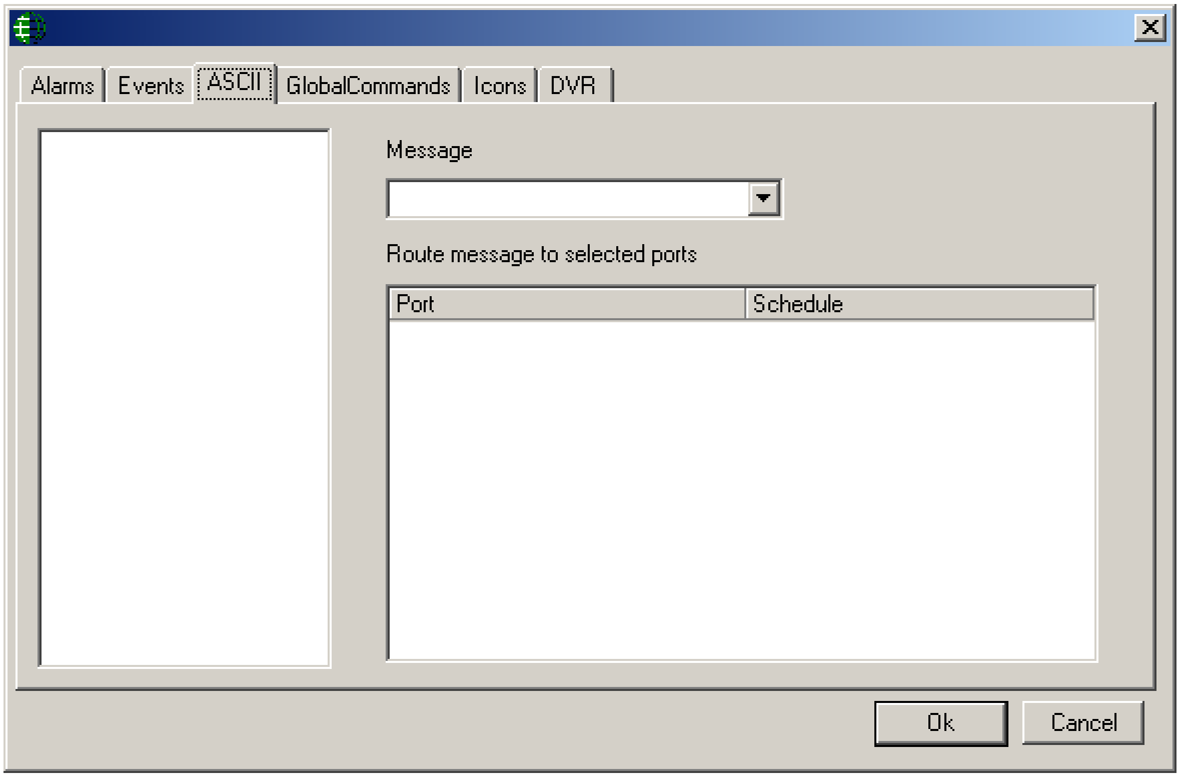
Events


Alarms
Events
ASCII
GlobalCommands
Icons
DVR
Event Blocking Schedule (Screen)
...
Block Event Logging to History
Ok
Cancel

Event Blocking Schedule

Use the *Browse/Ellipsis button* to select the *Schedule* during which this item will not display messages on the *Event Viewer*.

ASCII

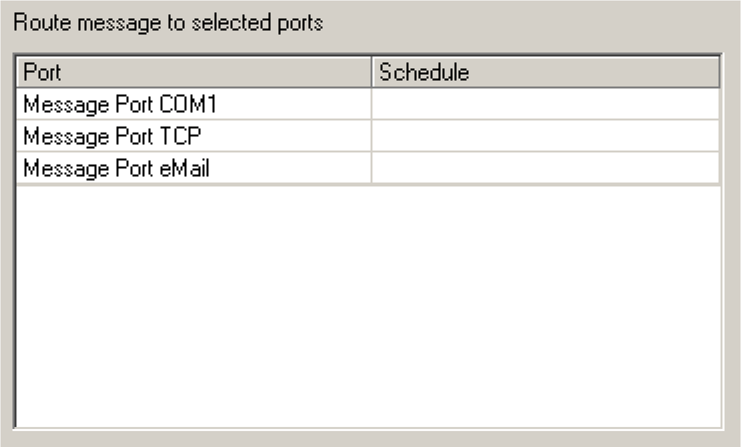


ASCII Message

Select from the pull down list an ASCII message to be transmitted when the event occurs.

Port Type

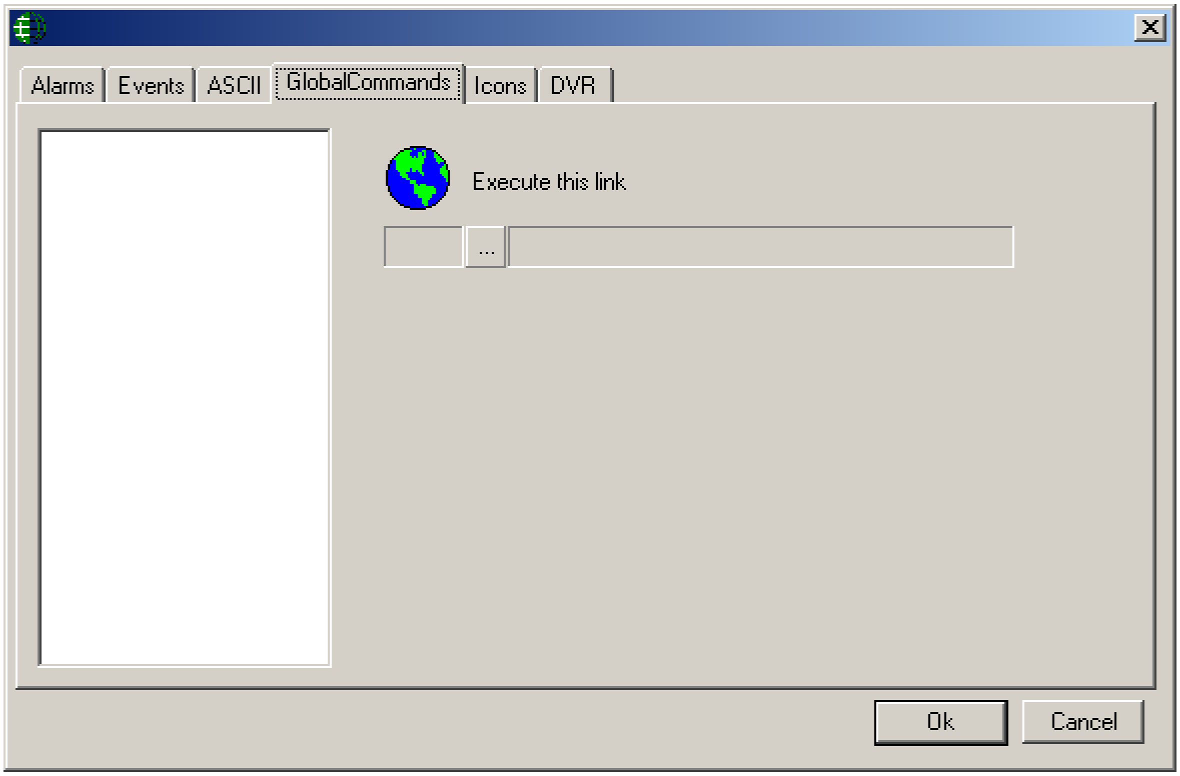
After selecting the message to be sent, select the method of sending that message from the list provided. You can send out the message from different ports, each on its own schedule.



Route message to selected ports

Port	Schedule
Message Port COM1	
Message Port TCP	
Message Port eMail	

Global Commands



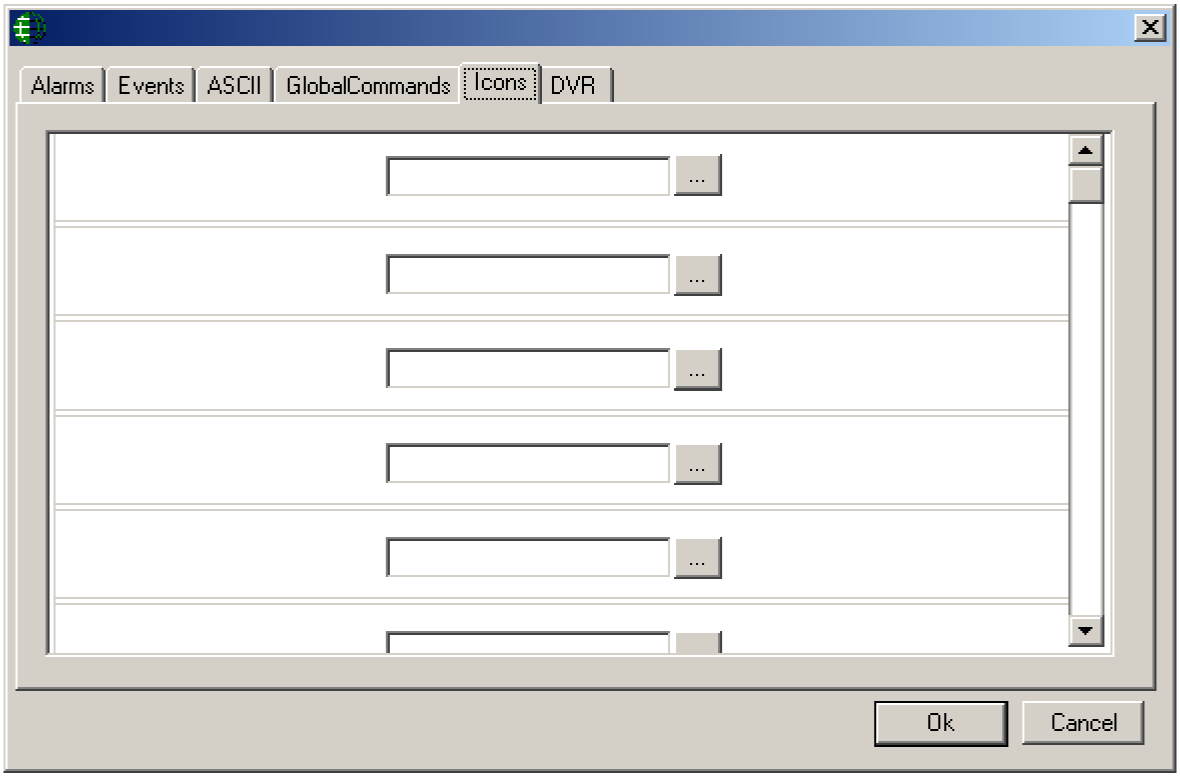
Execute this link

Select an event then click the Browse/Ellipsis button to find the link to be executed when the chosen event occurs

***Global Commands* are executed by the *CommsServer*. The event that triggers the link (*Global Command*) must be on a network connected to the same**

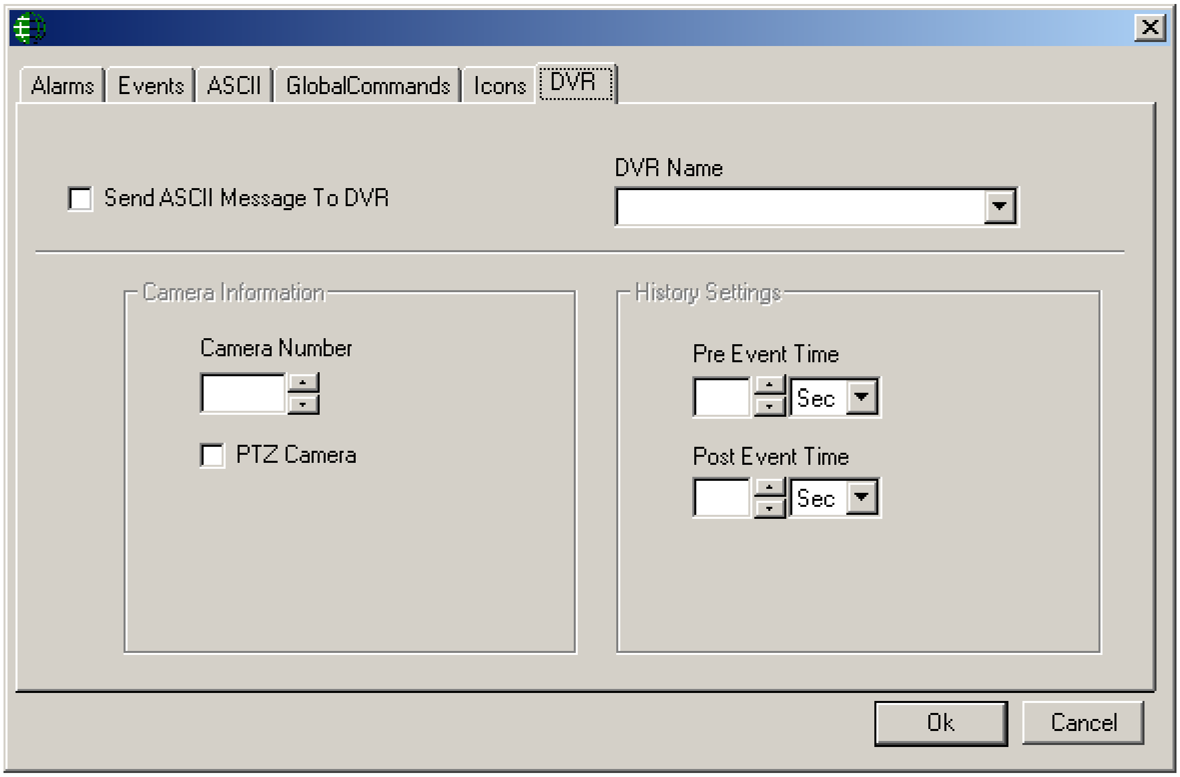
***CommsServer* that the network on which the link is being executed on is connected to.**

Icons



Click the Browse/Ellipsis button to change the status icon for the selected event. Some icons are provided with the system or you can create your own.

DVR



Send ASCII Message to DVR

With '*Send ASCII Message to DVR*' not selected the system can send messages to a known DVR to playback a camera associated with a specific device.

DVR Name

Select a DVR from the pull-down menu.

Camera Information

Camera Number

Enter the camera number associated with the chosen item that is attached to the above DVR. The video from this camera is to be played back to view alarms associated with this item.

☑ PTZ Camera

Check here if this camera is mounted with Pan/Tilt/Zoom capability. PTZ cameras can be controlled with the DVR module.

History Settings

Pre Event Time:

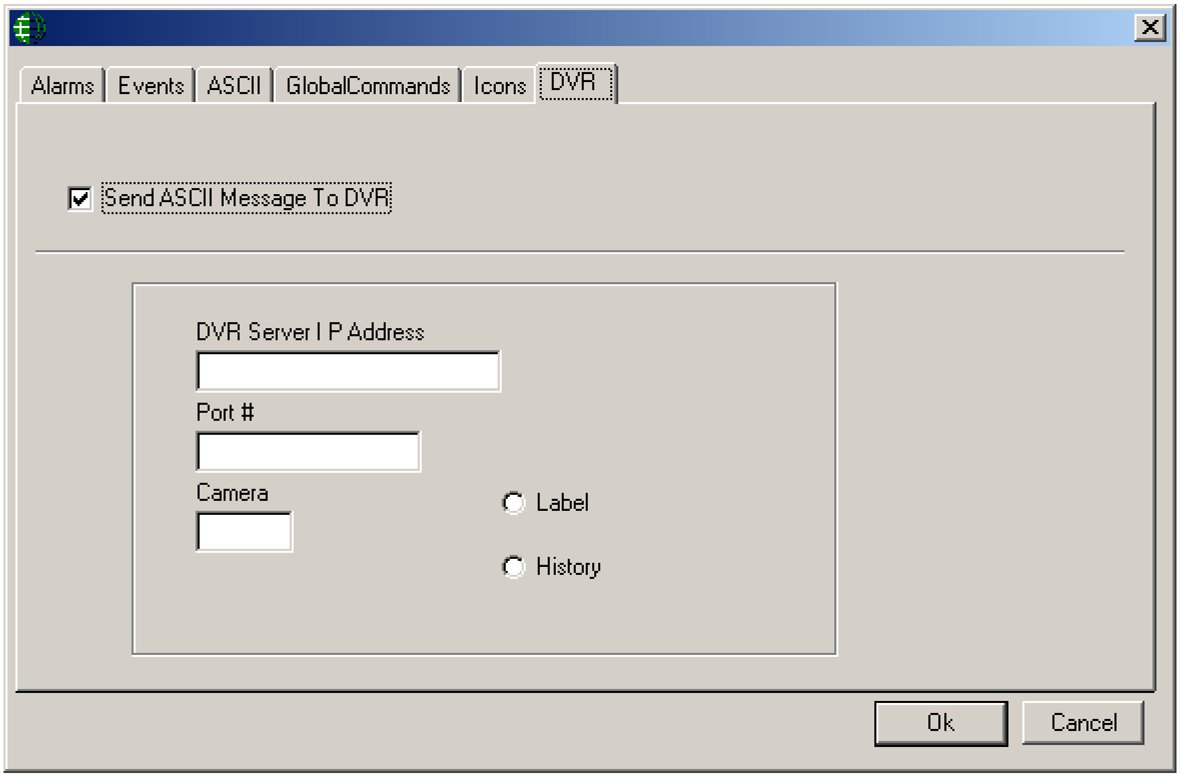
For history playback from a DVR the *Pre Event Time* is the amount of time before the Event's time. A five second *Pre Event Time* will start the playback five seconds before the event.

Post Event Time:

The *Post Event Time* is how long the playback will run from the Event's time. A fifty-five second *Post Event Time* means that; the playback will continue for fifty-five seconds after the time of the event.

☑ Send ASCII Message to DVR

Checking *Send ASCII Message to DVR* configures the system so that ASCII messages can be sent to the DVR. ASCII messages are messages created by the user. (For information on ASCII messages see *Messages* on page 214.)



DVR Server IP Address

Enter the IP Address of the DVR associated with the chosen item.

Port

Enter the Port Number for the above IP address of the DVR.

Camera

Enter the camera number associated with the chosen item that is attached to the above DVR. The video from this camera is to be played back to view alarms associated with this item.

◉ Label

When label is selected the *Alarm Event* message is sent to the DVR along with the time and date of the event, and the camera number. The DVR then plays back that camera from that time/date displaying the Alarm event message on the video screen.

◉ History

When *History* is selected, only the time and date of the event, and the camera number are sent to the DVR. The DVR then plays back that camera from that time/date.

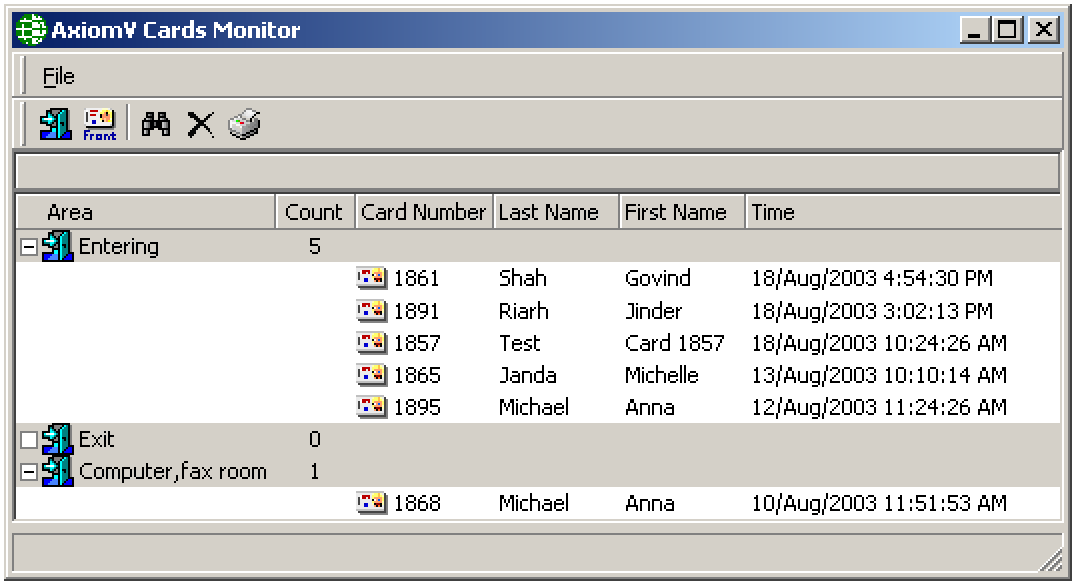
More details on System Status are provided in Chapter 6 on page 165.

Cards Monitor

The *Cards Monitor Screen* will display cardholders (*First Name*, *Last Name*, and *Card Number*), the area the cardholder is in, the last reader the cardholder presented their card to, and the time they presented their card at that reader. The system first has to have areas created and access points need to be configured with those areas before this information can be displayed.

Areas

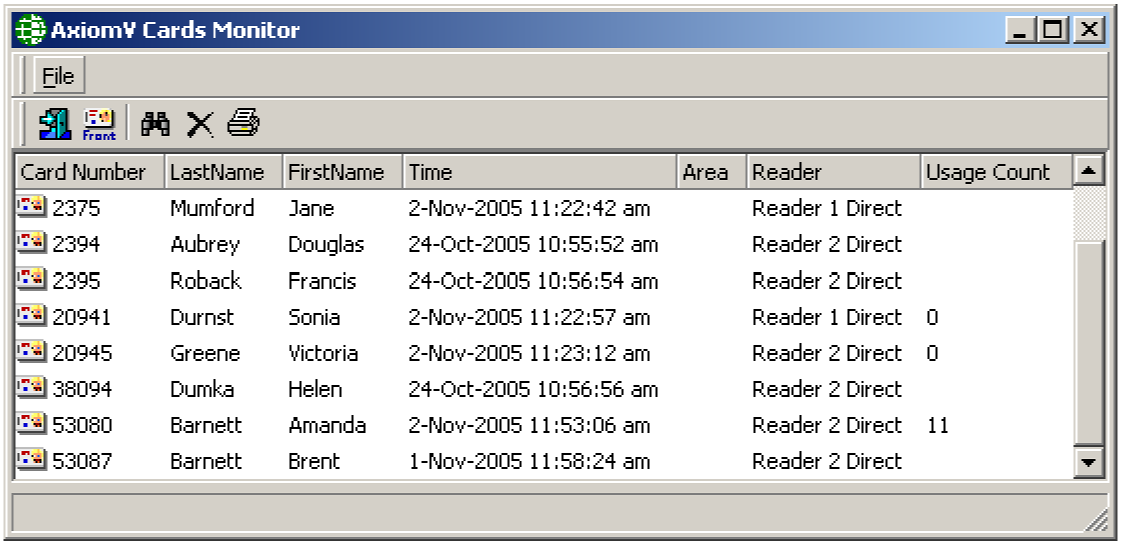
Cardholders can be selected and sorted by *Areas*, as chosen in the *Search Window*.



Area	Count	Card Number	Last Name	First Name	Time
⊟ Entering	5				
		1861	Shah	Govind	18/Aug/2003 4:54:30 PM
		1891	Riarh	Jinder	18/Aug/2003 3:02:13 PM
		1857	Test	Card 1857	18/Aug/2003 10:24:26 AM
		1865	Janda	Michelle	13/Aug/2003 10:10:14 AM
		1895	Michael	Anna	12/Aug/2003 11:24:26 AM
□ Exit	0				
⊟ Computer,fax room	1				
		1868	Michael	Anna	10/Aug/2003 11:51:53 AM

Cards

Display cardholders from the selection made in the *Search Window*

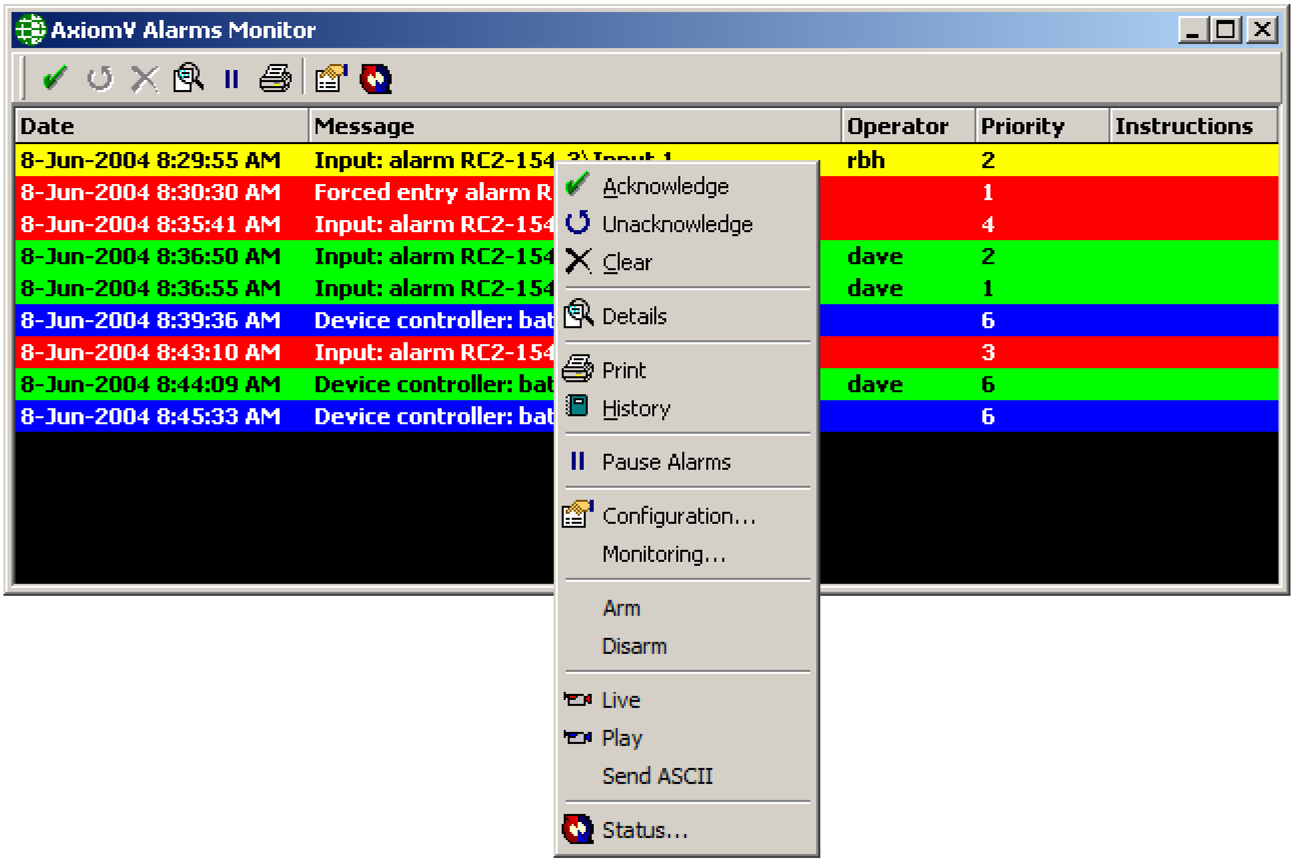


Card Number	LastName	FirstName	Time	Area	Reader	Usage Count
2375	Mumford	Jane	2-Nov-2005 11:22:42 am		Reader 1 Direct	
2394	Aubrey	Douglas	24-Oct-2005 10:55:52 am		Reader 2 Direct	
2395	Roback	Francis	24-Oct-2005 10:56:54 am		Reader 2 Direct	
20941	Durnst	Sonia	2-Nov-2005 11:22:57 am		Reader 1 Direct	0
20945	Greene	Victoria	2-Nov-2005 11:23:12 am		Reader 2 Direct	0
38094	Dumka	Helen	24-Oct-2005 10:56:56 am		Reader 2 Direct	
53080	Barnett	Amanda	2-Nov-2005 11:53:06 am		Reader 2 Direct	11
53087	Barnett	Brent	1-Nov-2005 11:58:24 am		Reader 2 Direct	

Alarms Monitor

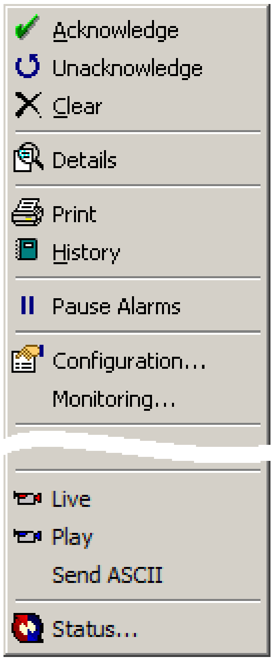
The *Alarms Monitor Screen* will list all of the Alarms to be acknowledged and cleared. Alarms are events that are significant enough to require operator intervention. (E.g. a 'Door Held Open Alarm' might not be important enough to require the attention of the operator.) Access Point and Input states with the word 'alarm' in then are not necessarily Alarm events. Which events are Alarms is set in *Monitoring* of each individual item.

The Alarm Monitoring screen will maintain its view when an alarm is selected so that new alarms coming in won't affect the operator's ability to handle the selected alarm.



Date	Message	Operator	Priority	Instructions
8-Jun-2004 8:29:55 AM	Input: alarm RC2-154 3\ Input 1	rbh	2	
8-Jun-2004 8:30:30 AM	Forced entry alarm R		1	
8-Jun-2004 8:35:41 AM	Input: alarm RC2-154		4	
8-Jun-2004 8:36:50 AM	Input: alarm RC2-154	dave	2	
8-Jun-2004 8:36:55 AM	Input: alarm RC2-154	dave	1	
8-Jun-2004 8:39:36 AM	Device controller: bat		6	
8-Jun-2004 8:43:10 AM	Input: alarm RC2-154		3	
8-Jun-2004 8:44:09 AM	Device controller: bat	dave	6	
8-Jun-2004 8:45:33 AM	Device controller: bat		6	

Standard Commands



✓ Acknowledge

Acknowledge is the first step in handling Alarms. All queued Alarms must be acknowledged to turn off the Alarms' audible, if selected. Acknowledged Alarms will be shown in green or yellow, depending upon if Alarm shown on monitor in the first place was in blue or red.

Unacknowledge

Only the operator that *acknowledged* an Alarm can *clear* the Alarm. Therefore in order to change operators, an Alarm must first be unacknowledged, so that another operator can acknowledge it.

✕ Clear

Clear is the final step in handling Alarms. When an Alarm is cleared all data pertaining to that Alarm is saved. Alarm reports can be generated from the *History Reports Screen*.

Acknowledge All

Acknowledge All acknowledges all the unacknowledged alarms in Alarm Monitor

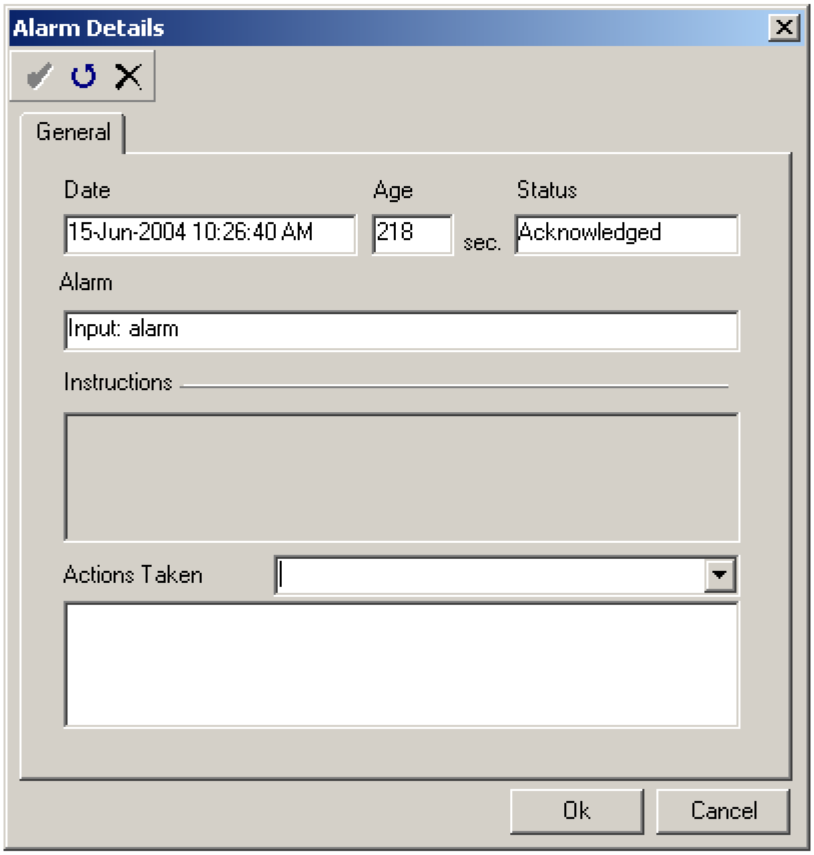
Clear All

Clear All clears all the acknowledged alarms in Alarm Monitor.

Only the operator that acknowledged the alarm can clear the alarm. It is important therefore that an operator is not deleted if that operator has outstanding acknowledged alarms, as other operators won't be able to clear the alarms (not even by re-creating the operator). Therefore, the later versions of AxiomV™ doesn't let you delete an operator if it has outstanding acknowledged alarms in Alarm monitor.

Details

Alarm Details provides a place where instruction messages can be located. It also provides a space for the operator to enter what action was taken in regards to this Alarm. Instruction and Action messages are included in the *Alarm Report*.



Alarm Details

Date: 15-Jun-2004 10:26:40 AM

Age: 218 sec.

Status: Acknowledged

Alarm: Input: alarm

Instructions

Actions Taken

An Alarm can be acknowledged, unacknowledged, or cleared from the *Details Window*.

Print

Use *Print* to produce a printout of selected alarms.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

Pause Alarms

Like the *Events Viewer* the *Alarm Monitor Screen* shifts down to the bottom of the queue to display all new incoming alarms/messages. *Pause Alarms* will freeze the *Alarm Screen* view so that this won't happen. Incoming alarms will not then hinder the operator from handling alarms that already exist in the queue.

Configuration…

Configuration will call up the configuration window for the device associated with the selected alarm event.

Monitoring…

Monitoring will call up the monitoring window for the device associated with the selected alarm event.

Live

Selecting *Live* will start live play of a camera configured for the selected item.

Play

Selecting *Play* will start DVR playback for the selected item starting from the time stamp of the selected event. DVR and cameras must be configured for this command to function.

Send ASCII

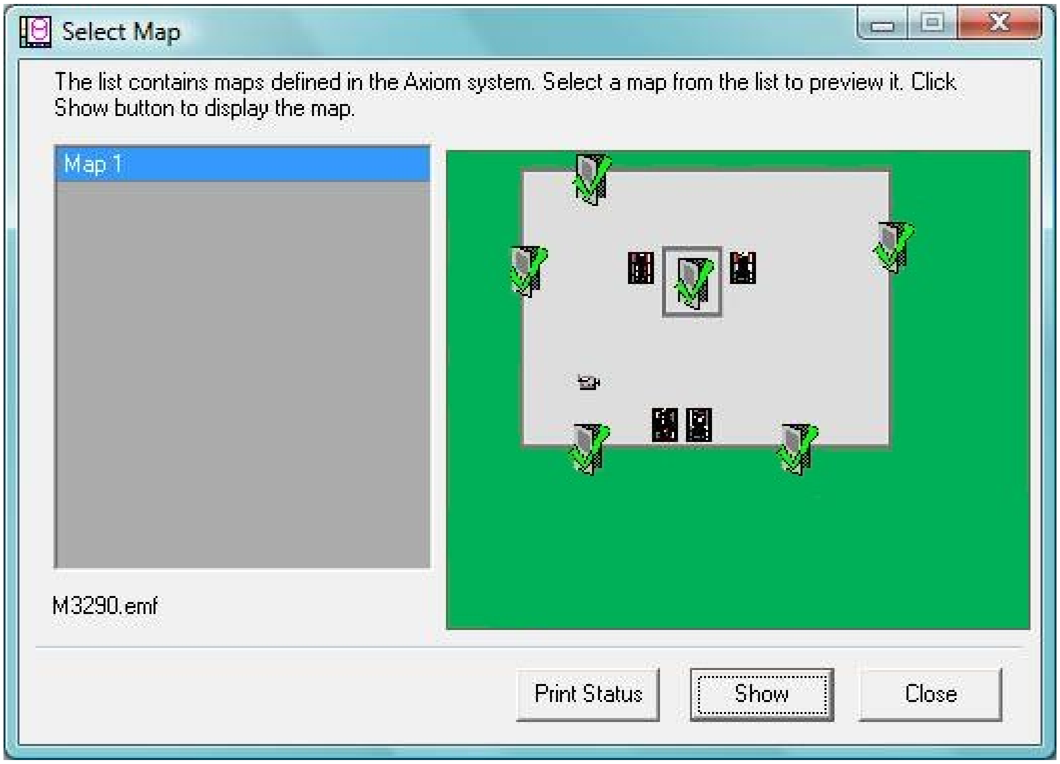
Send ASCII will trigger the sending of the appropriate ASCII message for the selected alarm. This option will only show up for items that have previously been programmed for *ASCII Messages*.

Status…

Status will call up the detail status window for the device associated with the selected alarm event.

Maps Display

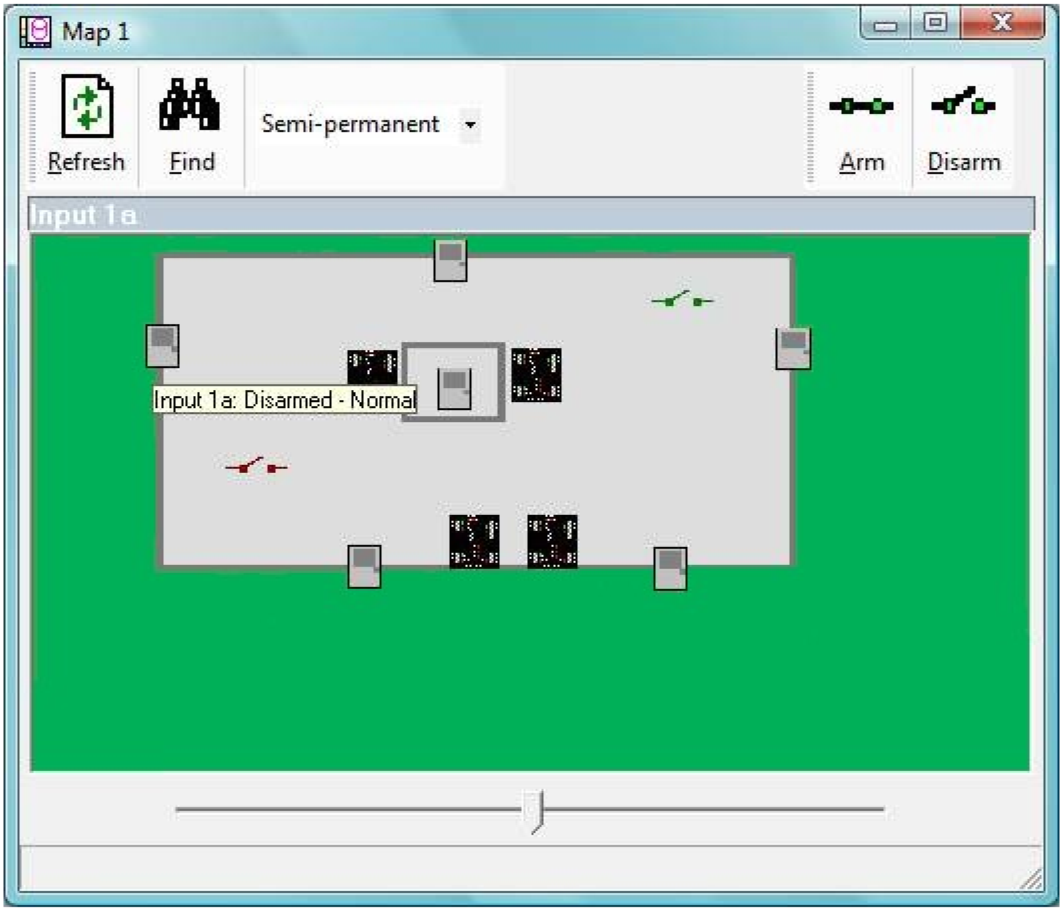
The *Maps Display* can provide a graphical view of system status. Maps are first created in *MapMaker* to display specific items in a graphic view.



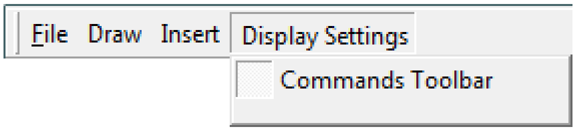
The list contains maps defined in the Axiom system. Select a map from the list to preview it. Click Show button to display the map.

M3290.emf

Click on *Maps Display* and select one of the maps from the list by highlighting the map's name and clicking *Show*.

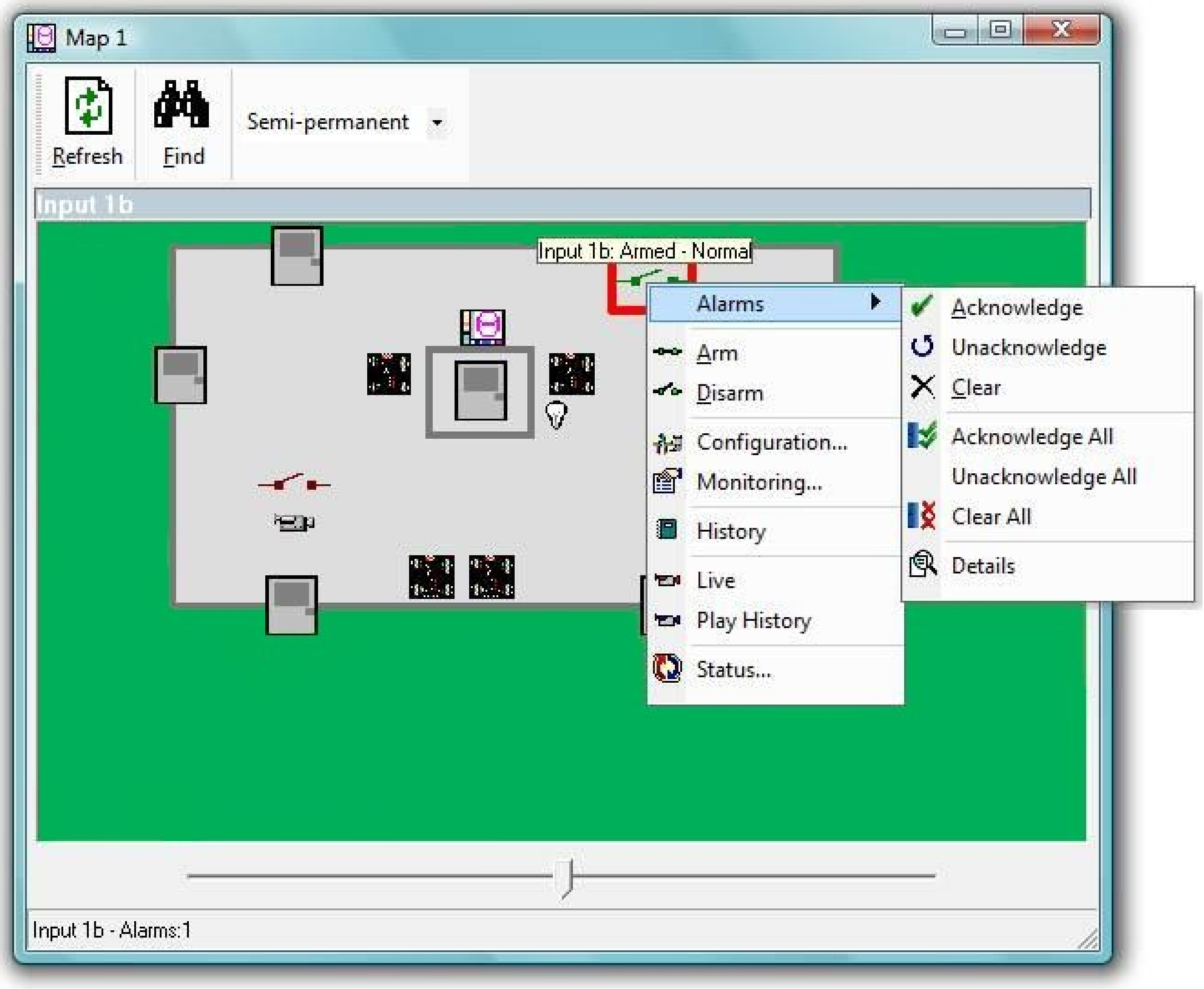


Icons for each item will change as that item’s status changes. You can also **right-click** on an icon and the system will produce a command list. The commands for each item are listed in Chapter 6 System Status.



If *Commands Toolbar* is activated the associated commands for an icon will appear on top of the map in the toolbar. Only the last selected icon’s commands will be on the toolbar.

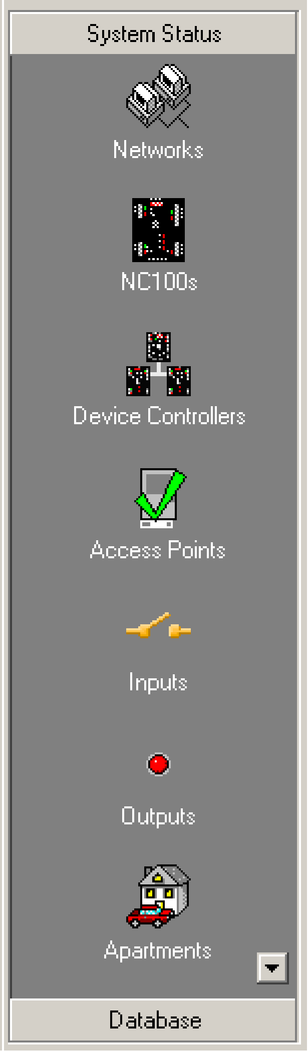
Alarms can also be handled from the *Maps Display*. A red box will appear around the item in alarm. **Right-click** on the icon and the command list will include alarm handling selections (acknowledge, unacknowledged, and clear). Alarm handling is not available from the *Commands Toolbar*.

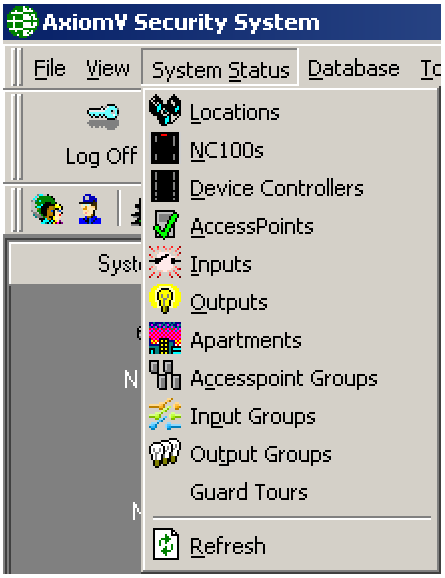


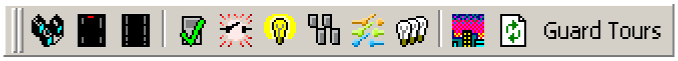
Input 1b - Alarms:1

Chapter 6
System Status

This chapter describes how to use the *System Status* pane in the AxiomV™ system. Operators can view the status of items in the system and execute commands on those items. Selections can be made from the *Module Selector*, *Menu*, or *Toolbar*.

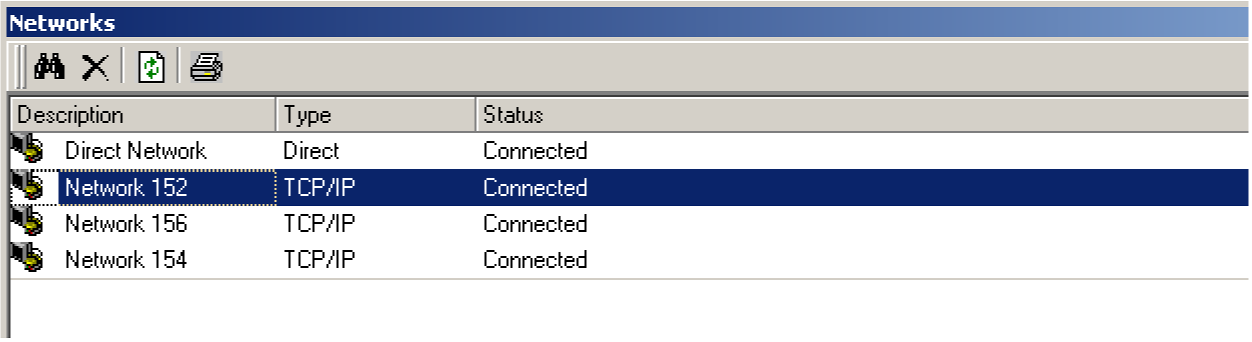






Networks

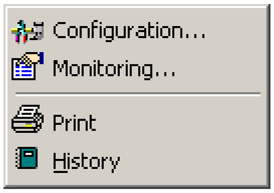
Networks



Networks

Description	Type	Status
Direct Network	Direct	Connected
Network 152	TCP/IP	Connected
Network 156	TCP/IP	Connected
Network 154	TCP/IP	Connected

Right click on a network to bring up the command menu.



Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on the Network Properties window is given in Chapter 7.

Monitoring…

The following list of events for an NC100 can be set in *Monitoring* to trigger alarms and/or send ASCII messages.

- Network Online
- Network Offline
- Controller Online
- Controller Offline
- NC100 Trouble
- NC100 Restore
- Device Trouble
- Device Restore

Print

Use *Print* to produce a printout of the current status of all selected items.

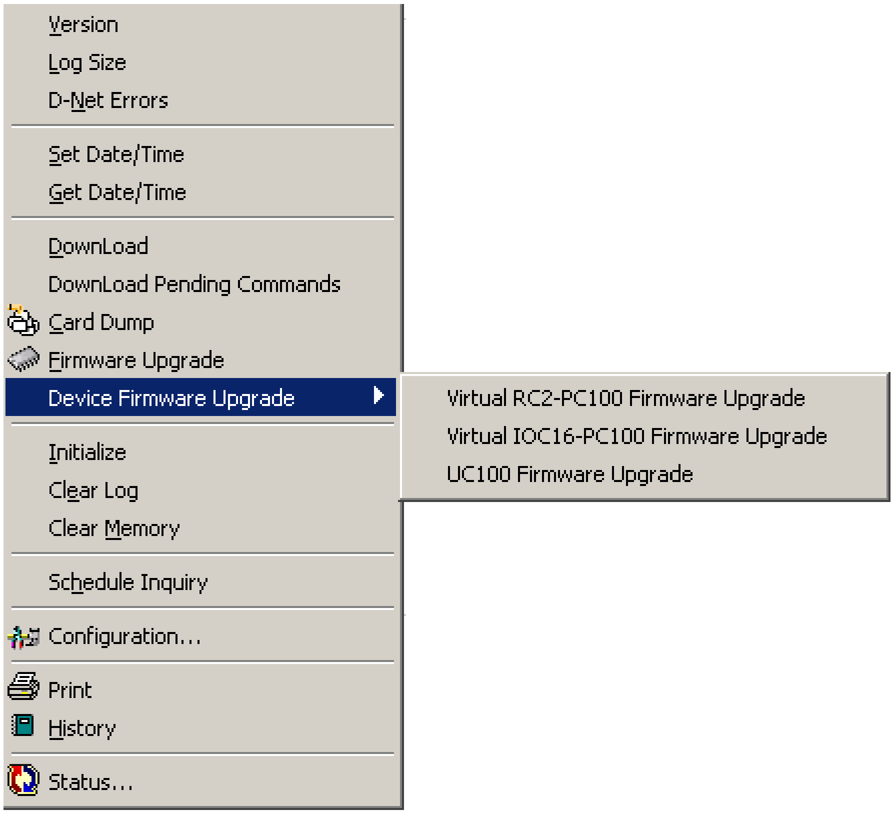
History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

See Chapter 5 System Status Pane – Monitoring **for more information on the monitoring parameters.**

NC100s/UNC500s

NC100s/UNC500s



Version

Version will return the firmware version of the selected NC100s/UNC500s

Log Size

Log Size will return the amount of memory the selected NC100s/UNC500s have to store event messages when they are not connected to the PC.

D-Net Errors

D-Net Errors will return the error count window for that NC100/UNC500.

Set Date/Time

Set Date/Time is used to set the date and time for the selected NC100s/UNC500s.

Get Date/Time

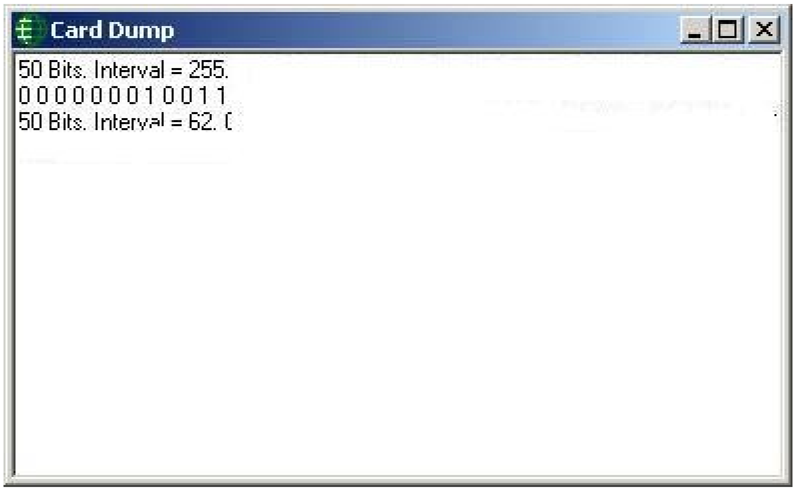
Get Date/Time: will return the current date and time in the selected NC100s/UNC500s.

Download

Download: will send all database files to the selected NC100s/UNC500s.

Card Dump

Card Dump is a diagnostic tool used to verify card data.

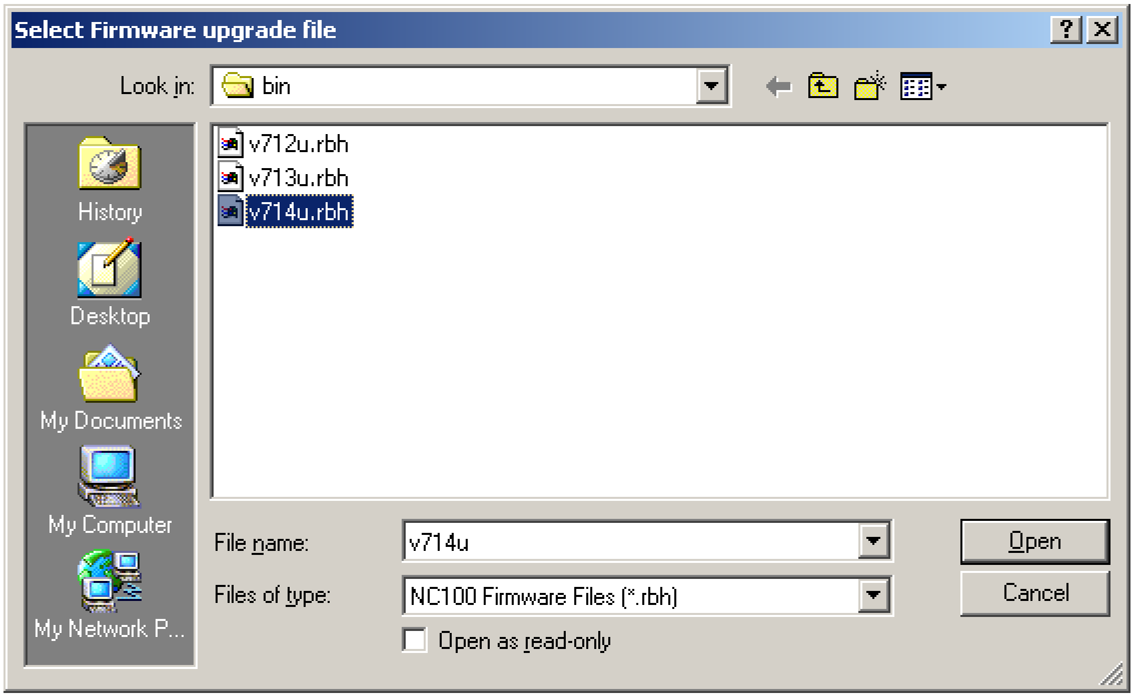


```
50 Bits. Interval = 255.
0 0 0 0 0 0 0 0 1 0 0 1 1
50 Bits. Interval = 62. (
```

The card data (in binary) will be displayed after the card is read.

Firmware Upgrade

Firmware Upgrade is used to change the firmware in the NC-100/UNC500. It may be necessary to browse your machine or network depending on where the firmware file is being stored. All firmware files end with the extension **rbh**.



Select Firmware upgrade file

Look in: bin

v712u.rbh
v713u.rbh
v714u.rbh

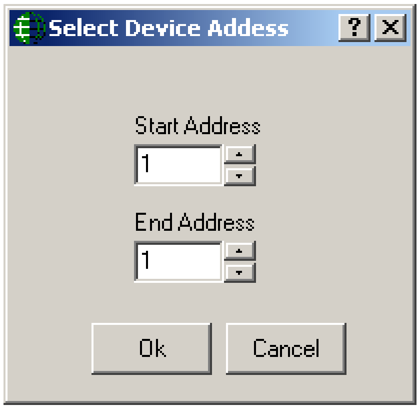
File name: v714u

Files of type: NC100 Firmware Files (*.rbh)

☐ Open as read-only

Device Firmware Upgrade

All of the *Device Firmware Upgrades* start the same as the NC100 *Firmware Upgrade*. First you select the firmware file (by browsing, just like the NC100 *Firmware Upgrade*), and then you have to select the range of addresses of the devices that are to be upgraded. The file is first sent down to the NC100/UNC500, and then to the devices from the NC100/UNC500 after the file type has been verified.



Select Device Addess

Start Address: 1

End Address: 1

Select the starting address and the ending address. These are the addresses of the devices (RC2s, IOC16s, **or** UC100s) that will have their firmware upgraded (inclusive). When you select *RC2 Firmware Upgrade* you will only be allowed to select addresses 1 to 4. Selecting *IOC16 Firmware Upgrade* will allow only addresses from 5 to 20 to be selected. While the selection of *UC100 Firmware Upgrade* allows addresses form 1 to 255. If you try to upgrade a device with the wrong type of firmware the upgrade will not proceed, and the message will indicate that there is a file type mismatch.

All UC100 (SafeSuite™) firmware is upgradeable, but only RC2 v40+ and IRC16 v40+ are upgradeable. Earlier versions still require a chip change.

Initialize

Initialize will initialize the microprocessor of all selected NC100s/UNC500s.

Clear Log

Clear Log will delete all messages from the selected NC100s/UNC500s log buffer.

Clear Memory

Clear Memory will remove all data in the selected NC100s/UNC500s' RAM. This will include all database files and log messages.

Schedule Inquiry

Schedule Inquiry will return the status of all schedules for all selected NC100s/UNC500s.

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on the NC100 Properties window is given in Chapter 7.

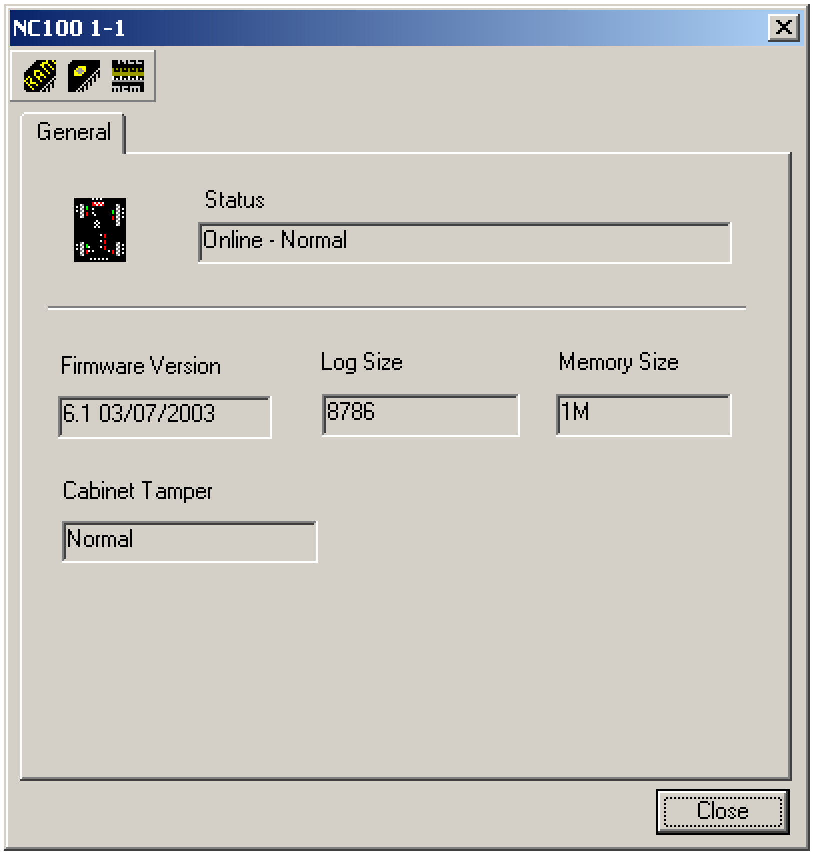
Print

Use *Print* to produce a printout of the current status of all selected items.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

Status…



NC100 1-1

General

Status: Online - Normal

Firmware Version: 6.1 03/07/2003

Log Size: 8786

Memory Size: 1M

Cabinet Tamper: Normal

Command Buttons

Clear Memory

This command will delete the entire memory of the NC100/UNC500.

Initialize

This command will re-boot the NC100/UNC500's processor.

Clear Log

This command will delete all of the logged history in the NC100/UNC500.

Status

Status will display the current status of the NC100/UNC500 (e.g. Online – Normal).

Firmware Version

Firmware will display the firmware version of the NC100/UNC500.

Log Size

Log Size will display the amount of memory available to log history events.

Memory Size

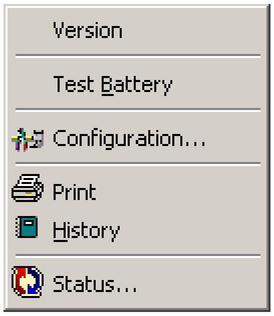
Memory Size will display the memory capacity of the NC100/UNC500 (256k, 8M).

Cabinet Tamper

Cabinet Tamper will display the status of the NC100's cabinet tamper input.

Device Controllers

Devices



Version

Version will return the firmware version of the selected devices.

Test Battery

Test Battery is used to immediately have the batteries tested on all selected devices.

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on the RC2 Properties window and the IOC16 Properties window is given in Chapter 7.

Print

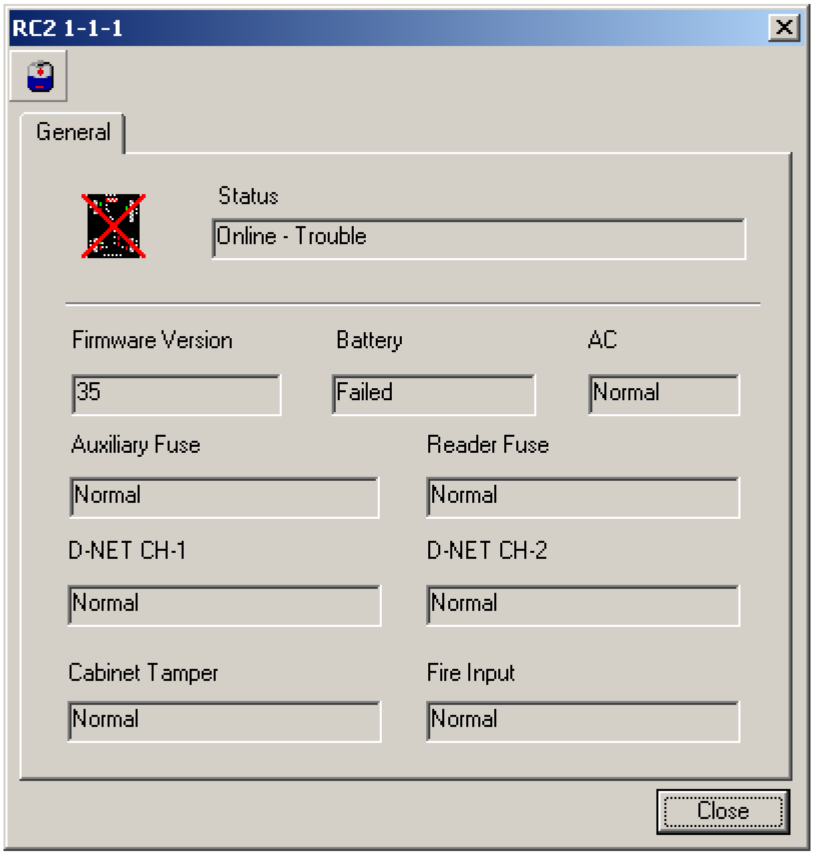
Use *Print* to produce a printout of the current status of all selected items.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

Status…

RC2



Status: Online - Trouble

Firmware Version: 35

Battery: Failed

AC: Normal

Auxiliary Fuse: Normal

Reader Fuse: Normal

D-NET CH-1: Normal

D-NET CH-2: Normal

Cabinet Tamper: Normal

Fire Input: Normal

Command Buttons

Battery Test

This command will immediately test the battery of the RC2.

Firmware Version

The RC2's firmware version will be displayed here.

Battery

Battery will display the status of the RC2's battery (normal or failed).

AC

AC will display the status of the RC2's 16vac input (normal, high or low).

Auxiliary Fuse

Auxiliary Fuse will display the status of the RC2's auxiliary power fuse (normal or failed).

Reader Fuse

Reader Fuse will display the status of the RC2's reader power fuse (normal or failed).

D-Net CH1

D-Net CH1 will display the status of communication channel 1 of the RC2's D-Net (normal or failed).

D-Net CH2

D-Net CH2 will display the status of communication channel 2 of the RC2's D-Net (normal or failed).

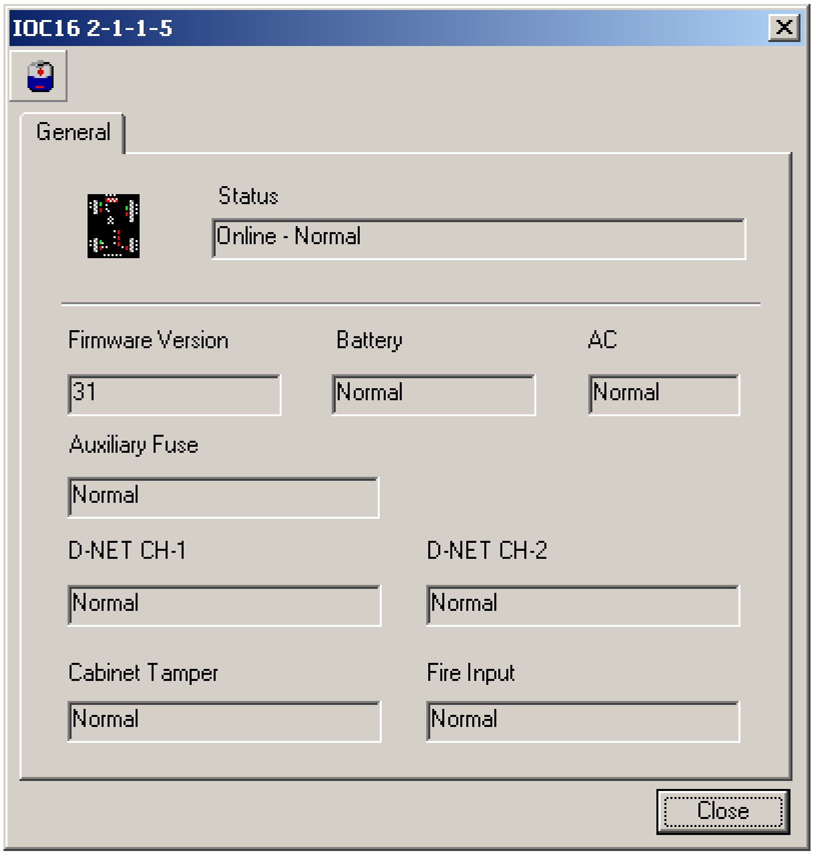
Cabinet Tamper

Cabinet Tamper will display the status of the RC2's cabinet tamper input.

Fire Signal

Fire Signal will display the status of the RC2's fire signal input (normal or failed).

IOC16



IOC16 2-1-1-5

Status: Online - Normal

Firmware Version: 31

Battery: Normal

AC: Normal

Auxiliary Fuse: Normal

D-NET CH-1: Normal

D-NET CH-2: Normal

Cabinet Tamper: Normal

Fire Input: Normal

Command Buttons

Battery Test

This command will immediately test the battery of the IOC16.

Firmware Version

The IOC16’s firmware version will be displayed here.

Battery

Battery will display the status of the IOC16’s battery (normal or failed).

AC

AC will display the status of the IOC16’s 16vac input (normal, high or low).

Auxiliary Fuse

Auxiliary Fuse will display the status of the IOC16’s auxiliary power fuse (normal or failed).

D-Net CH1

D-Net CH1 will display the status of communication channel 1 of the IOC16’s D-Net (normal or failed).

D-Net CH2

D-Net CH2 will display the status of communication channel 2 of the IOC16’s D-Net (normal or failed).

Cabinet Tamper

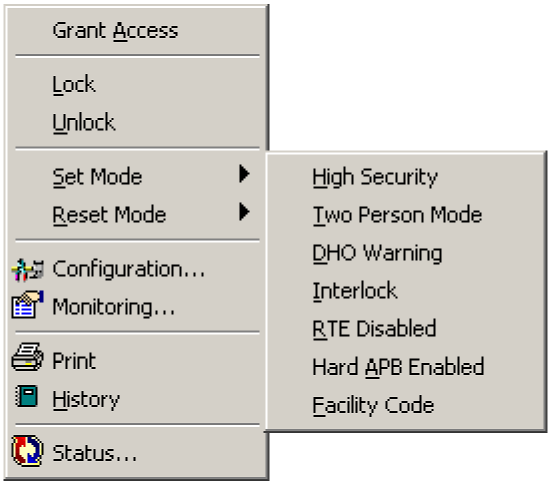
Cabinet Tamper will display the status of the IOC16’s cabinet tamper input.

Fire Signal

Fire Signal will display the status of the IOC16’s fire signal input (normal or failed).

Access Points

AccessPoints



Grant Access

Grant Access will grant access to all the selected access points.

Lock

Lock will lock all the selected access points.

Unlock

Unlock will unlock all the selected access points.

Set Mode and Reset Mode

Set Mode and Reset Mode are used to turn on or off different modes (High Security, Two Person, Door Held Open, Interlock, Request to Exit Disabled, Hard Antipassback Enabled, and Facility Code) on the selected access points.

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on the Access Point Properties window is given in Chapter 7.

Monitoring…

The following list of events for an Access Point can be set in *Monitoring* to trigger alarms, to block message, and/or to send ASCII messages.

- Access Granted
- Access Denied
- Door Not Open
- Door Held Open
- Forced Entry
- Tamper
- Secure

In addition, the status icons for the Access Point can be changed here.

Print

Use *Print* to produce a printout of the current status of all selected items.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

Status…

Command Buttons

Grant Access

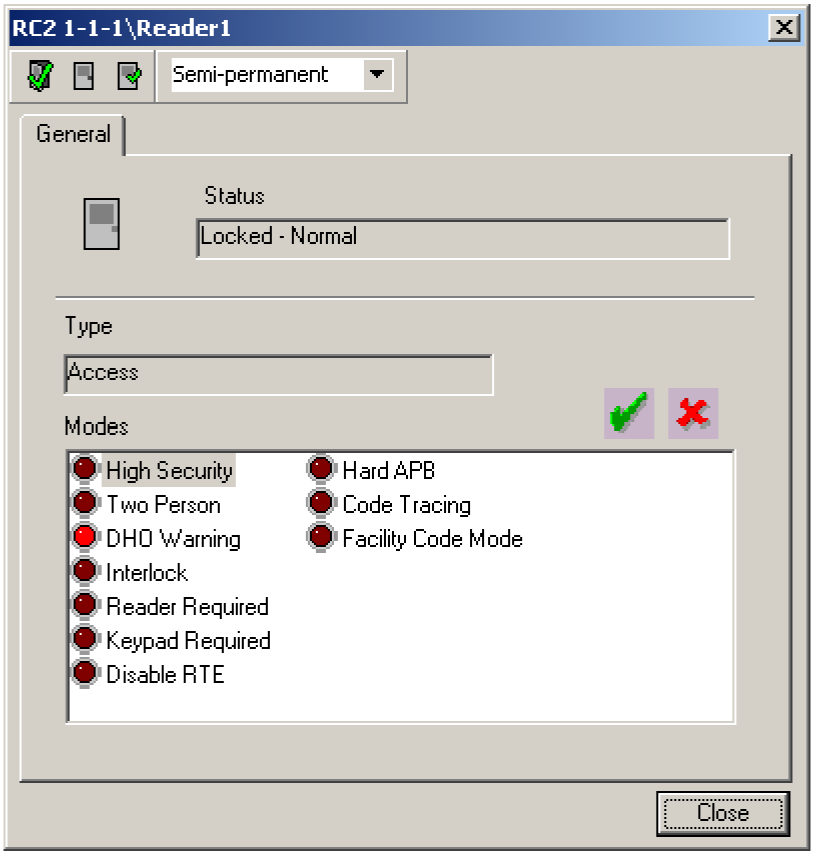
This command will immediately execute a grant access on the access point.

Lock

This command will immediately lock the access point.

Unlock

This command will immediately unlock the access point.



Status: Locked - Normal

Type: Access

Modes:

- ● High Security
- ● Two Person
- ● DHO Warning
- ● Interlock
- ● Reader Required
- ● Keypad Required
- ● Disable RTE
- ● Hard APB
- ● Code Tracing
- ● Facility Code Mode

Status

Status will display the current status of the Access Point (e.g. Locked – Normal).

Type

Type will indicate this access point's type.

Mode

Mode will show (via the LED icons) which access point modes are on and which are off. These modes can be turned on and off by highlighting the mode and either clicking the green check (on) or the red X (off).

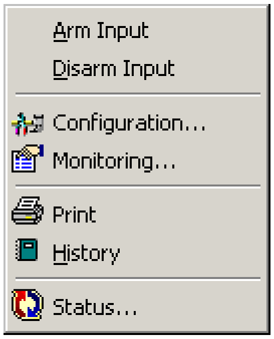
✓ ✗

Mode List:

- High Security
- Two Person
- DHO Warning
- Interlock
- Reader Required
- Keypad Required
- Disable RTE
- Hard APB
- Code Tracing
- Facility Code Mode

Inputs

Inputs



Arm Input

Arm Input is used to arm the selected inputs.

Disarm Input

Disarm Input is used to disarm the selected inputs.

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on the Input Properties window is given in Chapter 7.

Print

Use *Print* to produce a printout of the current status of all selected items.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

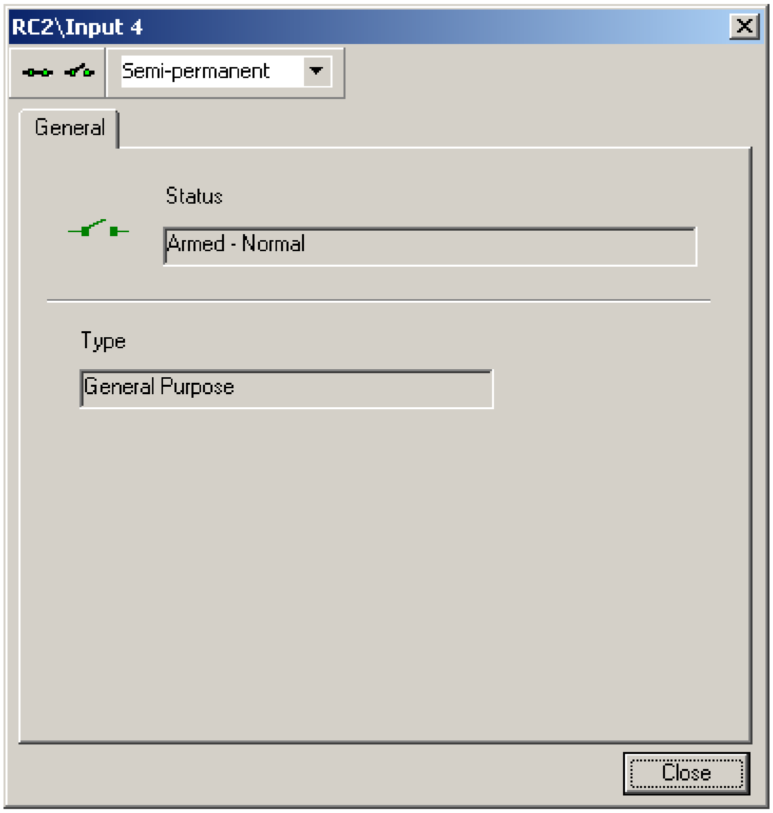
Monitoring…

The following list of events for an Input can be set in *Monitoring* to trigger alarms, to block message, and/or to send ASCII messages.

- Alarm, Restore, Abnormal, Normal, & Trouble

In addition, the status icons for the Input can be changed here.

Status…



Status: Armed - Normal

Type: General Purpose

Command Buttons

Arm

This command will immediately arm the input.

Disarm

This command will immediately disarm the input.

Status

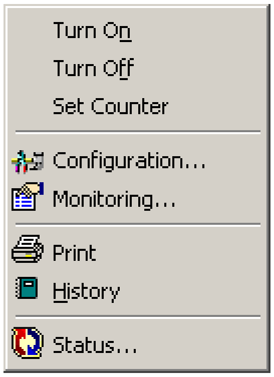
Status will display the current status of the input (e.g. Armed – Normal).

Type

Type will indicate this input's type.

Outputs

Outputs



Turn On

Turn On will turn all selected outputs on.

Turn Off

Turn Off will turn all selected outputs off.

Set Counter

Set Counter will set the current level of the count for all selected outputs

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on the Output Properties window is given in Chapter 7.

Monitoring…

The following list of events for an Output can be set in *Monitoring* to trigger alarms, to block message, and/or to send ASCII messages.

- On, Off

In addition, the status icons for the Output can be changed here.

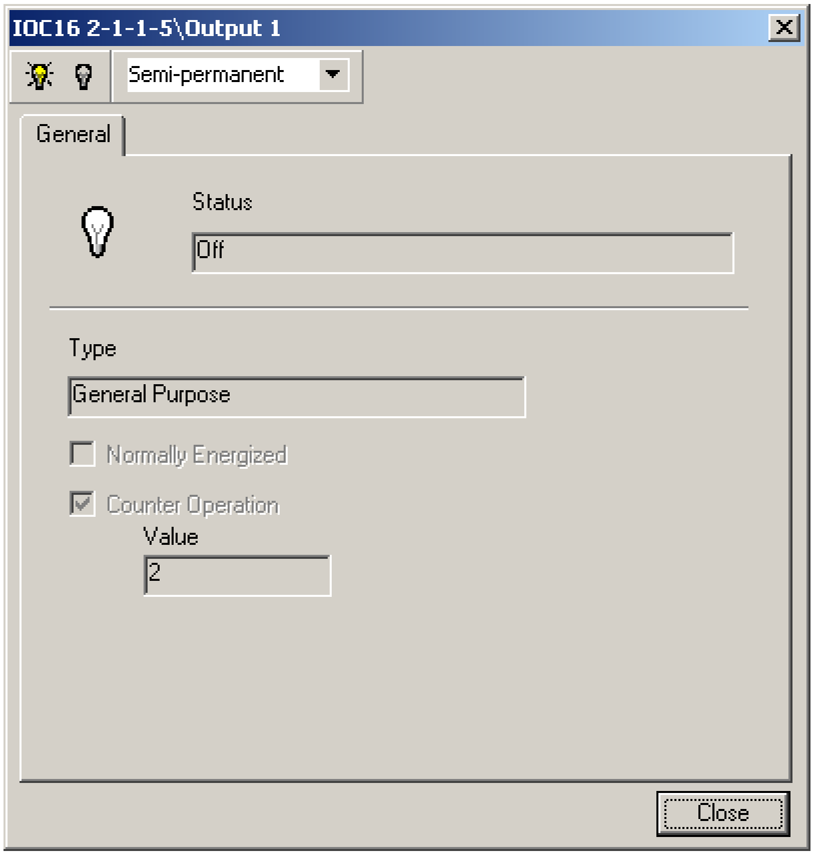
Print

Use *Print* to produce a printout of the current status of all selected items.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

Status…



IOC16 2-1-1-5\Output 1

Semi-permanent

General

Status: Off

Type: General Purpose

☐ Normally Energized

☑ Counter Operation

Value: 2

Command Buttons

On

This command will immediately turn on the output.

Off

This command will immediately turn off the output.

Status

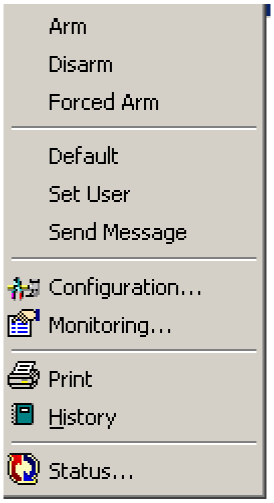
Status will display the current status of the input (e.g. Armed – Normal).

Type

Type will indicate this input's type.

Apartments

Apartments



Arm

Arm will arm the keypad(s) of the selected apartment(s).

Disarm

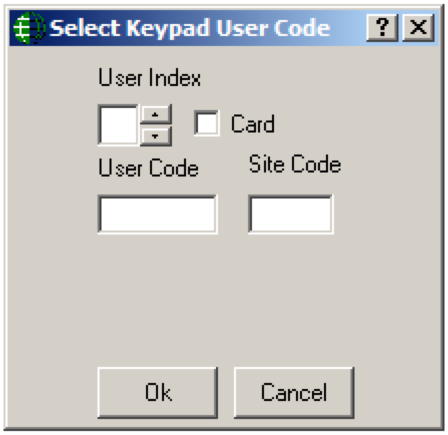
Disarm will disarm the keypad(s) of the selected apartment(s).

Forced Arm

Forced Arm will arm the keypad(s) of the selected apartment(s) even though one or more zones are in violation.

Set User

Set User will allow the operator to set user codes in the SafeSuite™ panels.



User Index

Select the user (1-8) whose code you wish to set.

User Code

Enter the code for that user.

Card

Check this box if you are actually entering a card number and not a user code. Limited card formats are available through this function; other formats can be used by inputting the card data directly at the reader.

Site Code

If a card number is being entered, input the appropriate site code for that card here.

Default

This selection will reset the user codes of the panel back to default. User 1 is reset back to 1234 and the other seven are cleared.

Send Message

This button will pop up a small screen so that you can enter a text message to be sent to the Liquid Crystal Display of the panel. (See Page 188 for more details.)

Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on Keypads given in Chapter 7.

Monitoring…

The following list of events for an *Apartment* can be set in *Monitoring* to trigger alarms, to block message, and/or to send ASCII messages.

- Zone Restore
- Zone Alarm
- Zone Trouble
- Zone Shunted
- Zone Unshunted
- Zone Output
- Zone Arm/Disarm
- User Commands
- Keypad Messages
- Keypad Alarm

In addition, the status icons for the *Apartment* can be changed here.

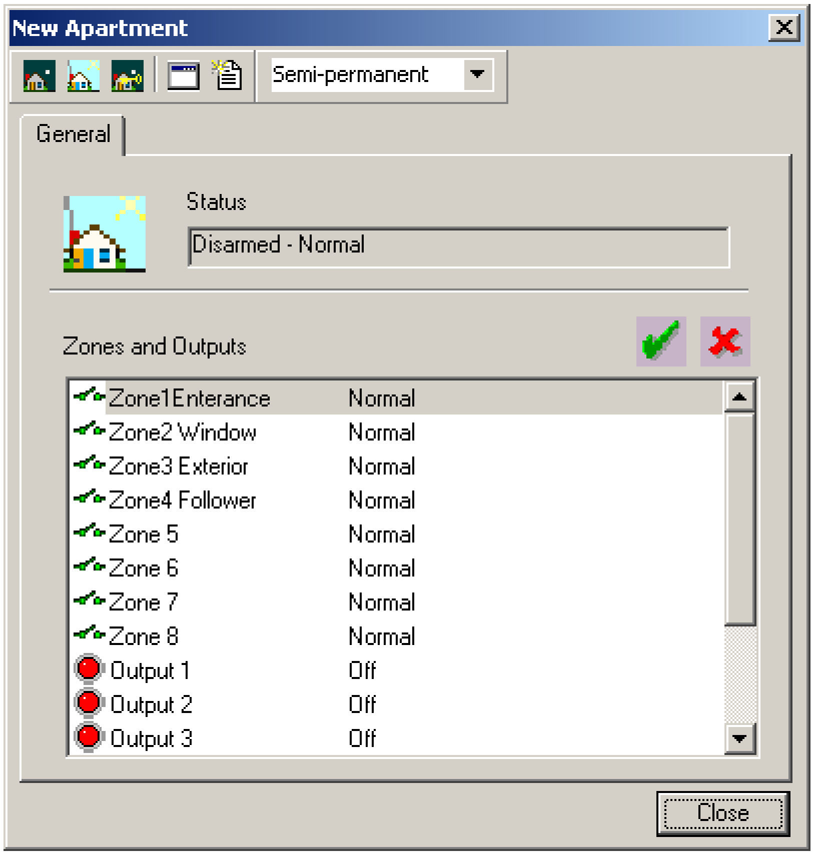
Print

Use *Print* to produce a printout of the current status of all selected items.

History

Clicking History will produce a report of up to the last ten events that occurred for the selected item(s) for the current date.

Status…



Status: Disarmed - Normal

Zones and Outputs

Zone1 Enterance	Normal
Zone2 Window	Normal
Zone3 Exterior	Normal
Zone4 Follower	Normal
Zone 5	Normal
Zone 6	Normal
Zone 7	Normal
Zone 8	Normal
Output 1	Off
Output 2	Off
Output 3	Off

Armed Away

This button will arm the panel in the *Away Mode*.

Disarm

This button will disarm the panel.

Forced Arm

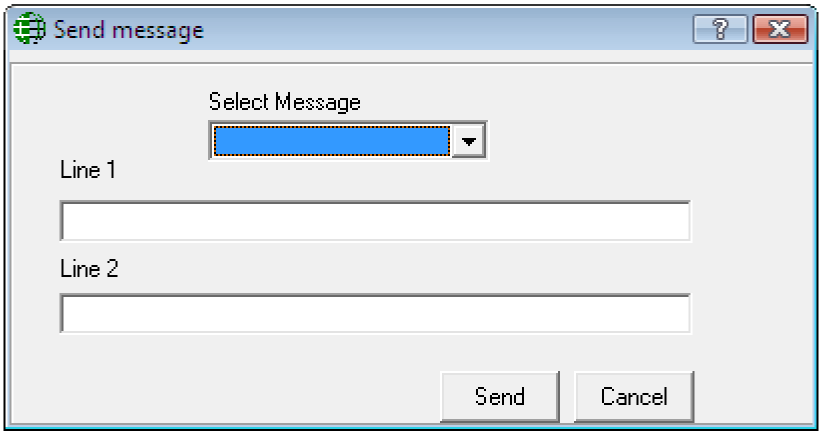
This button will arm the panel in the *Away Mode* even if one or more zones are in violation.

Default

This button will reset the user codes of the panel back to default. User 1 is reset back to 1234 and the other seven are cleared.

Message

This button will pop up a small screen so that you can enter a text message to be sent to the Liquid Crystal Display of the panel. Two lines of sixteen characters each can be typed in, or predefined *Instruction Messages* may be selected. After typing in or selecting the message click *Send*.



Messages can only be sent to LCD panels, LED panels cannot display messages.

Status

Status will display the armed and alarm status of the panel.

Zones and Outputs

Set Mode On

Set Mode On will shunt zones and turn on outputs.

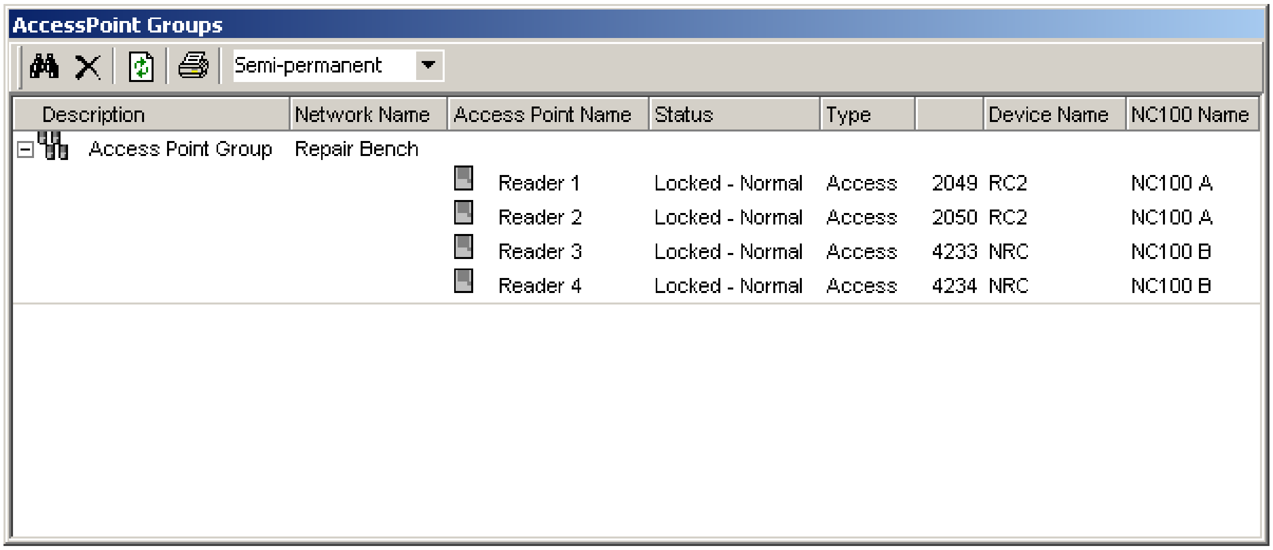
Set Mode Off

Set Mode Off will unshunt zones and turn off outputs.

Highlight the desired zone(s) or output(s) then click *Set Mode On* or *Set Mode Off*.

Access Point Groups

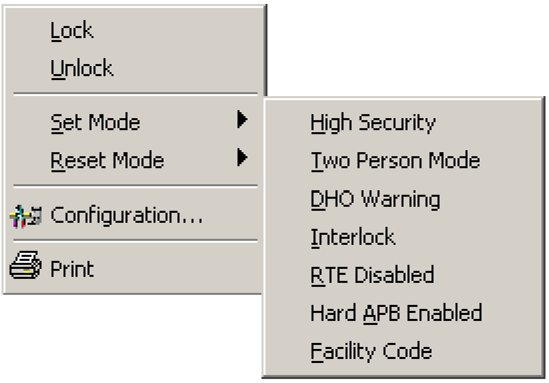
AccessPoint Groups



AccessPoint Groups

Semi-permanent

Description	Network Name	Access Point Name	Status	Type		Device Name	NC100 Name
⊟ Access Point Group	Repair Bench						
		Reader 1	Locked - Normal	Access	2049	RC2	NC100 A
		Reader 2	Locked - Normal	Access	2050	RC2	NC100 A
		Reader 3	Locked - Normal	Access	4233	NRC	NC100 B
		Reader 4	Locked - Normal	Access	4234	NRC	NC100 B



Lock

Lock will lock all selected access points groups

Unlock

Unlock: will unlock all selected access points groups.

Set Mode and Reset Mode

Set Mode and Reset Mode are used to turn on or off different modes (High Security, Two Person, Door Held Open, Interlock, Request to Exit Disabled, Hard Antipassback Enabled, and Facility Code) on the selected access points.

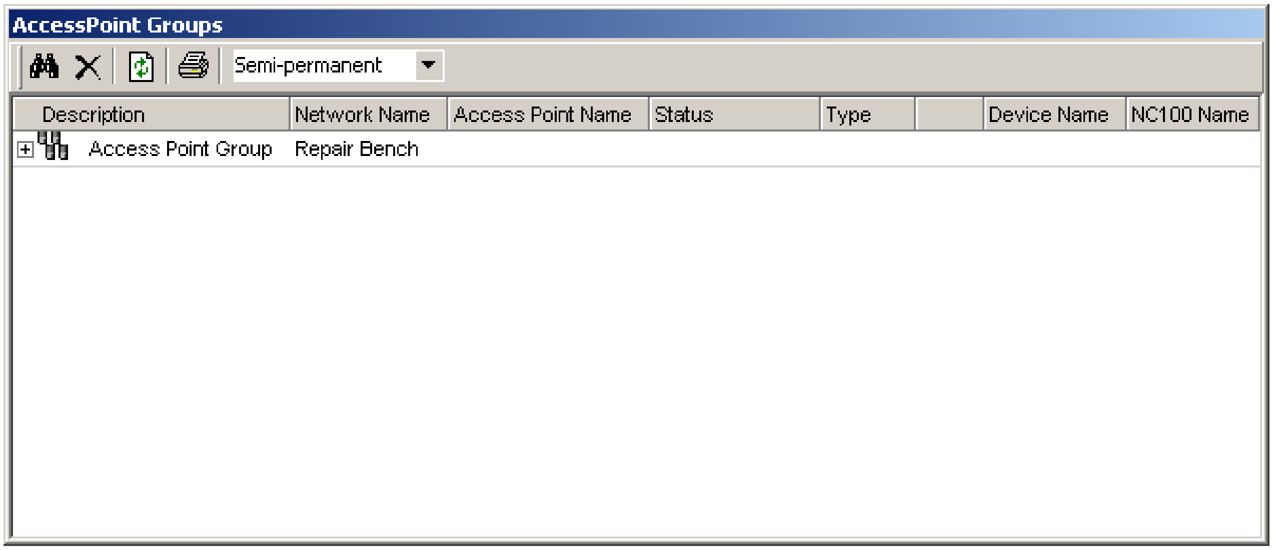
Configuration…

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on AccessPoint Groups is given in Chapter 7.

Print

Use *Print* to produce a printout of the current status of all selected items.

Commands can be sent to the group or to individual members.

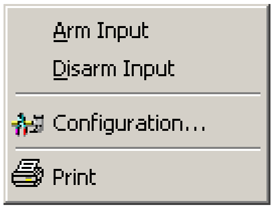


Description	Network Name	Access Point Name	Status	Type		Device Name	NC100 Name
Access Point Group	Repair Bench						

The minus sign will hide the group members and the plus sign will reveal them.

Input Groups

Input Groups



Arm Input

Arm Input is used to arm the selected input groups.

Disarm

Disarm Input is used to disarm the selected input groups.

Configuration…

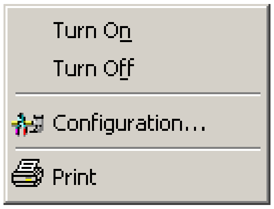
Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on Input Groups is given in Chapter 7.

Print

Use *Print* to produce a printout of the current status of all selected items.

Output Groups

Output Groups



Turn On

Turn On will turn all selected outputs on.

Turn Off

Turn Off will turn all selected outputs off.

Configuration…

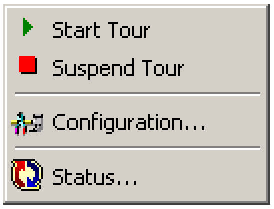
Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on Output Groups is given in Chapter 7.

Print

Use *Print* to produce a printout of the current status of all selected items.

Guard Tours[8]

Guard Tours



Start Tour

Start Tour will immediately start the tour manually.

Suspend Tour

Suspend Tour will immediately stop the tour manually.

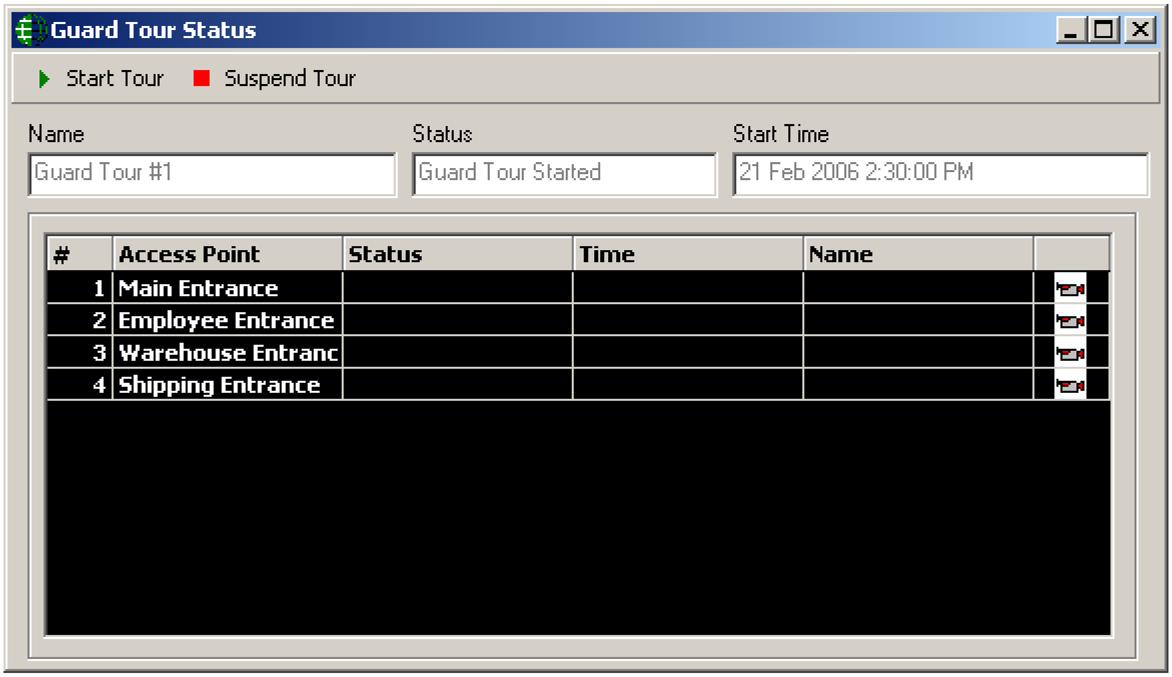
Configuration

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information on Guard Tours is given in Chapter 7.

Status

Status will display the current status of the selected guard tour.

[8] This selection is only available if the optional license for the Guard Tour Software has been purchased and installed.



Name: Guard Tour #1

Status: Guard Tour Started

Start Time: 21 Feb 2006 2:30:00 PM

#	Access Point	Status	Time	Name	
1	Main Entrance				📹
2	Employee Entrance				📹
3	Warehouse Entranc				📹
4	Shipping Entrance				📹

Guard Tour Status can show you if the tour has started and if so when. It can show which guard has reached which access points and when. With the DVR module setup the *Guard Tour Status* can access live views from cameras associated with access points in the tour.

Refresh

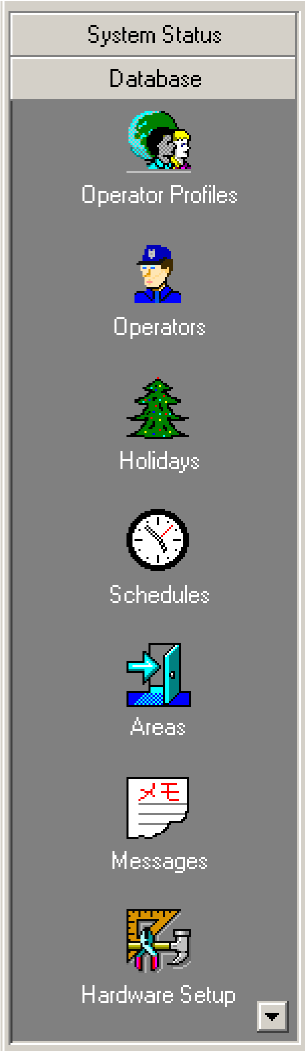
Refresh

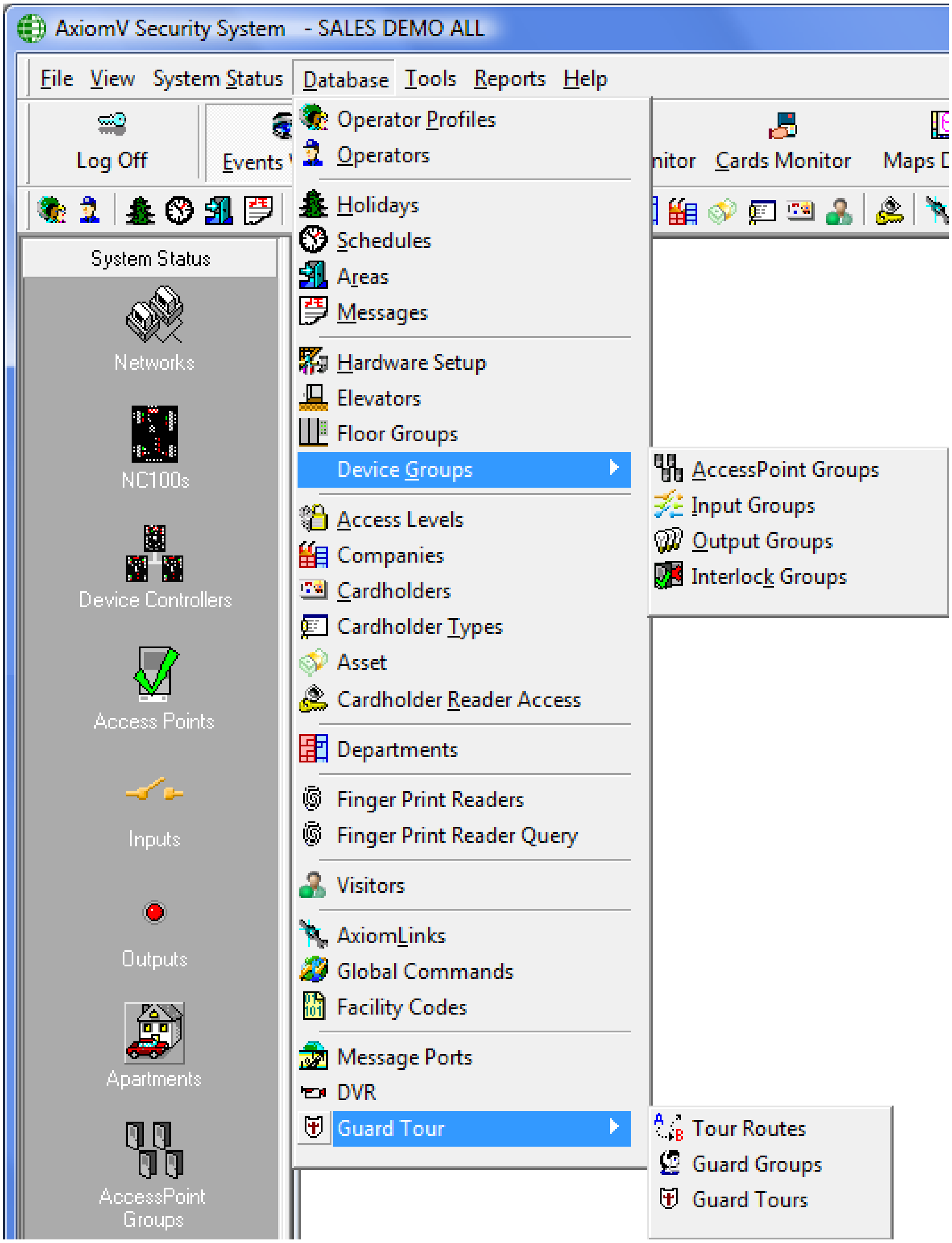
Refresh will re-query all highlighted items and update their status on the display.

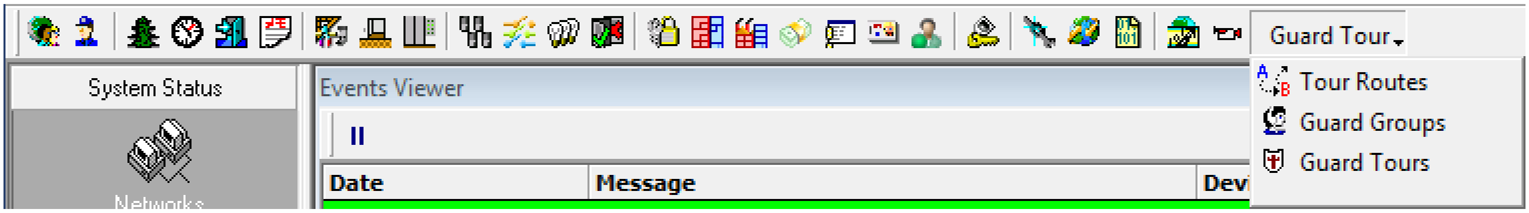
Part 5

Chapter 7
Database

This chapter describes how to program the AxiomV™ system *Database* parameters. Typically the System Administrator performs this function. Make a selection from the *Module Selector*, *Menu*, or *Toolbar*.

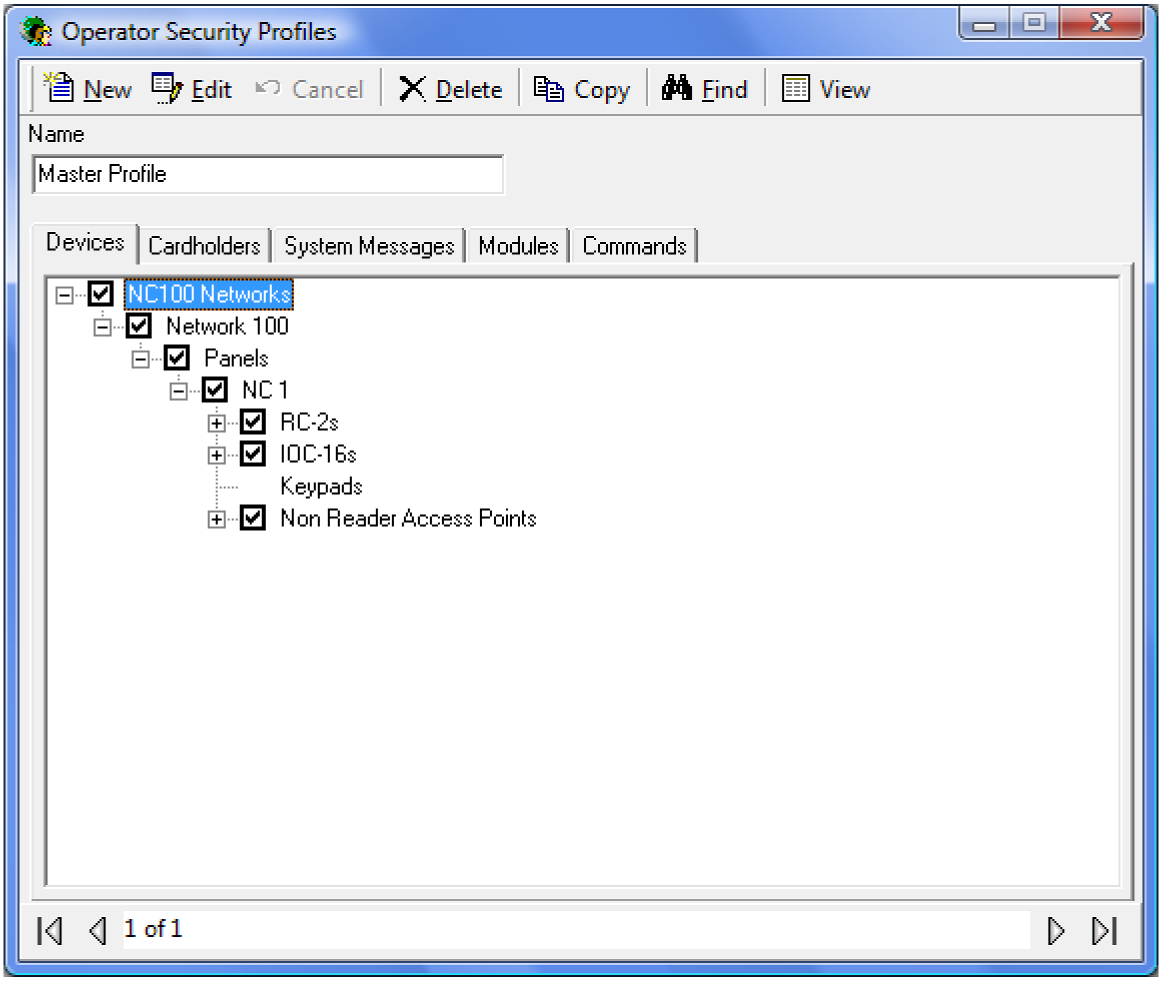



AxiomV Security System - SALES DEMO ALL
File
View
System Status
Database
Tools
Reports
Help
Log Off
Events
nitor
Cards Monitor
Maps
System Status
Networks
NC100s
Device Controllers
Access Points
Inputs
Outputs
Apartments
AccessPoint Groups
Operator Profiles
Operators
Holidays
Schedules
Areas
Messages
Hardware Setup
Elevators
Floor Groups
Device Groups
Access Levels
Companies
Cardholders
Cardholder Types
Asset
Cardholder Reader Access
Departments
Finger Print Readers
Finger Print Reader Query
Visitors
AxiomLinks
Global Commands
Facility Codes
Message Ports
DVR
Guard Tour
AccessPoint Groups
Input Groups
Output Groups
Interlock Groups
Tour Routes
Guard Groups
Guard Tours


Guard Tour
System Status
Networks
Events Viewer
Date
Message
Dev
Tour Routes
Guard Groups
Guard Tours

Operator Profiles

Operator Profiles set the privileges for the operators. Create as many profiles as required. The Master Profile can be renamed but otherwise cannot be edited.



Name: Master Profile

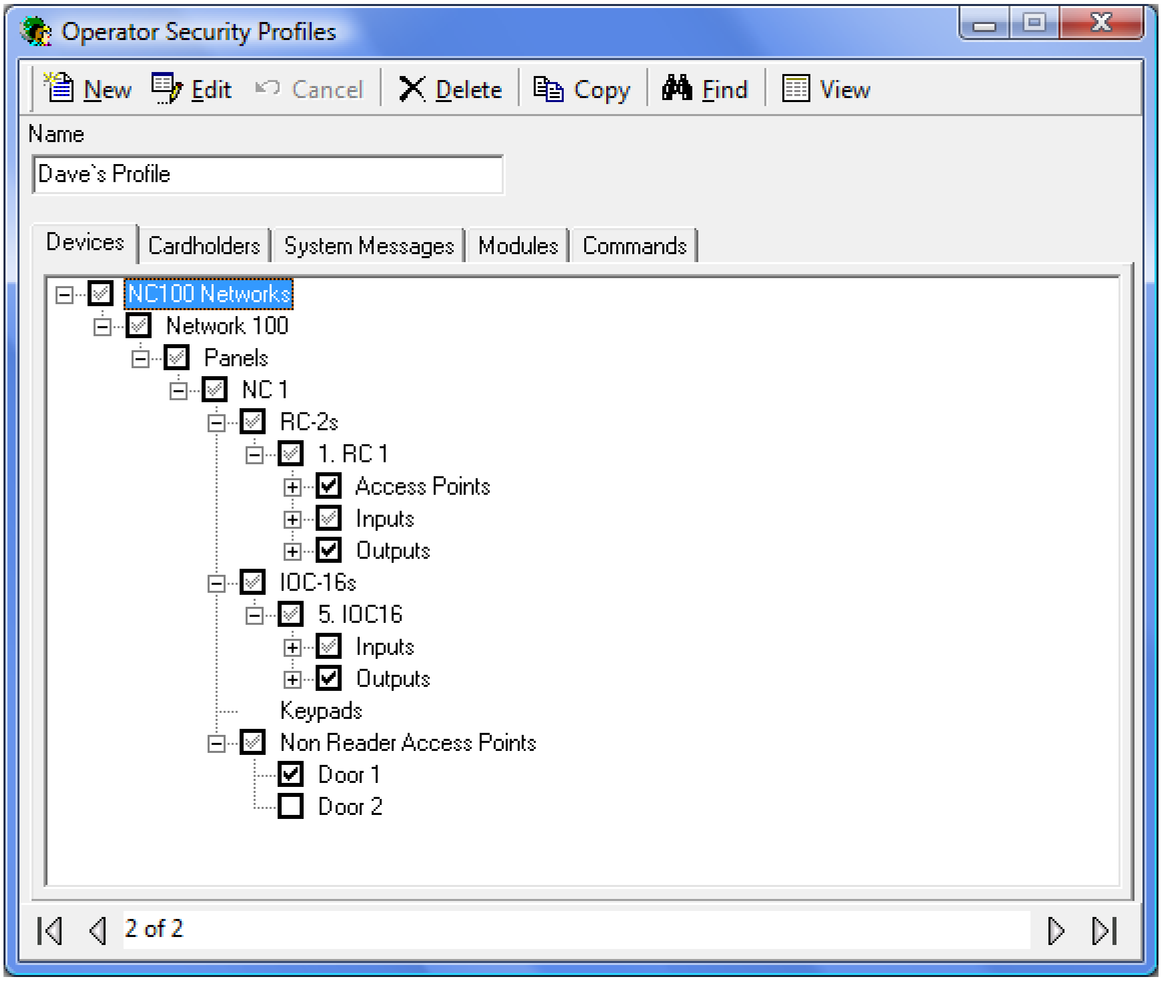
- ☑ NC100 Networks
  - ☑ Network 100
    - ☑ Panels
      - ☑ NC 1
        - ☑ RC-2s
        - ☑ IOC-16s
        - Keypads
        - ☑ Non Reader Access Points

Name

Up to 50 alphanumeric characters may be entered here.

Devices

From the *Devices* tab the operator can be restricted in which device they can see and interact with in the system. The operator can be restricted by networks, panel, access points, or even inputs and outputs. Only items that are selected here will be available to the operator.



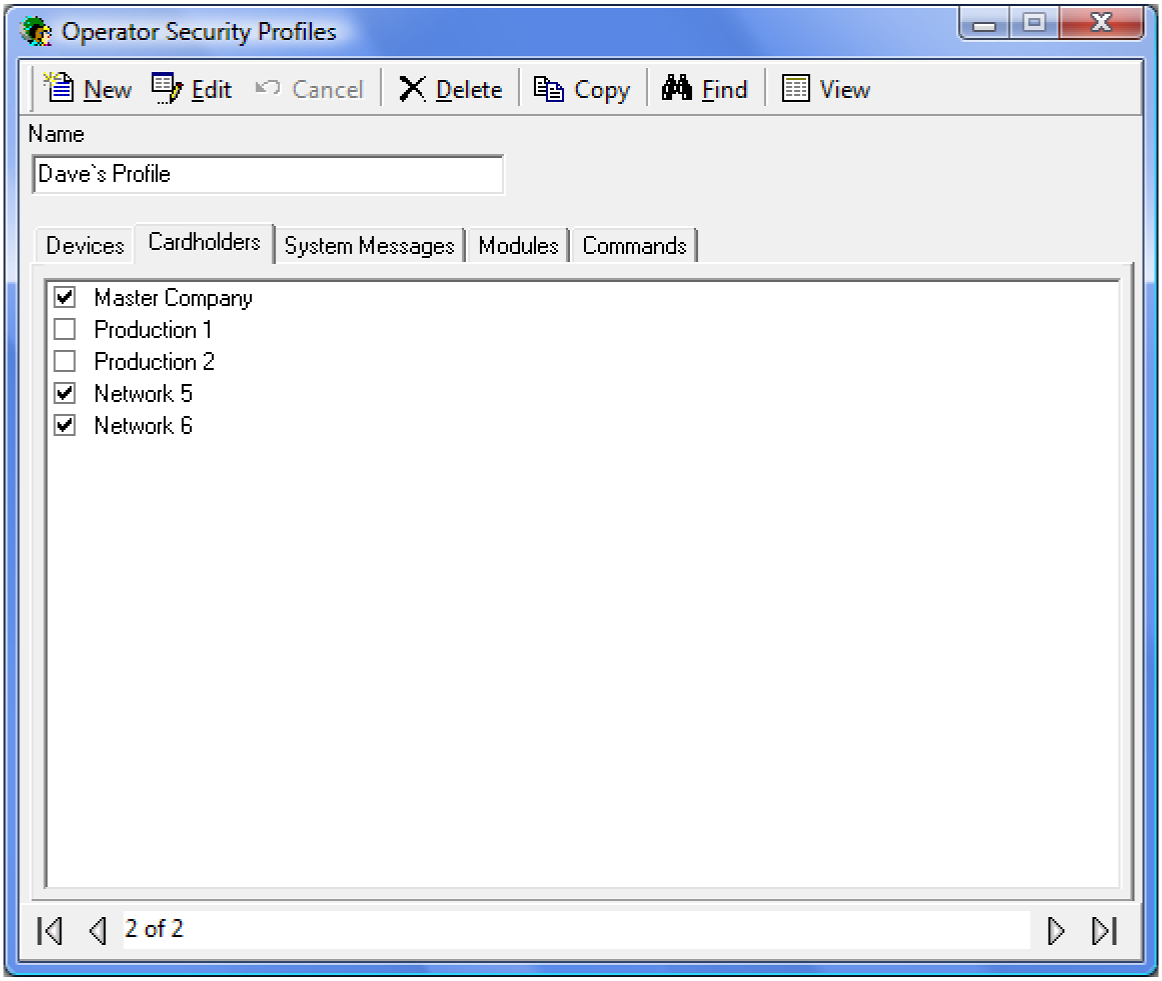
Name: Dave`s Profile

- ☑ NC100 Networks
  - ☑ Network 100
    - ☑ Panels
      - ☑ NC 1
        - ☑ RC-2s
          - ☑ 1. RC 1
            - ☑ Access Points
            - ☑ Inputs
            - ☑ Outputs
        - ☑ IOC-16s
          - ☑ 5. IOC16
            - ☑ Inputs
            - ☑ Outputs
        - Keypads
        - ☑ Non Reader Access Points
          - ☑ Door 1
          - □ Door 2

2 of 2

Cardholders

From the *Cardholders* tab the operator can be restricted by which groups of cardholders are available to them. Cardholders are grouped in Companies and operators can be given limited access to the cardholders by not giving them every company.



Name

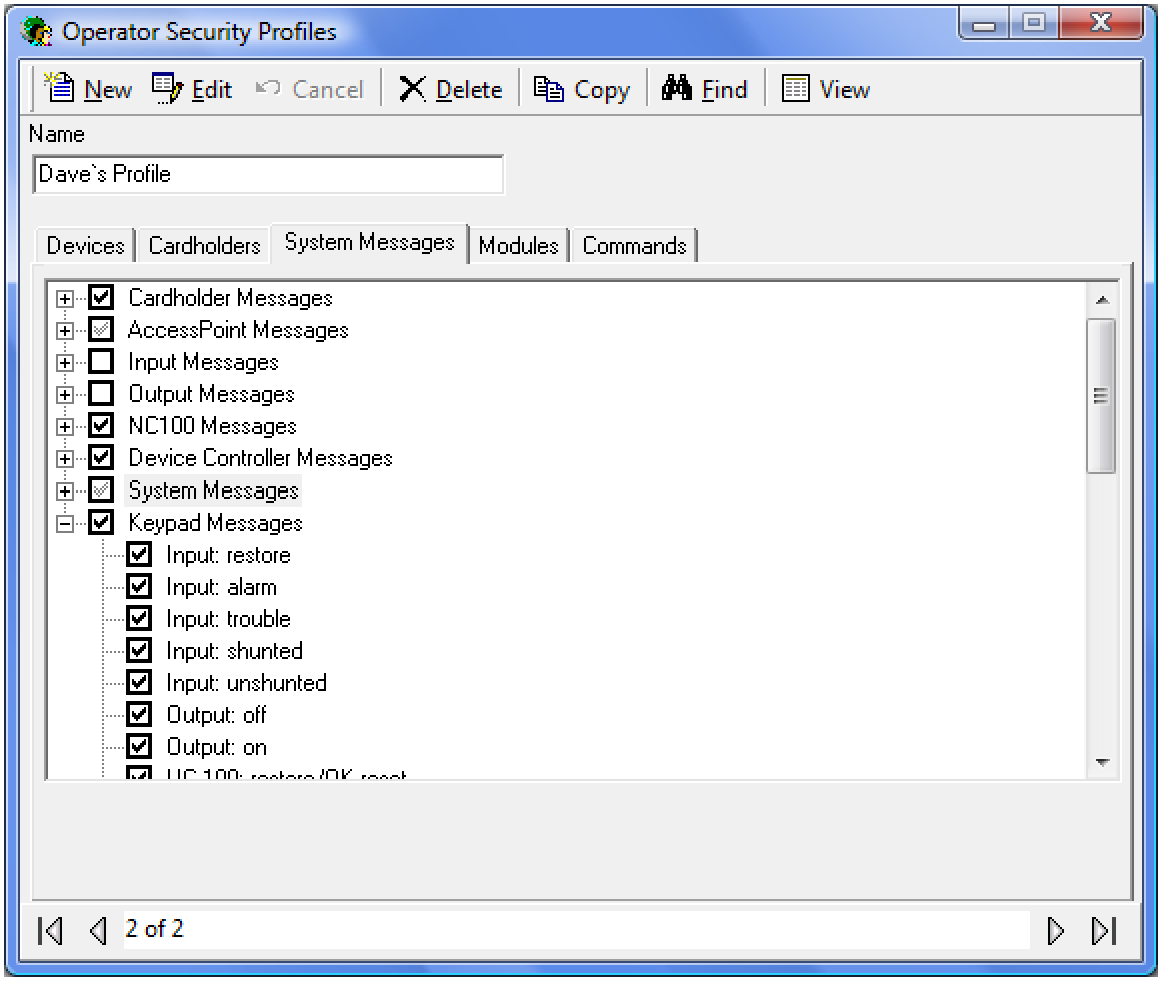
Dave`s Profile

☑ Master Company
☐ Production 1
☐ Production 2
☑ Network 5
☑ Network 6

2 of 2

System Messages

The *System Messages* tab not only allows the restriction of messages the operator can see but also provides the ability to play a .wav file when the message appears. The sound can help alert the operator when certain events happen.



Name

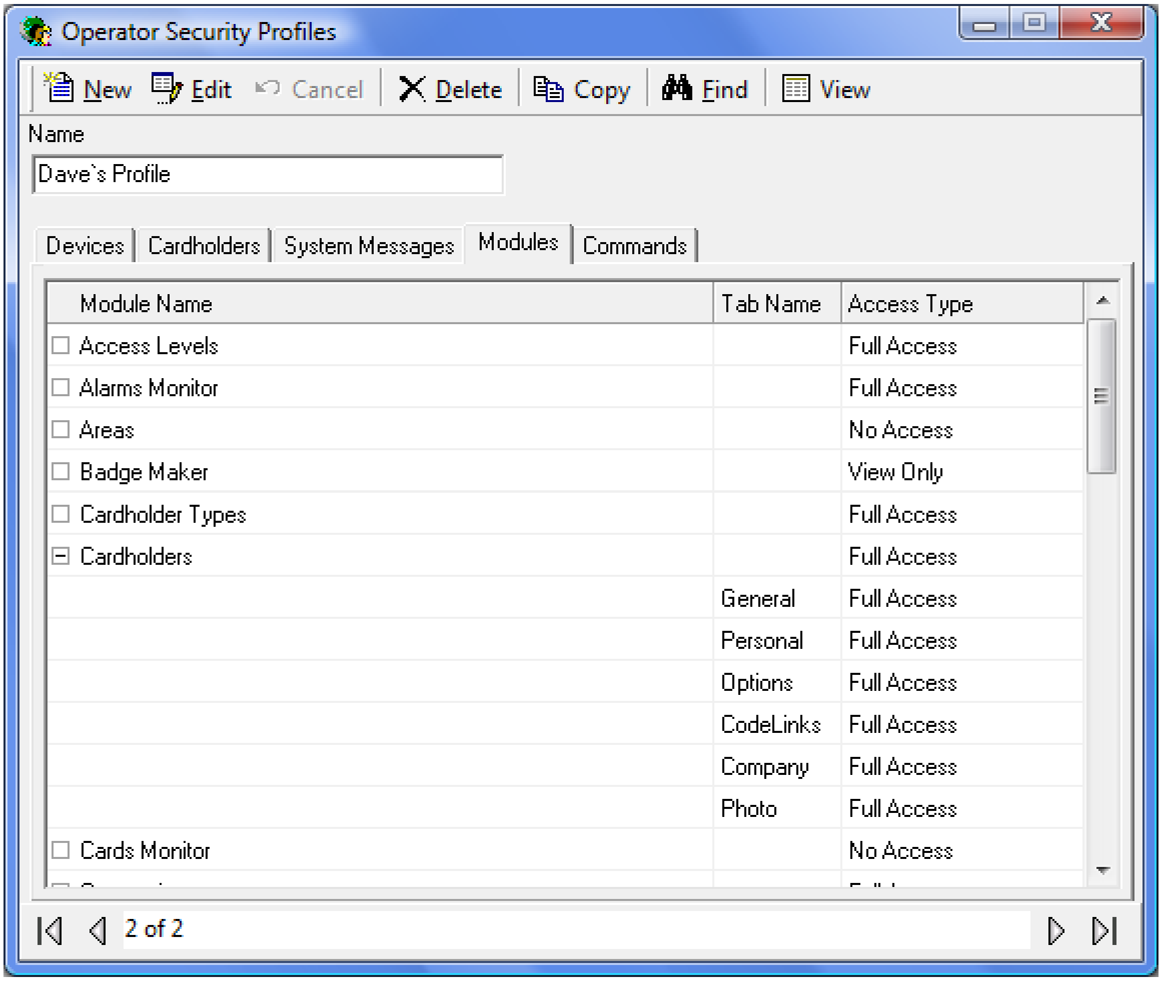
Dave`s Profile

- ☑ Cardholder Messages
- ▨ AccessPoint Messages
- □ Input Messages
- □ Output Messages
- ☑ NC100 Messages
- ☑ Device Controller Messages
- ▨ System Messages
- ☑ Keypad Messages
  - ☑ Input: restore
  - ☑ Input: alarm
  - ☑ Input: trouble
  - ☑ Input: shunted
  - ☑ Input: unshunted
  - ☑ Output: off
  - ☑ Output: on
  - ☑ UC 100: restore/OK reset

2 of 2

Modules

From the *Modules* tab the operators' access to the software can be restricted. They can be given No Access, View Only, or Full Access to sections of the software.



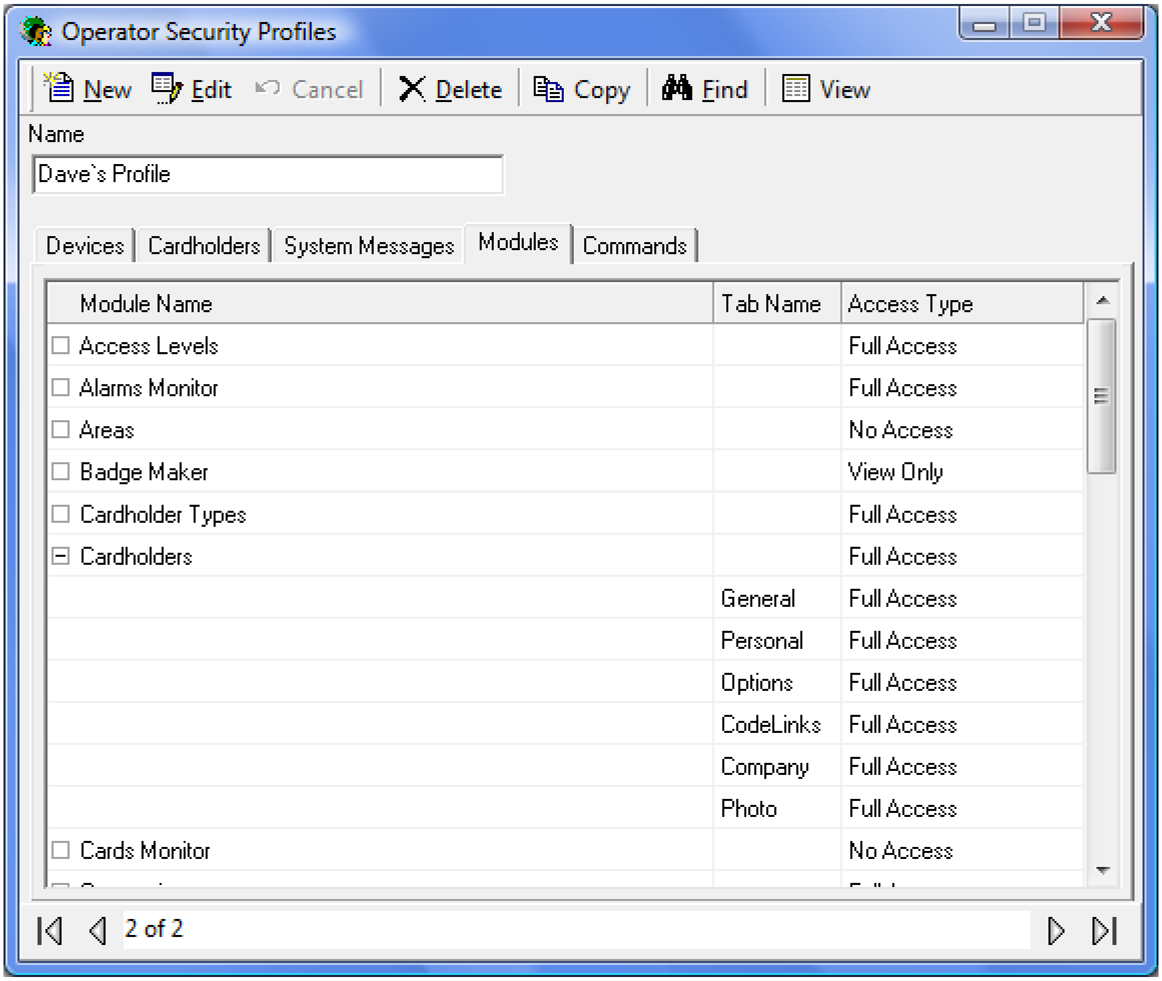
Name: Dave`s Profile

Module Name	Tab Name	Access Type
☐ Access Levels		Full Access
☐ Alarms Monitor		Full Access
☐ Areas		No Access
☐ Badge Maker		View Only
☐ Cardholder Types		Full Access
⊟ Cardholders		Full Access
	General	Full Access
	Personal	Full Access
	Options	Full Access
	CodeLinks	Full Access
	Company	Full Access
	Photo	Full Access
☐ Cards Monitor		No Access

Each **tab** under *Cardholder* has its own 'Access Type' so that operators can have access to some cardholder data without having access to all cardholder data.

Commands

From the *Commands* tab the operator can be restricted to perform only certain commands. These commands of course can only be executed on devices selected in the *Devices* tab.



Name
Dave`s Profile

Module Name	Tab Name	Access Type
□ Access Levels		Full Access
□ Alarms Monitor		Full Access
□ Areas		No Access
□ Badge Maker		View Only
□ Cardholder Types		Full Access
⊟ Cardholders		Full Access
	General	Full Access
	Personal	Full Access
	Options	Full Access
	CodeLinks	Full Access
	Company	Full Access
	Photo	Full Access
□ Cards Monitor		No Access

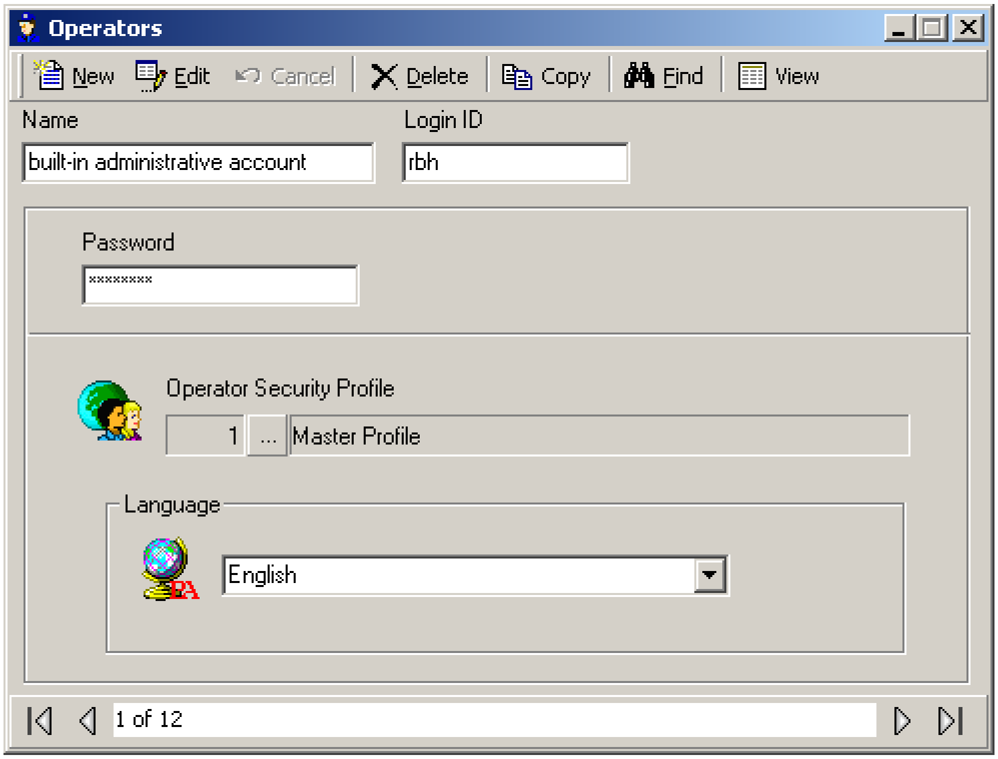
Operators

From the Operators Screen the following can be done:

- Create and manage operator accounts for the AxiomV™ system
- Set the operator's logon password
- Set the operator's language preference.

Operator rights are defined by *Operator Security Profiles* (which are created elsewhere).

The *built-in administrative account* cannot be deleted. It can be edited by changing its name, its password, or its language but its profile cannot be changed (there must be at least one operator with full access).



Name: built-in administrative account
Login ID: rbh
Password: ********
Operator Security Profile: 1 ... Master Profile
Language: English
1 of 12

If the system is setup and licensed for the *Active Directory* option then the AxiomV™ system can use the current domain user's authentication to login. For more information on *Active Directory* see Appendix B.

Name

Up to 50 alphanumeric characters may be entered here.

Login ID

The operator when logging into the software uses his/her *Login ID*.

Password

This is the log in password for the operator. It is entered twice for confirmation.

Operator Security Profile

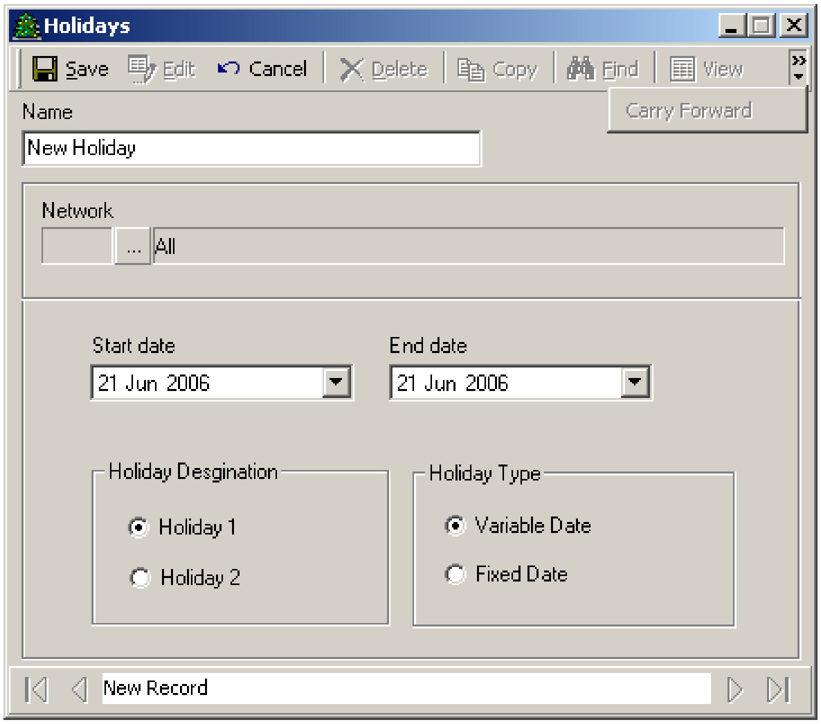
Click the *Browse/Ellipsis button* and select a profile from the list.

Language

Click the down arrow and select a language from the list. When the operator logs in this language is set up in the software.

Holidays

Use the *Holidays* window to define *Holiday* dates. AxiomV™ allows any day or days of the year to be designated a *Holiday* – Type 1 or Type 2. These days provide an automatic override of normal *Schedule* parameters for the seven days of the week, and invoke the appropriate *Holiday* scheduling instead.



Name: New Holiday

Network: ... All

Start date: 21 Jun 2006

End date: 21 Jun 2006

Holiday Desgination
- ● Holiday 1
- ○ Holiday 2

Holiday Type
- ● Variable Date
- ○ Fixed Date

New Record

Name

Up to 50 alphanumeric characters may be entered here.

Network

Holidays can be designated for all networks or for one specific network. In this way holidays can be different for different locations using the same database. To designate a holiday in multiple networks, but not all networks, will require multiple holiday records.

Start Date

Start Date is the date on which the holiday begins in MM-DD-YYYY[9] format. For single day holidays (e.g., Labour Day), enter the date only. For holidays that span several days (e.g., Christmas break) this is the first day of the holiday (e.g., Dec 25/04).

[9] Date is displayed in the format selected in the Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.

End Date

End Date is the date on which the holiday ends in MM-DD-YYYY[10] format. For holidays that span several days (e.g., Christmas break), this is the last day of the holiday period. For example, if the Christmas break is from Dec 25/04 through Dec 28/04, enter 12/28/2004.

Holiday Designation

Radio buttons (*Holiday 1* or *Holiday 2*) designate the holiday as one of two types. The holiday type depends on the *Schedule* settings that are specified for Holidays type 1 and type 2.

Holiday Types 1 and 2

AxiomV™ provides two distinct Holiday types to increase system flexibility. Each Holiday type has its own schedule. Holiday Type 1 is normally used for Statutory Holidays, where all employees are off. Holiday Type 2 is commonly used in situations such as a summer shutdown, where the majority of employees take a fixed 2-week summer vacation but certain maintenance staff members continue to work during this period. When assigning access levels, maintenance workers can be given access during the 2-week vacation shut down and all other employees can be denied access.

All *Schedules* have a nine-day schedule, with the eighth day designated the Holiday 1 schedule and the ninth, the Holiday 2 schedule. Holidays replace the regular day of the week. The week with Labour Day in it will be; Sunday, Holiday, Tuesday, Wednesday, Thursday, Friday, and Saturday. There won't be a Monday in the week with Labour Day.

Type

Radio buttons (*Fixed Date* or *Variable Date*) designate whether the holiday occurs on the same calendar date each year (*Fixed Date*) or varies from year to year (*Variable Date*). E.g. Labour Day is a *Variable Date* while New Year's Day is a *Fixed Date*.

Carry Forward

Click on Carry Forward to copy Fixed Holidays that have past to the next year. For example it would create the Fixed Holiday 'New Year's Day – 1 Jan 2013' from the Fixed Holidays 'New Year's Day – 1 Jan 2012'.

[10] Date is displayed in the format selected in the Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.

Schedules

Schedules are a fundamental concept of access control, and they assume that the week is the basic recurring unit of time to be used in defining how the system will operate. A Schedule is essentially a two dimensional matrix with the days of the week along one axis and user-defined start time and end time settings along the other axis.

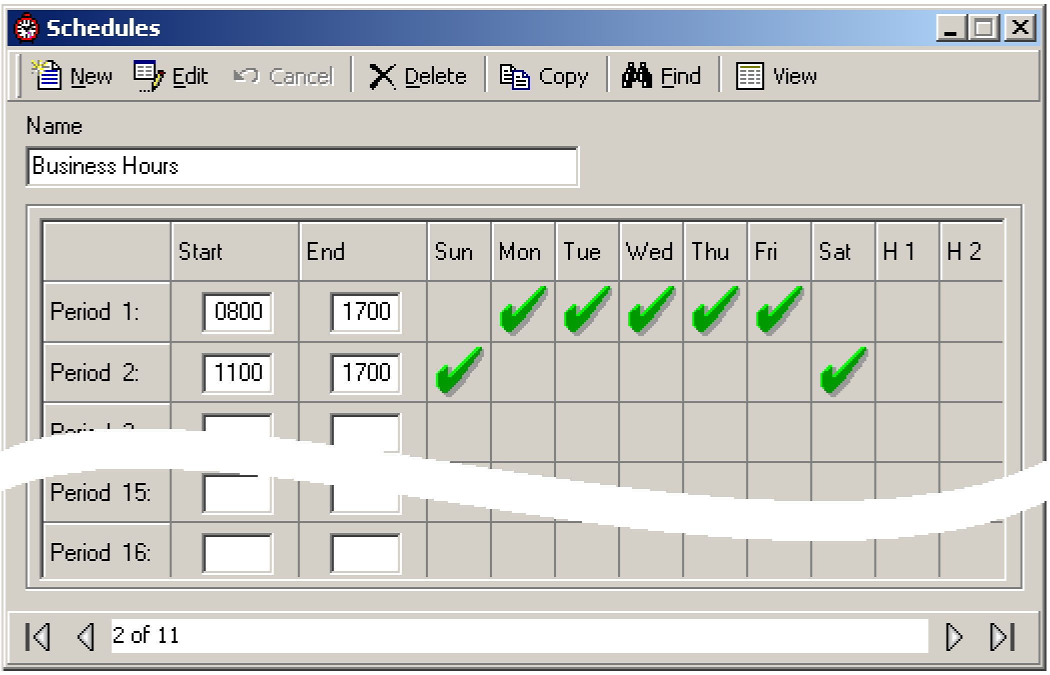
Once Schedules are defined they may be assigned, along with various operating instructions, to components of an access control system, thereby governing how the system behaves from week to week. Components that may be controlled using Schedules include Access Point operation, Input arming and disarming, Output switching, Cardholder Modes and Privileges, Printers, Modems, Event Log Messages, and more.

A *Period* is comprised of a start time, an end time and the days of the week to which the start and end time settings apply. A Schedule, such as Business Hours for a company, may contain one or more periods (maximum sixteen). In a schedule when the first start time occurs on any day, from any period in the schedule, the schedule will turn on. Any system features, functions, and operating modes associated with that schedule are enabled until the next occurrence of an end time from any period for this schedule, or in the case of individual functions, until manually turned off by operator command or a pending command.

It is important to note that a P*eriod* does not represent a continuous block of time. The start and end times are independent of one another, although AxiomV™ requires that the Start Time be a lower value than the End Time. It is useful to think of start and end times as on and off commands for the *Schedule*. It is possible to define a *Schedule* where multiple start times occur before any stop times. The only effect of consecutive start times is to re-enable any functions that have been disabled with a semi-permanent command.

For additional programming flexibility, AxiomV™ defines the week as having 2 additional days (*Holidays Type 1* and *2*) which can be scheduled differently than the normal 7 days, thereby providing a means of accommodating irregular days such as holidays (see *Holidays setup* on page 206).

As An example you want to define “Business Hours” as 8:00 a.m. to 5:00 p.m. Monday through Friday, plus 11:00 a.m. to 5:00 p.m. Saturday and Sunday, excluding *Holidays*. The Business Hours *Schedule*, contains two periods, and appears as follows.



Name

Business Hours

	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H 1	H 2
Period 1:	0800	1700		✓	✓	✓	✓	✓			
Period 2:	1100	1700	✓						✓		
Period 3:											
Period 15:											
Period 16:											

2 of 11

Name

Up to 50 alphanumeric characters may be entered here.

Start Time

Start Time (using a 24-hour clock hh:mm) defines the starting time of a period.

End Time

End Time (using a 24-hour clock hh:mm) defines the ending time for a period.

Weekday/Holiday check boxes

Use these check boxes to select days on which the *Period* applies. H1 and H2 refer to *Holiday* Type 1 and Type 2, as defined in the *Holidays* window.

Schedule Tips

Schedule Operation during Panel Reset

Whenever the NC100 panel is reset, (due to operator command, power loss etc.), the following decision process takes place.

First, the system checks to determine if the current date is a holiday and if it is, the start and end times for the respective holiday type are used for the reset test. Otherwise the day of the week determines which start and end times are considered in the reset test.

Second, the current reset time is compared against the start time and end time for each time zone under the day of the week selected in the first step above. Unless the following *Reset Condition* is satisfied, for at least one time zone in a *Schedule*, the underlying *Schedule* will be inactive (turned off) on reset. The *Schedule* will remain inactive, until the next start time occurs for that *Schedule*.

If, the following *Reset Condition* is satisfied, for at least one period in a *Schedule*, the underlying *Schedule* will be active (turned on) on reset. The *Schedule* will remain active, until the next end time occurs for that *Schedule*.

Reset Condition

Start Time < Current Reset Time < End Time

If TRUE, THEN restart with *Time Group* active.

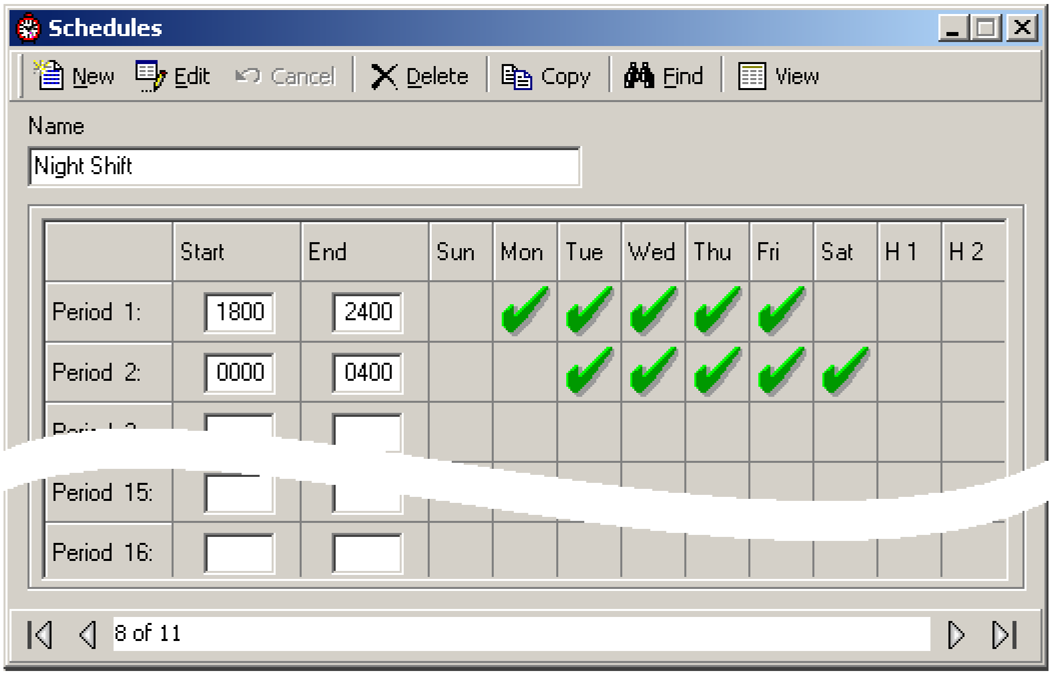
If FALSE, THEN restart with *Time Group* inactive.

When designing *Periods* and *Schedules*, AxiomV™ insists that start times should always be less than end times for all Periods. Otherwise, the current reset time may not fall between the start time and end time, and the system would reset with the *Schedule* inactive.

However, "24:00" and "00:00" are both legitimate times for the Reset Condition testing in the previous section. Therefore, it may make sense to include 24:00 as an end time in a time zone in order to insure proper reset behavior.

Schedules that Span Midnight

When creating a schedule that needs to remain on through midnight, care should be taken. For example, suppose you want to define a *Schedule* as Late Shift from 6:00 p.m. to 4:00 a.m. Monday through Friday. Since the *End Time* must be greater than the *Start Time*, time groups that span midnight will require at least two *Periods*.



Name

Night Shift

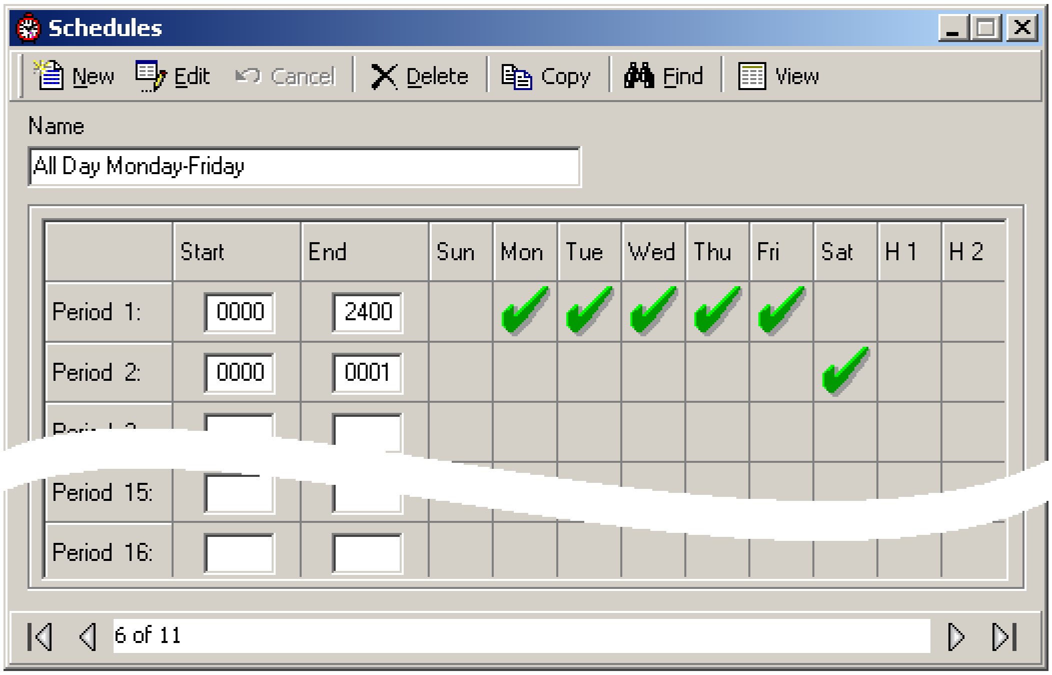
	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H 1	H 2
Period 1:	1800	2400		✓	✓	✓	✓	✓			
Period 2:	0000	0400			✓	✓	✓	✓	✓		
Peri											
Period 15:											
Period 16:											

8 of 11

The above *Schedule* restarts at midnight on Tuesday, Wednesday, Thursday, Friday, and Saturday even though it is already on from the previous day at 18:00. The midnight *schedule* activation on these five days is not problematic for AxiomV™. Note, however, that the restart will turn on the schedule if any semi-permanent operator commands were issued to turn it off since 18:00 the previous day.

24 Hour “On” Schedules

Occasionally a *Schedule* that provides 24-hour access may be required. In the following example, the first time zone sets up a perpetual schedule that will never stop, not even on reset. The second time zone causes the *Schedule* to turn off at 00:01 a.m. on Saturday. The *Schedule* is turned on again at 00:00:01 a.m. on Monday.



Name

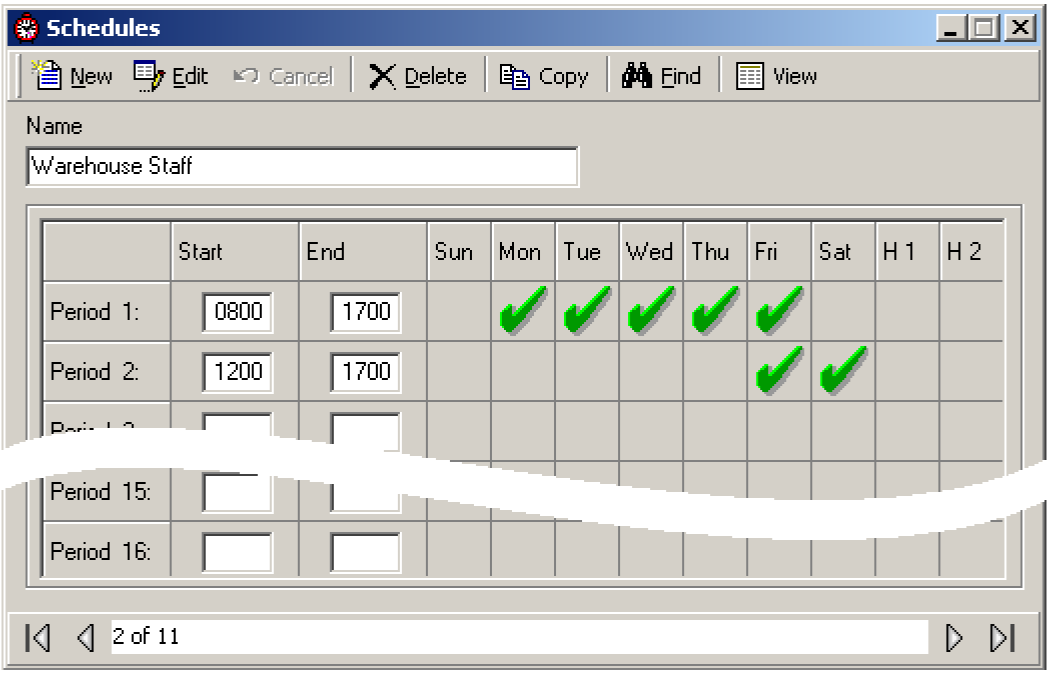
All Day Monday-Friday

	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H 1	H 2
Period 1:	0000	2400		✓	✓	✓	✓	✓			
Period 2:	0000	0001							✓		
Period 3:											
Period 15:											
Period 16:											

6 of 11

Duplicate Start Time or End Time Entries

Duplicated start time or end time entries within the same *Schedule* may yield unexpected results and should be avoided. The following is an example of a poorly designed *Schedule*.



Name

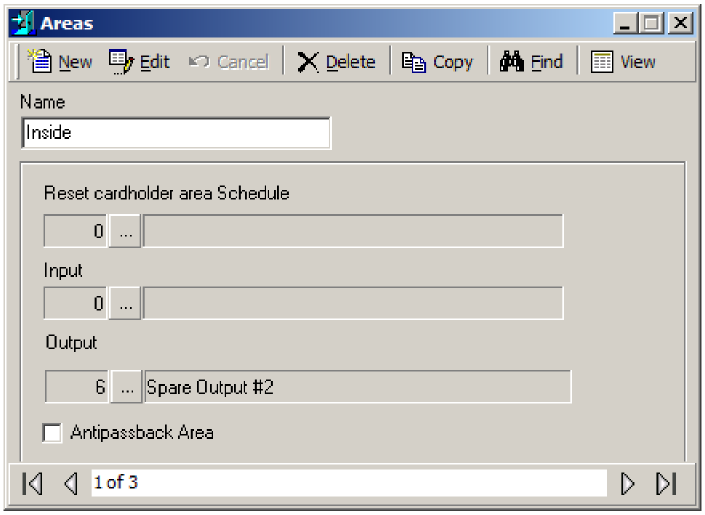
Warehouse Staff

	Start	End	Sun	Mon	Tue	Wed	Thu	Fri	Sat	H 1	H 2
Period 1:	0800	1700		✓	✓	✓	✓	✓			
Period 2:	1200	1700						✓	✓		
Period 3:											
Period 15:											
Period 16:											

2 of 11

Areas

Areas need to be setup to control and monitor cardholder movement. They are primarily used in conjunction with Antipassback.



Name
Inside

Reset cardholder area Schedule
0 ...

Input
0 ...

Output
6 ... Spare Output #2

□ Antipassback Area

1 of 3

Name

Up to 50 alphanumeric characters may be entered here.

Reset Cardholder Area Schedule

Click on the Browse/Ellipsis button and select a schedule for when the reset is active. A Monday to Friday schedule would mean that the reset wouldn’t happen on Saturday or Sunday. Reset will be executed at the *start time* of the schedule. If more than one line is configured in the schedule selected, it will reset the Area at the *start time* of each line.

Input

Click on the Browse/Ellipsis button and select an input. When that input goes into an Input Alarm state it will immediately generate an area report for the area listing all the cardholders that are currently in the area.

Output

Click on the Browse/Ellipsis button and select an output. When the area becomes empty (cardholder count drops to zero) the output will turn on (semi-permanently).

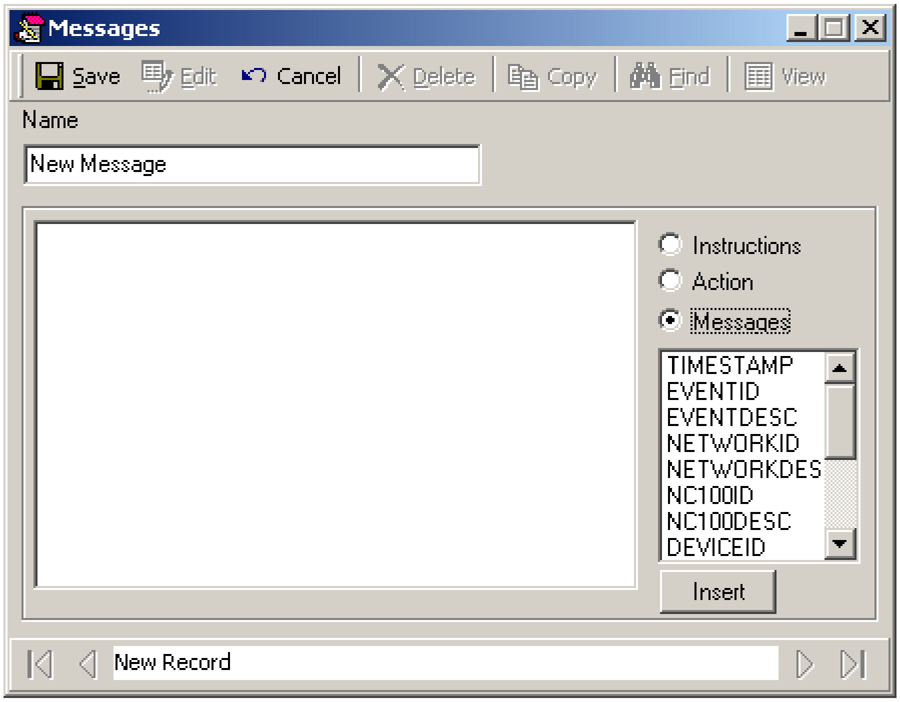
This feature automatically turns *ON* the output selected when Area is Empty, but doesn’t turn off the output when Area is not empty (cardholder count>0). The operator needs to turn it *Off* by operator command.

Antipassback Area

This is a check box to select if this area is an Antipassback Area. See Antipassback on page 20 for more details on antipassback.

Messages

Use the *Messages* window to define text to be associated with alarm messages. The message text provides instructions to operators monitoring security access with AxiomV™. These instructions can provide information on how to respond to a specific alarm, and standardized operator actions taken in response to an alarm. In this screen you can add, delete, change, or view these messages.



Name: New Message

○ Instructions
○ Action
● Messages

TIMESTAMP
EVENTID
EVENTDESC
NETWORKID
NETWORKDES
NC100ID
NC100DESC
DEVICEID

New Record

Name

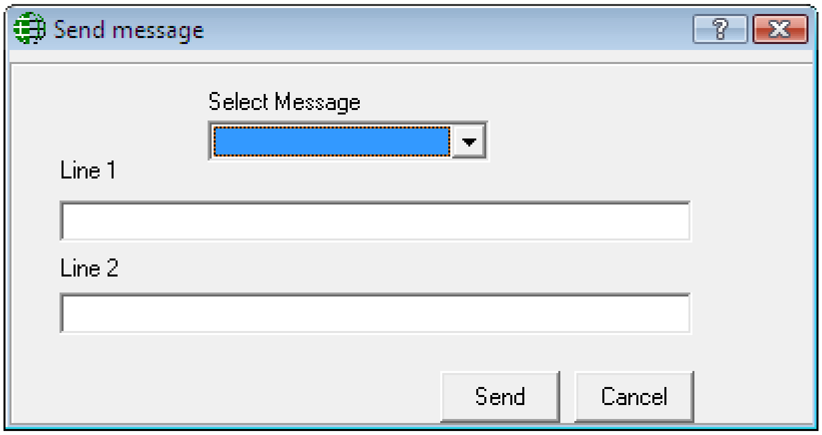
Up to 50 alphanumeric characters may be entered here.

Message Type

⊙ Instructions

Instruction message types are standard phrases that outline how an operator should respond to a particular alarm event. These instruction messages may be attached to specific alarm events and will pop-up to prompt the operator to behave in a predetermined way. Instruction messages are used to ensure standardized response to alarm events no matter which operator handles the alarm.

These messages can also be selected to send to SafeSuite™ keypads under the keypad command *Send Message*.



⦿ Action

Action message types are standard descriptions of the actions an operator might take frequently in responding to alarms. These messages are available for the operator to use when documenting how they handled a specific alarm event in the Alarm Details screen.

⦿ Messages

'Message' messages constitute an electronic instruction that may be defined and saved for transmission via a RS232 serial port on the Host PC, to any peripheral device that supports the ASCII standard. These messages may be assigned to access control events in the Advanced Programming screens for C-Net Networks, Access Points, and Inputs. The message will then be sent automatically upon the occurrence of the underlying event within the specified schedule.
There are a number of variables that may be inserted into your messages so that you can possibly use one message multiple times. Messages that you want to have the name of the point that caused the event or the time the event happened are examples of how these inserts can be used.

Inserts

TIMESTAMP	Date & Time of the event, acquired from the event message.
EVENTID	Identification number associated with the event.
EVENTDES	Description of the event, acquired from the event message.
NETWORKID	Identification number associated with the network of the event.
NETWORKDES	Description of the network, associated with the event message.
NC100ID	Identification number associated with the NC100 of the event.
NC100DES	Description of the NC100, associated with the event message.
DEVICESID	Identification number associated with the device (RC2, IOC16, or SafeSuite™ panel) of the event.
DEVICEDES	The description of the device (RC2, IOC16, or SafeSuite™ panel) associated with the event message.
CARDID	Identification number associated with the Card

CARDNUMBER Card number associated with the event.

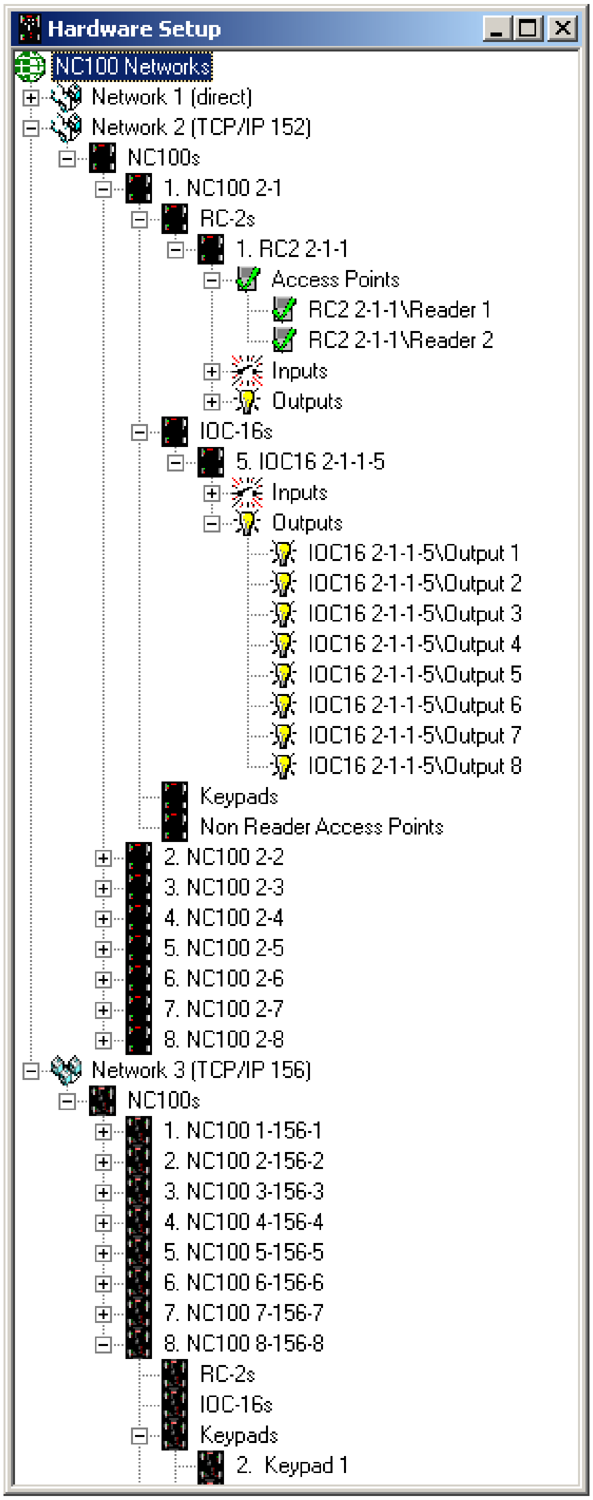
CARDHOLDER Name of the cardholder associated with the event.

USAGECOUNT Usage count assigned to a card.

Any fields that have been added under Custom Fields will also be on this list.

Hardware Setup

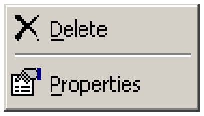
The *Hardware Setup* screen is where new hardware items are added to the system



```
NC100 Networks
  Network 1 (direct)
  Network 2 (TCP/IP 152)
    NC100s
      1. NC100 2-1
        RC-2s
          1. RC2 2-1-1
            Access Points
              RC2 2-1-1\Reader 1
              RC2 2-1-1\Reader 2
            Inputs
            Outputs
        IOC-16s
          5. IOC16 2-1-1-5
            Inputs
            Outputs
              IOC16 2-1-1-5\Output 1
              IOC16 2-1-1-5\Output 2
              IOC16 2-1-1-5\Output 3
              IOC16 2-1-1-5\Output 4
              IOC16 2-1-1-5\Output 5
              IOC16 2-1-1-5\Output 6
              IOC16 2-1-1-5\Output 7
              IOC16 2-1-1-5\Output 8
        Keypads
        Non Reader Access Points
      2. NC100 2-2
      3. NC100 2-3
      4. NC100 2-4
      5. NC100 2-5
      6. NC100 2-6
      7. NC100 2-7
      8. NC100 2-8
  Network 3 (TCP/IP 156)
    NC100s
      1. NC100 1-156-1
      2. NC100 2-156-2
      3. NC100 3-156-3
      4. NC100 4-156-4
      5. NC100 5-156-5
      6. NC100 6-156-6
      7. NC100 7-156-7
      8. NC100 8-156-8
        RC-2s
        IOC-16s
        Keypads
          2.  Keypad 1
```

Networks

Right click on *NC100 Networks* to add a new network to the system. This will bring up the network properties window to set the properties of the new network. Under the newly created Network will be an icon to add NC100s. Up to fifteen NC100s/UNC500s can be connected on one network.



Right click on a Network to either delete that Network or to go into the Network's properties screen.

Network Properties

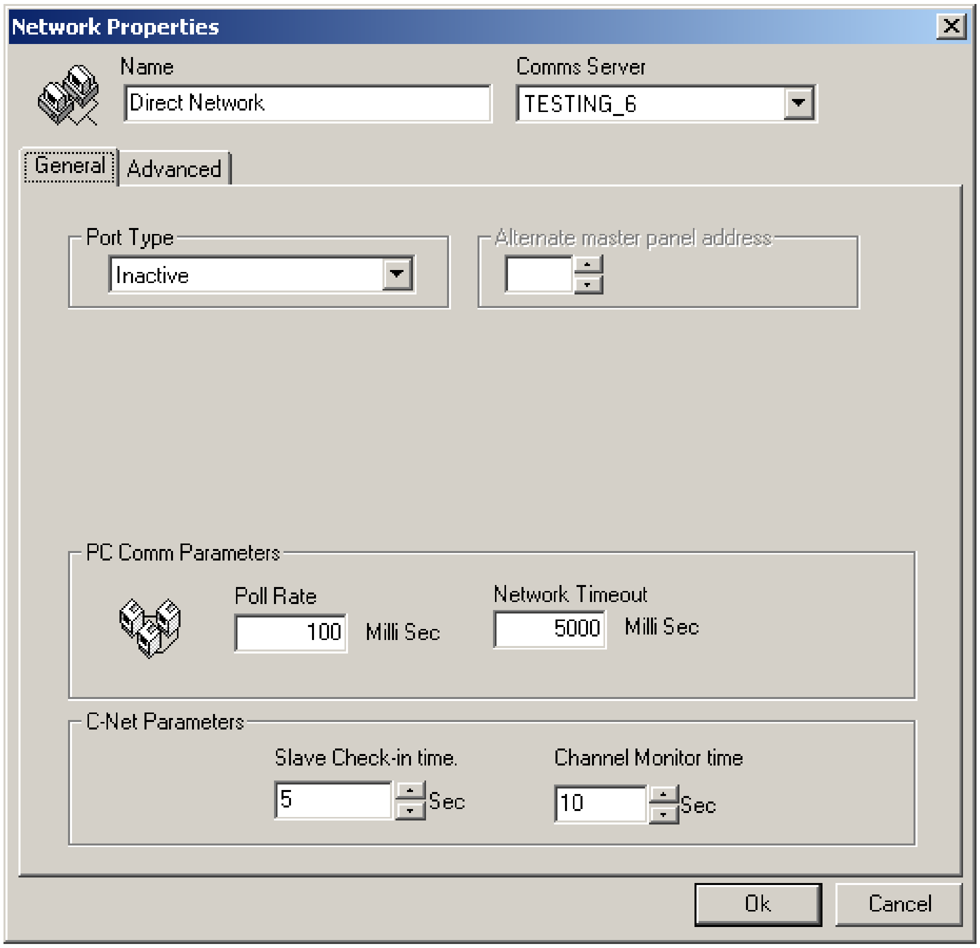
Name

Up to 50 alphanumeric characters may be entered here.

Comms Server

Select which Comms Server this network is connected to.

General



Network Properties

Name: Direct Network

Comms Server: TESTING_6

Port Type: Inactive

Alternate master panel address:

PC Comm Parameters

Poll Rate: 100 Milli Sec

Network Timeout: 5000 Milli Sec

C-Net Parameters

Slave Check-in time. 5 Sec

Channel Monitor time 10 Sec

Port Type

AxiomV™ supports the following applications for communication ports:

Inactive

Inactive is the default setting for ports not in use. This setting is also selected to disable the port.

Direct Network

Direct Network supports a controller network (*C-NET*) connected directly to the host PC via serial connections.

TCP/IP Network

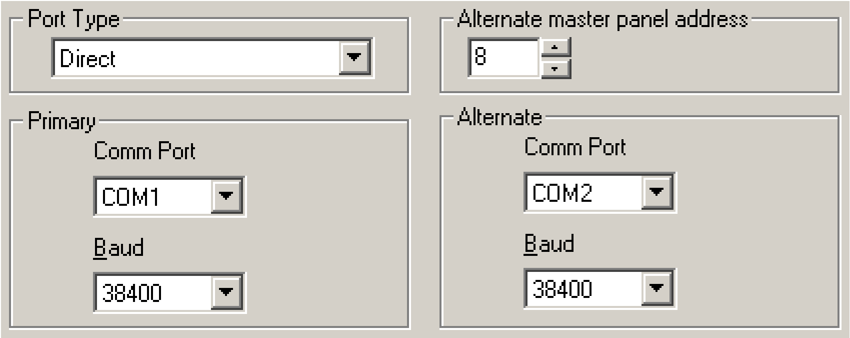
TCP/IP Network supports TCP/IP controller network (*C-NET*) through a LAN connection.

Alternate master panel address[11]

Use the spin buttons to select the address of the alternative or backup master NC-100. If the Axiom server loses communications with the primary master NC-100 panel (address #1) it will switch to the alternate master panel to resume communications with the network. This feature requires NC100 firmware version 7.40+.

Port Properties

Direct Network Properties



Port Type: Direct

Alternate master panel address: 8

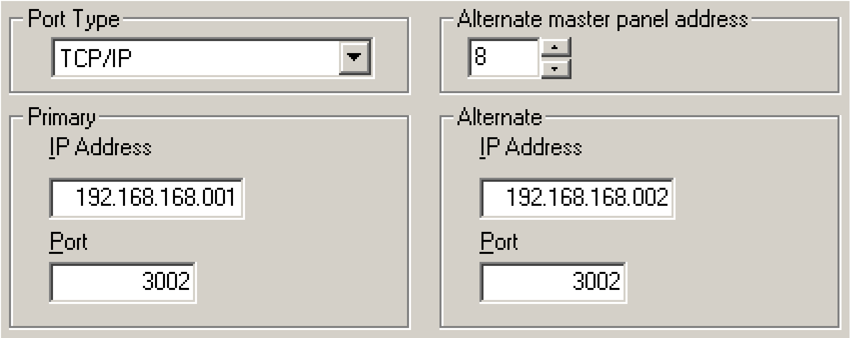
Primary
Comm Port: COM1
Baud: 38400

Alternate
Comm Port: COM2
Baud: 38400

Select the Comm port and Baud rate for the direct connection of this network.

[11] This selection is only available if the optional license for the Alternate Master NC100 Software has been purchased and installed.

TCP Network Properties



Port Type: TCP/IP

Alternate master panel address: 8

Primary
IP Address: 192.168.168.001
Port: 3002

Alternate
IP Address: 192.168.168.002
Port: 3002

Enter the IP address of the LIF200 (Network module) connected to NC100 as well as its port number.

PC Comm Parameters

PC Polling parameters specify the times used by the PC in polling the Master controller on the C-NET. Normally, the default settings do not need to be changed.

Poll Rate

Poll Rate establishes the interval between PC initiated polling attempts.

Network Timeout

Network Timeout establishes the duration of time that must expire before the PC will declare a '*Communications Offline'* condition. AxiomV™ comes with a default timeout of 1000-milliseconds

C-Net Parameters

The C-Net parameters are for communications between the master NC100 controller and slave NC100 controllers on the C-Net. The master NC100 does not poll the slaves. Rather, each slave NC100 on the C-Net sends test signals to the master NC100 approximately every 10 milliseconds, alternating between communications channel A, and communications channel B.

Slave Check In Time

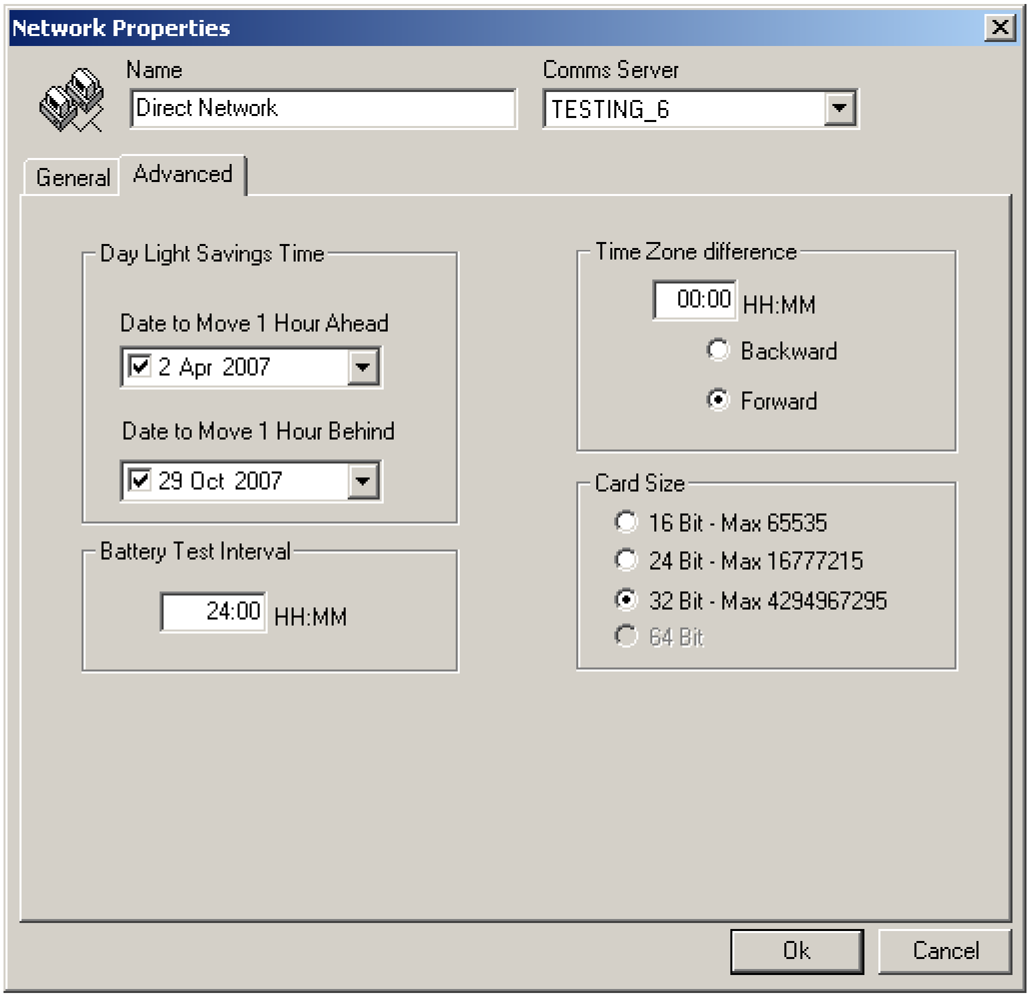
Slave Check In Time establishes the maximum amount of time, in seconds that can elapse between communications of any kind with the slave NC100 on either channel A or channel B. Beyond this value, the master NC100 will declare the slave *Offline* and generate an alarm.

Channel Monitor time

Establishes the maximum amount of time that can elapse between successful tests either of the communication channels A and B. Beyond this value, a *Channel Fault Condition* will be declared and reported for the channel whose monitor time expired.

Advanced

The *Advanced* tab has additional parameters for the network.



Network Properties

Name: Direct Network

Comms Server: TESTING_6

Day Light Savings Time

Date to Move 1 Hour Ahead: ☑ 2 Apr 2007

Date to Move 1 Hour Behind: ☑ 29 Oct 2007

Battery Test Interval: 24:00 HH:MM

Time Zone difference: 00:00 HH:MM

○ Backward

● Forward

Card Size

○ 16 Bit - Max 65535

○ 24 Bit - Max 16777215

● 32 Bit - Max 4294967295

○ 64 Bit

Day Light Savings Time

Check the boxes to enable the NC100 to change the time of day because of Day Light Savings Time. Enter the dates to change on by selecting them from the pull down calendar or by typing it in. These dates are not automatically set for the next year so they need to be entered every year. The actual change is done by the NC100 (not the PC) so the dates need to be downloaded to the NC100 before the change date.

Battery Test Interval

The Battery Test Interval is set in hours and minutes only.

☞ **The battery test is an *interval* and not a time of day.** The time of day that the battery is tested cannot be set manually.

Time Zone Difference

The *Time Zone Difference* is set in hours and minutes. It is used when a network is located in a different Time Zone than the server. Downloads to set the time on the network will be adjusted by this setting.

Card Size

The card size will limit the functionalities of cards by not allowing certain functions like Lock/Unlock and high security privilege for a larger card numbers(Card #> 65535) when only 16 bit card size is selected. Maximum card number allowed in the cardholder database is 4294967295.Allowing larger card numbers will use more of the NC100's memory.

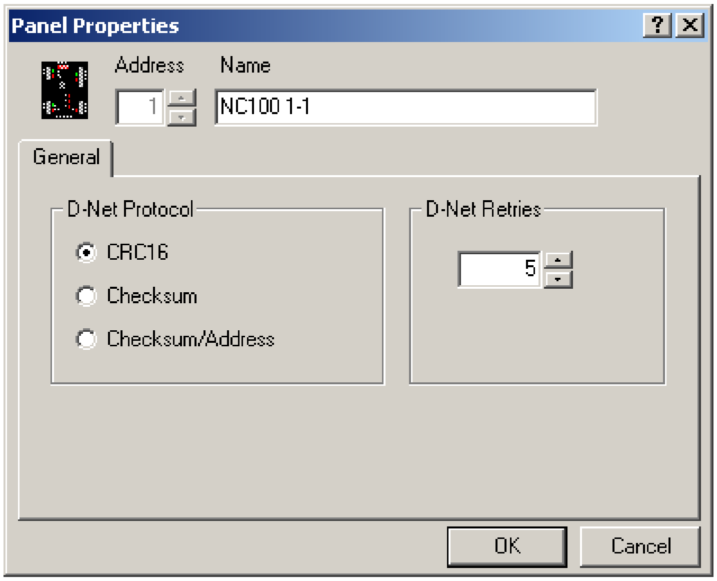
NC100s

Right click on *NC100s* to add a new NC100 /UNC500 panel to the system. This will bring up the panel properties window to set the properties of the new NC100/UNC500. Under the newly created NC100 will be four icons: to add RC2s, IOC16s, Keypad and Non Reader Access points. Up to four RC2s, sixteen IOC16s and 255 keypads can be connected on each NC100/UNC500.

Right click on an NC100 to either delete the NC100 or to go into the NC100's properties screen.

NC100 Properties

Properties for the NC100 are set in this window. The address is set when the NC100 is created in the system and cannot be edited later.



Address: 1
Name: NC100 1-1

D-Net Protocol
● CRC16
○ Checksum
○ Checksum/Address

D-Net Retries: 5

Name

Up to 50 alphanumeric characters may be entered here.

General

D-Net Protocol

Select one of three protocols for the D-Net.

- ***CRC16*** is a newer more up to date protocol that is now programmed into all devices.
- ***Checksum*** is the original protocol for the D-Net and is still included in the system for backward compatibility to original devices that are still working out in the field.
- ***Checksum/Address*** was created for a special application and adds sixteen to the address of all devices in the network.

D-Net Retries

D-Net Retries specify the number of times that the NC100 will try to communicate with the D-Net (Device Network) controllers, i.e. RC2s and IOC16s before declaring and reporting an Offline condition. The default is five.

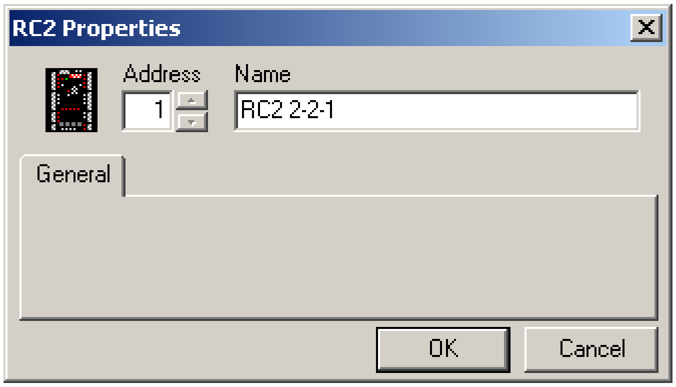
RC2s

Right click on *RC2s* to add a new RC2 to the system. This will bring up the RC2 properties window to set the properties of the new RC2. Adding an RC2 will also add two access points, eight inputs, and eight outputs. The eight outputs and four of the inputs will be defaulted for the access points but can be changed to general purpose if needed.

Right click on an RC2 to either delete the RC2 or to go into the RC2's properties screen.

RC2 Properties

Properties for the RC2 are set in this window. The address is set when the RC2 is created in the system and cannot be edited later.



Address: 1

Name: RC2 2-2-1

Address

RC-2s can only be addressed 1-4; no other addresses are valid for RC-2s

Name

Up to 50 alphanumeric characters may be entered here.

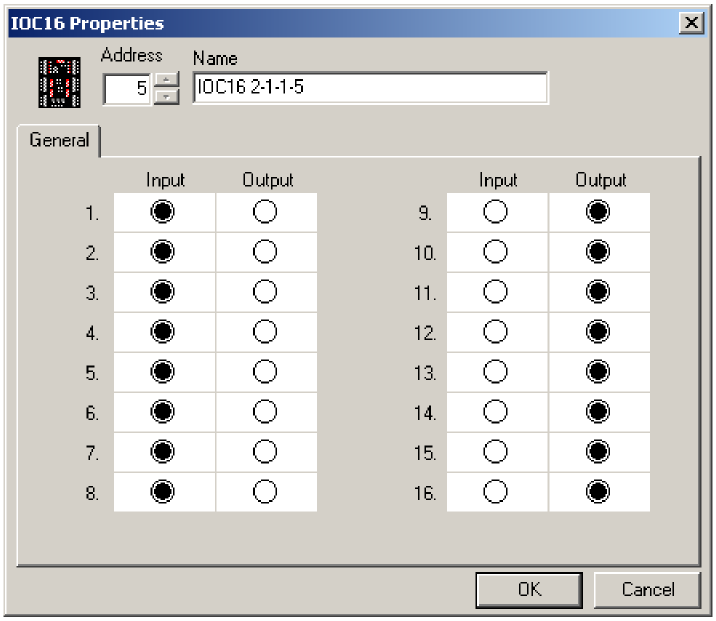
IOC16s

Right click on IOC*16s* to add a new IOC16 to the system. This will bring up the IOC16 properties window to set the properties of the new IOC16.

Right click on an IOC16 to either delete the IOC16 or to go into the IOC16's properties screen.

IOC16 Properties

Properties for the IOC16 are set in this window. The address is set when the IOC16 is created in the system and cannot be edited later.



Address: 5

Name: IOC16 2-1-1-5

General

	Input	Output		Input	Output
1.	●	○	9.	○	●
2.	●	○	10.	○	●
3.	●	○	11.	○	●
4.	●	○	12.	○	●
5.	●	○	13.	○	●
6.	●	○	14.	○	●
7.	●	○	15.	○	●
8.	●	○	16.	○	●

Address

IOC-16s can only be addressed 5-20; no other addresses are valid for IOC-16s

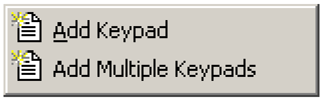
Name

Up to 50 alphanumeric characters may be entered here.

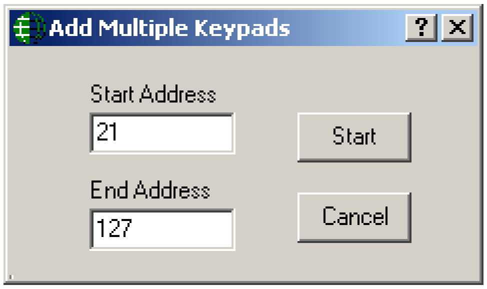
General

For each of the sixteen ports of the IOC-16 choose whether that port is to be an input or an output.

Keypads

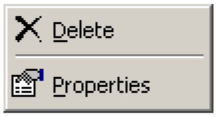


Right click on Keypads to either add one new Keypad to the system or a group of consecutively addressed Keypads. Adding one will bring up the Keypad properties window to set the properties of the new Keypad. Selecting *Add Multiple Keypads* will bring up a window to set the start and end addresses of the keypads being added.



Start Address: 21
End Address: 127

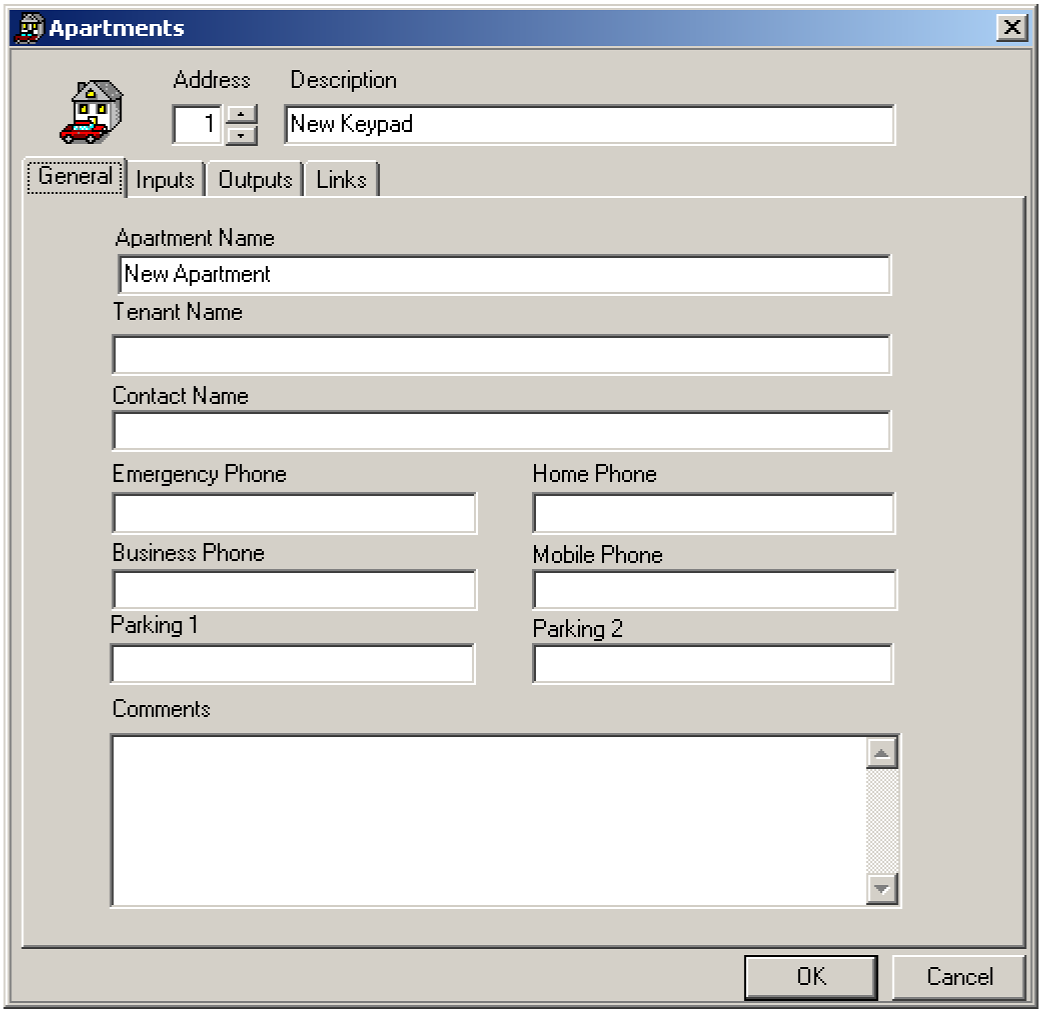
Click *Start* to add the keypads.



Right click on a Keypad to either delete the Keypad or to go into the Keypad's properties screen.

Keypad Properties

Properties for the Keypad are set in this window. The address is set when the Keypad is created in the system and cannot be edited later.



Address: 1
Description: New Keypad

Apartment Name: New Apartment
Tenant Name:
Contact Name:
Emergency Phone:
Home Phone:
Business Phone:
Mobile Phone:
Parking 1:
Parking 2:
Comments:

Address

Keypads can be addressed from 1-255. Be aware of RC-2 and IOC-16 addressing, it is possible to duplicate addresses and cause communication problems. It is advisable to start addressing Keypad at 21 so that future expansion can add RC-2s and IOC-16s.

Keypads added singly are addressed from the properties screen while keypads added as a group are addressed as they are added.

Description

Up to 50 alphanumeric characters may be entered here.

General

Apartment Name

Up to 50 alphanumeric characters may be entered here.

Tenant Name

Up to 50 alphanumeric characters may be entered here.

Contact Name

Up to 50 alphanumeric characters may be entered here.

Emergency Phone

Up to 50 alphanumeric characters may be entered here.

Home Phone

Up to 50 alphanumeric characters may be entered here.

Business Phone

Up to 50 alphanumeric characters may be entered here.

Mobile Phone

Up to 50 alphanumeric characters may be entered here.

Parking 1

Up to 50 alphanumeric characters may be entered here.

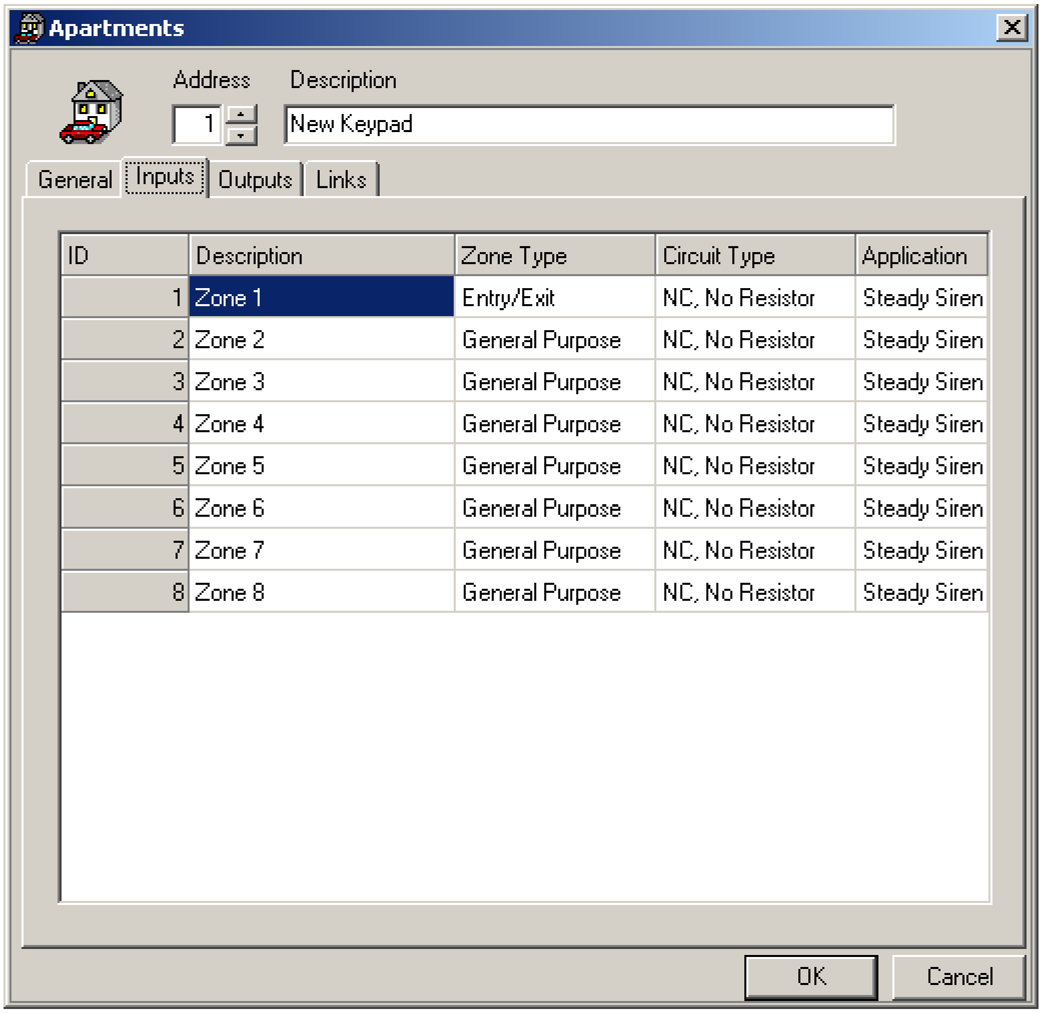
Parking 2

Up to 50 alphanumeric characters may be entered here.

Comments

Up to 255 alphanumeric characters may be entered here.

Inputs



Address: 1

Description: New Keypad

ID	Description	Zone Type	Circuit Type	Application
1	Zone 1	Entry/Exit	NC, No Resistor	Steady Siren
2	Zone 2	General Purpose	NC, No Resistor	Steady Siren
3	Zone 3	General Purpose	NC, No Resistor	Steady Siren
4	Zone 4	General Purpose	NC, No Resistor	Steady Siren
5	Zone 5	General Purpose	NC, No Resistor	Steady Siren
6	Zone 6	General Purpose	NC, No Resistor	Steady Siren
7	Zone 7	General Purpose	NC, No Resistor	Steady Siren
8	Zone 8	General Purpose	NC, No Resistor	Steady Siren

Description

Up to 50 alphanumeric characters may be entered here.

Zone Type

General Purpose: Never armed.

Entry/Exit: Provides Entry Delay time to disarm before the keypad goes into alarm, and Exit Delay time to leave the protected area before the keypad fully arms.

Follower: Follows the delay time of the Entry/Exit zone but only if the Entry/Exit zone is tripped first.

Interior: Not armed in Instant mode or Home mode.

Exterior:	Instant acting zone that is armed and disarmed with the Keypad.
24 Hour Delayed:	Always armed zone that provides a time period to clear the zone before initiating an alarm.
24 Hour:	Always armed zone.
Arm/Disarm Switch:	Tripping this zone arms or disarms the keypad.

Circuit Type

NC, No Resistor

NO, No Resistor

NC, One Resistor

NO, One Resistor

NC, Two Resistors

NO, Two Resistors

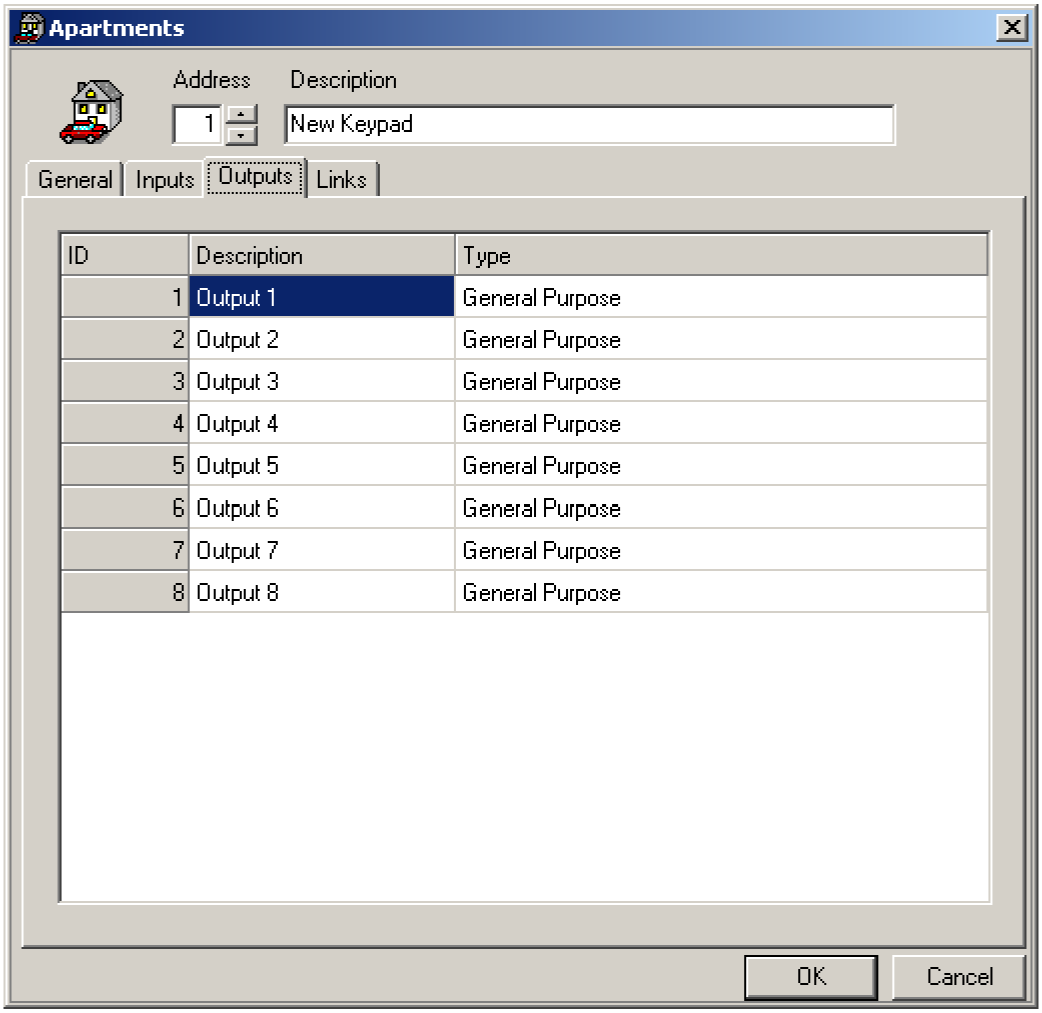
NC & NO, One Resistor

See the Hardware Manual for more information on Circuit Types.

Application

Buzzer:	Sound only the Keypad buzzer on alarm.
Pulse Siren:	Pulse the siren output on and off during an alarm.
Pulse Siren /Buzzer:	Pulse the siren output and the Keypad buzzer on an alarm.
Silent:	No output on an alarm.
Steady Siren:	Turn on the siren output during an alarm.
Steady Siren/Buzzer:	Turn on the siren output and the Keypad buzzer during an alarm.

Outputs



Address: 1

Description: New Keypad

ID	Description	Type
1	Output 1	General Purpose
2	Output 2	General Purpose
3	Output 3	General Purpose
4	Output 4	General Purpose
5	Output 5	General Purpose
6	Output 6	General Purpose
7	Output 7	General Purpose
8	Output 8	General Purpose

Description

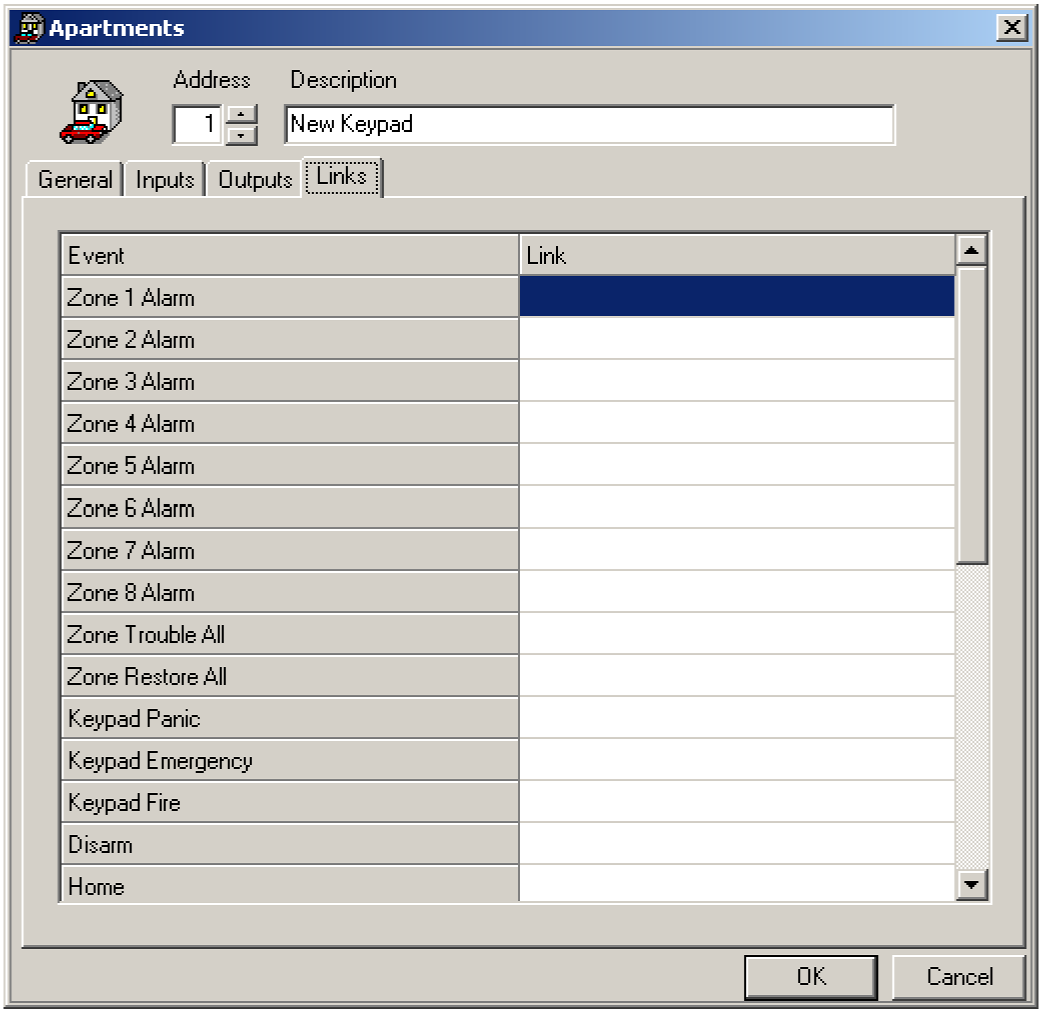
Up to 50 alphanumeric characters may be entered here.

Type

General Purpose:	Has no predetermined function.
Siren:	Turns on to power an audible device for Alarms.
Status LED:	Turn on to indicate that the Keypad is armed.
OK to Arm LED:	Turn on to indicate that all zones are normal and the Keypad may be armed.
Buzzer:	Turns on to drive an audible that follows the Keypad's buzzer.
Lock:	This output is used to activate a door lock.

LED1: & *LED2*: These outputs are used to drive the red and green LEDs of a card reader connected to the Keypad.

Links



Address: 1

Description: New Keypad

Event	Link
Zone 1 Alarm	
Zone 2 Alarm	
Zone 3 Alarm	
Zone 4 Alarm	
Zone 5 Alarm	
Zone 6 Alarm	
Zone 7 Alarm	
Zone 8 Alarm	
Zone Trouble All	
Zone Restore All	
Keypad Panic	
Keypad Emergency	
Keypad Fire	
Disarm	
Home	

From here you can select a link and have it executed on an event appropriate to the Keypad. For example you could turn on an output when a specific zone went into alarm.

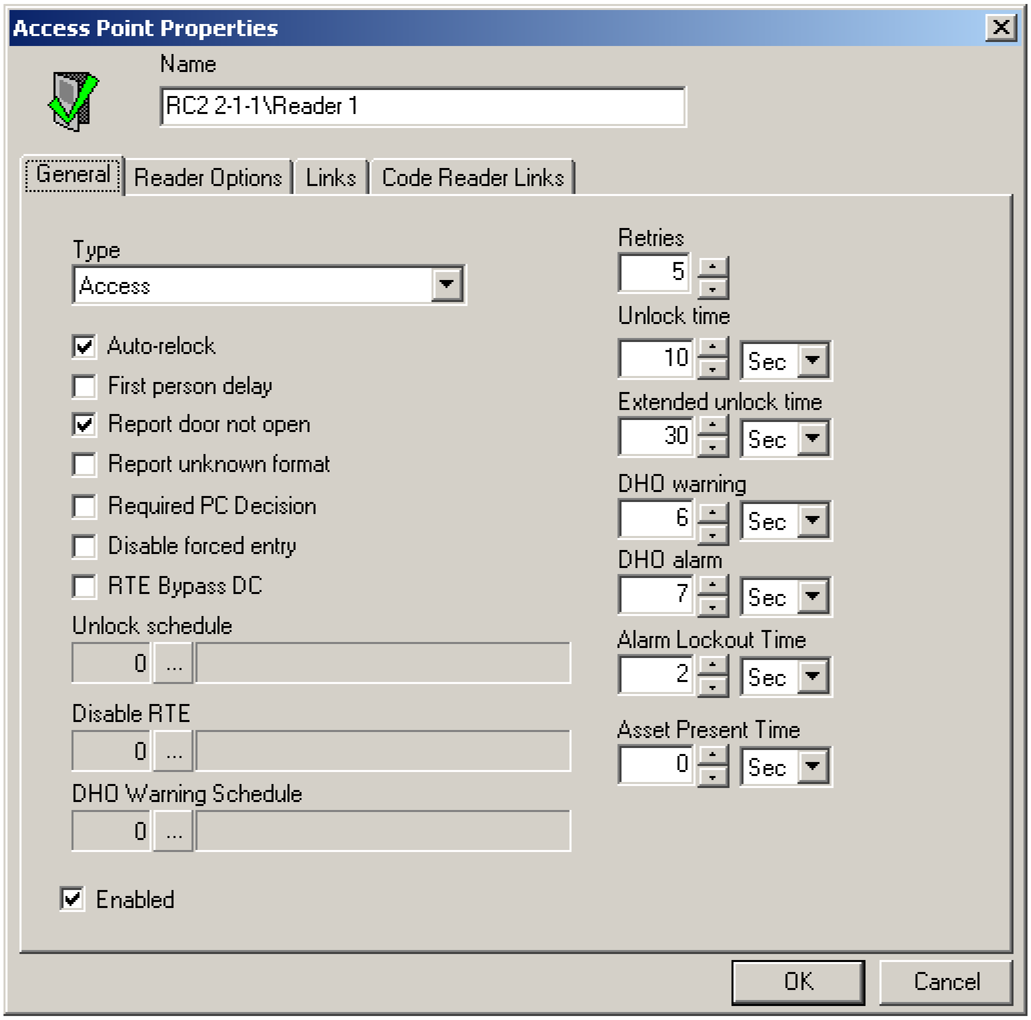
To select a link click on the box under *Link* that is beside the event you want the link to be executed by. Then click the *Browse/Ellipsis button* and search for the desired link.

Access Points

Two access points are created automatically when an RC2 is added.

Access Point Properties

Set the Access Point’s properties from this window.



Access Point Properties

Name: RC2 2-1-1\Reader 1

Type: Access

☑ Auto-relock
☐ First person delay
☑ Report door not open
☐ Report unknown format
☐ Required PC Decision
☐ Disable forced entry
☐ RTE Bypass DC

Unlock schedule: 0
Disable RTE: 0
DHO Warning Schedule: 0

☑ Enabled

Retries: 5
Unlock time: 10 Sec
Extended unlock time: 30 Sec
DHO warning: 6 Sec
DHO alarm: 7 Sec
Alarm Lockout Time: 2 Sec
Asset Present Time: 0 Sec

Name

Up to 50 alphanumeric characters may be entered here.

General

Type

The types of access point are:

Access – normal operation, system controls access to door via a reader.

Elevator – allows user to select a floor button after valid card presentation.

Patient Door – patient monitoring system card reader.

Patient Elevator – patient reader installed in elevator cab.

Time and Attendance – for future use.

Sentex – for Telephone Entry integration.

Asset Door – for Asset tracking.

Asset Reporting – for Asset monitoring.

Random Search-for additional security screening where 12 out of every 256 reads are denied access randomly.

Auto Relock

Check this box to enable the *Auto Relock* feature. When enabled, the door will lock, (or return to normal lock position), following a valid access code entry or access request, as soon as the door contact closes. When disabled, the lock output remains unlocked for the duration of the *Unlock Time* that is assigned. (See Unlock Time below.)

First Person Delay

When this box is checked, the *First Person Delay* feature is activated. For systems where the door is automatically unlocked by a schedule, this feature overrides the unlock schedule until a valid card is presented at the reader. After the first valid person enters the door, the lock reverts to the time group schedule.

As an example, consider a store that opens from 9am to 6pm and where the entrance door is controlled by an unlock schedule. If for any reason store employees are late arriving, we do not want the schedule to open the store. By enabling *First Person Delay*, the store will remain locked until the first person arrives regardless of how late he/she may be.

Report Door Not Open

Check this box to activate the *Report Door Not Open* alarm feature. With this feature enabled, a Door Not Open alarm will be generated and reported on the monitor screen, each time a valid card is presented at the reader, but no one actually enters through the access point. This feature is useful in time and attendance applications.

If this feature is disabled, the Door Not Open event will still be logged in the history file, but will not display on the Monitor screen. If so selected under *Advanced Programming* for access points, a Door Not Open alarm will display on the Alarm screen.

Report Unknown Format

Check this box to activate the *Report Unknown Format* feature. If a card with an unknown format is then presented at this reader, the system will generate an Unknown Format Alarm and display it on the Monitor screen.

If this feature is disabled, the Unknown Format event will still be logged in the history file, but will not display on the screen. If so selected under *Advanced Programming* for access points, an Access Denied alarm will display on the Alarm screen each time a card with an unknown format is presented to this reader.

Required PC Decision

When this box is checked the decision to grant access is not made by the NC100. The NC100 will do its regular verification of the card but will not grant access. Instead it will simply notify the PC if access is to be granted a command must come from the PC.

Disabled Forced Entry

Check this box, to disable normal *Forced Entry* alarm operation. When *Forced Entry* is disabled, opening the door simulates the operation of the request to exit input.

RTE Bypass DC

Check this box to enable the *Request-to-Exit Bypass Door Contact Only* feature. When enabled, a request to exit input at the access point, bypasses the door contact only, and does not unlock the door. This operation is typically selected where a motion detector is connected to the request to exit input and the door uses a door strike that can be manually opened from the inside.

Unlock Schedule

Use the *Browse/Ellipsis button* to select the *Schedule* during which this access point is to remain unlocked.

Disable Request to Exit

Use the *Browse/Ellipsis button* to select the *Schedule* during which the RTE function is disabled at this access point. In other words, the system does not respond to requests to exit.

Disable DHO Warning

Use the *Browse/Ellipsis button* to select the *Schedule* during which *Door Held Open* (*DHO*) warning is disabled for this access point.

Retries

Retries specifies the maximum number of consecutive invalid card/PIN reads permitted (1-16), before a lockout alarm is created and the system rejects further access attempts to grant access.

Unlock Time

Unlock Time sets the amount of time a door will remain unlocked after a valid RTE or card presentation. The system default is 10 seconds. The *Unlock Time* applies to the door and is valid for all cardholders in the system.

When *Auto Relock* is enabled on the access point window, the access point will lock when the door is shut, or when the unlock time expires, whichever happens first.

Extended Unlock Time

The *Extended Unlock Time* feature may be used to allow particular cardholders, who require more than the standard *Unlock Time*, to pass through an access point. Use *Extended Unlock Time* to set the amount of time, (usually more than the Unlock Time), that a door remains unlocked after presentation by a cardholder that has been given '*Extended Unlock'* privilege.

When *Auto Relock* is enabled on the access point window, the access point will lock when the door is shut, or when the Extended unlock time expires (for the cardholders who are assigned Extended unlock time), whichever happens first.

DHO Alarm

This setting is used to set the maximum amount of time a door can be held open beyond the expiry of the *Unlock Time* without generating an alarm. On expiry of the *DHO* time, the system creates an alarm and emits a continuous warning sound until the door is closed.

DHO Warning

This setting is used to set the maximum amount of time a door can be held open beyond the expiry of the *Unlock Time* without generating a warning. On expiry of the *DHO Warning* time, the system reports to the PC and the card reader emits a periodic warning sound until the door is closed.(DHO Warning is reported on screen only for the schedule assigned for *DHO warning schedule* and is not reported at all if no schedule is assigned)

DHO Alarm overrides the DHO Warning. Generally the alarm time is longer than the warning time so that a warning will be activated before the alarm. If the alarm time is shorter than the warning time there won't be a warning only an alarm

Alarm Lockout Time

This setting is used to set the minimum duration that a reader locks out any further access attempts, when the *Number Retries* is exceeded.

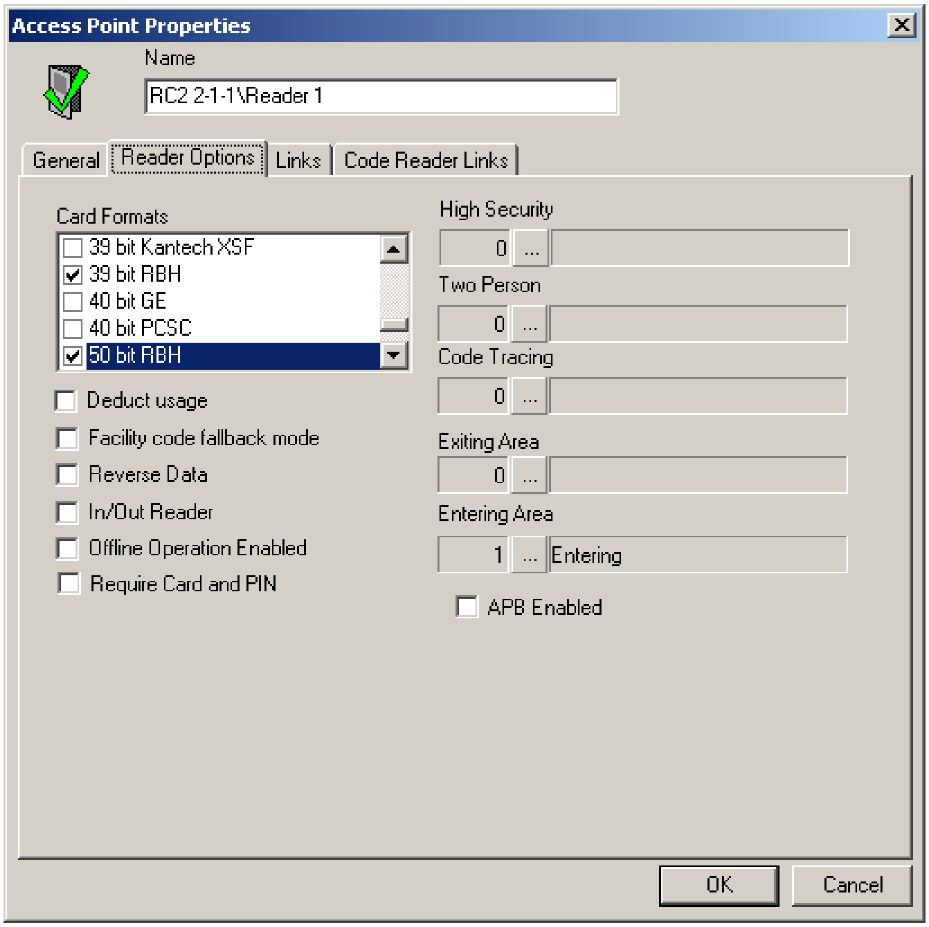
Asset Present Time

Asset Present Time is the amount of time that the Access Point will be in Asset Mode waiting for the Asset's owner to present their card.

☑ Enabled

Unchecking the *Enabled* box will make the access point unavailable to the status list. Since it is not on the status list commands cannot be sent to it. It will not be removed from the database or prevented from sending messages.

Reader Options



Name: RC2 2-1-1\Reader 1

Card Formats
- □ 39 bit Kantech XSF
- ☑ 39 bit RBH
- □ 40 bit GE
- □ 40 bit PCSC
- ☑ 50 bit RBH

- □ Deduct usage
- □ Facility code fallback mode
- □ Reverse Data
- □ In/Out Reader
- □ Offline Operation Enabled
- □ Require Card and PIN

High Security: 0 ...
Two Person: 0 ...
Code Tracing: 0 ...
Exiting Area: 0 ...
Entering Area: 1 ... Entering

□ APB Enabled

Reader Formats

This window lists all available card reader bit formats. Readers may be configured to support up to five different formats simultaneously. Click to select (check) or unselect (uncheck) a format on the list.

Deduct Usage

If this box is checked, a usage is deducted each time access is granted to a card that has been configured with a limited number of uses. (For more information on *Usage Count* check page 280 in Chapter 7).

Facility Code Fall Back

When an access card is presented under normal conditions the NC100 gets the card number and facility code from the RC2 and decides whether or not to grant access. If communication is lost between the NC100 and the RC2, the RC2 still can grant access based on correct facility code, if the *Facility Code Fallback* feature is enabled. Check this box to enable the *Facility Code Fallback* feature for this access point.

Reverse Data

Check this box to enable the *Reverse Data* feature. When enabled, the RC2 will reverse the data string read from the card. This is generally used in insertion readers so that the proper data is read when the card is removed from the reader, and not when the card is inserted.

In/Out Reader

In/Out Reader mode is used when a single RC2 has both its readers controlling the same door, one for entry, and one for exit (two readers, one door lock, and one door contact). The door lock, the door contact, and the entry reader are connected to the A-side of the RC2. The exit reader is connected to the B-side of the RC2. In this configuration, the B-side of the RC2 acts as a slave to the A-side. Both readers can be configured separately with different parameters. Yet when activated the B-side reader will use the A-side inputs and outputs.

☞ **This box must be checked for both the side A and side B readers.**

Offline Operation Enabled

Checking this box means that the NC-100 will download card data to the reader controller. This will allow the controller to function after losing communications with the NC-100/UNC500.

Hardware Requirements

NC-100 firmware must be 8.27. An NRC must be used with firmware version 9.1, instead of RC-2. For more detailed information check Technical Bulletin ‘TB_58 RC Stand Alone Mode”.

Require Card and PIN

Checking the *Require Card and PIN* box will cause this access point to only grant access if the correct PIN is entered after a card is read. This is used to increase the level of security at an access point, since only presenting a card will not be given an access granted.

High Security

Use the *Browse/Ellipsis button* to select the *Schedule* during which *High Security* mode is automatically enabled. In *High Security* mode, only cards with high security privileges, may gain access to this access point.

Two Person

Use the *Browse/Ellipsis button* to select the *Schedule* during which two valid cards must be presented in order for access to be granted. Note that the second card must be presented within ten seconds of the first.

Code Tracing

Use the *Browse/Ellipsis button* to select the *Schedule* during which this reader traces cards that have been defined with the *Trace This Card* option enabled in the *Cardholder Configuration* screen.

Exiting Area

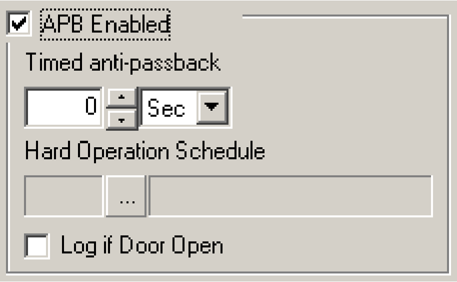
Exiting Area is used to set the area from which the access point leaves. This area must be specified in order to use the *Area Antipassback* feature.

Entering Area

Entering Area is used to set the area into which the access point goes into. This area must be specified in order for *Antipassback*, *Mustering,* and *Card Tracing* features to operate.

APB Enabled

Check this box to enable Antipassback.



☑ APB Enabled

Timed anti-passback

0 Sec

Hard Operation Schedule

☐ Log if Door Open

Timed Antipassback

Use this setting to set the minimum amount of time that must expire, before a card that was presented to this reader previously, may be used again at this same reader.

To use Reader/Area antipassback but not *Timed Antipassback* ensure that the time in *Timed Antipassback* is set to zero. Once a time is set in *Timed Antipassback* then *Timed Antipassback* will be in effect instead of any other form of antipassback.

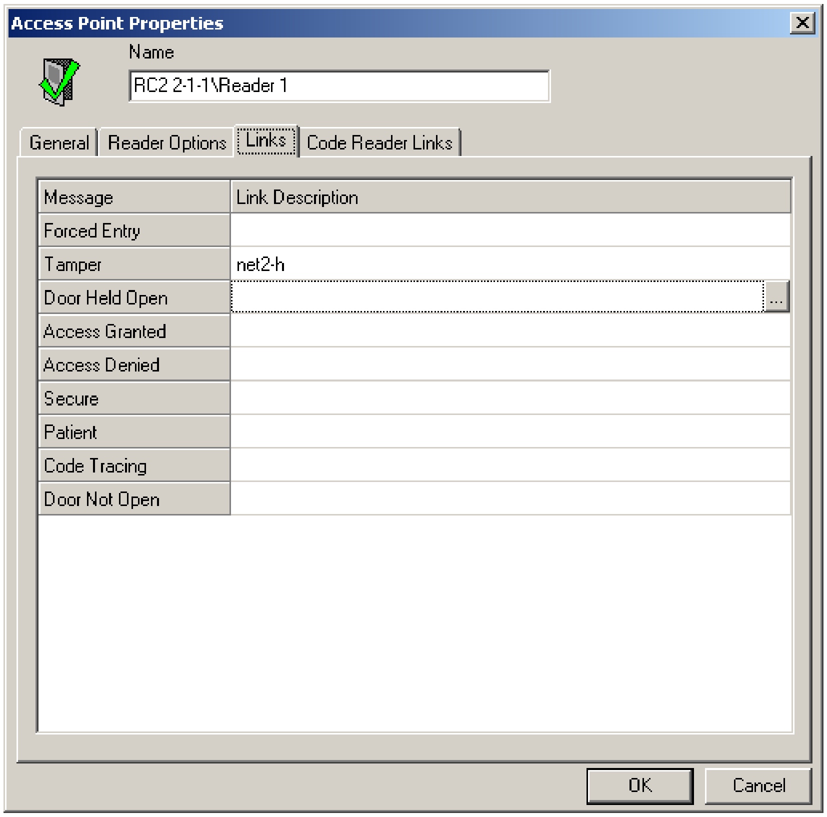
Hard Operation Schedule

Use the *Browse/Ellipsis button* to select the *Schedule*, during which, access will be denied when either a *Reader Antipassback* or an *Area Antipassback* violation occurs. When the violation occurs outside of this *Schedule,* access is permitted and reported as an "Access Granted Antipassback Reader".

Log if Door Open

Place a checkmark in this box to activate the *Log If Door Open* feature. When active, the cardholder must present their card and actually open the door before they are logged (in the Cardholder database) into the area being entered. If this box is not checked then a successful grant access will log the cardholder into the *Entering Area* even if they don't open the door.

Links

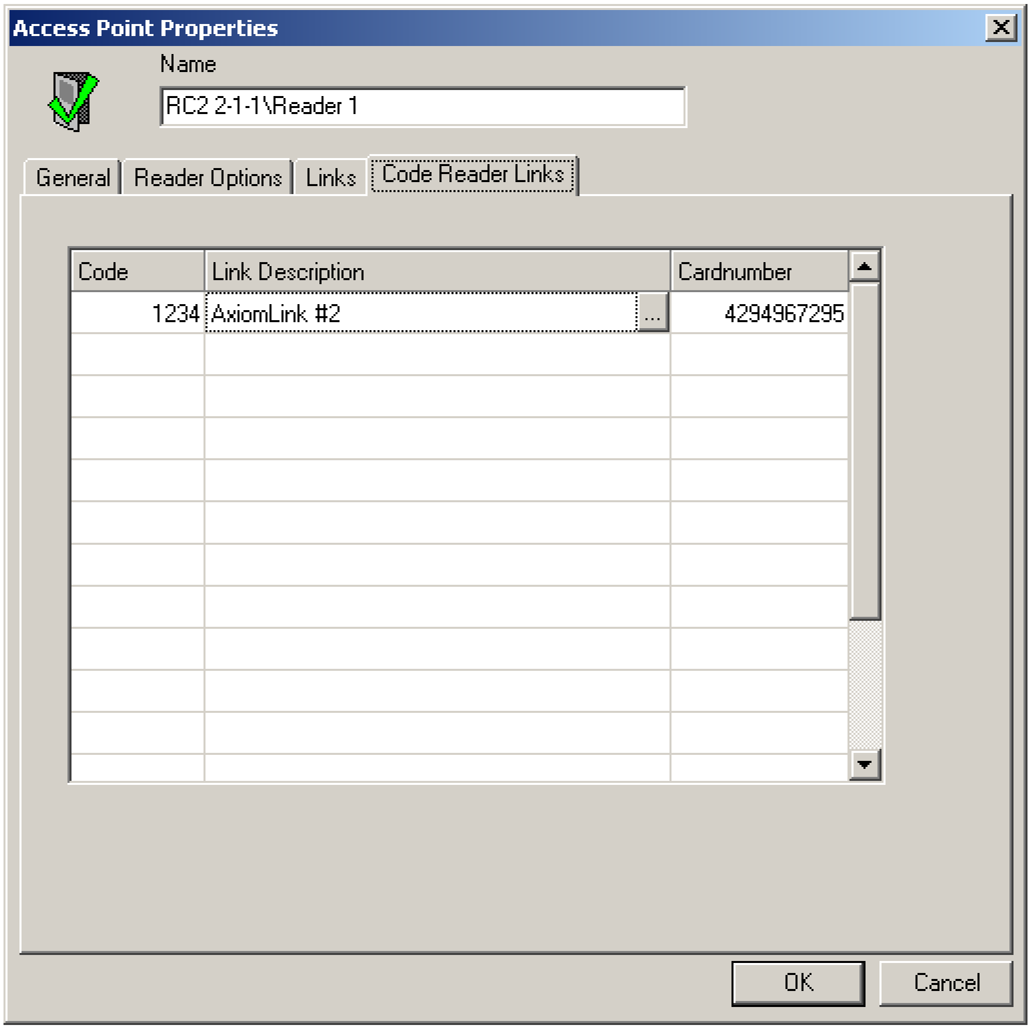


Name: RC2 2-1-1\Reader 1

Message	Link Description
Forced Entry	
Tamper	net2-h
Door Held Open	
Access Granted	
Access Denied	
Secure	
Patient	
Code Tracing	
Door Not Open	

To establish a link click in the *Link Description* box beside the *Message* you want the link activated on. Then click the *Browse/Ellipsis button* and select the desired link from the list presented. The name of the chosen link will be shown in the *Link Description* box to confirm the link programming.

Code Reader Links



Name: RC2 2-1-1\Reader 1

Code	Link Description	Cardnumber
1234	AxiomLink #2	4294967295

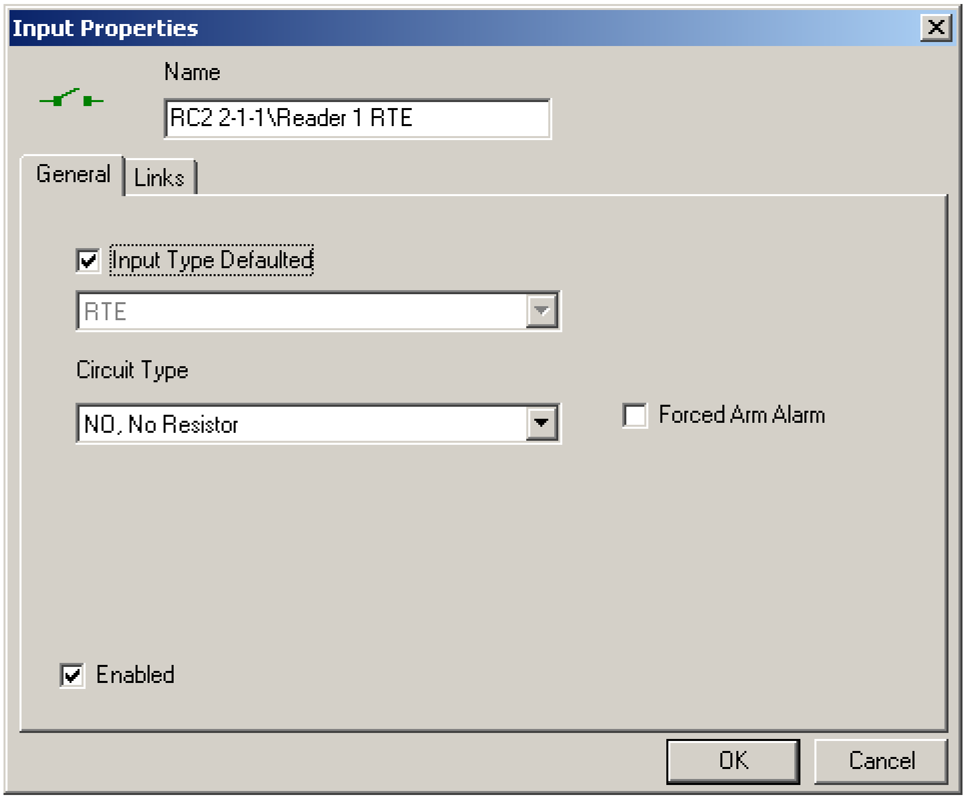
Code Reader Links will execute the designated link after a specific code is entered. The code is punched into a keypad after the noted *Cardnumber* has been Granted Access. If the *Cardnumber* is left blank then after any Grant Access the code will execute the assigned link.

Inputs

Inputs are created with the creation of RC2s and IOC16s. They can be either defaulted to an access point (RC2s only) or general purpose.

Input Properties

Set the Input's properties from this window. A General Purpose input will be shown here. Default inputs, being tied to an access point, don't have all the features of a General Purpose input to program.



Name: RC2 2-1-1\Reader 1 RTE

☑ Input Type Defaulted

RTE

Circuit Type: NO, No Resistor

☐ Forced Arm Alarm

☑ Enabled

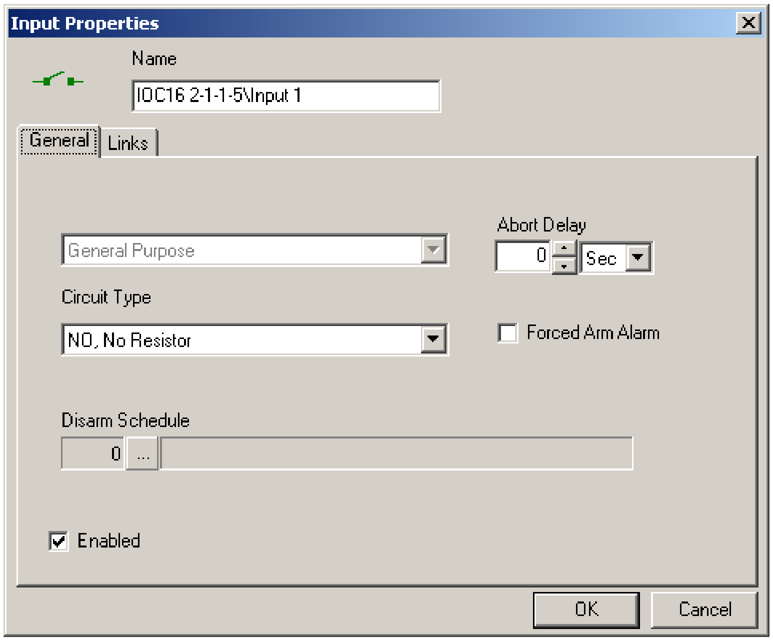
Name

Up to 50 alphanumeric characters may be entered here.

General

☑ Input Type Defaulted

Inputs 1 and 2 on an RC2 can be set as either general-purpose inputs or they can be defaulted. Input 1, when defaulted will be used as a Request-to-Exit input for the access point and Input 2 when defaulted will be used as a Door Contact input for that same access point. Side A and side B of the RC2 both have their own input 1 and input 2 to be defaulted or used as general-purpose inputs. Defaulted inputs are part of an access point and should not be considered as separate entities.



Name: IOC16 2-1-1-5\Input 1

General Purpose

Circuit Type: NO, No Resistor

Abort Delay: 0 Sec

☐ Forced Arm Alarm

Disarm Schedule: 0

☑ Enabled

Circuit Type

Use the list box to select the type of circuit that the Input is connected to. The system supports seven different circuit types ranging from unsupervised loops to partially supervised (*single resistor*) and fully supervised (*two resistor*) loops. *Refer to the Hardware Installation Manual for full details of the circuit types.*

The selection must match the physical circuit connection. The system uses 1K (1000 ohm) end-of-line resistors.

Disarm Schedule

Use the *Browse/Ellipsis button* to select the *Schedule* during which the input is automatically disarmed by the system schedule (Option available only for General purpose inputs).

Abort Delay

This field specifies the maximum duration (from 1 second to 127 minutes) that an *Input* can remain in the Alarm State without reporting the alarm event to the computer. If the *Input* changes state and returns to normal within the abort delay time period, no alarm is sent to the computer. Each *Input* may be programmed with a unique abort delay time.

Temperature monitoring is one application where abort delay is used effectively. Suppose we want to generate a freezer alarm if the freezer temperature rises above a preset threshold for more than five minutes. We are not concerned if the temperature rises for a few seconds and then returns to normal. Try using a general-purpose Input and setting the abort delay to five minutes to accomplish this.

Forced Arm Alarm

Use the check box to specify whether this input generates a *Forced Arm Alarm.* A *Forced Arm* occurs when an *Input* device is armed while it is in an abnormal state. Once armed, by definition, the abnormal state becomes an Alarm state. The system administrator has options in specifying how AxiomV™ should handle this Forced Arm situation.

Checked

Check this field, and the system will generate an Alarm immediately upon arming, and execute all attendant commands and messages.

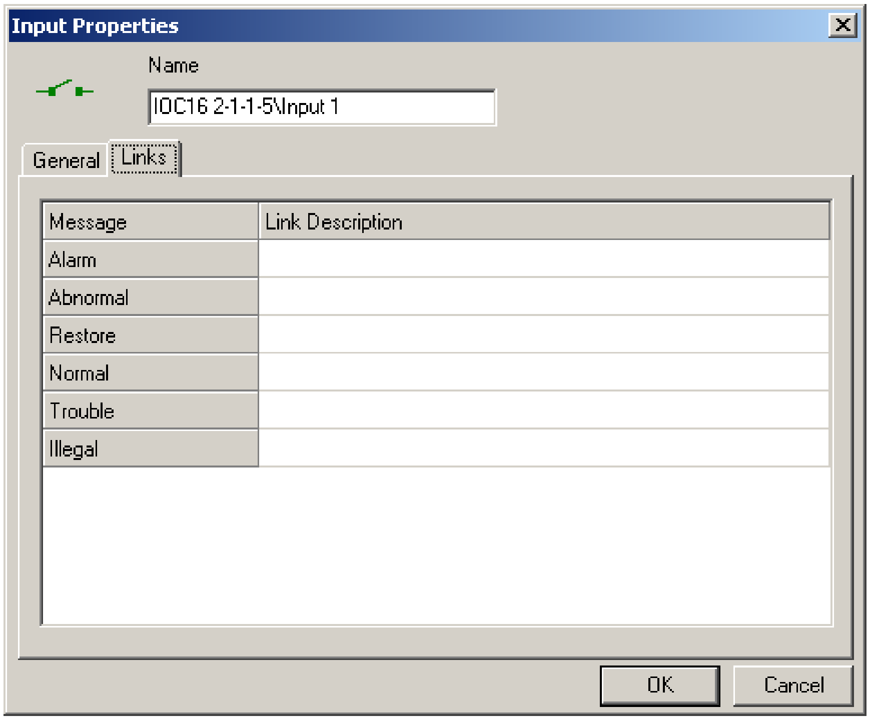
Unchecked

Leave this field unchecked and the system will delay generating an Alarm until the system Restores and goes into Alarm a subsequent time.

☑ Enabled

Unchecking the *Enabled* box will make the input unavailable to the status list. Since it is not on the status list commands cannot be sent to it. It will not be removed from the database or prevented from sending messages.

Links



Input Properties

Name: IOC16 2-1-1-5\Input 1

Message	Link Description
Alarm	
Abnormal	
Restore	
Normal	
Trouble	
Illegal	

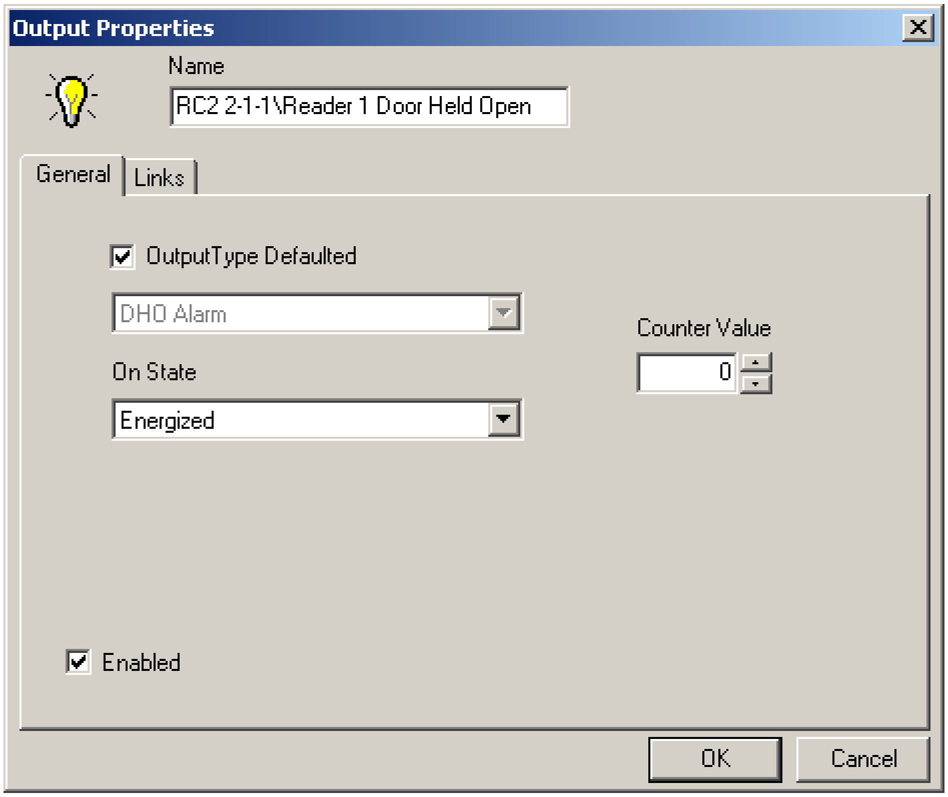
To establish a link click in the *Link Description* box beside the *Message* you want the link activated on. Then click the *Browse/Ellipsis button* and select the desired link from the list presented. The name of the chosen link will be shown in the *Link Description* box to confirm the link programming.

Outputs

Outputs are created with the creation RC2s and IOC16s. They can be either defaulted to an access point (RC2s only) or general purpose.

Output Properties

Set the Output's properties from this window. A General Purpose output will be shown here. Default outputs, being tied to an access point, don't have all the features of a General Purpose output to program.



Output Properties

Name: RC2 2-1-1\Reader 1 Door Held Open

☑ OutputType Defaulted

DHO Alarm

On State: Energized

Counter Value: 0

☑ Enabled

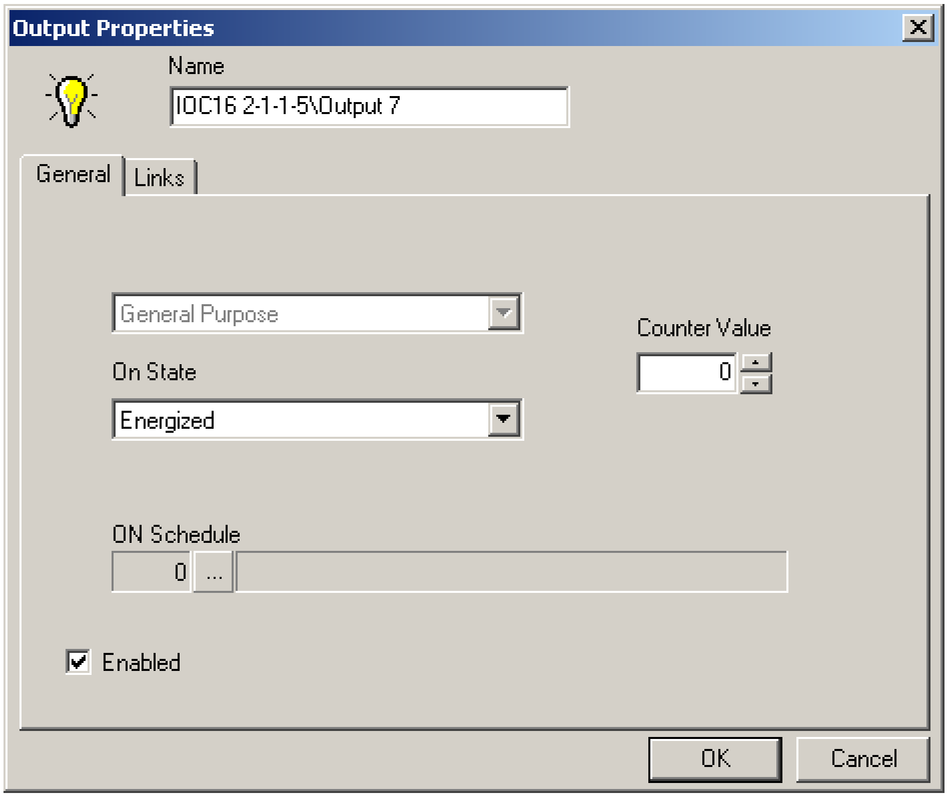
Name

Up to 50 alphanumeric characters may be entered here.

General

☑ Output Type Defaulted

RC-2 outputs can be set as either general-purpose outputs or they can be defaulted. When defaulted, output 1 will be used as a Lock output for the access point. Output 2 when defaulted will be used as a Forced/Tamper output for that same access point. Output 3 when defaulted will be used for Door Held Open warning and alarm. Output 4 when defaulted will be used for Alarm Shunt. Side A and side B both have their own outputs to be defaulted or used as general-purpose outputs. Defaulted outputs are part of an access point and should not be considered as separate entities.



On State

Use the list box to specify the *Output*'s normal *On State* as either *Energized* or *De-energized*. When the output is turned on is it powered or is power removed?

On schedule

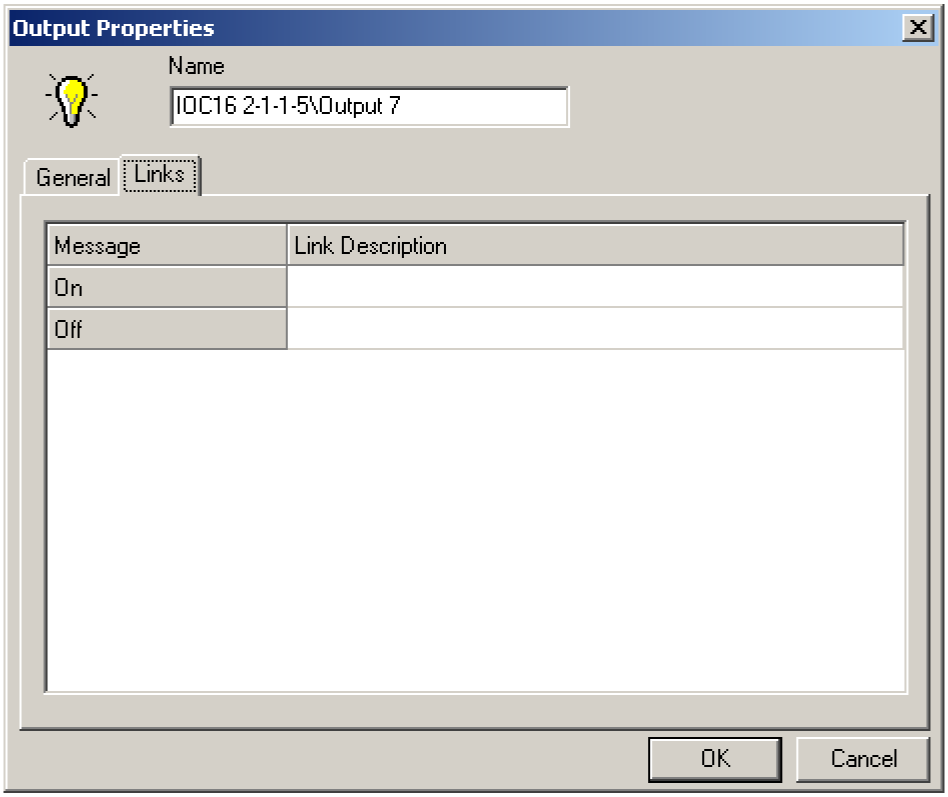
Use the *Browse/Ellipsis button* to select the *Schedule* during which the output is turned 'ON' (available only for General purpose outputs).

Counter Value

Enter a value greater than zero to activate *Counter* mode operation. *Counter* mode is used in applications where the output is only turned on after a certain number of commands telling it to turn on. Any *General Purpose* output in the system may be configured for *Counter* mode. The *Counter* value can be set from 1 to 32,767, in this box. This value is a threshold setting. When the count for an output is equal to or above this value the output turns on. When the count is below this value the output is turned off. The counter maintains a running count of on/off operations. Each time a counter output is instructed to turn on, the count is increased by one. Each off command decreases the count by one. The count will not go negative or increase above 32767. When an *Output* is set to operate in *Counter* mode, the respective links will only execute when the output turns on or off and not when the output's count is changed.

A 'Lot Full' sign in a parking lot is one application where the threshold counter feature may be used. If the lot capacity is one hundred, the sign should turn on if the number of cars reaches one hundred and turn off as soon as the number goes below one hundred. In this example, the on link is executed when the count reaches one hundred and the counter output is turned on. Subsequent ON commands will increment the count but will not alter the state of the output or execute the on link. An OFF command will turn off the output and execute the off link only when the count value goes down to ninety nine. Subsequent OFF commands will reduce the count but won't alter the Output State or execute the off link.

Links



Name: IOC16 2-1-1-5\Output 7

Message	Link Description
On	
Off	

To establish a link click in the *Link Description* box beside the *Message* you want the link activated on. Then click the *Browse/Ellipsis button* and select the desired link from the list presented. The name of the chosen link will be shown in the *Link Description* box to confirm the link programming.

Non Reader Access Points

Non-reader access points do not use reader ports and are created by the user from selected General Purpose inputs and outputs.

Right click on Non Reader Access Points to add a new Non Reader Access Point to the system. This will bring up the Non Reader Access Point properties window to set the properties of the new Non Reader Access Point.

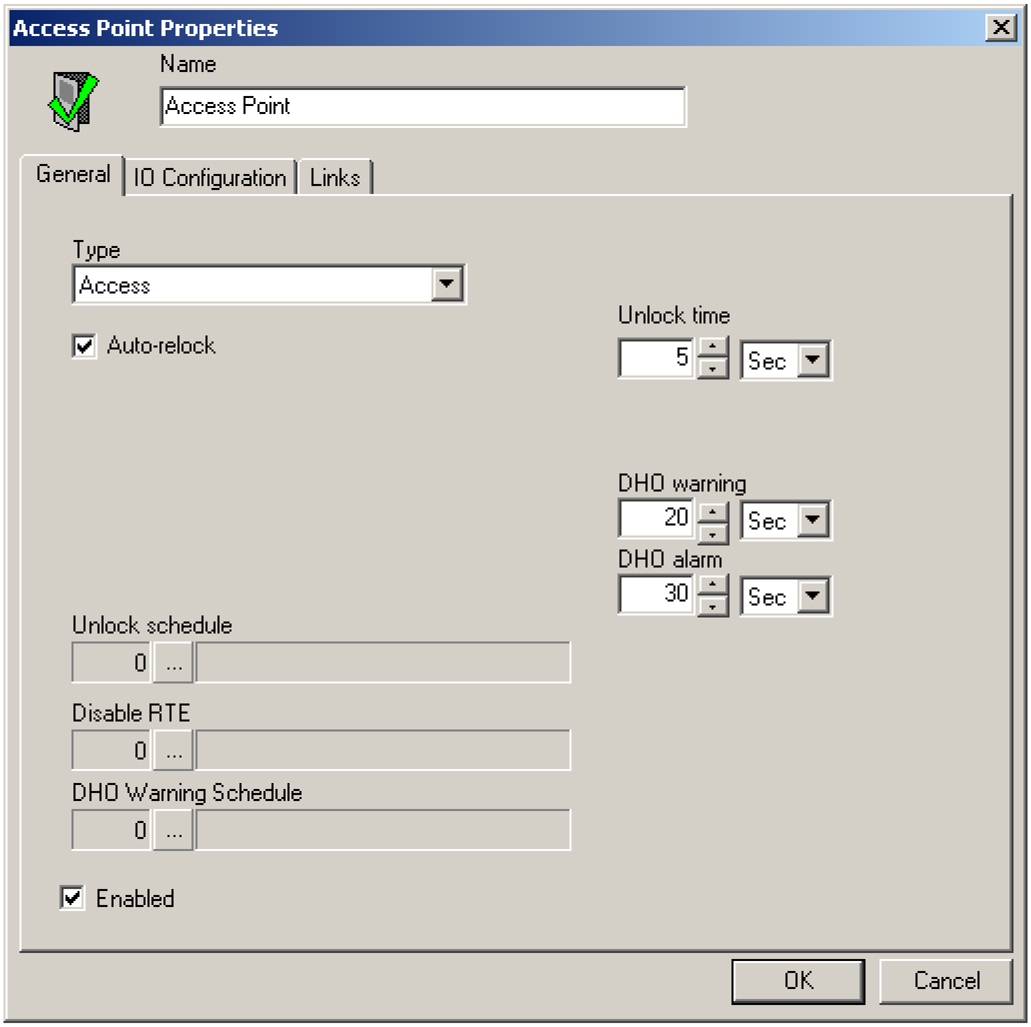
Right click on a Non Reader Access Point to either delete the Non Reader Access Point or to go into the Non Reader Access Point's properties screen.

☞ **Only General Purpose inputs and outputs on IOC16s connected to the NC100 should be used to create Non Reader Access Points for that NC100, even though RC2s general purpose inputs and outputs may be available.**

Non Reader Access Point Properties

Non Reader Access Points do not have all the features of regular Access Points (without a reader, some features are irrelevant). The features they do have work the same way they would for a regular Access Point. They can even be added to Access Point Groups.

General



Access Point Properties

Name: Access Point

Type: Access

☑ Auto-relock

Unlock time: 5 Sec

DHO warning: 20 Sec

DHO alarm: 30 Sec

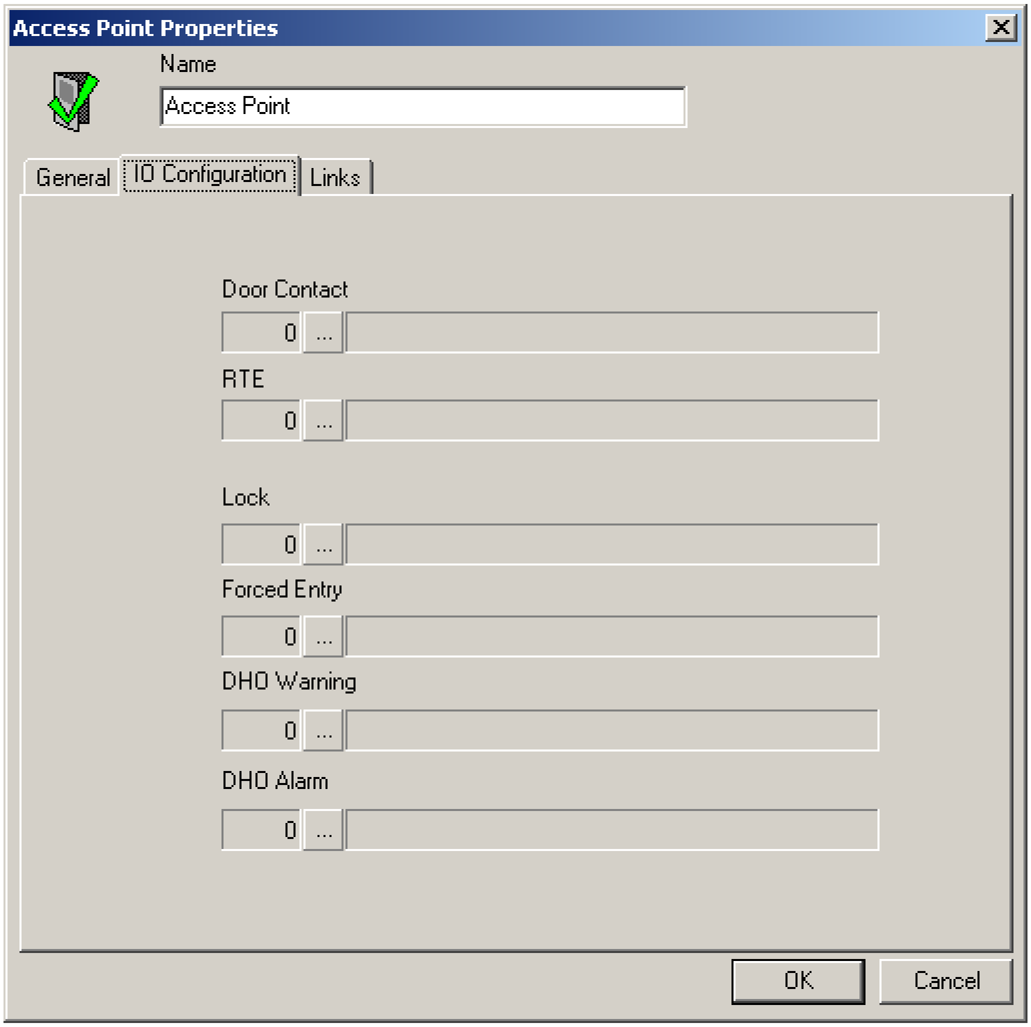
Unlock schedule: 0 ...

Disable RTE: 0 ...

DHO Warning Schedule: 0 ...

☑ Enabled

IO Configuration



Name: Access Point

Door Contact: 0

RTE: 0

Lock: 0

Forced Entry: 0

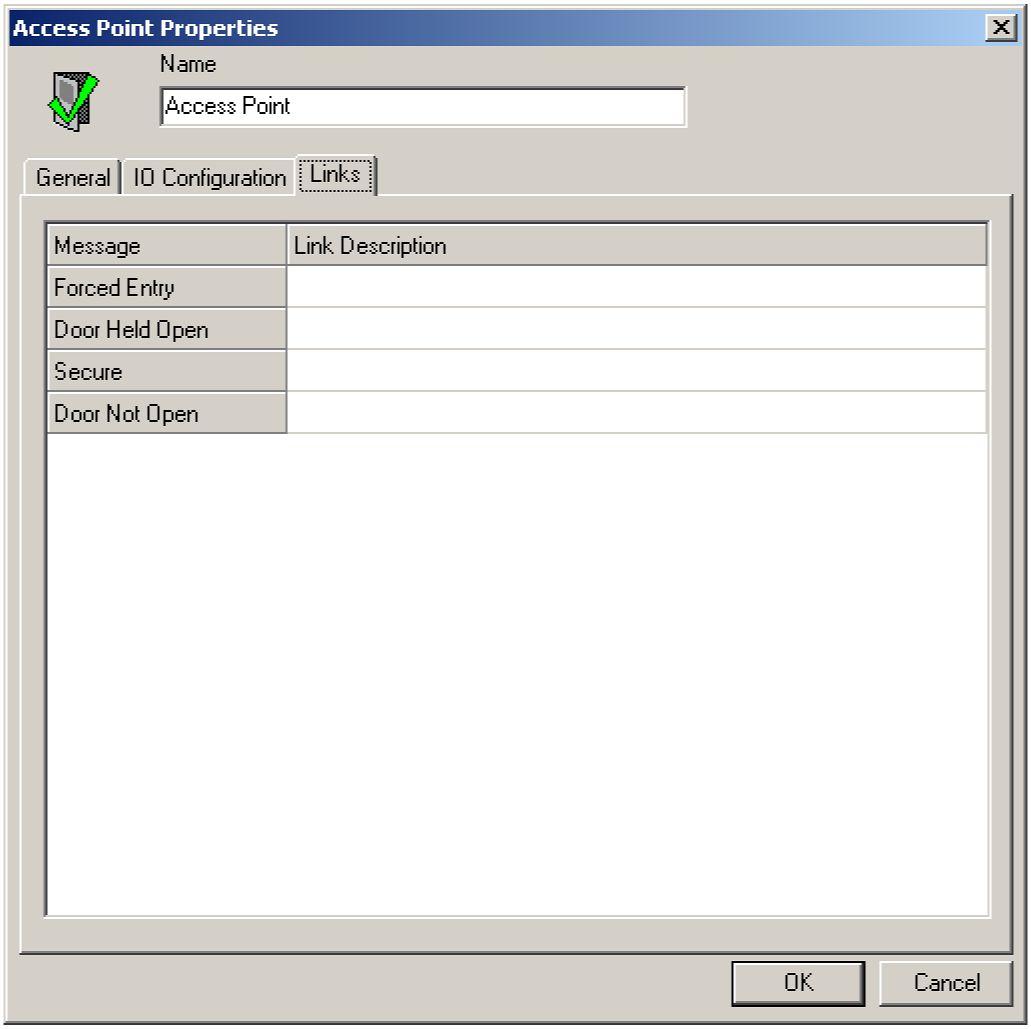
DHO Warning: 0

DHO Alarm: 0

Click the Browse/Ellipsis button ... for each point: Door Contact, RTE, Lock, Forced Entry, DHO Warning, and DHO Alarm. A list of available points (input/Output) to select from will pop up. Make a selection for each point and click OK. Points that are not required may be left blank.

Regular Access Points have only one output for Door Held Open that pulses for warning and is on steady for alarm while Non Reader Access Points have two outputs for Door Held Open, one for warning, and one for alarm.

Links



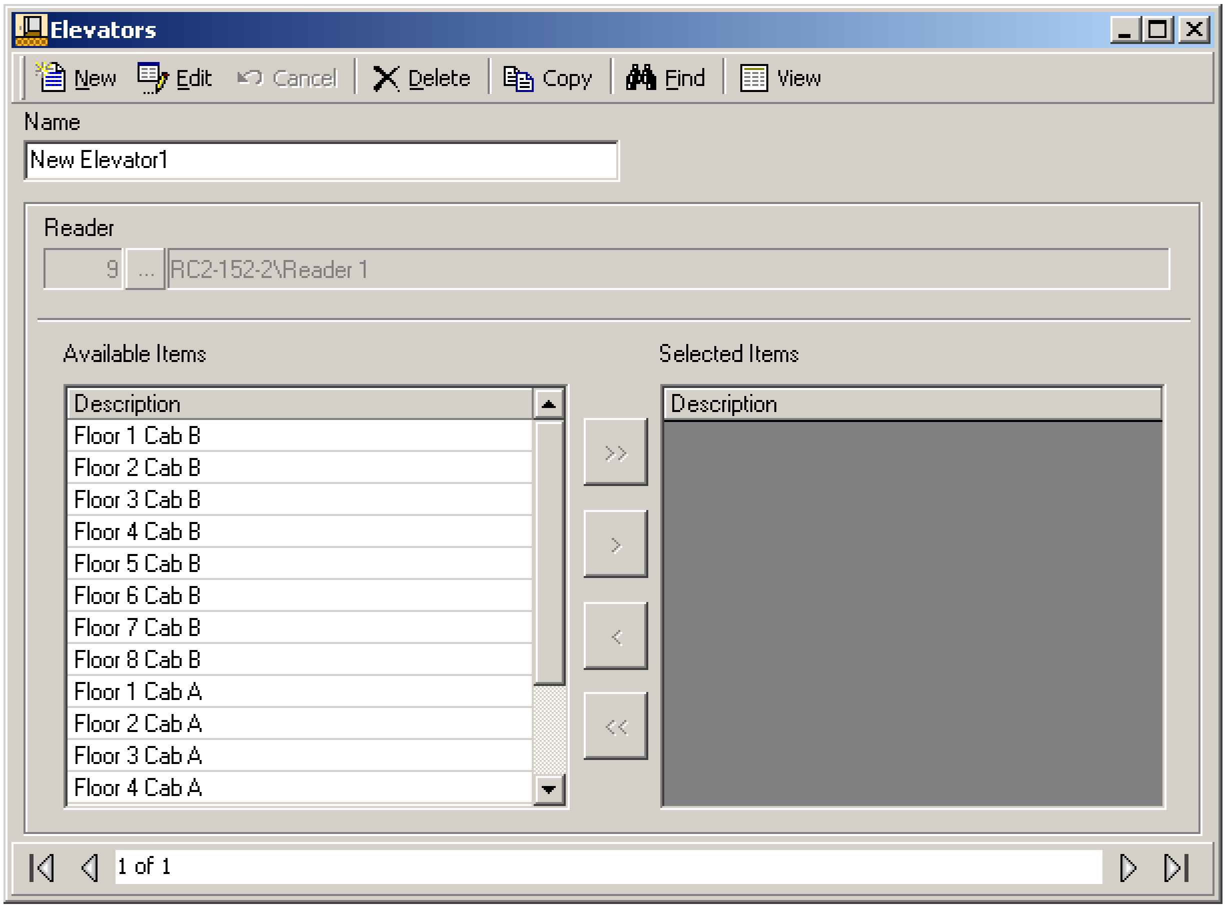
Name: Access Point

Message	Link Description
Forced Entry	
Door Held Open	
Secure	
Door Not Open	

To establish a link click in the *Link Description* box beside the *Message* you want the link activated on. Then click the *Browse/Ellipsis button* and select the desired link from the list presented. The name of the chosen link will be shown in the *Link Description* box to confirm the link programming.

Elevators

For elevator control the system needs to know which outputs are to be associated with which Elevator Reader. Every floor button on every elevator cab that is to be controlled requires a relay output to activate or deactivate. For example, if you want to control access to five different floors in a building with four elevators you will need twenty outputs.



Name

New Elevator1

Reader

9 ... RC2-152-2\Reader 1

Available Items

Description
Floor 1 Cab B
Floor 2 Cab B
Floor 3 Cab B
Floor 4 Cab B
Floor 5 Cab B
Floor 6 Cab B
Floor 7 Cab B
Floor 8 Cab B
Floor 1 Cab A
Floor 2 Cab A
Floor 3 Cab A
Floor 4 Cab A

Selected Items

Description

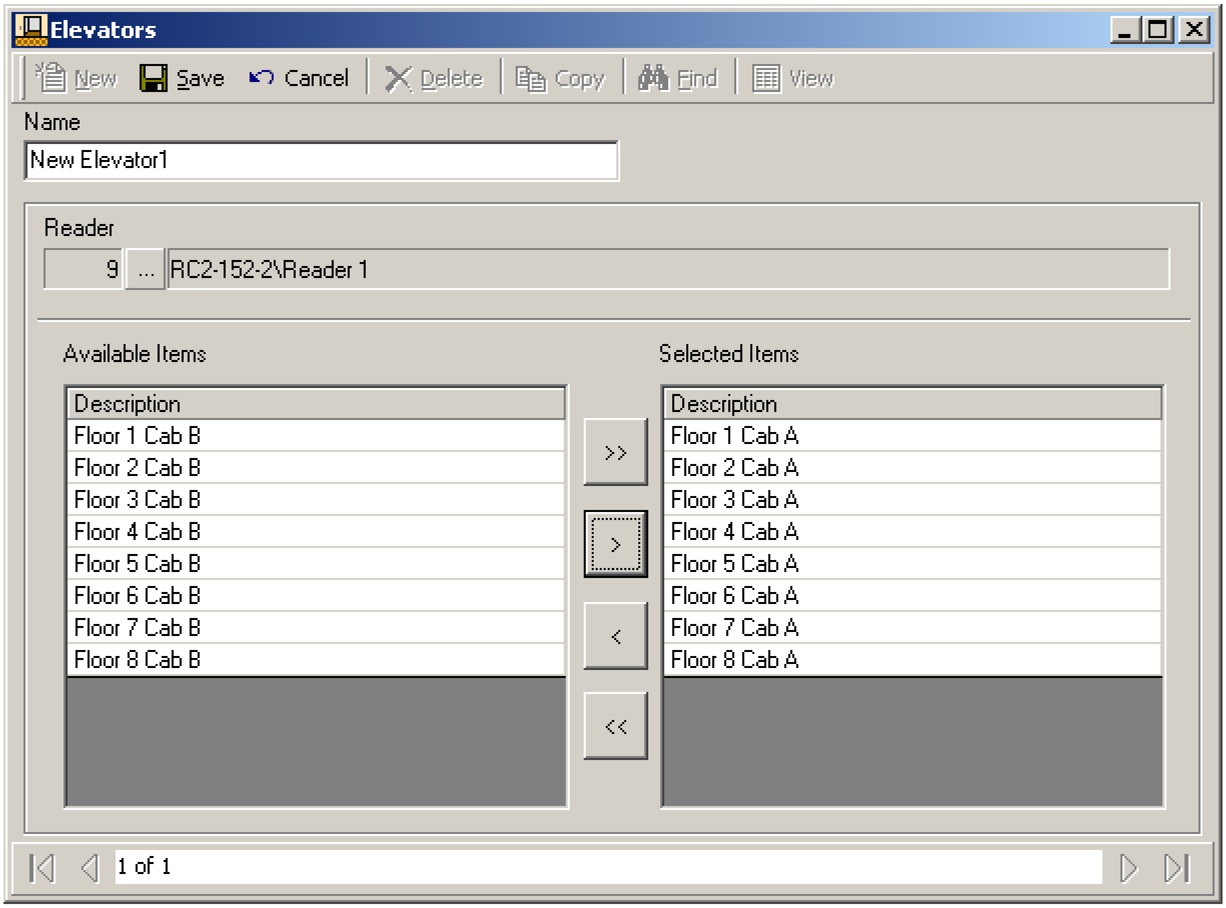
1 of 1

Name

Up to 50 alphanumeric characters may be entered here.

Reader

Browse and select the desired elevator reader.



Name: New Elevator1

Reader: 9 ... RC2-152-2\Reader 1

Available Items: Description
Floor 1 Cab B
Floor 2 Cab B
Floor 3 Cab B
Floor 4 Cab B
Floor 5 Cab B
Floor 6 Cab B
Floor 7 Cab B
Floor 8 Cab B

Selected Items: Description
Floor 1 Cab A
Floor 2 Cab A
Floor 3 Cab A
Floor 4 Cab A
Floor 5 Cab A
Floor 6 Cab A
Floor 7 Cab A
Floor 8 Cab A

Available Items & Selected Items

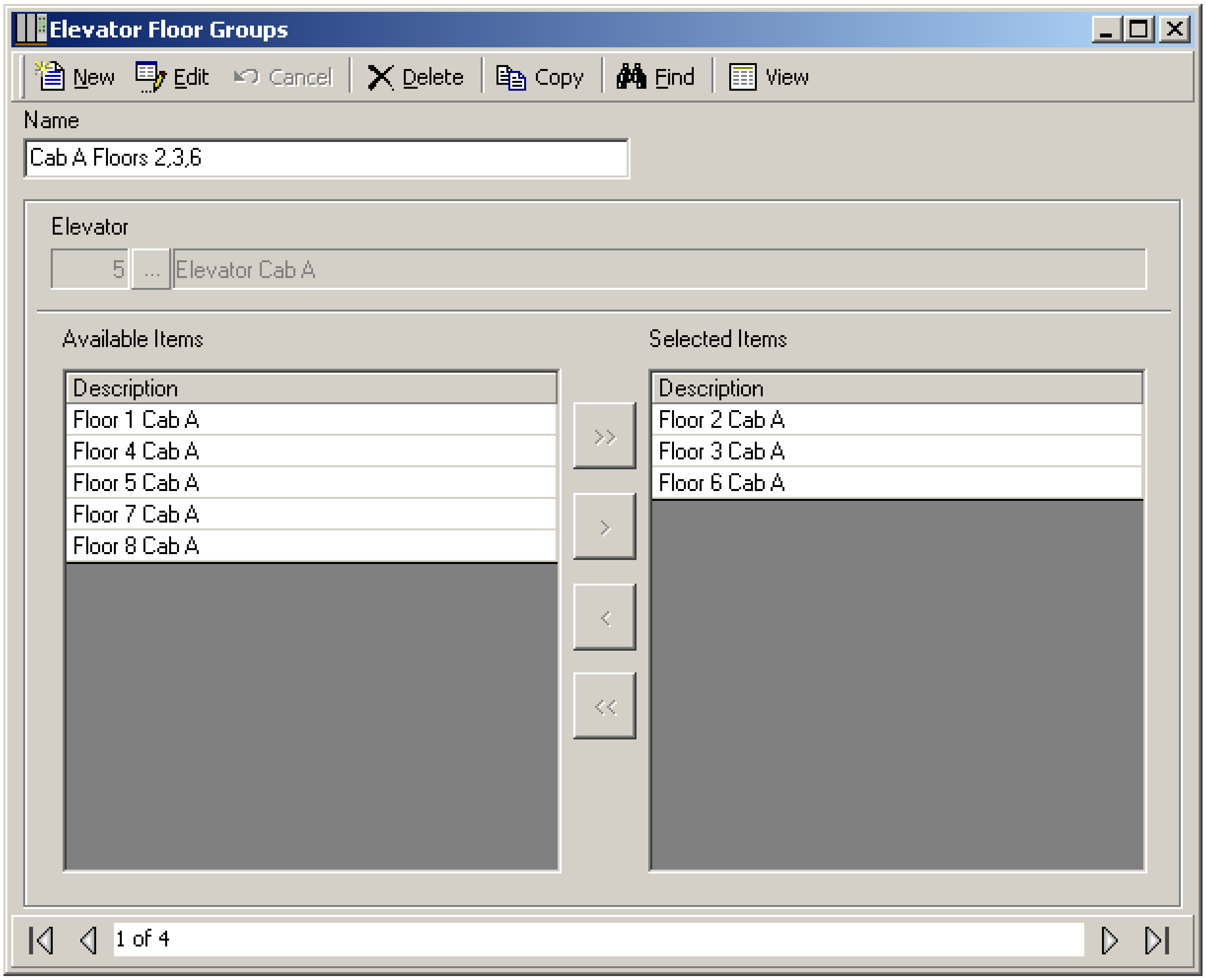
Only general-purpose outputs related to the NC-100 (which the selected elevator reader is connected to) will be listed in *Available Items*.

☞ **It is recommended to use only the general purpose outputs of IOC for elevators.**

Shift the floor outputs between available and selected to configure the elevator cab with the proper floor outputs.

Floor Groups

Create Floor Groups to limit access to only the floors included in the group.



Name: Cab A Floors 2,3,6

Elevator: 5 ... Elevator Cab A

Available Items

Description
Floor 1 Cab A
Floor 4 Cab A
Floor 5 Cab A
Floor 7 Cab A
Floor 8 Cab A

Selected Items

Description
Floor 2 Cab A
Floor 3 Cab A
Floor 6 Cab A

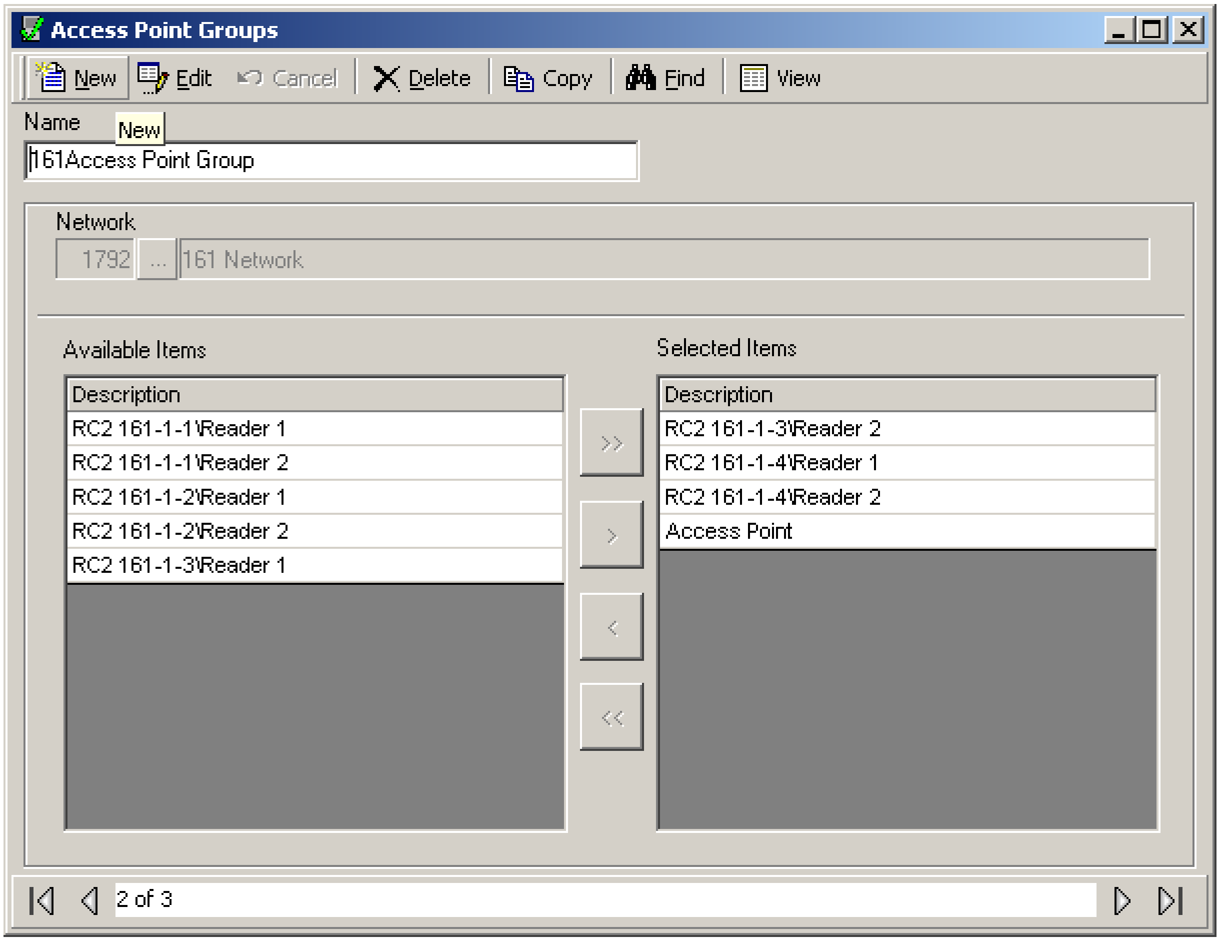
1 of 4

Floor Groups are tied to schedules and work in conjunction with Access Levels to control floor access for cardholders.

The only floor buttons to become active are the ones included in the cardholder's Floor Group assigned in access level. Therefore cardholders can only go to the floors they have access to.

AccessPoint Groups

Access Point Groups are used to create groups of access points. Once created *Access Point Groups* can be given commands, or they can be used in links. Access points are grouped for convenience. Instead of issuing a command to six individual access points, one command could be sent to a group of six, for example.



Name
161Access Point Group

Network
1792 ... 161 Network

Available Items

Description
RC2 161-1-1\Reader 1
RC2 161-1-1\Reader 2
RC2 161-1-2\Reader 1
RC2 161-1-2\Reader 2
RC2 161-1-3\Reader 1

Selected Items

Description
RC2 161-1-3\Reader 2
RC2 161-1-4\Reader 1
RC2 161-1-4\Reader 2
Access Point

2 of 3

Name

Up to 50 alphanumeric characters may be entered here.

Network

Browse the list of networks available in the system to select from.

Available Items

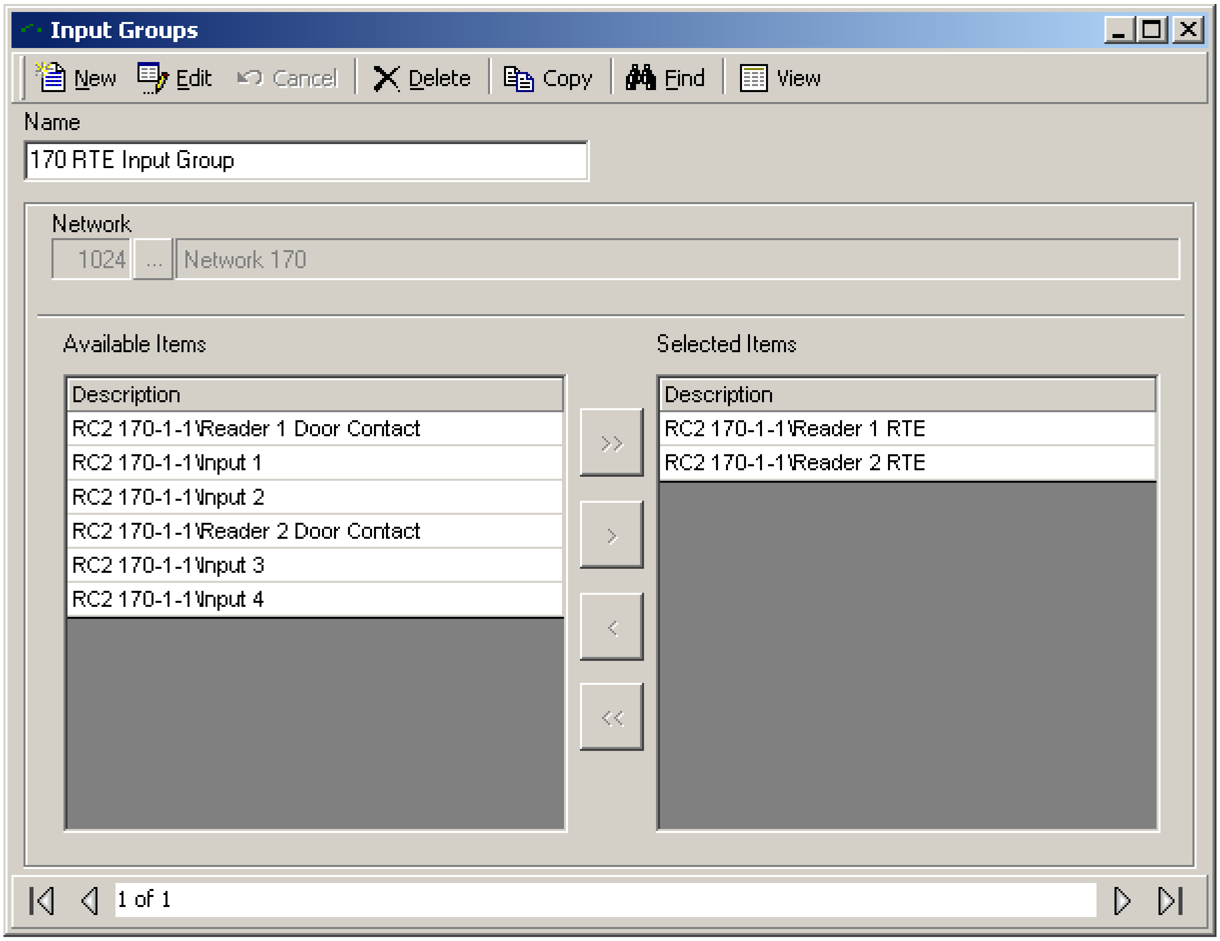
Available Items will show all of the access points of selected network.

Selected Items

Selected Item lists the selected access points that are members of the access point group.

Input Groups

Input Groups are used to create groups of inputs. Once created *Input Groups* can be given commands, or they can be used in links. Inputs are grouped for convenience. Instead of issuing a disarm command to six individual inputs, one command could be sent to a group of six inputs, for example.



Name
170 RTE Input Group

Network
1024 ... Network 170

Available Items

Description
RC2 170-1-1\Reader 1 Door Contact
RC2 170-1-1\Input 1
RC2 170-1-1\Input 2
RC2 170-1-1\Reader 2 Door Contact
RC2 170-1-1\Input 3
RC2 170-1-1\Input 4

Selected Items

Description
RC2 170-1-1\Reader 1 RTE
RC2 170-1-1\Reader 2 RTE

1 of 1

Name

Up to 50 alphanumeric characters may be entered here.

Network

Browse the list of networks available in the system to select from.

Available Items

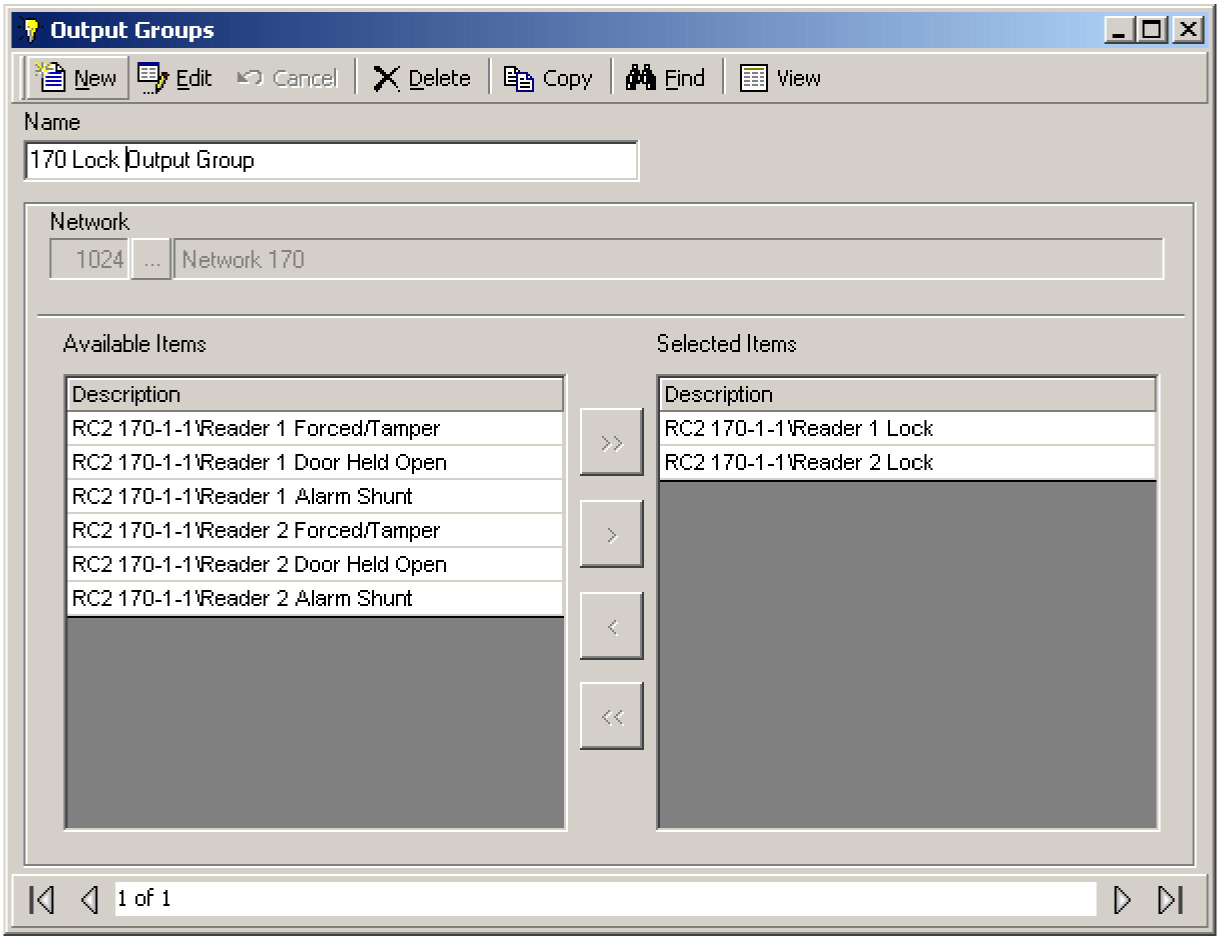
Available Items will show all of the inputs of selected network.

Selected Items

Selected Item lists the selected inputs that are members of the input group.

Output Groups

Output Groups are used to create groups of outputs. Once created *Output Groups* can be given commands, or they can be used in links. Outputs are grouped for convenience. Instead of issuing an on command to six individual outputs, one command could be sent to a group of six outputs, for example.



Name: 170 Lock Output Group

Network: 1024 ... Network 170

Available Items

Description
RC2 170-1-1\Reader 1 Forced/Tamper
RC2 170-1-1\Reader 1 Door Held Open
RC2 170-1-1\Reader 1 Alarm Shunt
RC2 170-1-1\Reader 2 Forced/Tamper
RC2 170-1-1\Reader 2 Door Held Open
RC2 170-1-1\Reader 2 Alarm Shunt

Selected Items

Description
RC2 170-1-1\Reader 1 Lock
RC2 170-1-1\Reader 2 Lock

1 of 1

Name

Up to 50 alphanumeric characters may be entered here.

Network

Browse the list of networks available in the system to select from.

Available Items

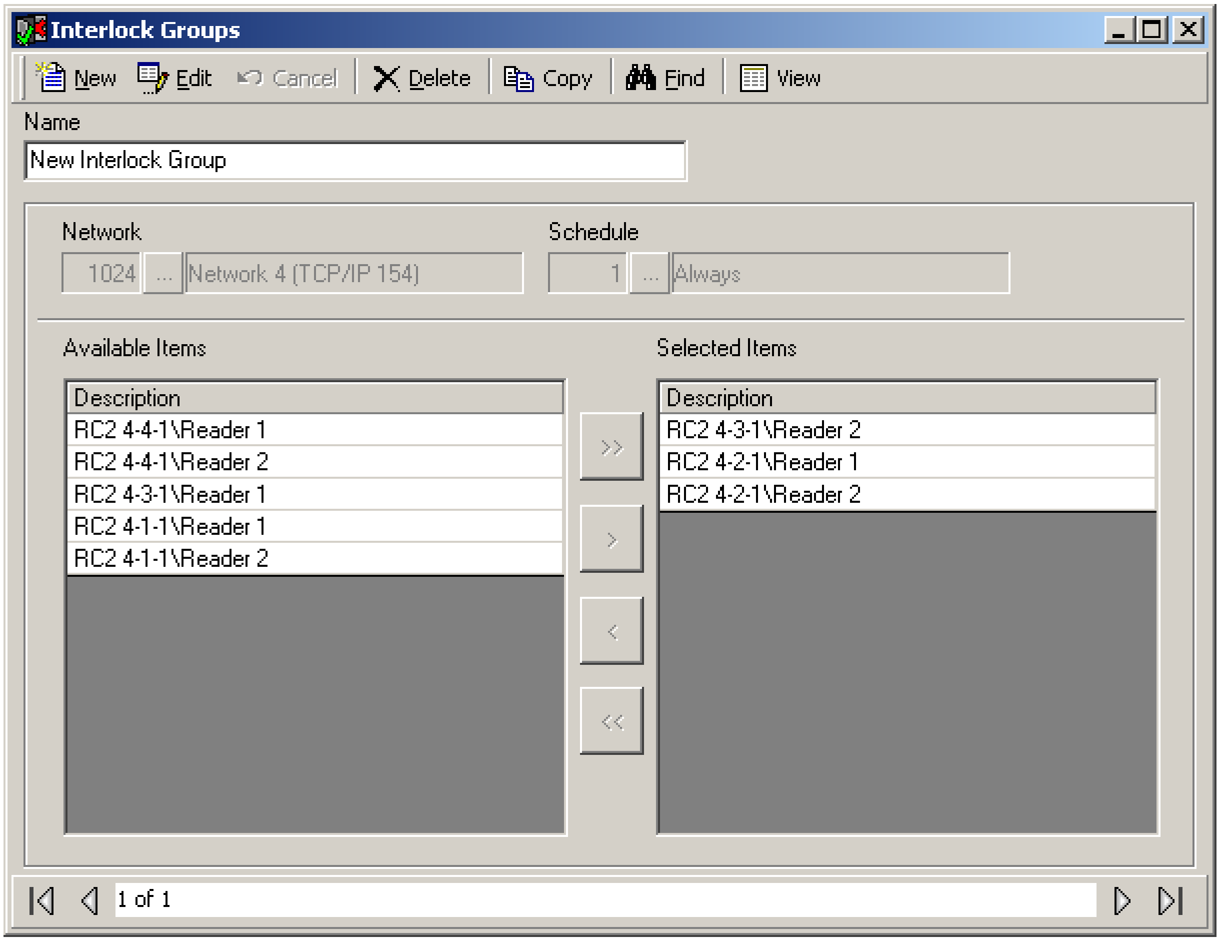
Available Items will show all of the outputs of selected network.

Selected Items

Selected Item lists the selected outputs that are members of the output group.

Interlock Groups

Interlock Groups are used to create groups of access points. These access points are only allowed to have one member open at a time. If one of these access point grants access and is opened none of the other members of the group will grant access for selected schedule. This feature is commonly used in mantrap applications.



Name: New Interlock Group

Network: 1024 ... Network 4 (TCP/IP 154)

Schedule: 1 ... Always

Available Items

Description
RC2 4-4-1\Reader 1
RC2 4-4-1\Reader 2
RC2 4-3-1\Reader 1
RC2 4-1-1\Reader 1
RC2 4-1-1\Reader 2

Selected Items

Description
RC2 4-3-1\Reader 2
RC2 4-2-1\Reader 1
RC2 4-2-1\Reader 2

1 of 1

Name

Up to 50 alphanumeric characters may be entered here.

Network

Browse the list of networks available in the system to select from.

Schedule

Browse the list of schedule available in the system to select from.

Available Items

Available Items will show all of the available access point of selected network

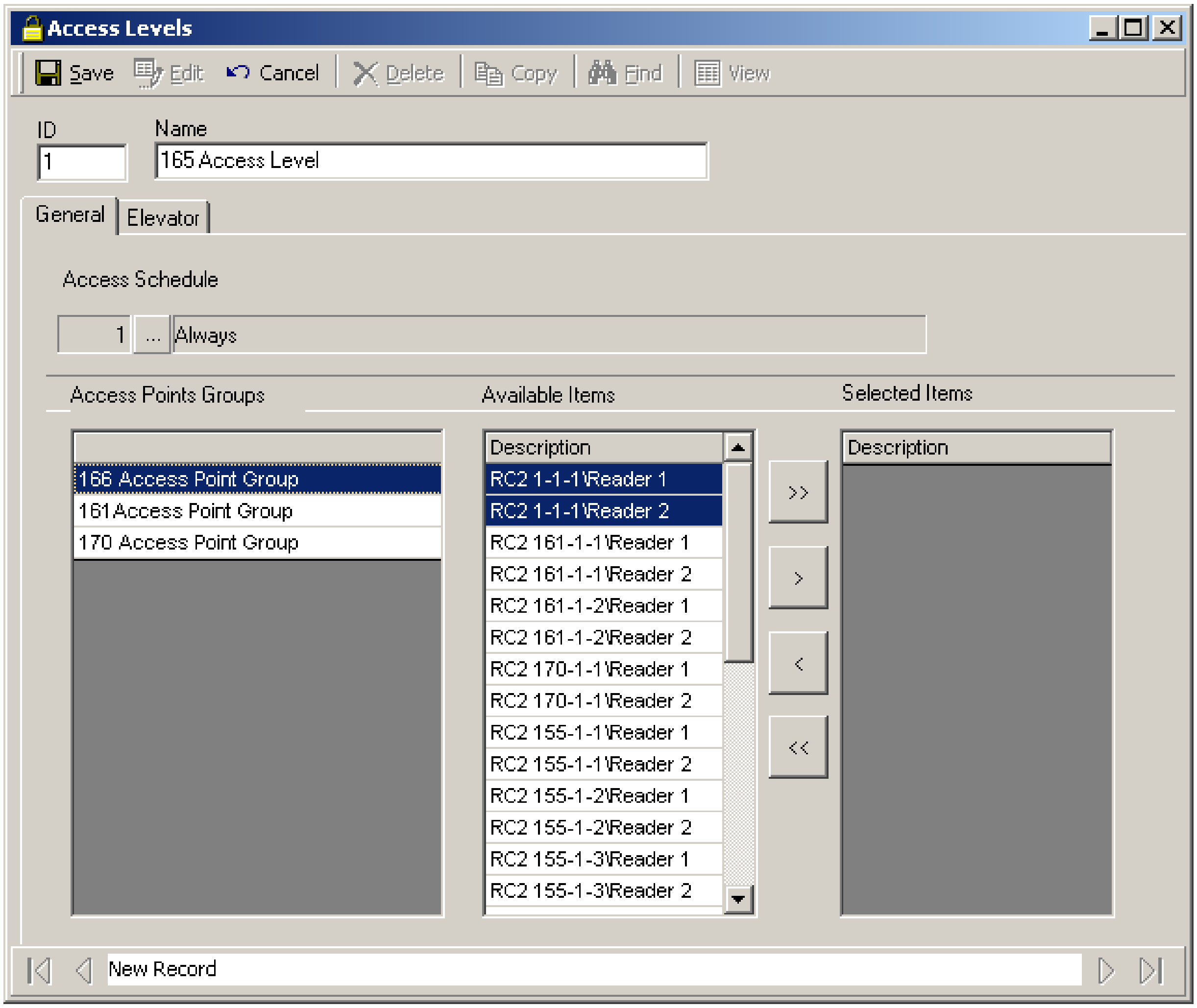
Selected Items

Selected Item lists the selected access points that are members of interlock group.

Access Levels

Access Levels are the main way to designate when a cardholder is allowed access. Essentially *Access Levels* combine access points with schedules. (I.e. this door at these times and that door at those times, etc.)

General(Standard Access Levels)



ID: 1

Name: 165 Access Level

Access Schedule: 1 ... Always

Access Points Groups

- 166 Access Point Group
- 161 Access Point Group
- 170 Access Point Group

Available Items

Description
RC2 1-1-1\Reader 1
RC2 1-1-1\Reader 2
RC2 161-1-1\Reader 1
RC2 161-1-1\Reader 2
RC2 161-1-2\Reader 1
RC2 161-1-2\Reader 2
RC2 170-1-1\Reader 1
RC2 170-1-1\Reader 2
RC2 155-1-1\Reader 1
RC2 155-1-1\Reader 2
RC2 155-1-2\Reader 1
RC2 155-1-2\Reader 2
RC2 155-1-3\Reader 1
RC2 155-1-3\Reader 2

Selected Items

Description

New Record

Name

Up to 50 alphanumeric characters may be entered here.

Access Point Groups

Access Point groups will show the list of all the access point groups configured in the system. Selecting access point group will automatically select the access points configured for those Access point groups at that time in the list of *Available Items.* This option is more useful for bigger systems where there are a lot of access points configured and grouping them would make it easier to create *Access levels*

Available Items

Available Items will show all of the access points in the system, (except the ones that have already been selected).

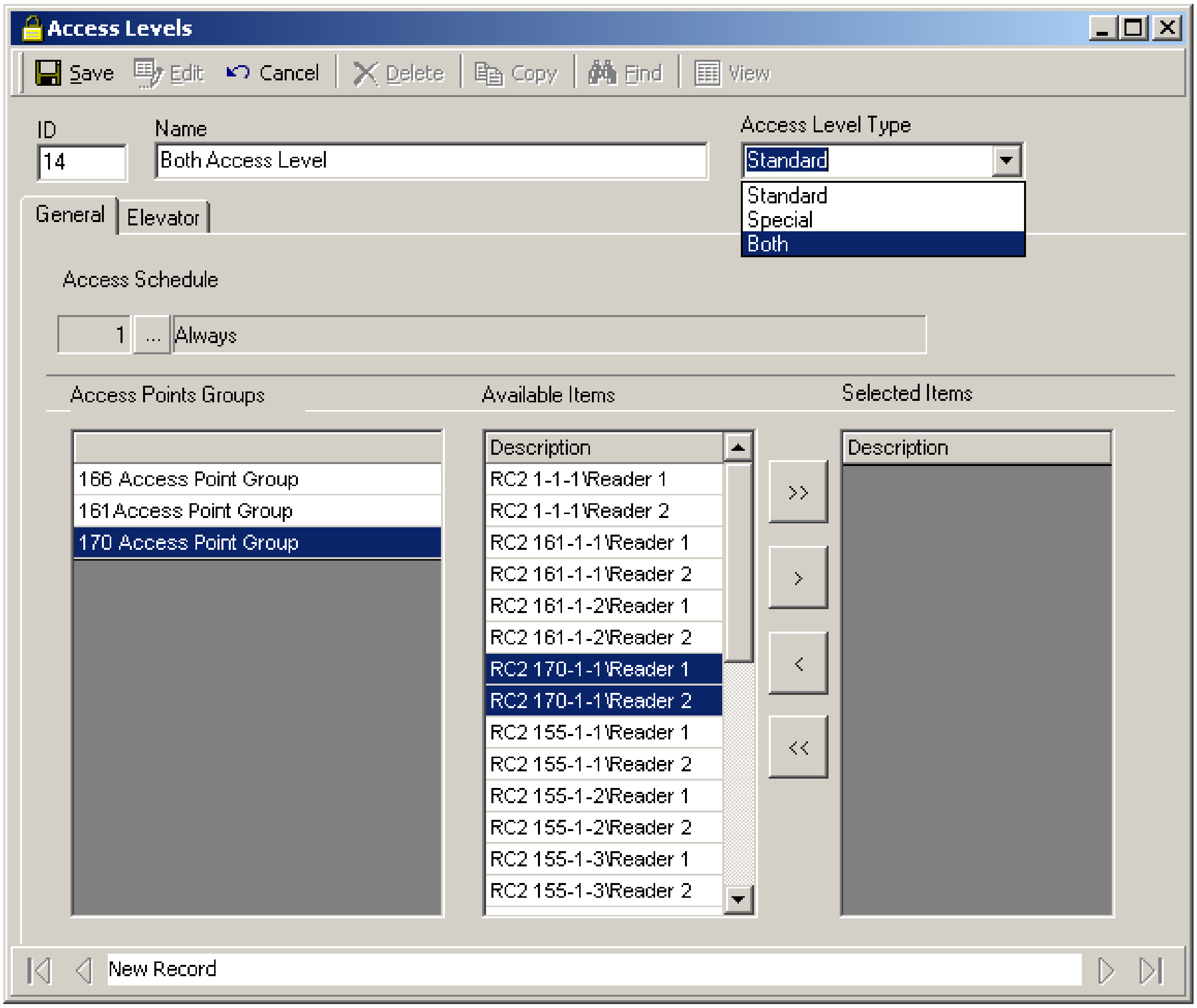
Selected Items

Selected Item lists the selected access points that are members of the access level.

Access Schedule

For each required schedule shift access points from the *Available Item* list to the *Selected Items* list. Access levels can have many access schedules but each access point can only be selected for one schedule. Once selected the access point is removed from the available list. All of the schedules don't need to be used, nor do all of the access points need to be selected.

General (Multiple Access Levels)



ID: 14

Name: Both Access Level

Access Level Type: Standard

Standard
Special
Both

Access Schedule: 1 ... Always

Access Points Groups

166 Access Point Group
161 Access Point Group
170 Access Point Group

Available Items

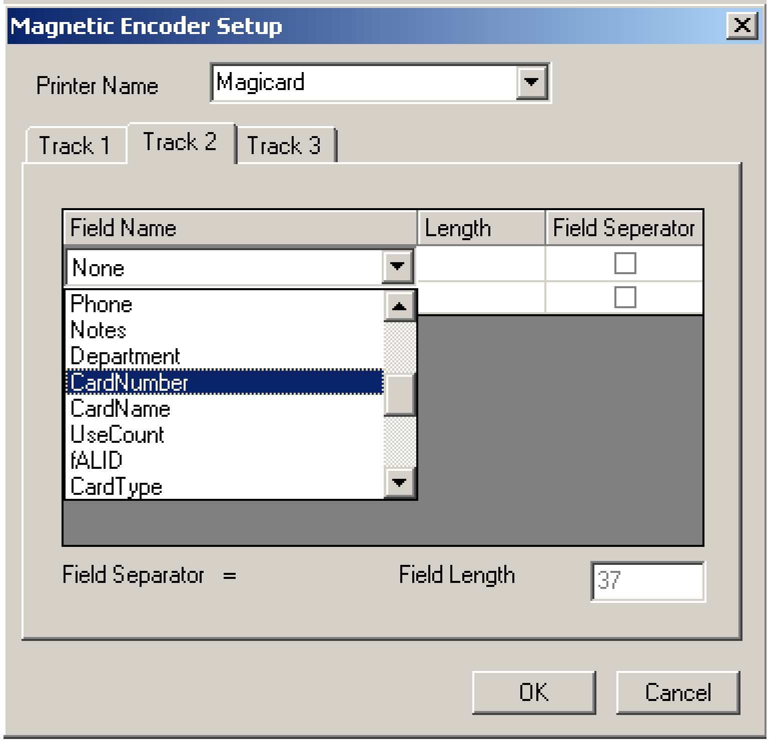
Description
RC2 1-1-1\Reader 1
RC2 1-1-1\Reader 2
RC2 161-1-1\Reader 1
RC2 161-1-1\Reader 2
RC2 161-1-2\Reader 1
RC2 161-1-2\Reader 2
RC2 170-1-1\Reader 1
RC2 170-1-1\Reader 2
RC2 155-1-1\Reader 1
RC2 155-1-1\Reader 2
RC2 155-1-2\Reader 1
RC2 155-1-2\Reader 2
RC2 155-1-3\Reader 1
RC2 155-1-3\Reader 2

Selected Items

Description

New Record

For systems with Multiple Access Levels selected an Access Level Type needs to be chosen for each Access Level created (see *System Settings* – System for information on selecting Multiple Access Levels).



Magnetic Encoder Setup

Printer Name: Magicard

Field Name	Length	Field Seperator
None		□
		□

Field Separator =

Field Length: 37

The ‘Standard’ access level type is used as a base or foundation access level. Only a ‘Standard’ access level can have elevator control.

‘Special’ access level types are additional access levels that can be assigned to a cardholder only as Multiple access level.

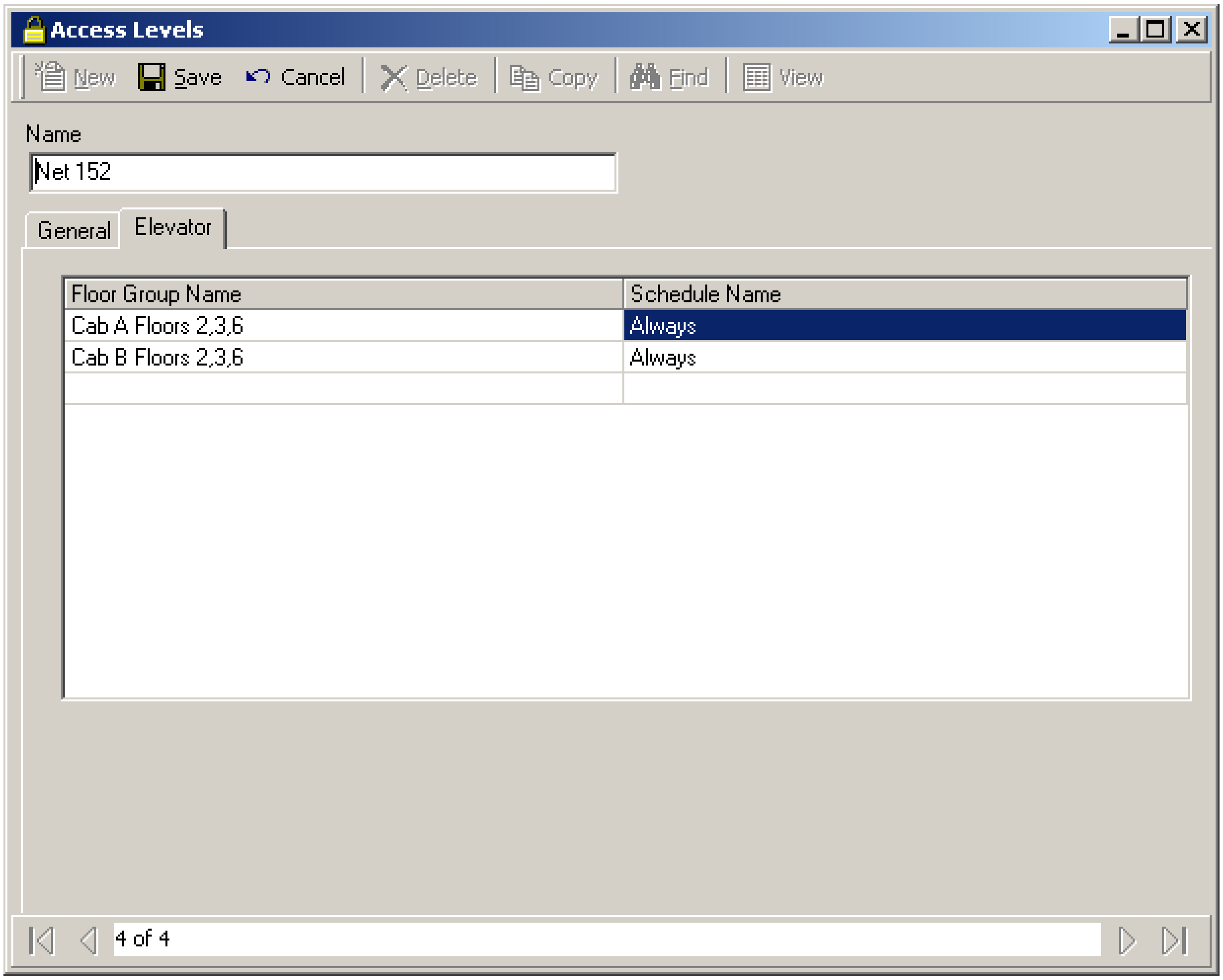
Access levels type as ‘Both’ can be assigned to a cardholder as either, a ‘General’ access level, or a ‘Multiple’ access level.

See Cardholder General Tab (Multiple Access Levels) for information on assigning these access levels to the cardholders.

There is more information on Special Access Levels under Reader Access.

Elevator

Elevator tab in Access Level is available only for *Standard* Type AL



Name: Net 152

Floor Group Name	Schedule Name
Cab A Floors 2,3,6	Always
Cab B Floors 2,3,6	Always

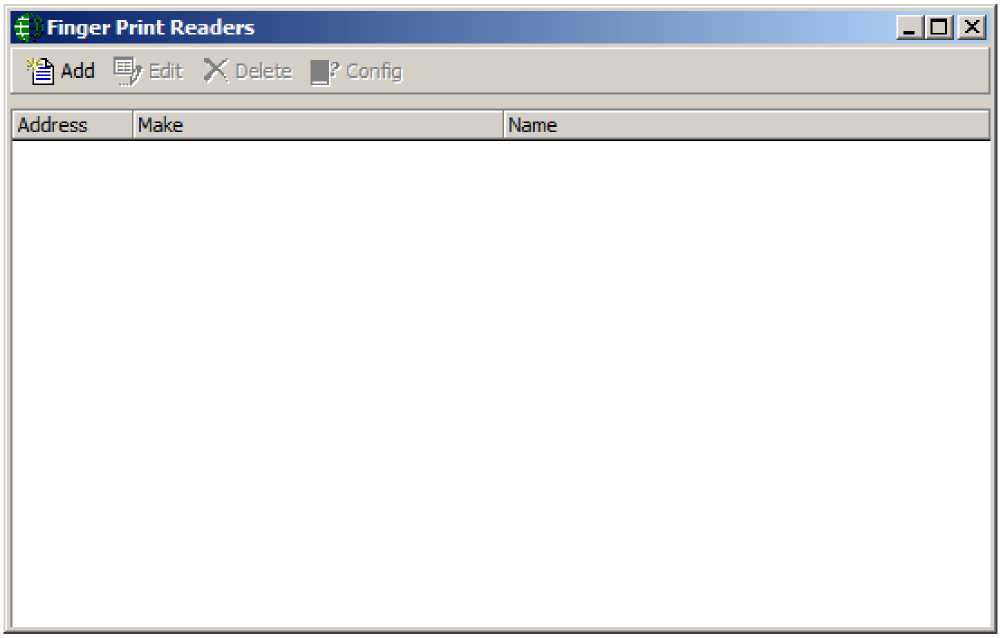
4 of 4

Under the *Elevator* tab *Floor Groups* are tied to *Schedules*. For *Elevator Access* to work the *Elevator* reader appropriate to the selected *Floor Groups* is not necessarily selected under the General tab.

When access is granted on the *Elevator* reader the system checks to see which floors associated with that reader are to be enabled. The *Floor Group* determines these floors.

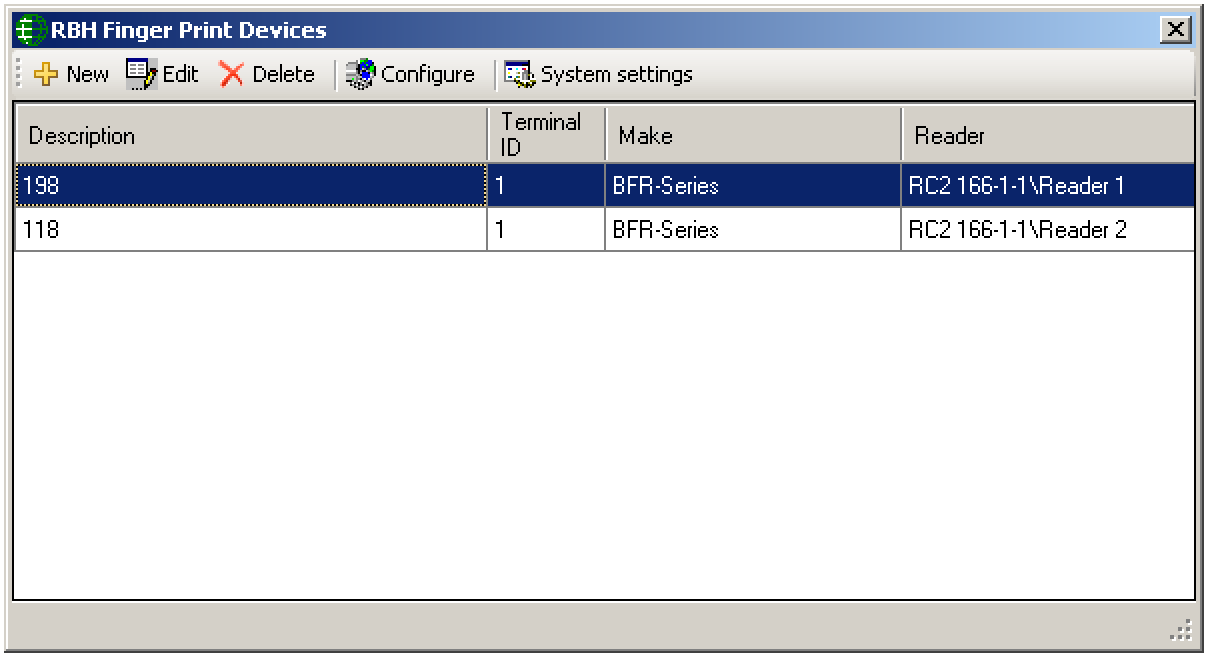
Finger Print Readers

Before entering a cardholder's finger prints the reader needs to be setup.



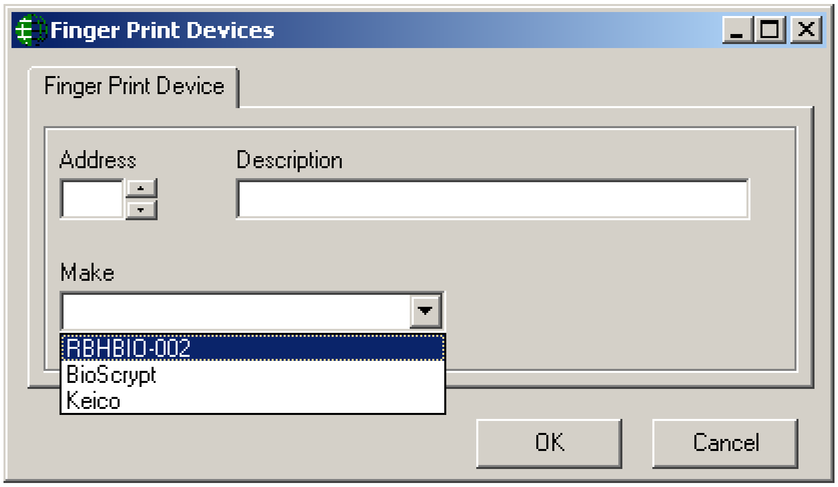
Address	Make	Name

OR



Description	Terminal ID	Make	Reader
198	1	BFR-Series	RC2 166-1-1\Reader 1
118	1	BFR-Series	RC2 166-1-1\Reader 2

Add a reader to the system.

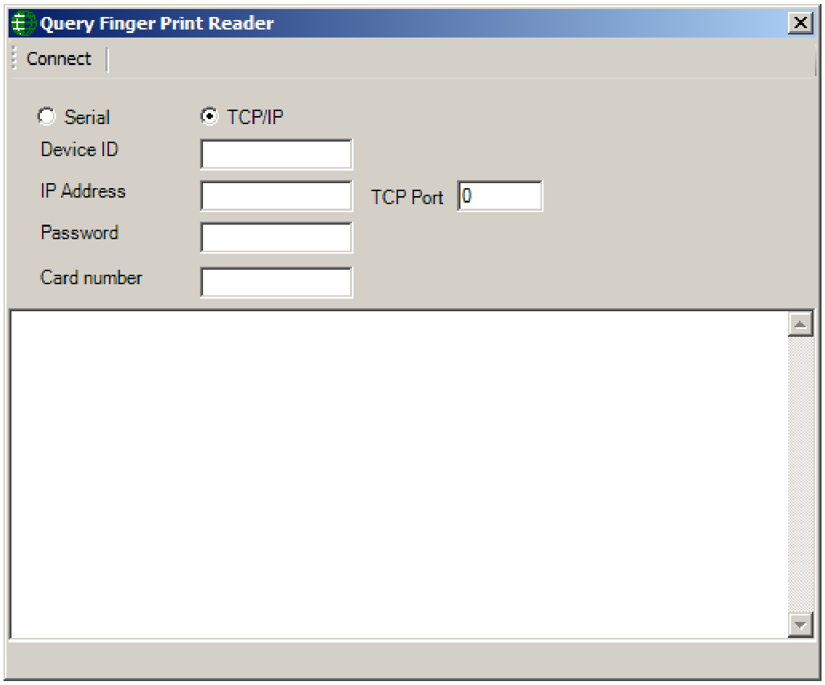


Select the manufacture of the Finger Print Reader and give the reader a meaningful description. The address entered here could actually be a Device ID.

Configure the reader according to the appropriate Finger Print Reader document. Look for Bioscrypt AxionV.pdf, Keico AxiomV.pdf, RBH-BIO readerAxiomV.pdf, or TB65_BFRQuickConfigGuide.pdf on the AxiomV™ installation CD.

Finger Print Reader Query

Information can be obtained from the Finger Print Reader using *Finger Print Reader Query*. (For RBH BFR reader it loads the same window as it loads for *Finger Print Reader*)

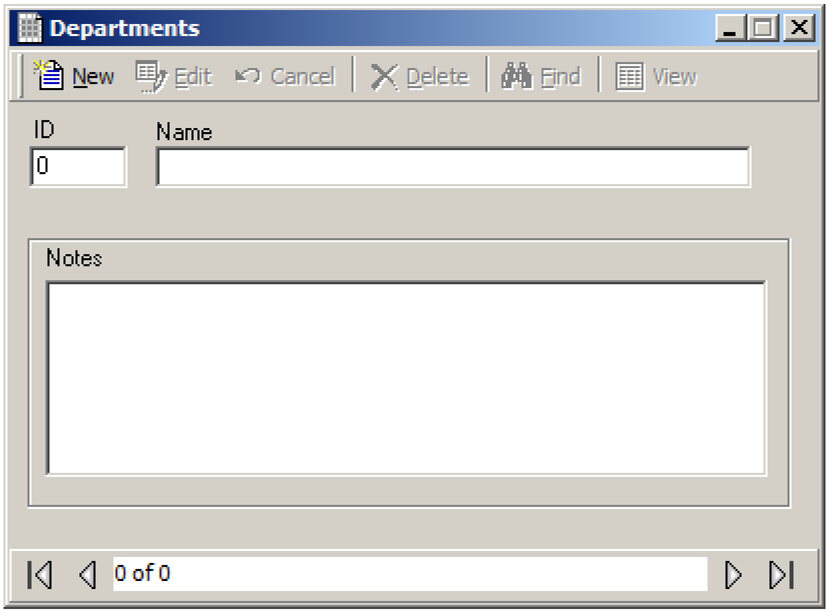


○ Serial ● TCP/IP

TCP Port 0

Enter the appropriate data as configured in the Finger Print Reader to connect to the reader. While connected to the reader you can execute commands on the reader. For more information see the documents on the AxiomV™ installation CD (Bioscrypt AxiomV.pdf, Keico AxiomV.pdf, RBH-BIO readerAxiomV.pdf, or TB65_BFRQuickConfigGuide.pdf)

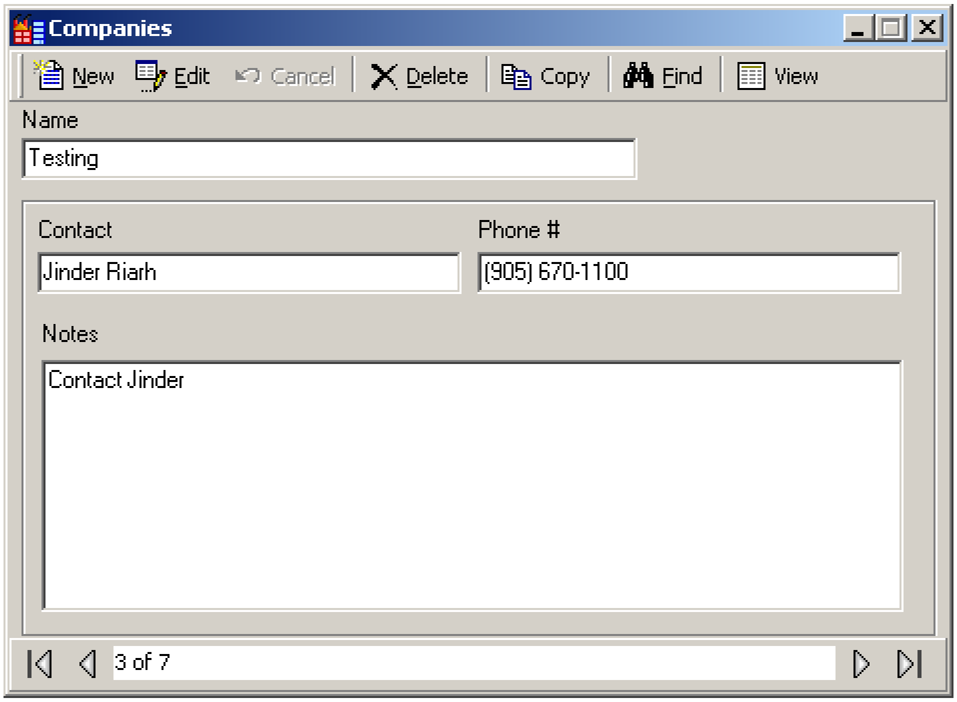
Departments



Here you can add the names of departments to fill the *Department 1* and *Department 2* fields in the *Cardholder – Personal* tab. These department names cannot be used in the *Departments* field. *Operator Profiles* does include access to this feature under *Modules*.

Companies

A company is a cardholder group and is used in operator profiles.



Name
Testing

Contact
Jinder Riarh

Phone #
(905) 670-1100

Notes
Contact Jinder

3 of 7

Name

Up to 50 alphanumeric characters may be entered here.

Contact

Up to 50 alphanumeric characters may be entered here.

Phone

Up to 50 alphanumeric characters may be entered here.

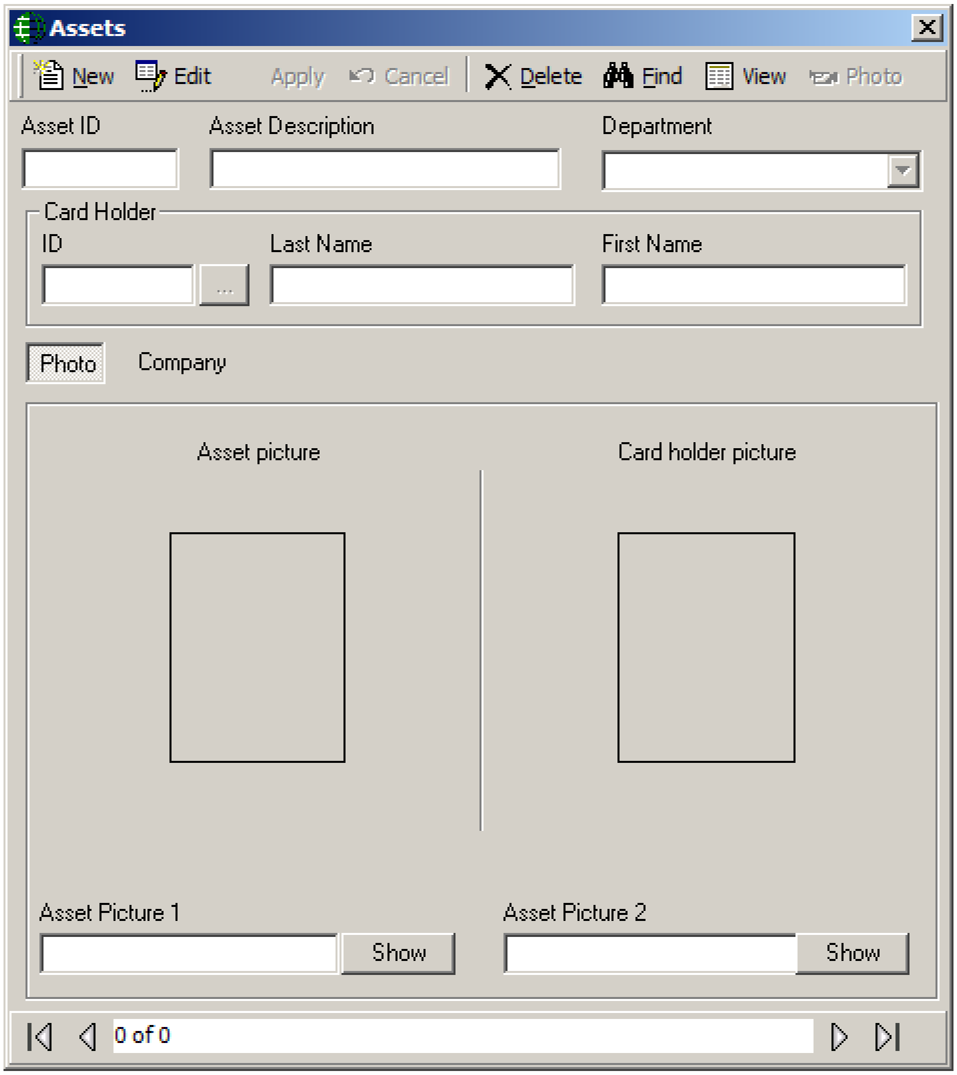
Notes

Notes provide an area to enter information pertaining to the company that doesn’t fit into any of the other fields.

Assets

Add an Asset

Assets are usually portable equipment or hardware that needs to be kept track of, like laptop computers or specialty metering/monitoring equipment.



Asset ID

Up to a ten digit number may be entered here.

Asset Description

Up to 50 alphanumeric characters may be entered here.

Department

Type in or select a department from the pull-down list.

Cardholder

ID

Browse the cardholder list and make a selection.

First Name / Last Name

First and last name will be inserted automatically for the selected ID.

View

An asset report can be generated to list all of the inputted assets along with their associated Cardholders.

Photo

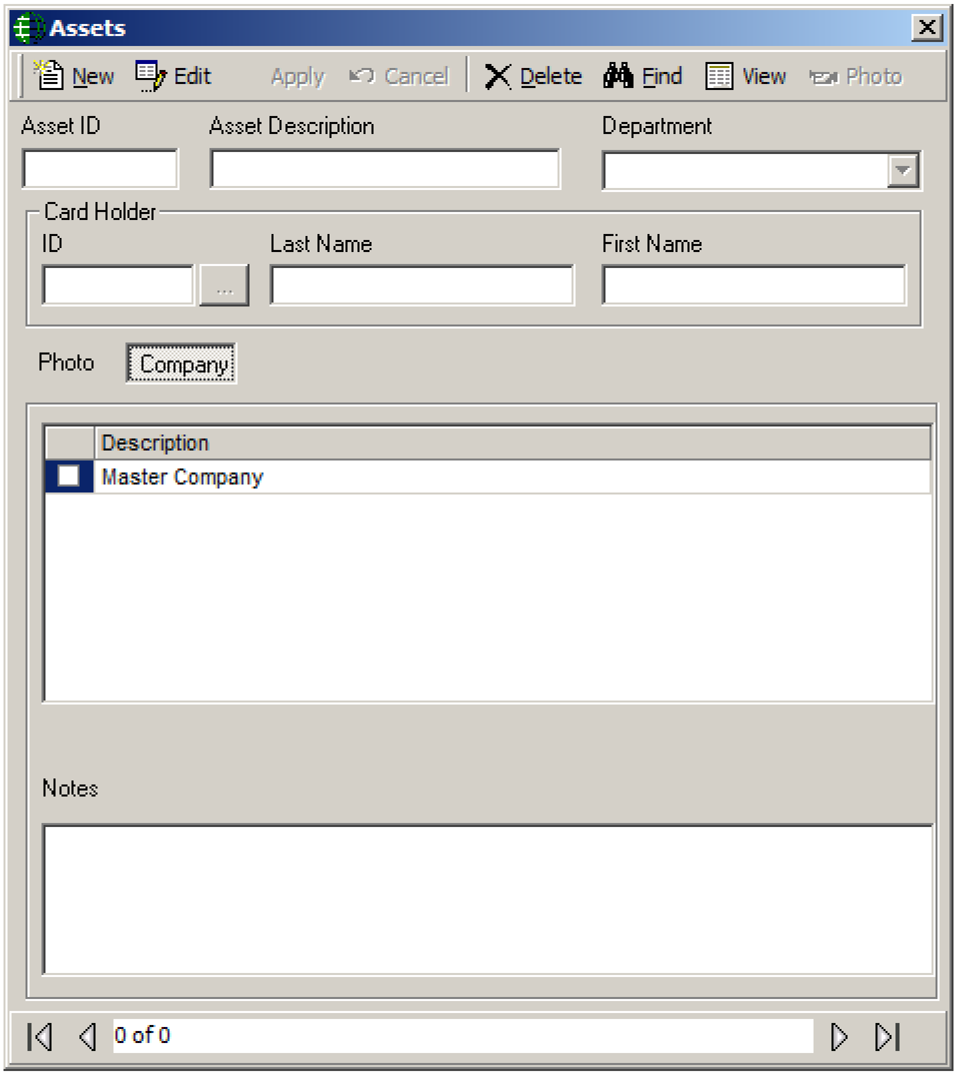
Capture and save one or two pictures of the asset. The cardholder's picture will also be displayed, based on the cardholder ID selected.

Company

The companies that the cardholder is associated with will be shown here.

Notes

Information regarding the asset can be entered here.



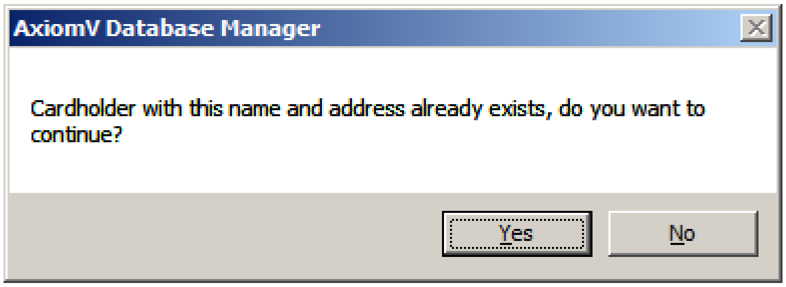
	Description
□	Master Company

0 of 0

Cardholder

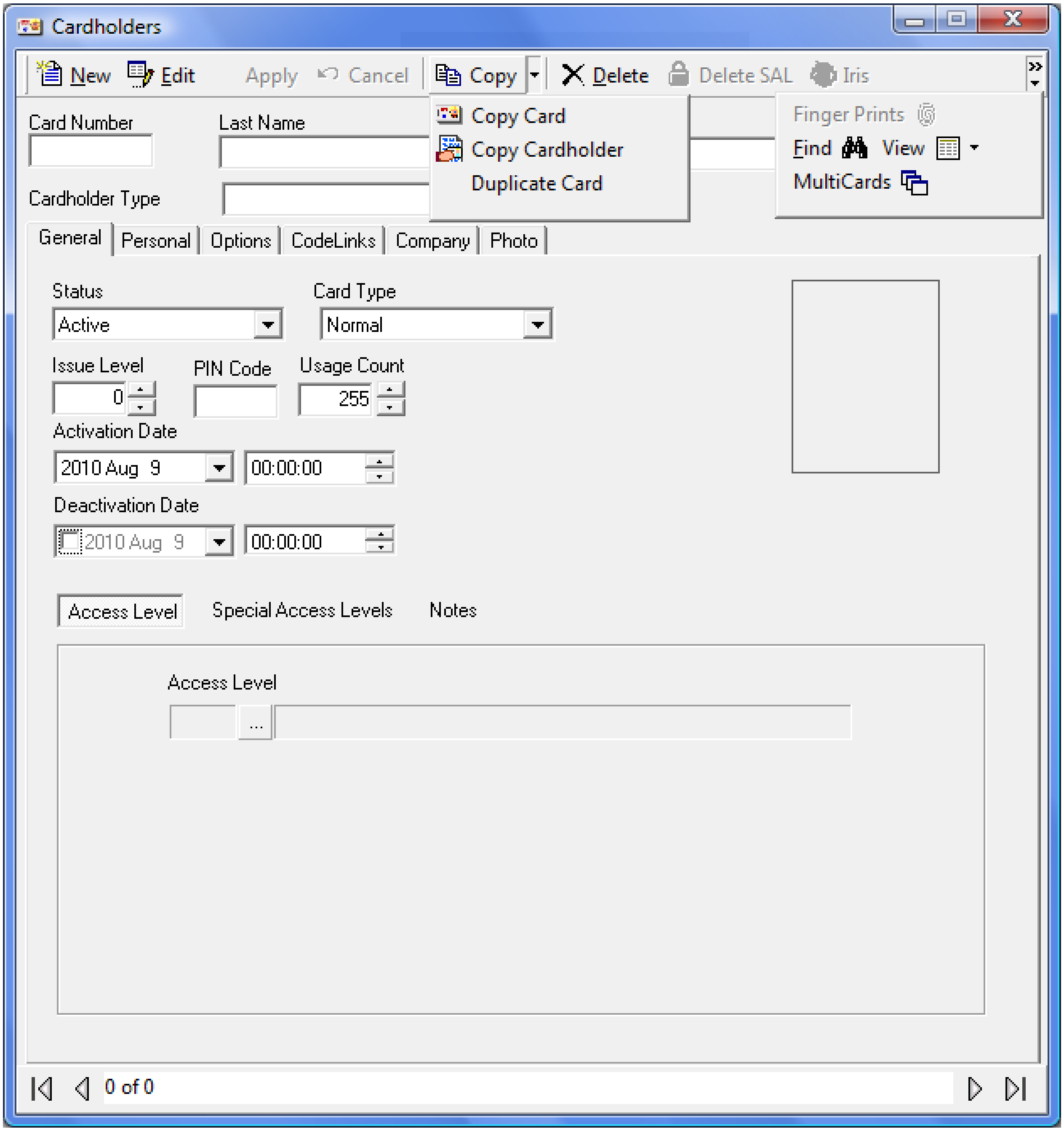
The *Cardholder* screen is used to manage all of the cardholders in the system.

If you enter an existing *Cardholder's* name the system will advise you of this before creating a duplicate *Cardholder*.



Cardholder with this name and address already exists, do you want to continue?

Cardholder Screen



Card Number

Last Name

Cardholder Type

Status: Active

Card Type: Normal

Issue Level: 0

PIN Code

Usage Count: 255

Activation Date: 2010 Aug 9 00:00:00

Deactivation Date: 2010 Aug 9 00:00:00

Access Level

0 of 0

Copy

Copy Card

Copy Card will bring up the *Copy Wizard* to copy card data only from one card to one or more cards (e.g. *Usage Count*, *Lock/Unlock*, *Activation Date*, & *De-activation Date*).

Copy Cardholder

Copy Cardholder will bring up the *Copy Wizard* to copy cardholder data only from one cardholder to one or more cardholders (e.g. Address, City, State, Department, & Photo).

Duplicate Card

Duplicate Card is used to transfer a Cardholder's record information to a new card number. If the card number is the only data you want to change it is best to make a duplicate card with the new number.

View

Cardholder Report

This selection will create a report showing the data on the current cardholder.

Cardholder Reader Report

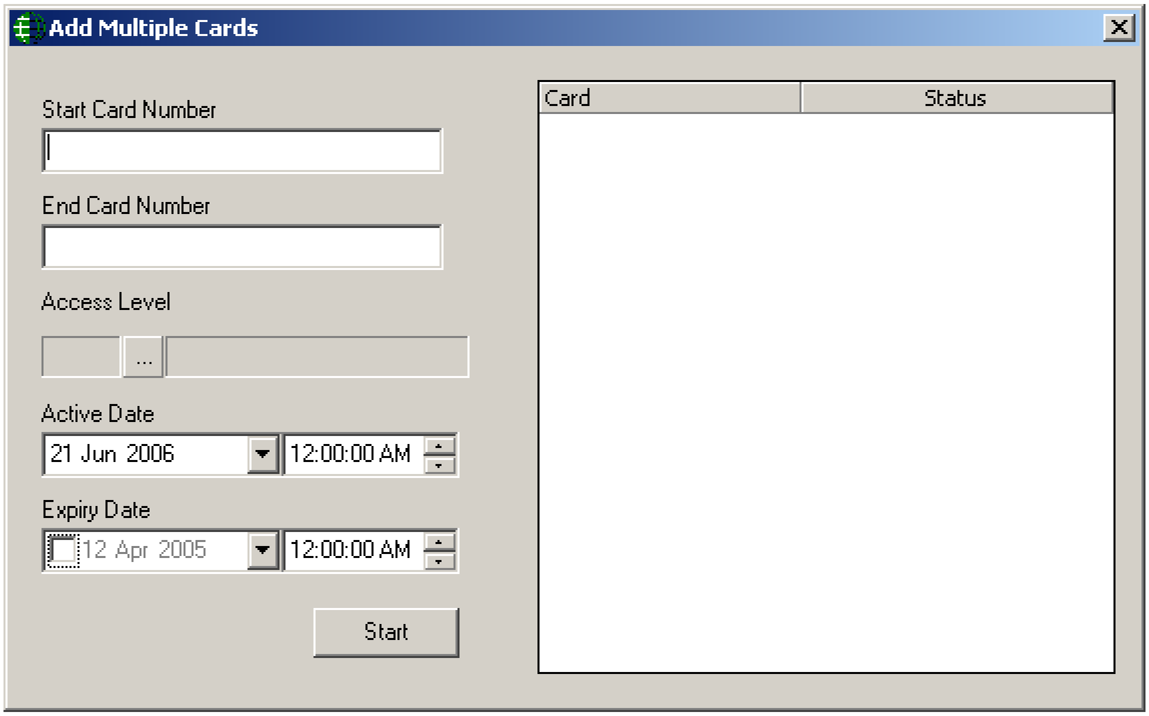
This selection will create a report showing all the readers that the specified cardholder(s) have access to.

Delete SAL

Click *Delete SAL* to remove all special access levels for the current cardholder.

MultiCards

Use *MultiCards* to bulk add cards to your database.



Start Card Number

End Card Number

Access Level

Active Date
21 Jun 2006 12:00:00 AM

Expiry Date
□ 12 Apr 2005 12:00:00 AM

Start Card Number

Enter the card number of the first card to be added.

End Card Number

Enter the card number of the last card to be added

Access Level

Enter the *Access Level* that is to be programmed in all added cards.

Active Date

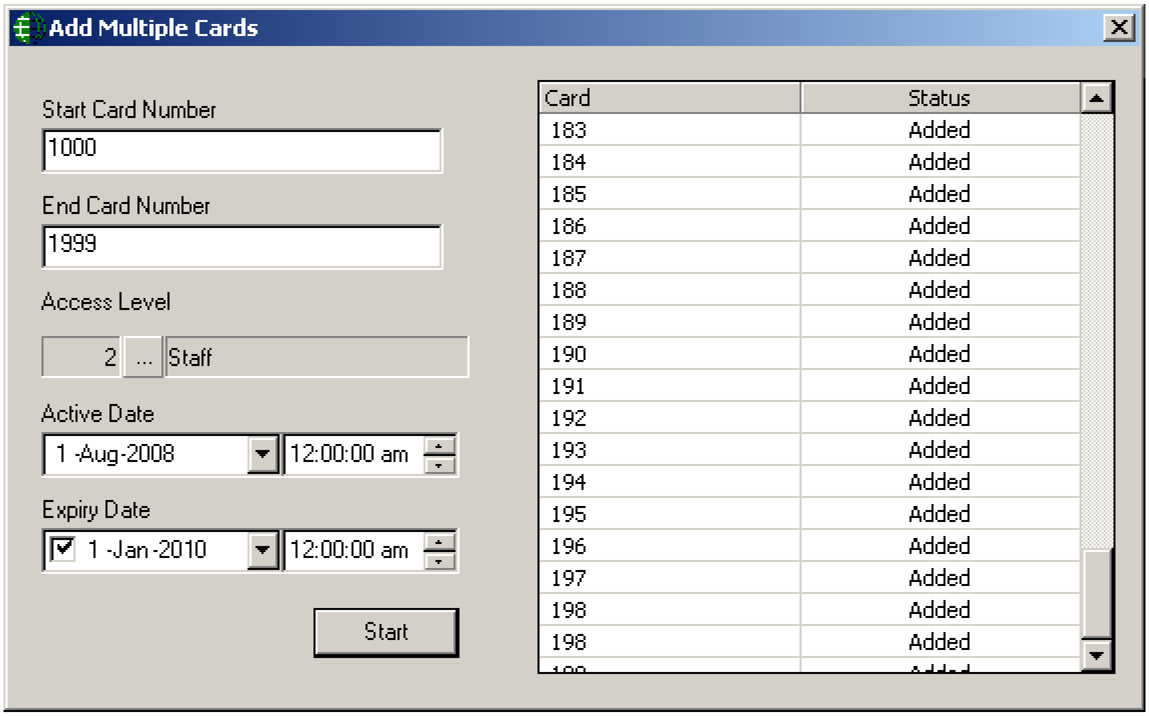
Enter the date that all cards are to be activated on. Selecting the current date will make the cards active right away.

Expiry Date

If applicable, enter the date that all cards are to expire on.

Start

Click *Start* to use the entered data to create new card in the system. Cards will be added sequentially starting at the *Start Card Number* and ending with the *End Card Number*.



Start Card Number: 1000

End Card Number: 1999

Access Level: 2 ... Staff

Active Date: 1 -Aug-2008 12:00:00 am

Expiry Date: ☑ 1 -Jan-2010 12:00:00 am

Card	Status
183	Added
184	Added
185	Added
186	Added
187	Added
188	Added
189	Added
190	Added
191	Added
192	Added
193	Added
194	Added
195	Added
196	Added
197	Added
198	Added
198	Added

Card Number

Card Number is the number of the card held by the cardholder. After a *Card Number* has been assigned it cannot be edited. All other data can be edited.

Last Name

Last Name is the family name or surname of the cardholder. The cardholder cannot be saved if this field is left blank.

First Name

First Name is the given or common name of the cardholder.

Initials

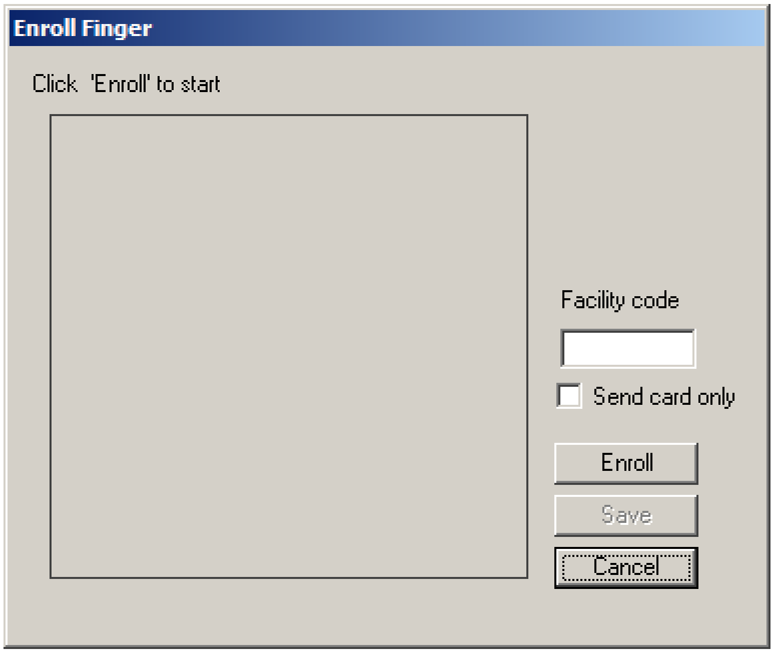
'Initials' is a field available for saving the cardholder's initials. Either the cardholder's full initials or just their middle initials can be entered here.

Cardholder Type

Select from the pull-down list which *Cardholder Type* (if any) that this cardholder is going to be a member of. (For more information on *Cardholder Types* see page 294.)

Finger Prints

At least one Finger Print Reader must first be configured before you can enroll a cardholder's finger prints.


Enroll Finger

Click 'Enroll' to start

Facility code

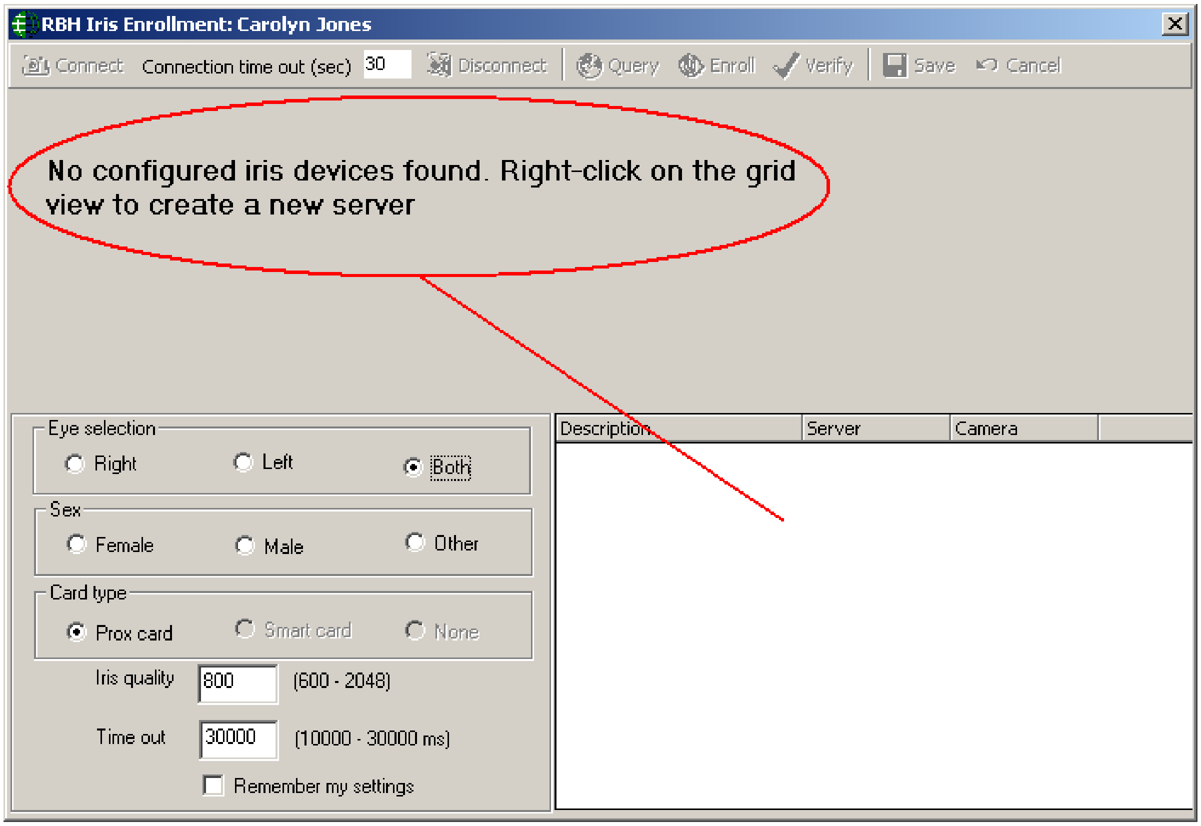
□ Send card only

The enrolment fingerprint varies depending upon the manufacture of the device. For more information on finger print enrollment see the documents on the AxiomV™ installation CD (Bioscrypt AxiomV.pdf, Keico AxiomV.pdf, RBH-BIO readerAxiomV.pdf, or TB65_BFRQuickConfigGuide.pdf).

Iris

Iris integration is an eye scanner integration which requires IrisAccess® iData EAC Software as well as ICU & ICAM as hardware. For more information on Iris integration see the document AxiomV Iris.pdf on AxiomV™ installation CD.

Clicking on *Iris* button on Cardholder screen will open up Iris Enrollment window.



Connection time out (sec) 30

No configured iris devices found. Right-click on the grid view to create a new server

Eye selection

○ Right ○ Left ● Both

Sex

○ Female ○ Male ○ Other

Card type

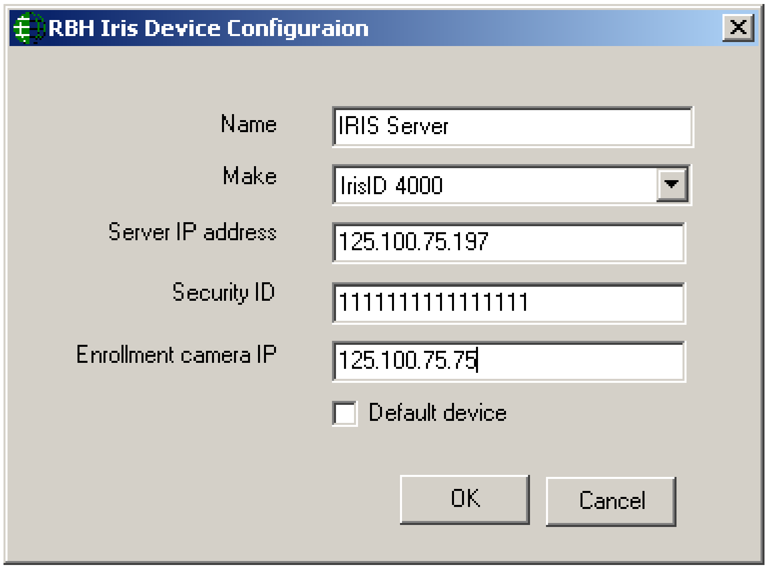
● Prox card ○ Smart card ○ None

Iris quality 800 (600 - 2048)

Time out 30000 (10000 - 30000 ms)

□ Remember my settings

Right-click on the 'grid view' and add a new server.



Name: IRIS Server

Make: IrisID 4000

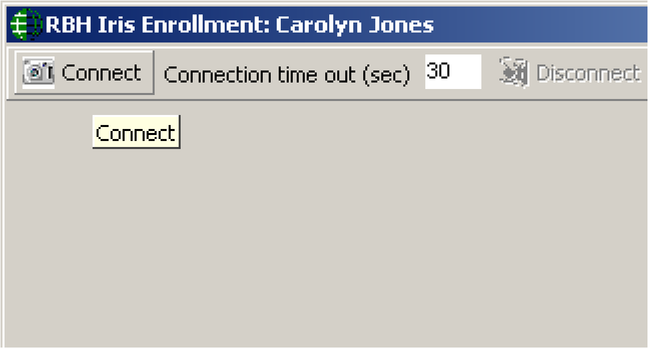
Server IP address: 125.100.75.197

Security ID: 1111111111111111

Enrollment camera IP: 125.100.75.75

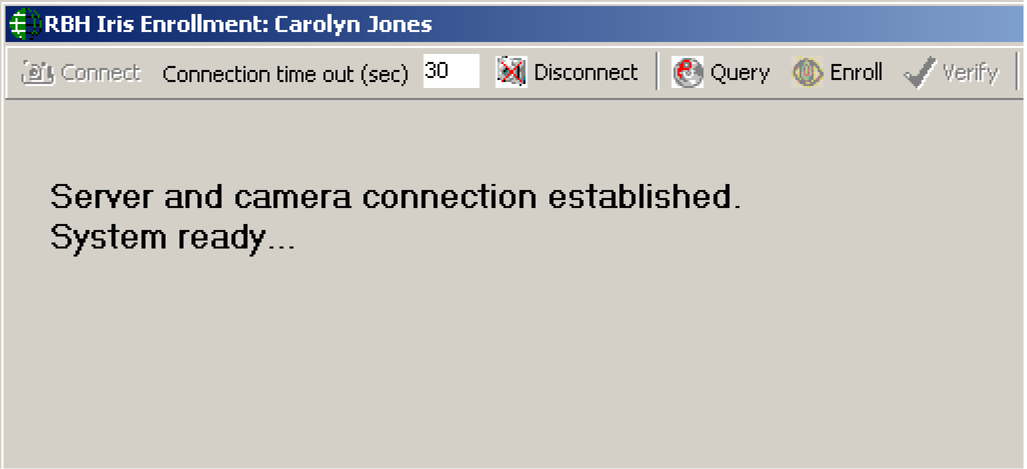
□ Default device

After adding the server, Click *Connect* to establish a connection with the Iris Server & ICAM



Connection time out (sec) 30

Ensure that you are logged into the Iris Server.



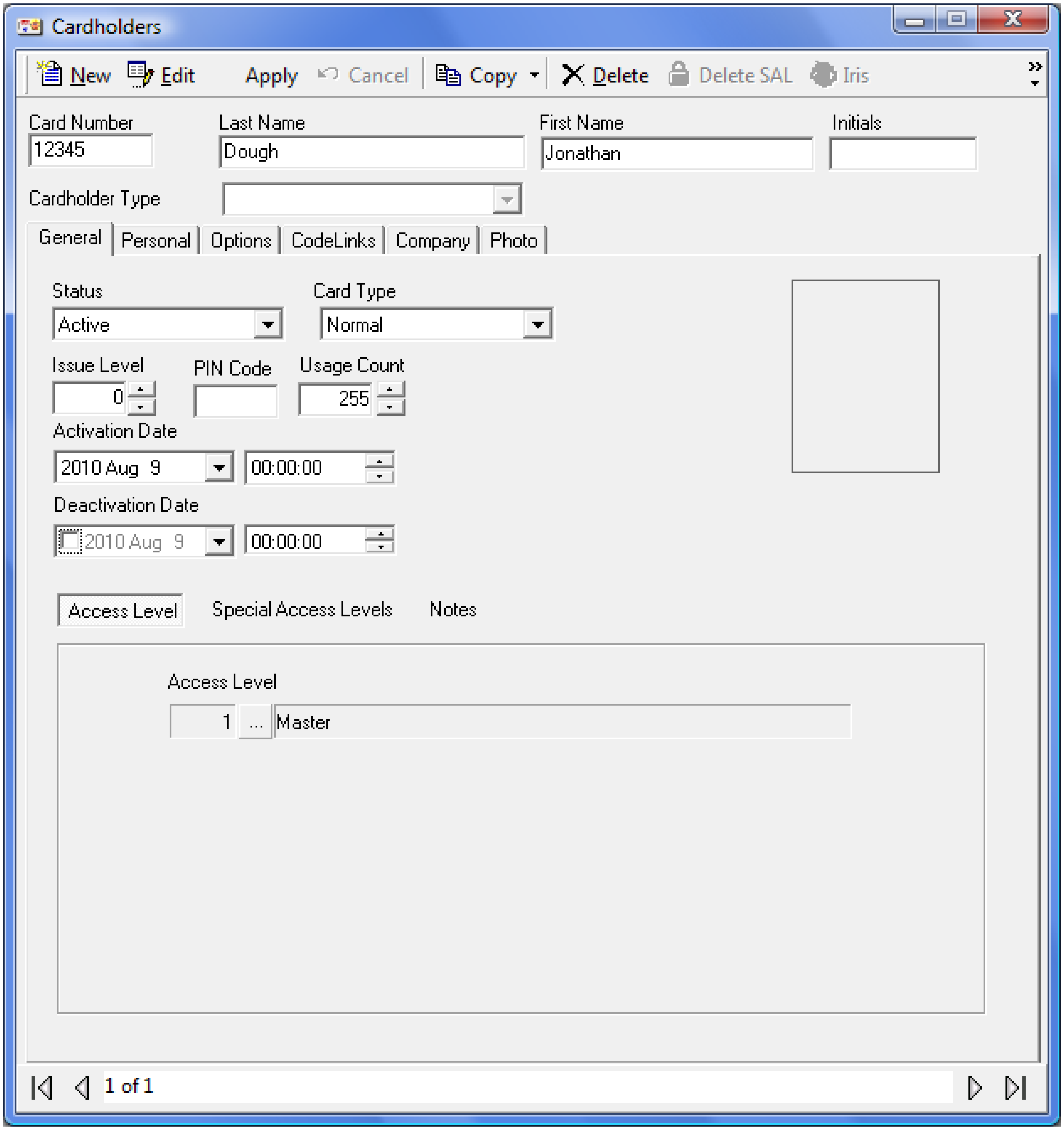
Connection time out (sec) 30

Server and camera connection established.
System ready...

With the connection established you can now enrol the cardholder.

Select ‘Save’ to save the enrolled cardholder’s data.

Cardholder General Tab (Special Access Levels)



Card Number	Last Name	First Name	Initials
12345	Dough	Jonathan	

Cardholder Type:

Status: Active

Card Type: Normal

Issue Level: 0

PIN Code:

Usage Count: 255

Activation Date: 2010 Aug 9 00:00:00

Deactivation Date: □ 2010 Aug 9 00:00:00

Access Level: 1 ... Master

1 of 1

Status

The status of the card can be set to *Active*, *Inactive*, *Pending*, *Stolen*, *Destroyed*, *Expired*, *Lost*, and *Suspended*. New cards are set to *Active* unless their activation date is set to sometime in the future, in which case they are set to *Pending*. Cards with a deactivation date in the past are set to *Expired*. *Stolen*, *Destroyed*, *Lost,* and *Suspended* are different ways of tagging a card for audit purposes. Inactive is an unspecified way of disabling a card with operator commands or links. Only *Active* cards will be granted access, all others will be denied access based on the card's status.

Card Type

There are four card types, *Normal*, *Supervisor*, *Visitor,* and *Contractor*. Almost all cards will be left as Normal. The purpose of the *Visitor* card is to log the location of the visitor and not allow them free access to the premises. Visitors are controlled through the Visitor Management (see page 300.)

Issue Level

Issue Level is used with magnetic strip cards only. The issue level is a number from zero to seven programmed into each Card. When a Card is first issued, its issue level should be programmed to zero to match the issue level field in each cardholder record, which automatically defaults to zero. If a card is lost, you can issue the cardholder with a new card programmed with a higher level, for example 1, and set the issue level field in the cardholder record to one as well. When you have done this, the old card with issue level 0 will not work and so cannot be used by someone who finds it to gain access.

The system also has the added benefit that the cardholder will always have the same card number in the history files.

PIN Code

PIN Code is a keypad-entered code. A *PIN Code* is required for Card & Code operation or for code only operation.

AxiomV™ only accepts *PIN Codes* that are transmitted in 8-bit format.

Some keypads and keypad-readers output their data in a card format (e.g. standard 26-bit). If these units are being used, add the code being punched in as a card number and not as a *PIN Code.*

Usage Count

Usage Count is used to give a cardholder a limited number uses. (E.g. a cardholder could purchase a limited number of days at a Health Club. Each time the cardholder enters the club one use is deduced.) When the count reaches zero access is denied ("No Usage Count"). The count can be set anywhere from 1 to 254. A usage count of 255 means unlimited usage.

Activation Date

When entering a new card the *Activation Date* defaults to the current date. This date can be changed if necessary. If the *Activation Date* is put into the future the card will not grant access until that date.

Deactivation Date

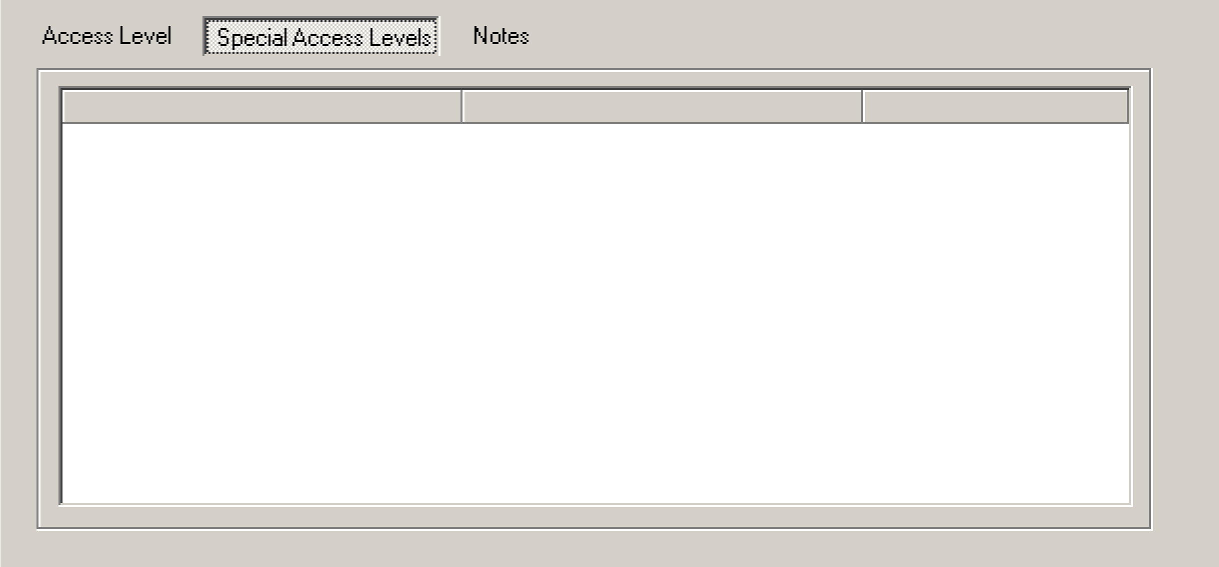
The *Deactivation Date* will specify the first date that the card will no longer work. If the *Deactivation Date* is not checked then the card will never expire.

Access Level

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

Special Access Levels

Special Access Levels allows the operator to customize the cardholder's access. Select an *Access Schedule* then check which access points the cardholder can access during that time. Additional schedules can be selected and access points checked for them. This is generally used along with the regular Access Level as an enhancement. Access points checked under a schedule will not show up under any other schedule.



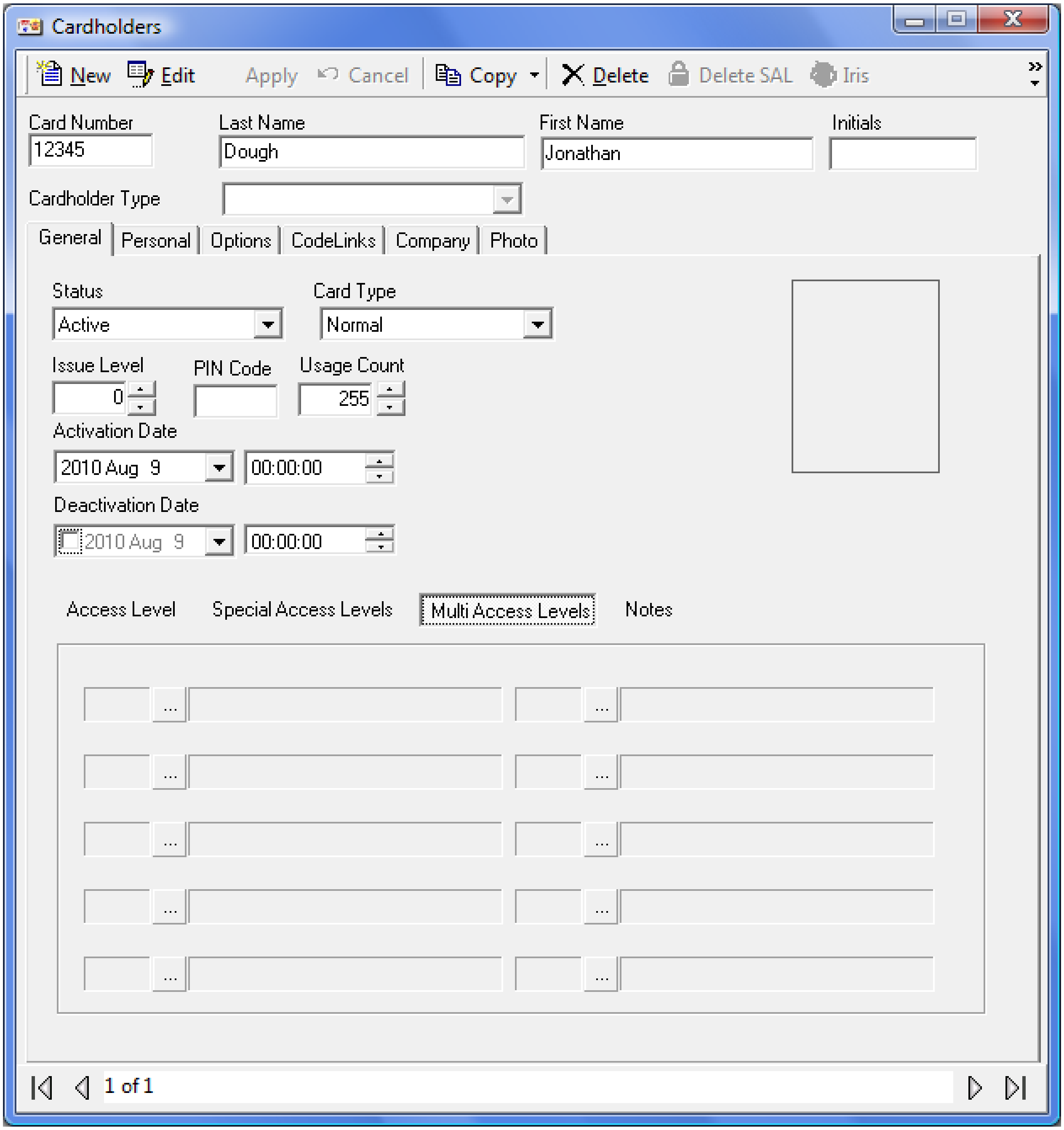
✏ **Run a *Cardholder Reader Report* to see a complete list of access points the cardholder has access to and the schedules associated with these access points.**

✏ **If either Access Level or Special Access Levels allows access then access will be granted.**

Notes

Notes provide an area to enter information pertaining to the cardholder that doesn't fit into any of the other fields.

Cardholder General Tab (Multiple Access Levels)

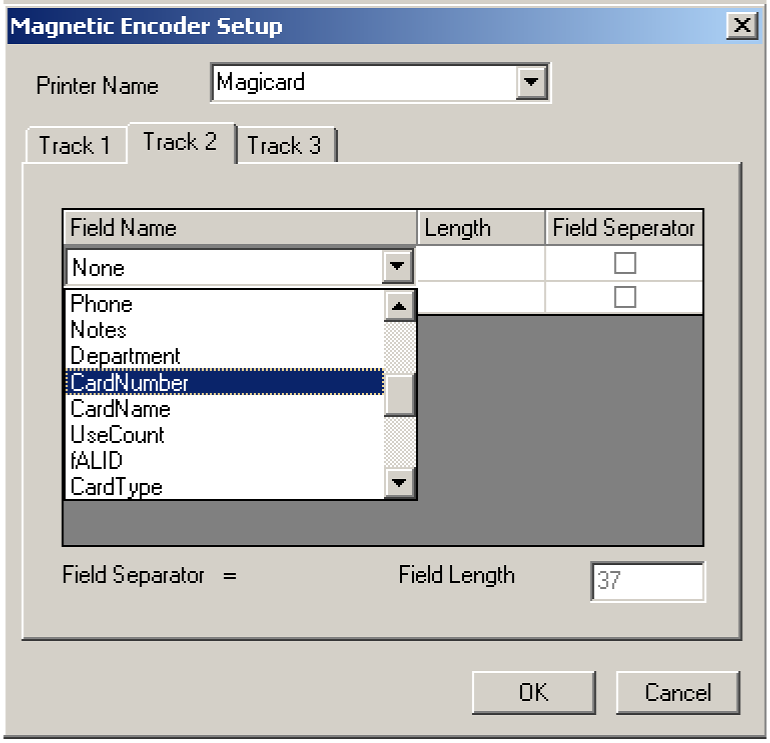


Card Number: 12345
Last Name: Dough
First Name: Jonathan
Initials:
Cardholder Type:
Status: Active
Card Type: Normal
Issue Level: 0
PIN Code:
Usage Count: 255
Activation Date: 2010 Aug 9 00:00:00
Deactivation Date: ☐ 2010 Aug 9 00:00:00

Multiple Access Levels

With *Multiple Access Levels* selected a cardholder can be given up to one standard access level and ten Multi access levels. In cases where two or more access levels provide access to the same access point then access will be granted if **any** access level would allow access. Cardholders do not <u>have</u> to have a standard access level; they <u>could</u> be given only multi access levels. Access levels configured as 'Both' could be given to a cardholder as either a standard or multi access level, and access levels type ‘Special’ could be assigned only as multi access level.

☞ **Information on turning on Multiple Access Levels is given in *System Options* -** System.



Magnetic Encoder Setup

Printer Name: Magicard

Track 1 | Track 2 | Track 3

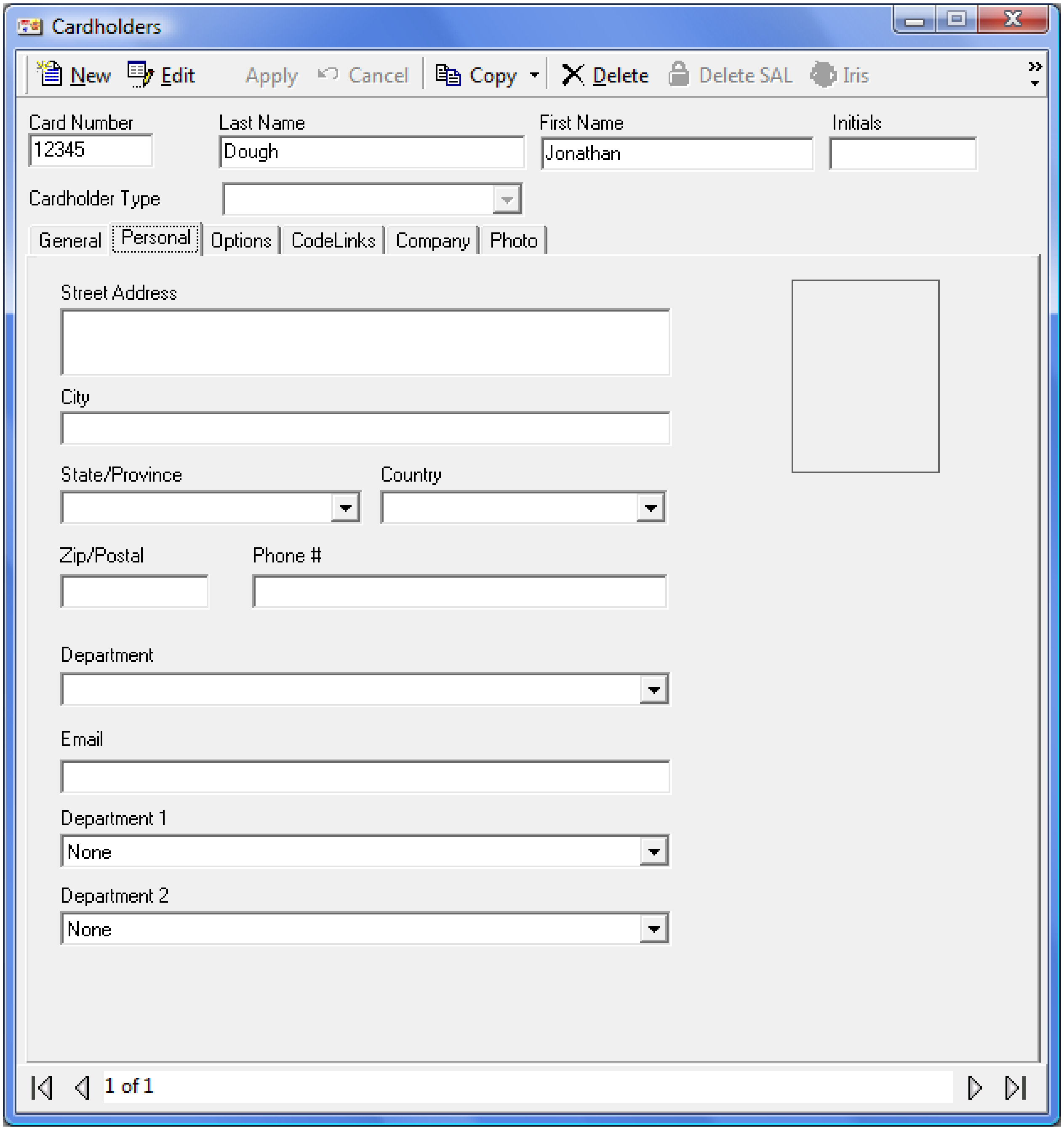
Field Name	Length	Field Seperator
None		□
		□

Field Separator =

Field Length: 37

☞ **Information on creating access levels is given in Access Levels - General (Multiple Access Levels.**

Cardholder Personal Tab



Card Number: 12345
Last Name: Dough
First Name: Jonathan
Initials:
Cardholder Type:
Street Address:
City:
State/Province:
Country:
Zip/Postal:
Phone #:
Department:
Email:
Department 1: None
Department 2: None

Street Address

Up to 50 alphanumeric characters may be entered here. Multiple lines are provided for this information.

City

Up to 50 alphanumeric characters may be entered here.

State/Province

Up to 50 alphanumeric characters may be entered here. Use the pull down list to select from previously entered data.

Country

Up to 50 alphanumeric characters may be entered here. Use the pull down list to select from previously entered data.

Zip/Postal

Up to 50 alphanumeric characters may be entered here.

Phone

Up to 50 alphanumeric characters may be entered here.

Department

Up to 50 alphanumeric characters may be entered here. Use the pull down list to select from previously entered data.

EMail

Up to 50 alphanumeric characters may be entered here.

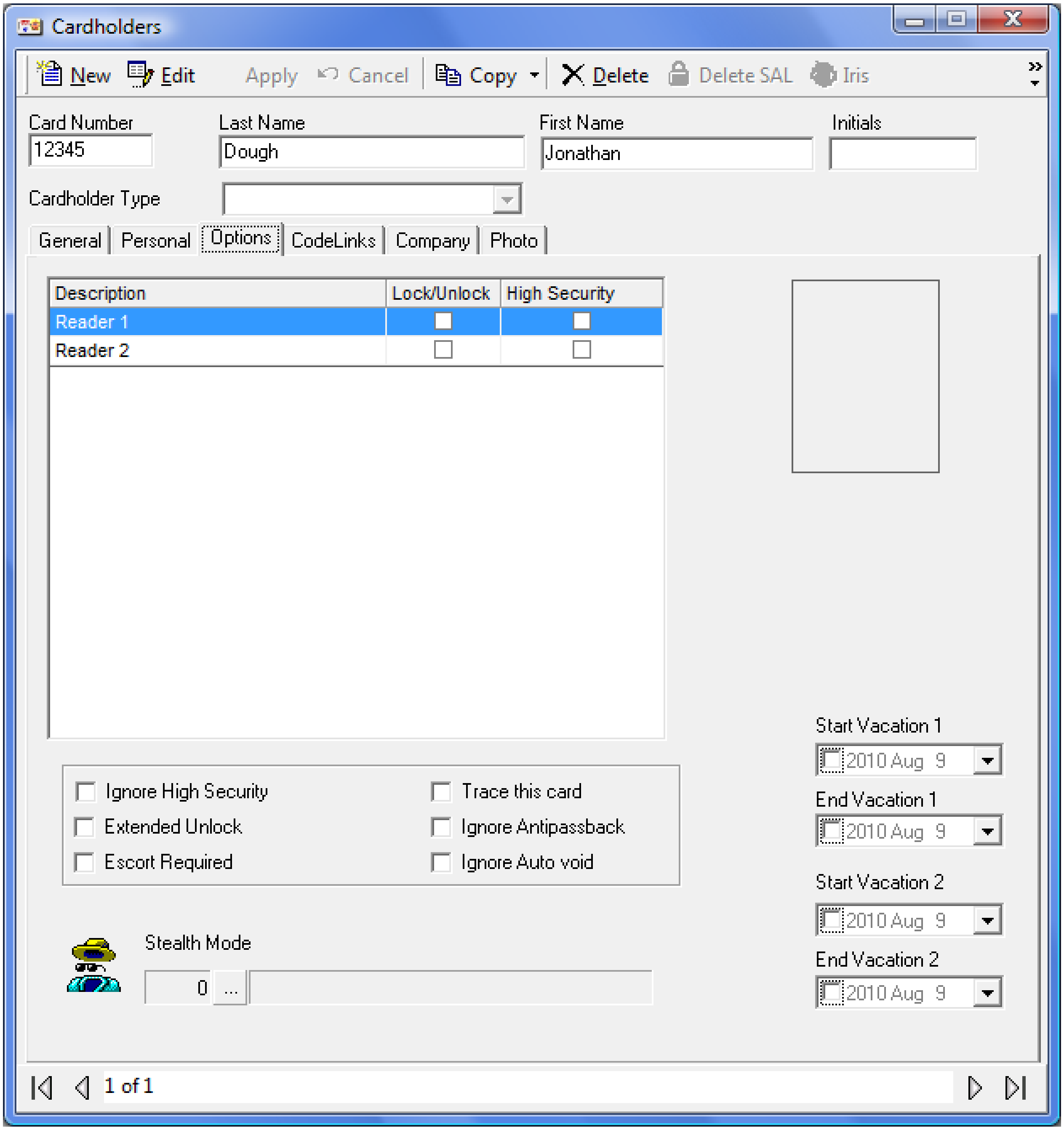
Department 1

Use the pull down list to select from the list of *Departments* configured in *Database* menu.

Department 2

Use the pull down list to select from the list of *Departments* configured in *Database* menu.

Cardholder Options Tab



Card Number: 12345

Last Name: Dough

First Name: Jonathan

Initials:

Cardholder Type:

Description	Lock/Unlock	High Security
Reader 1	□	□
Reader 2	□	□

□ Ignore High Security

□ Extended Unlock

□ Escort Required

□ Trace this card

□ Ignore Antipassback

□ Ignore Auto void

Stealth Mode: 0 ...

Start Vacation 1: □ 2010 Aug 9

End Vacation 1: □ 2010 Aug 9

Start Vacation 2: □ 2010 Aug 9

End Vacation 2: □ 2010 Aug 9

1 of 1

Access Point List

Select from the list which access points the cardholder has *Lock/Unlock* (double access granted) privilege, and which access points the cardholder has *High Security* on/off (quadruple access granted) capability.

Ignore High Security

When selected, the cardholder is able to gain access at readers that are in high security mode.

Extended Unlock

When selected, the cardholder is provided with extended unlock time (i.e., the cardholder is given extra time during which the door remains unlocked. This is used mainly for the disabled, the elderly, or anyone else that requires additional time to get through the door.)

Escort Required

When selected, a cardholder can only gain access when accompanied by a supervisor card. After the cardholder's card is presented, the supervisor's card must be presented immediately thereafter. Both the cardholder and supervisor are logged as having accessed the door.

Trace This Card

When selected, the system reports a trace alarm to the monitor screen whenever the card is used. Only access points with their *Code Tracing* schedule on will report an alarm.

Ignore Antipassback

When selected, the system ignores normal antipassback restrictions for this cardholder.

Ignore Auto Void

When this feature is selected, the selected cardholder will not be deactivated when the "Auto void cards after:" is activated.

Stealth Mode

When the schedule is on, *Stealth Mode* is active. During this mode, all cardholder activity is not printed or displayed. It is however still logged to history.

Vacation

Use the *Vacation* setting to define up to two vacation periods for the cardholder. During defined vacation periods the cardholder's card is inactive.

Start Date 1

Start Date 1 is the date (MM-DD-YYYY[12]) on which vacation 1 starts.

End Date 1

End Date 1 is the date (MM-DD-YYYY[13]) on which vacation 1 ends.

Start Date 2

Start Date 2 is the date (MM-DD-YYYY[13]) on which vacation 2 starts.

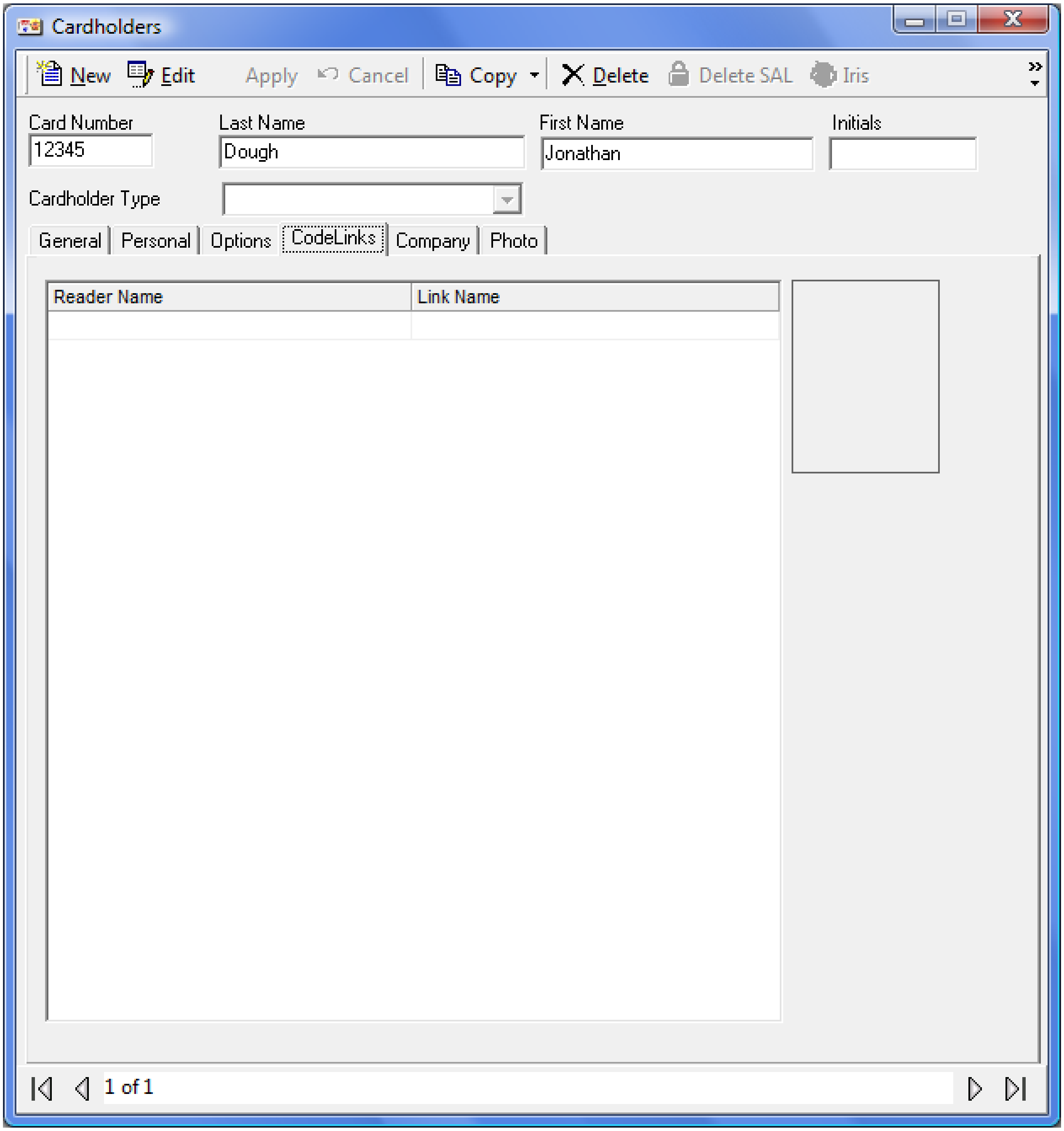
End Date 2

End Date 2 is the date (MM-DD-YYYY[13]) on which vacation 2 ends.

[12] Date is displayed in the format selected in the Windows – Control Panel – Regional Settings Properties-Date. If a two-digit year was chosen then it will be displayed in that form here.

For example a one-day vacation on August 22, 2012 would use 08-22-2012 as the *Start Date* and 08-23-2012 as the *End Date*. Likewise a 10-day vacation starting on September 1, 2012 would use 09-01-2012 as the *Start Date* and 09-10-2012 as the *End Date*.

Cardholder Code Links Tab



Card Number: 12345
Last Name: Dough
First Name: Jonathan
Initials:
Cardholder Type:

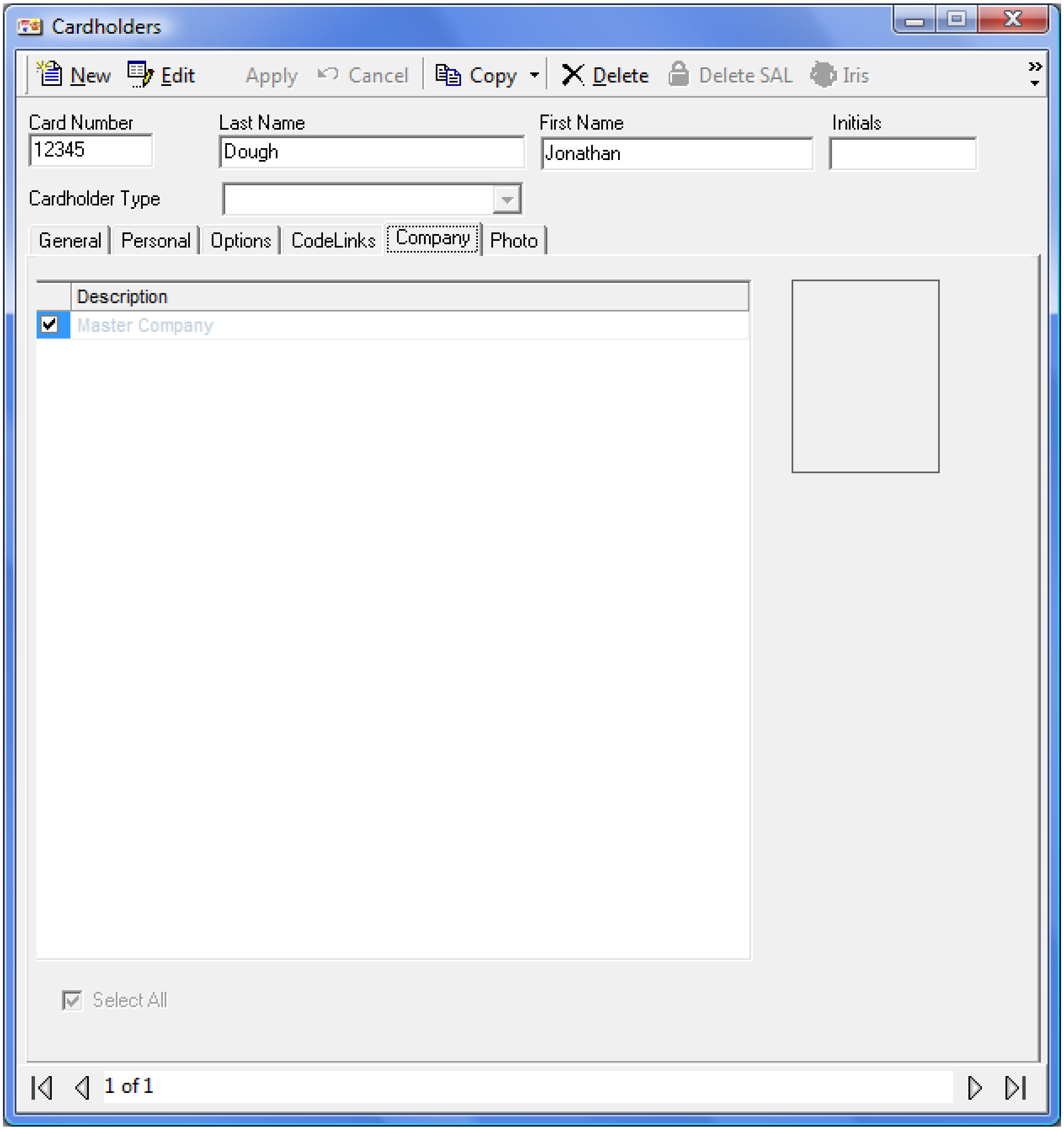
Reader Name	Link Name

1 of 1

Code Links

Code Links are a way of executing links based on the grant access of the cardholder at a specific access point. Each access point can be assigned only one link. To add a *Code Link* click in the blank box under *Reader Name* and then click the Browse/Ellipsis button. Select from the list of accessible reader then do the same for the link. When the cardholder is granted access at the access point the link will be executed.

Cardholder Company Tab



Card Number: 12345
Last Name: Dough
First Name: Jonathan
Initials:
Cardholder Type:

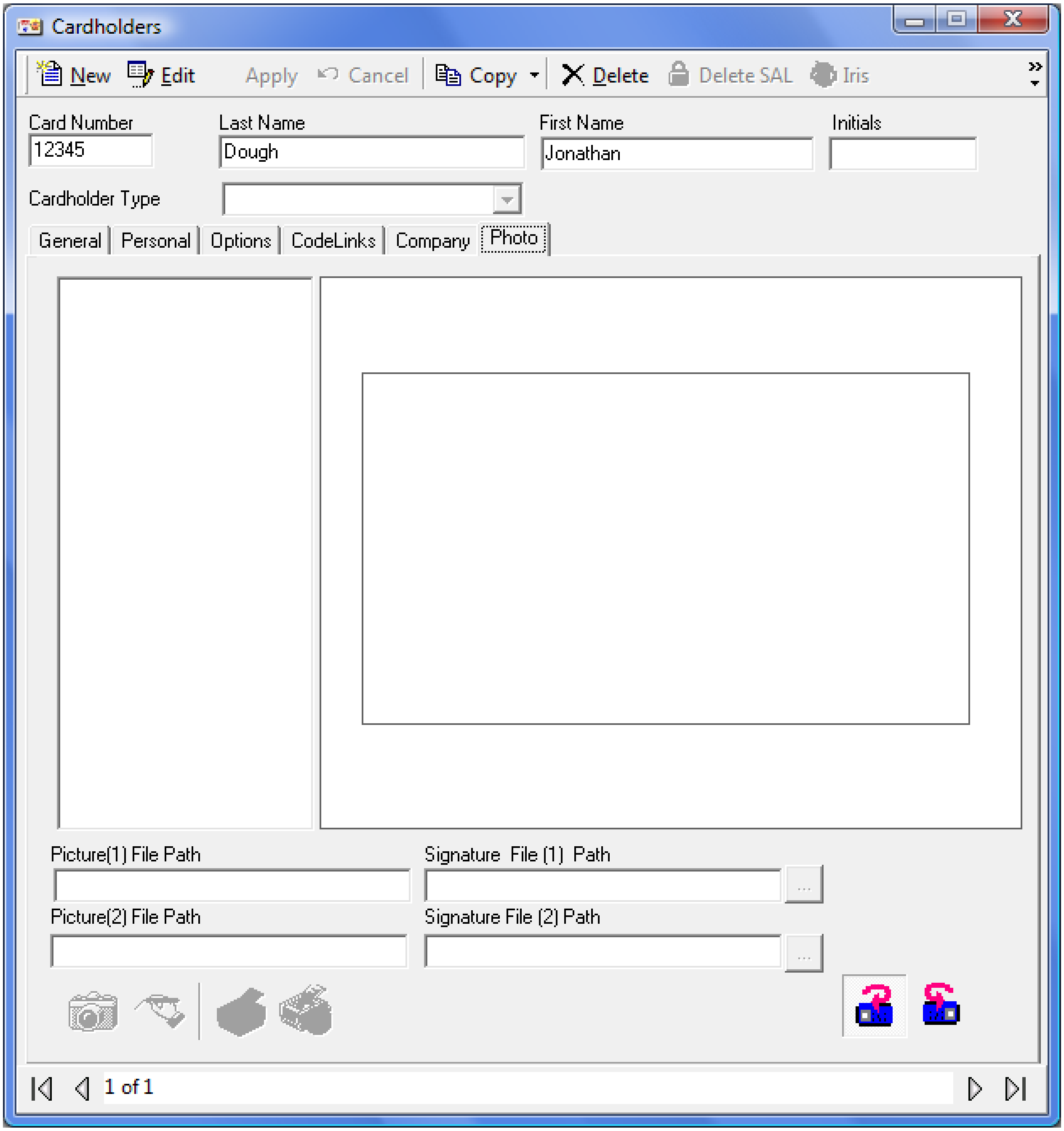
	Description
☑	Master Company

☑ Select All

Companies

Cardholder groups are called companies. Which companies (groups) the cardholder is a member of is selected here. Cardholder companies (groups) are used in operator profiles to determine which cardholders the operator will have access to.

Cardholder Photo Tab



Card Number: 12345

Last Name: Dough

First Name: Jonathan

Initials:

Cardholder Type:

Picture(1) File Path:

Signature File (1) Path:

Picture(2) File Path:

Signature File (2) Path:

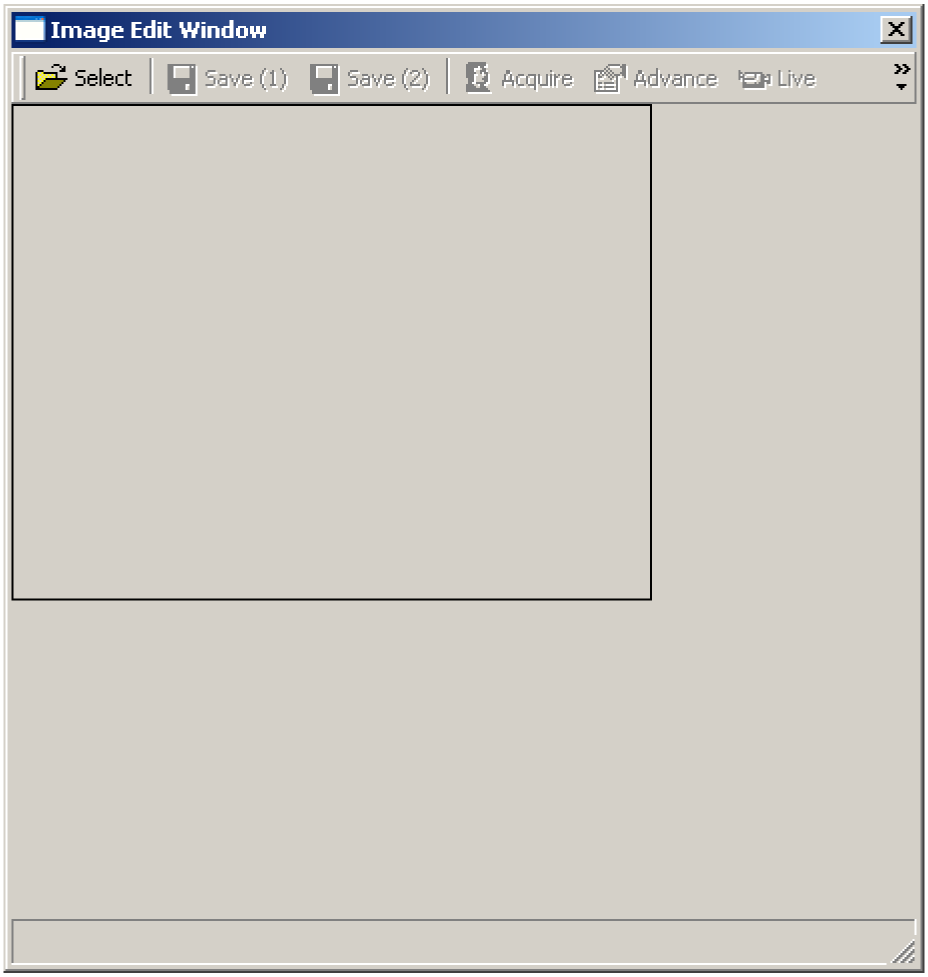
1 of 1

Templates

This box lists the badge templates. The selected template is displayed in the box on the right side of the window.

Take Picture

Click the *Take Picture* icon to capture a picture.



Use the Select button to select the previously Acquired/Saved picture.

While live video is being shown on this screen, click *Acquire* to freeze the image. Click on the image to produce a box the size to be captured. The box can then be moved around to encompass the desired area. Click *Save(1)* to save the image as *picturefile1* and *Save(2)* to save as *picture file2*. *Advanced* will open up a window for the modification of the advanced settings of the video source.

Print Card

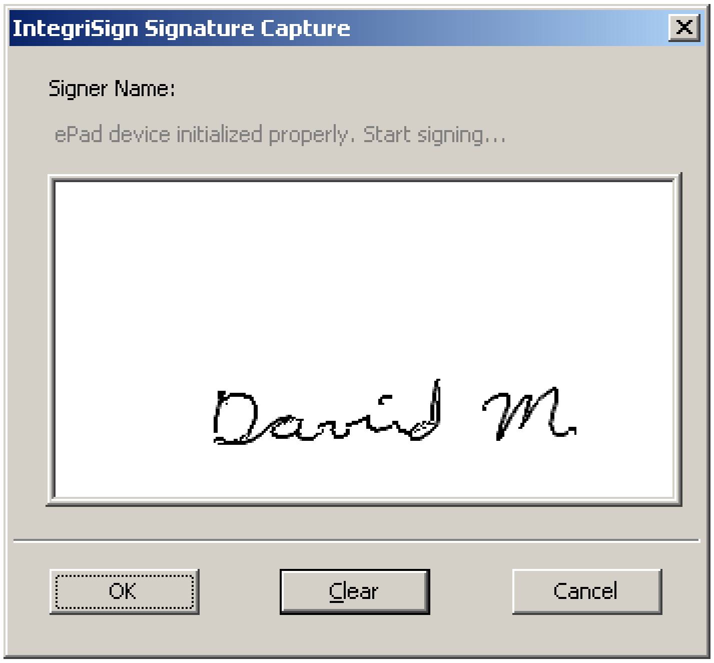
Clicking *Print Card* will send the displayed card to the printer.

Setup Printer

Setup Printer is used to edit the printer setup.

Capture Signature

Capture Signature is used to acquire a signature of the cardholder.



Signer Name:

ePad device initialized properly. Start signing...

Flip Card Side to Front

Flip Card Side to Front is used to change the card view from back to front.

Flip Card Side to Back

Flip Card Side to Back is used change the card view from front to back.

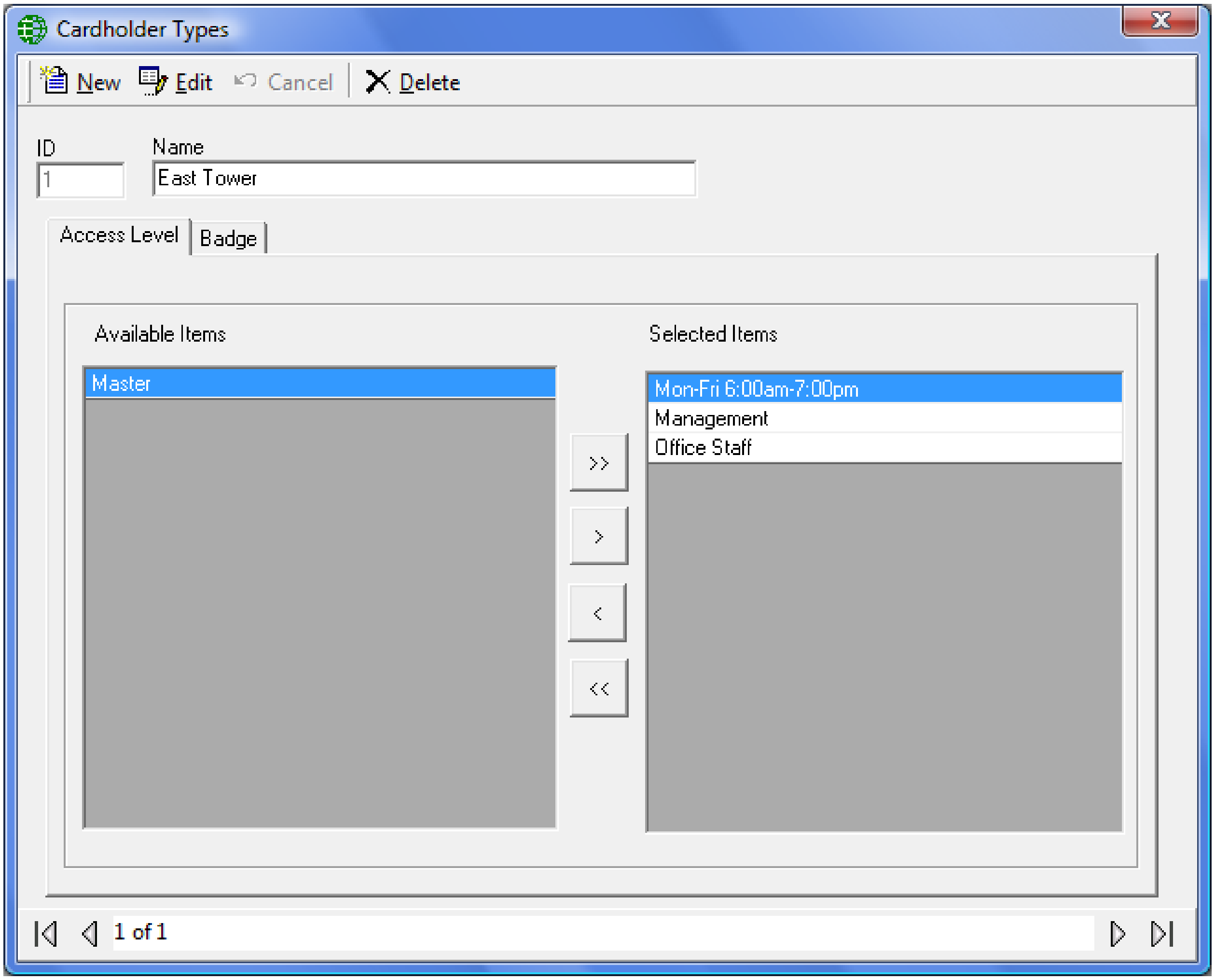
Picture File Path1/2

Picture File Path shows the name of the cardholder image. Images are saved to the Images folder.

Signature File Path1/2

Signature File Path shows the name of the signature images. Signature images are saved to the Images folder.

Cardholder Type



ID: 1

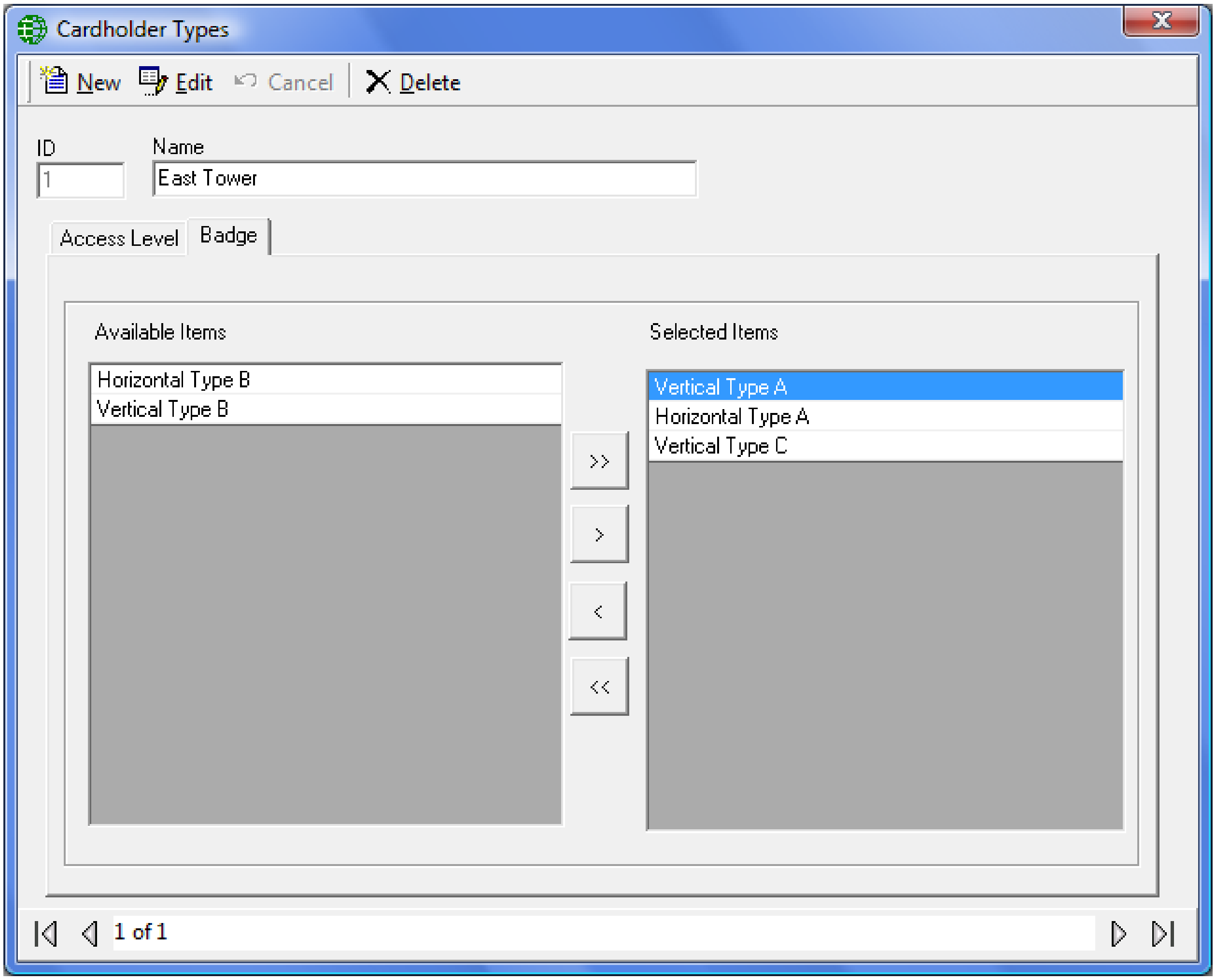
Name: East Tower

Available Items:
- Master

Selected Items:
- Mon-Fri 6:00am-7:00pm
- Management
- Office Staff

Cardholder Types is a means of grouping cardholders. For each 'type' move items from the available list to the selected list for both Access Levels and Badge templates. A cardholder that is given a cardholder type can only be given access levels and assigned badge templates that are listed for that cardholder type. Cardholders not given a *Cardholder Type* can be given any Access Levels and can be assigned any Badge templates.

The *Access level* availability list will only include regular *Access Levels* and access levels from *Multiple Access Levels*.



ID: 1

Name: East Tower

Available Items:
- Horizontal Type B
- Vertical Type B

Selected Items:
- Vertical Type A
- Horizontal Type A
- Vertical Type C

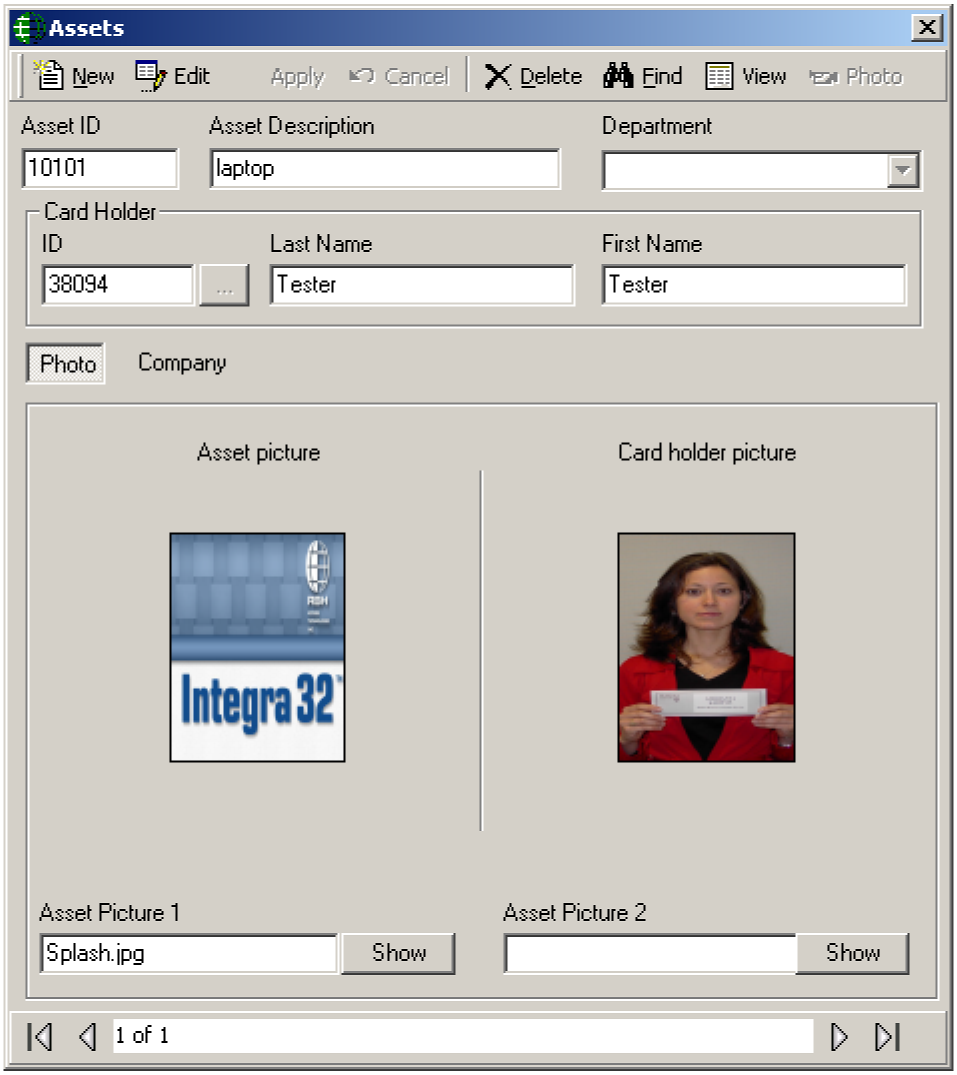
1 of 1

Asset Tracking[13]

This screen is used to configure your assets.

Asset Configuration

Assign the asset an ID number and give it a description. A department can be selected from the list. Search for and choose a cardholder to be the asset holder.



Asset ID: 10101
Asset Description: laptop
Department:
Card Holder
ID: 38094
Last Name: Tester
First Name: Tester
Asset Picture 1: Splash.jpg
Asset Picture 2:
1 of 1

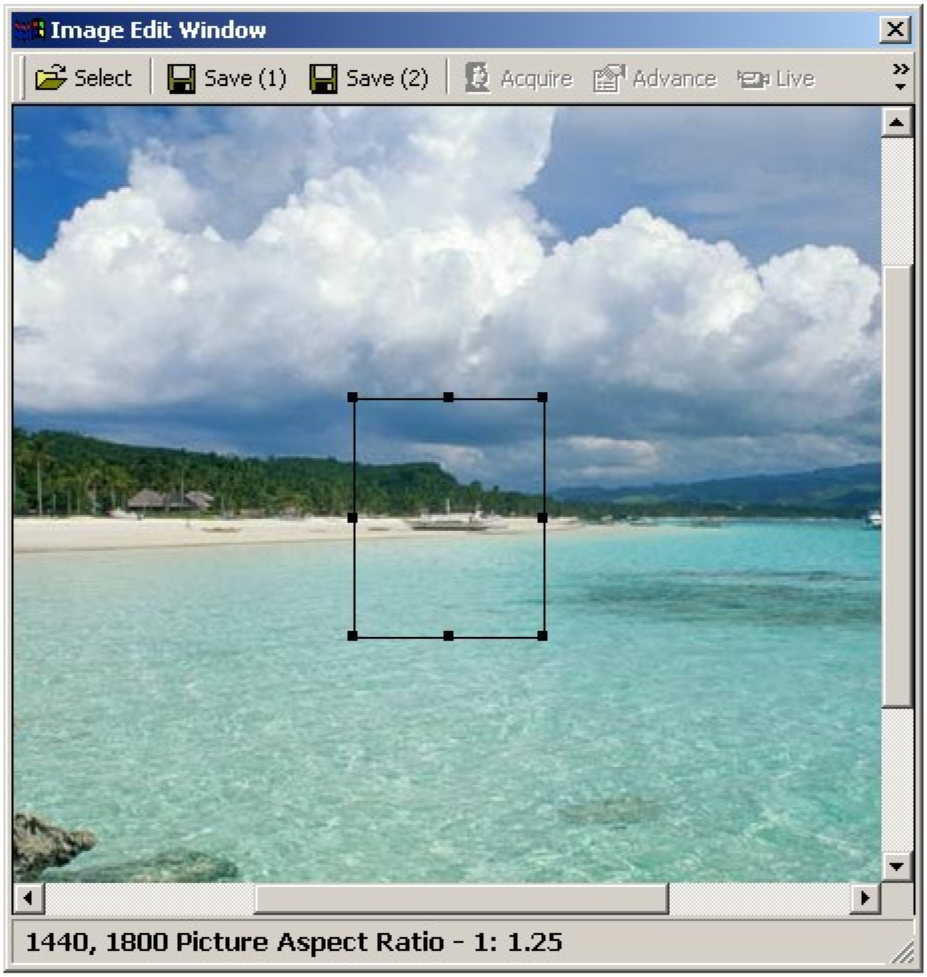
[13] This selection is only available if the optional license for the Asset Tracking Software has been purchased and installed.

Apply

Select *Apply* to have the system execute a partial download to the panels right away so that any changes made will take effect immediately.

Photo

In edit mode select *Photo* to acquire an image of the asset.



1440, 1800 Picture Aspect Ratio - 1: 1.25

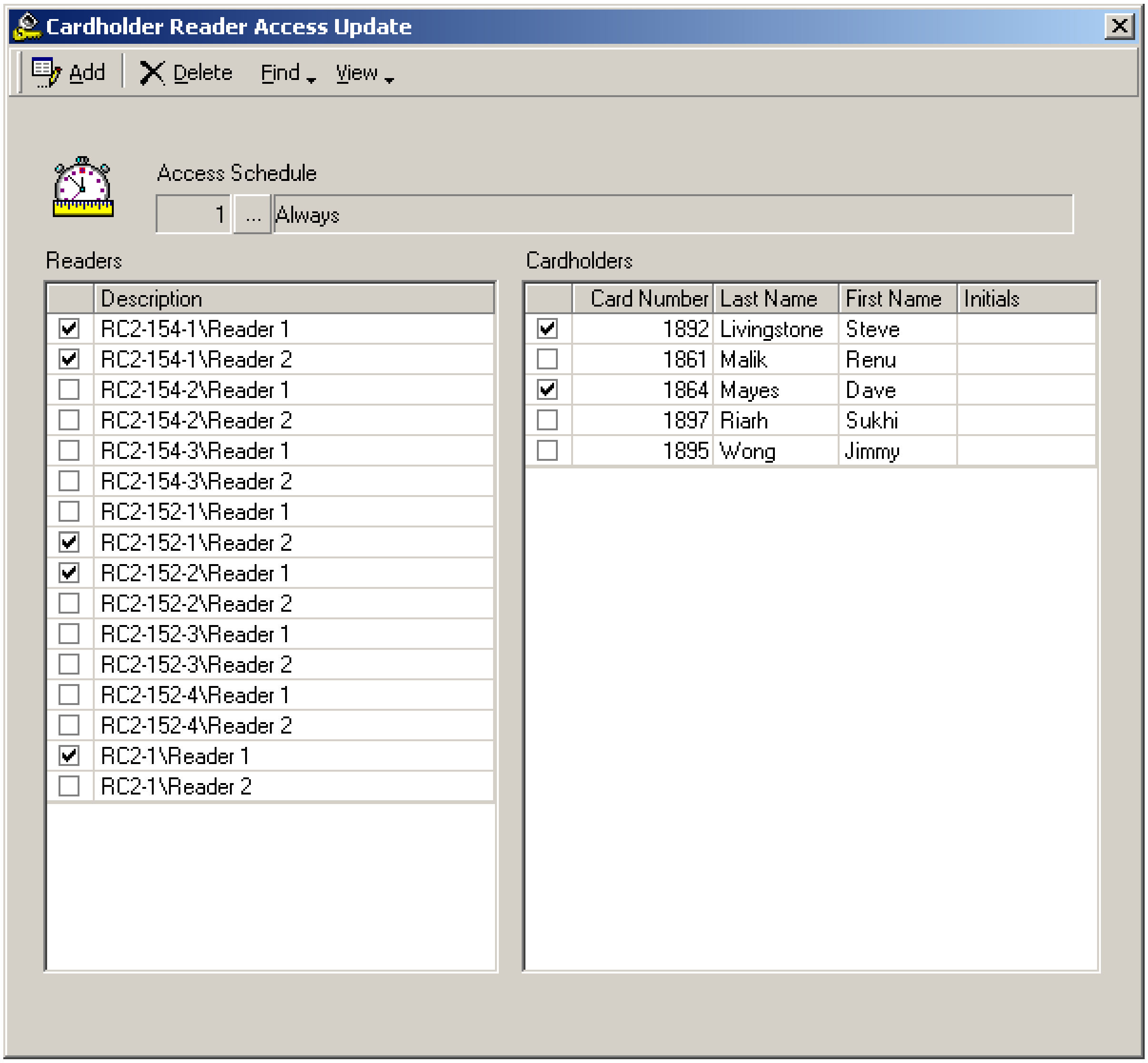
Select

Click *Select* and browse for the required picture. Crop as needed and save as *Save (1)* or *Save (2)*. For best results keep the aspect ratio as close to 1:1.25 as possible.

Reader Access

Cardholder Reader Access Update

Reader Access or Special Access Levels are used to customize a cardholder's access. It can be combined with regular Access Levels or used on its own. Instead of a cardholder being a member of an access group in cardholder can be given their own personal access level.



Access Schedule: 1 ... Always

Readers

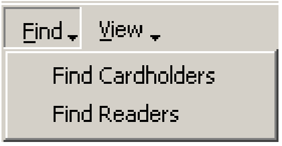
	Description
☑	RC2-154-1\Reader 1
☑	RC2-154-1\Reader 2
□	RC2-154-2\Reader 1
□	RC2-154-2\Reader 2
□	RC2-154-3\Reader 1
□	RC2-154-3\Reader 2
□	RC2-152-1\Reader 1
☑	RC2-152-1\Reader 2
☑	RC2-152-2\Reader 1
□	RC2-152-2\Reader 2
□	RC2-152-3\Reader 1
□	RC2-152-3\Reader 2
□	RC2-152-4\Reader 1
□	RC2-152-4\Reader 2
☑	RC2-1\Reader 1
□	RC2-1\Reader 2

Cardholders

	Card Number	Last Name	First Name	Initials
☑	1892	Livingstone	Steve	
□	1861	Malik	Renu	
☑	1864	Mayes	Dave	
□	1897	Riarh	Sukhi	
□	1895	Wong	Jimmy	

This utility is used to update the special accesses for cardholders. You can add one or multiple access point (for a schedule) to one or multiple cardholders, or you can delete one or multiple access point (for a schedule) from one or multiple cardholders.

Find



Find Cardholder and *Find Readers* will both bring up the search window. Search for the cardholders whose access you want to edit. Then search for the readers you want to edit. Finally browse and select the schedule to use in your edit.

Add

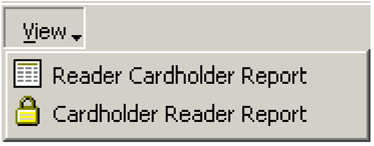
Click *Add* to have these items included in the cardholders' access.

Delete

Click *Delete* to have these items removed from the cardholders' access.

Only special access can be affected this way. Access given by a regular Access Level cannot be changed by this method.

View



Reader Cardholder Report

This selection will create a report showing all the cardholders that have access to the specified reader(s).

Cardholder Reader Report

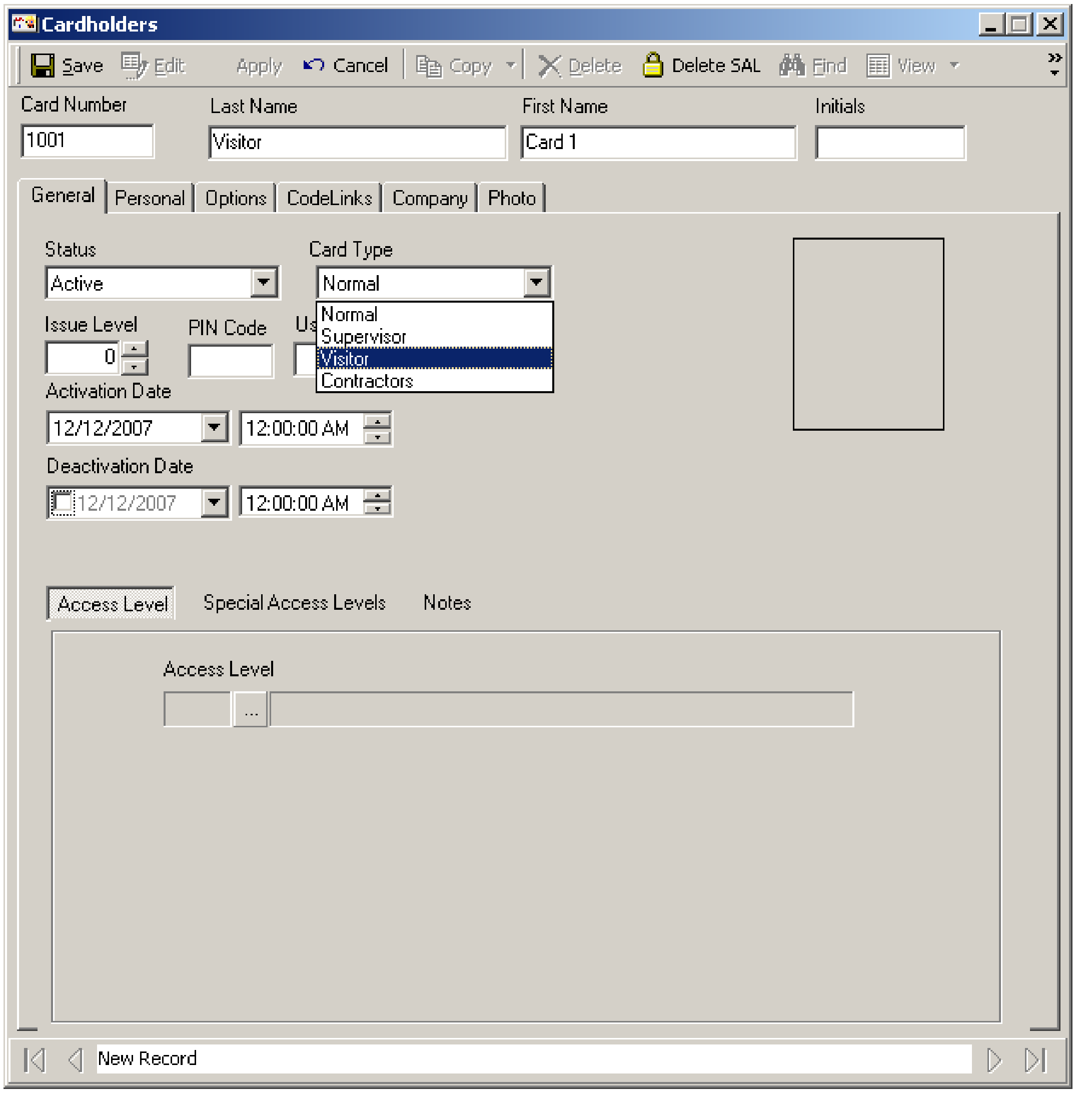
This selection will create a report showing all the readers that the specified cardholder(s) have access to.

Visitor Management[14]

The Visitor Management option is used to control and track visitors to a site.

To add a visitor into the system the card they are to use must first be entered into the cardholder screen and configured as "*Visitor" Card Type*. The first thing to be done therefore is to create cards that are going to be used by visitor to the site. Give each card an appropriate Access Level depending on where you wish to allow the visitor to go. *Visitor* can then be assigned cards with Access Levels appropriate to their needs.

It is best to keep unassigned visitor cards deactivated until needed for the first time.



Card Number: 1001
Last Name: Visitor
First Name: Card 1
Initials:

Status: Active
Card Type: Normal
Issue Level: 0
PIN Code:
Activation Date: 12/12/2007 12:00:00 AM
Deactivation Date: 12/12/2007 12:00:00 AM

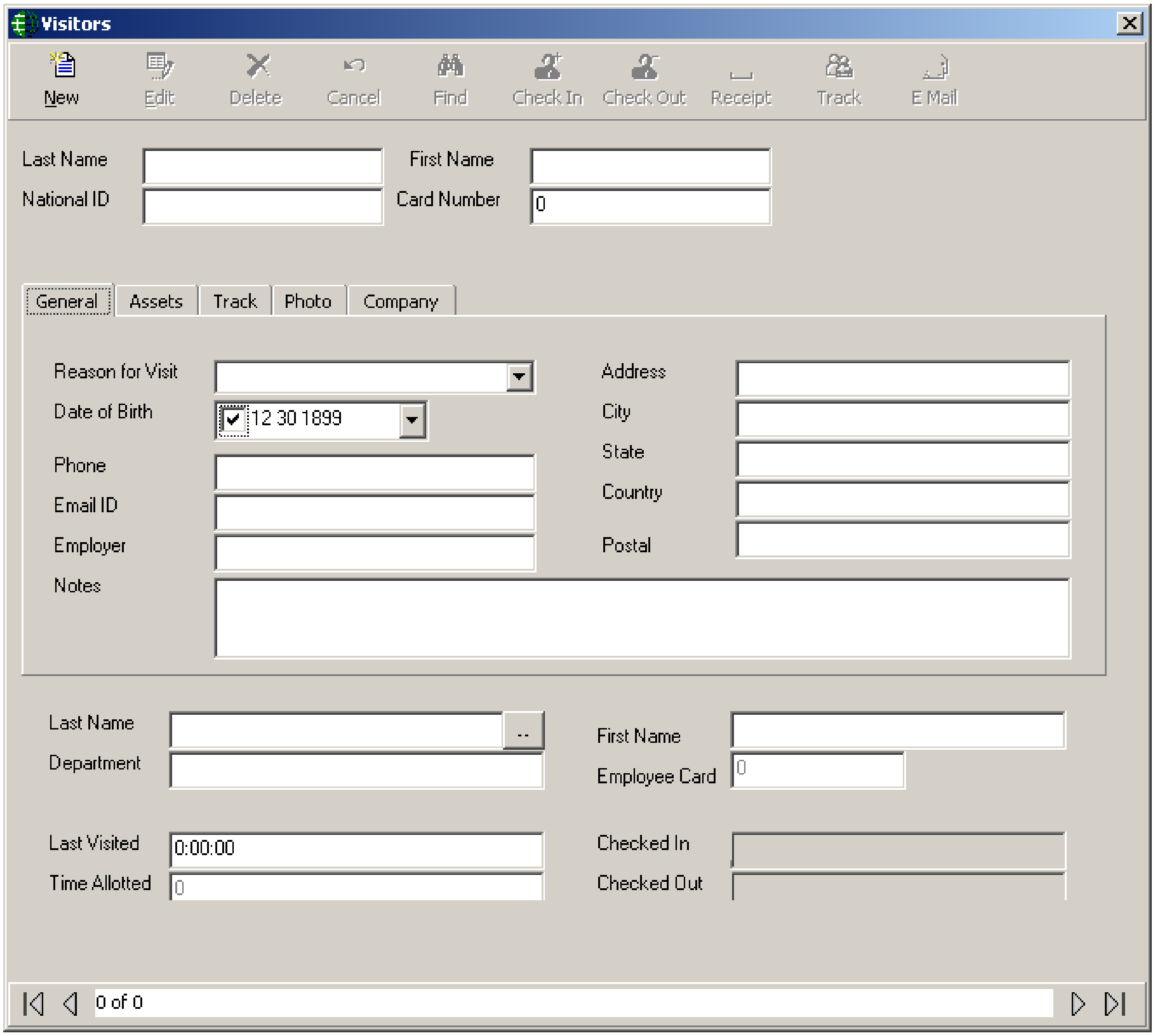
Access Level:

New Record

[14] This selection is only available if the optional license for the Visitor Management Software has been purchased and installed.

Visitors

After visitor cards have been created select *Visitors* from the Database menu or toolbar to configure visitors for the system.



Last Name:
First Name:
National ID:
Card Number: 0

Date of Birth: ☑ 12 30 1899

Employee Card: 0
Last Visited: 0:00:00
Time Allotted: 0

0 of 0

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.

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

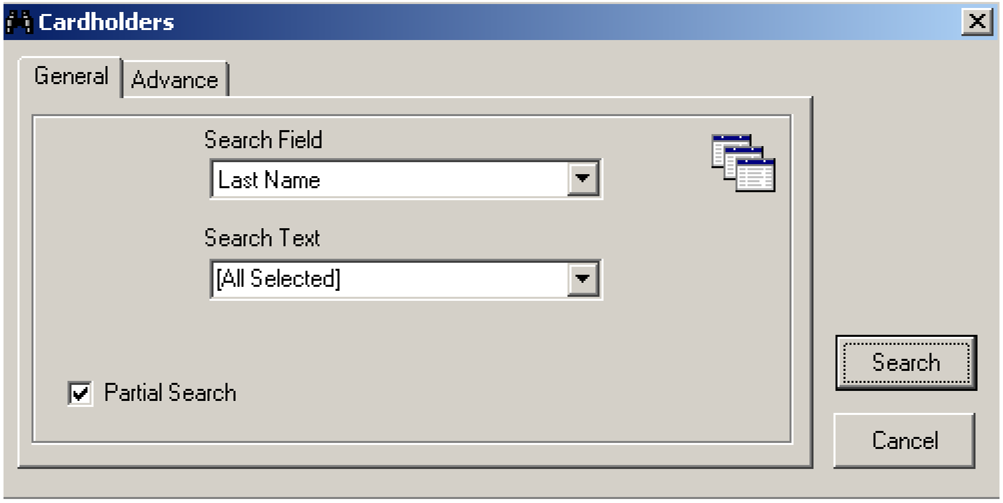
Click *Delete* to permanently remove a visitor from the database.

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.

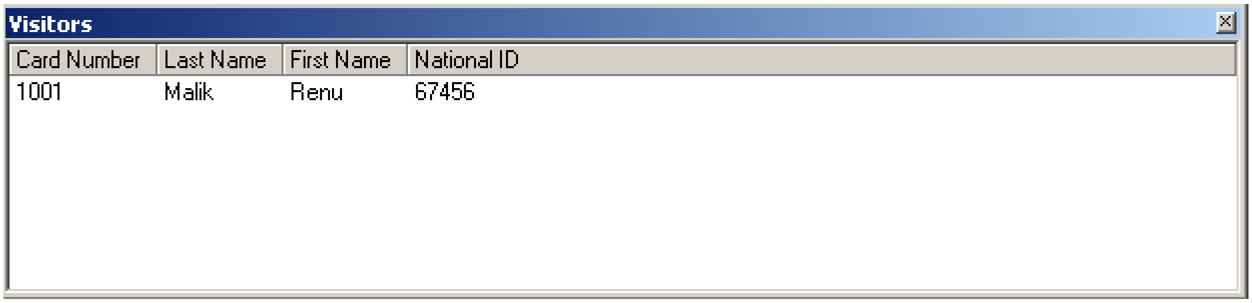


Search Field: Last Name

Search Text: [All Selected]

☑ Partial Search

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



Card Number	Last Name	First Name	National ID
1001	Malik	Renu	67456

Check In

Click *Check In* to have the visitor checked into the system. Checking in will activate the visitor's card.

Check Out

Click *Check Out* to have the visitor checked out of the system. Checking out will deactivate the visitor's card.

Track

Click *Track* to display the access points that the visitor has been granted access to while checked-in. This screen doesn't update automatically. You need to click on *Track* button every time to refresh Visitor's activity.

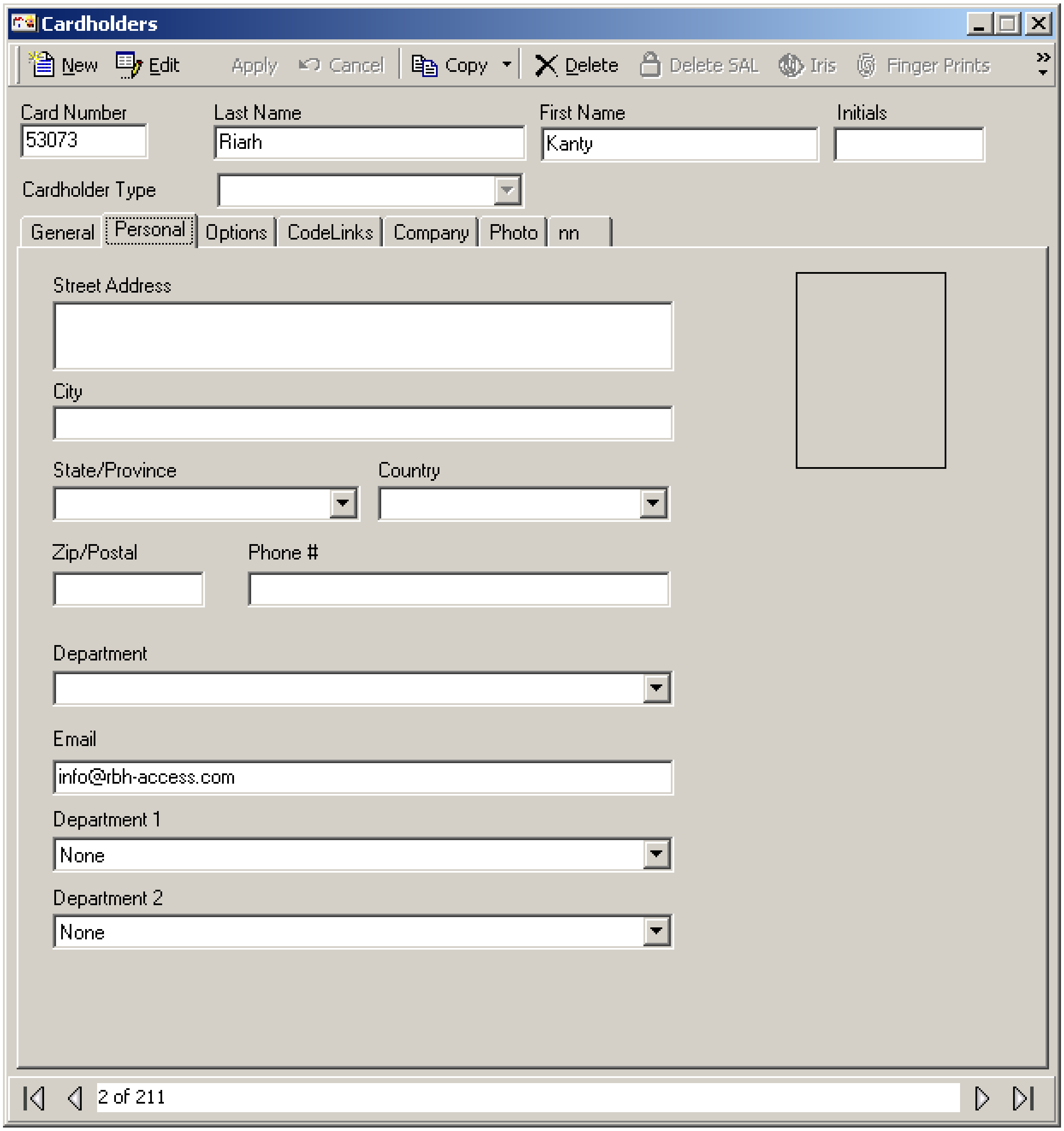
Receipt

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

Email

Click on *Email* to send an email to the cardholder being visited. For this to work the senders email information must be configured in *Email Config* under *System Settings.*

After configuring the sender's email under the system settings, the being visited cardholder's Personal Tab must have an email address.



Card Number: 53073

Last Name: Riarh

First Name: Kanty

Initials:

Cardholder Type:

Street Address:

City:

State/Province:

Country:

Zip/Postal:

Phone #:

Department:

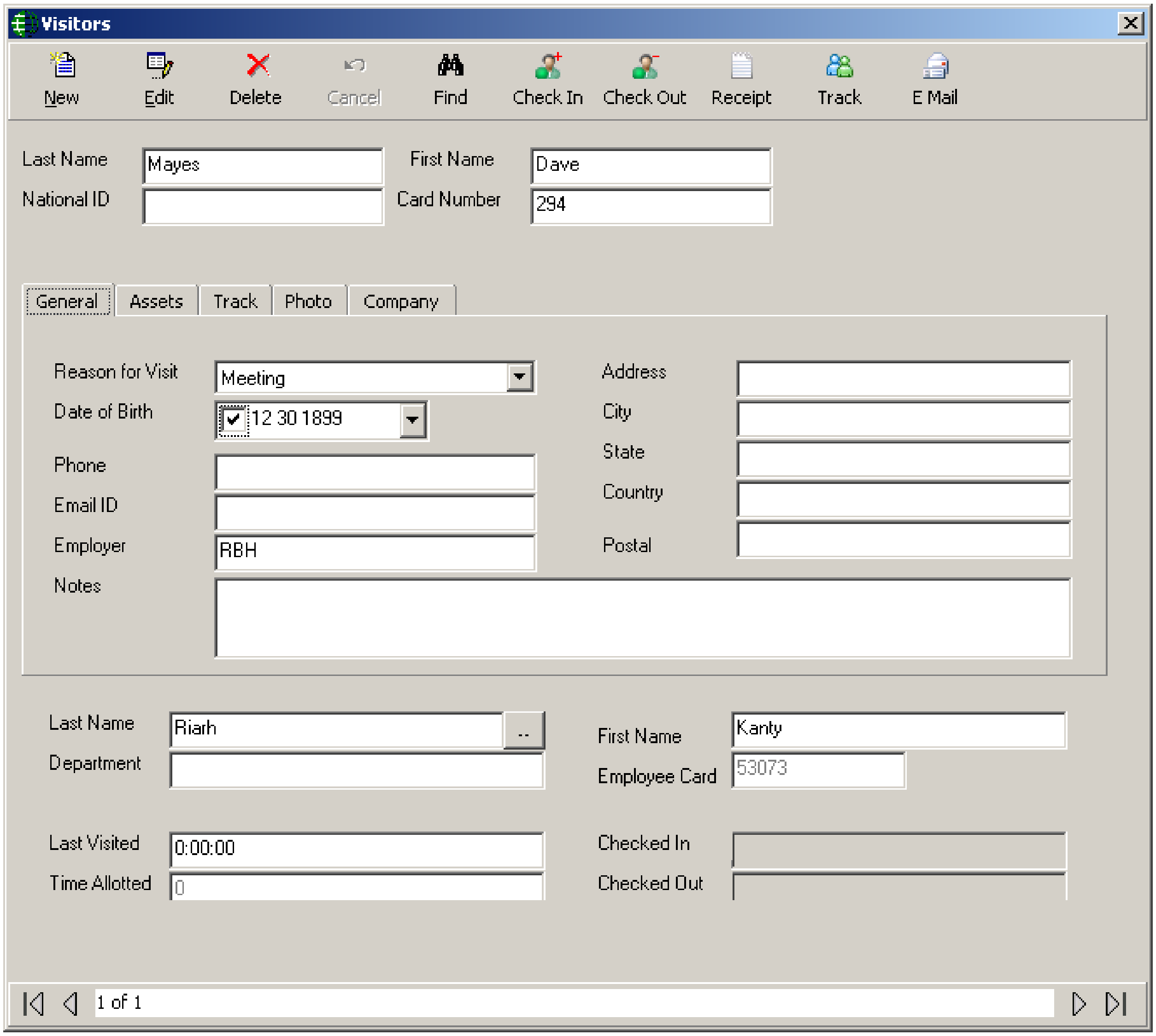
Email: info@rbh-access.com

Department 1: None

Department 2: None

2 of 211

General



Last Name: Mayes
First Name: Dave
National ID:
Card Number: 294

Reason for Visit: Meeting
Date of Birth: ☑ 12 30 1899
Phone:
Email ID:
Employer: RBH
Notes:
Address:
City:
State:
Country:
Postal:

Last Name: Riarh
First Name: Kanty
Department:
Employee Card: 53073
Last Visited: 0:00:00
Time Allotted: 0
Checked In:
Checked Out:

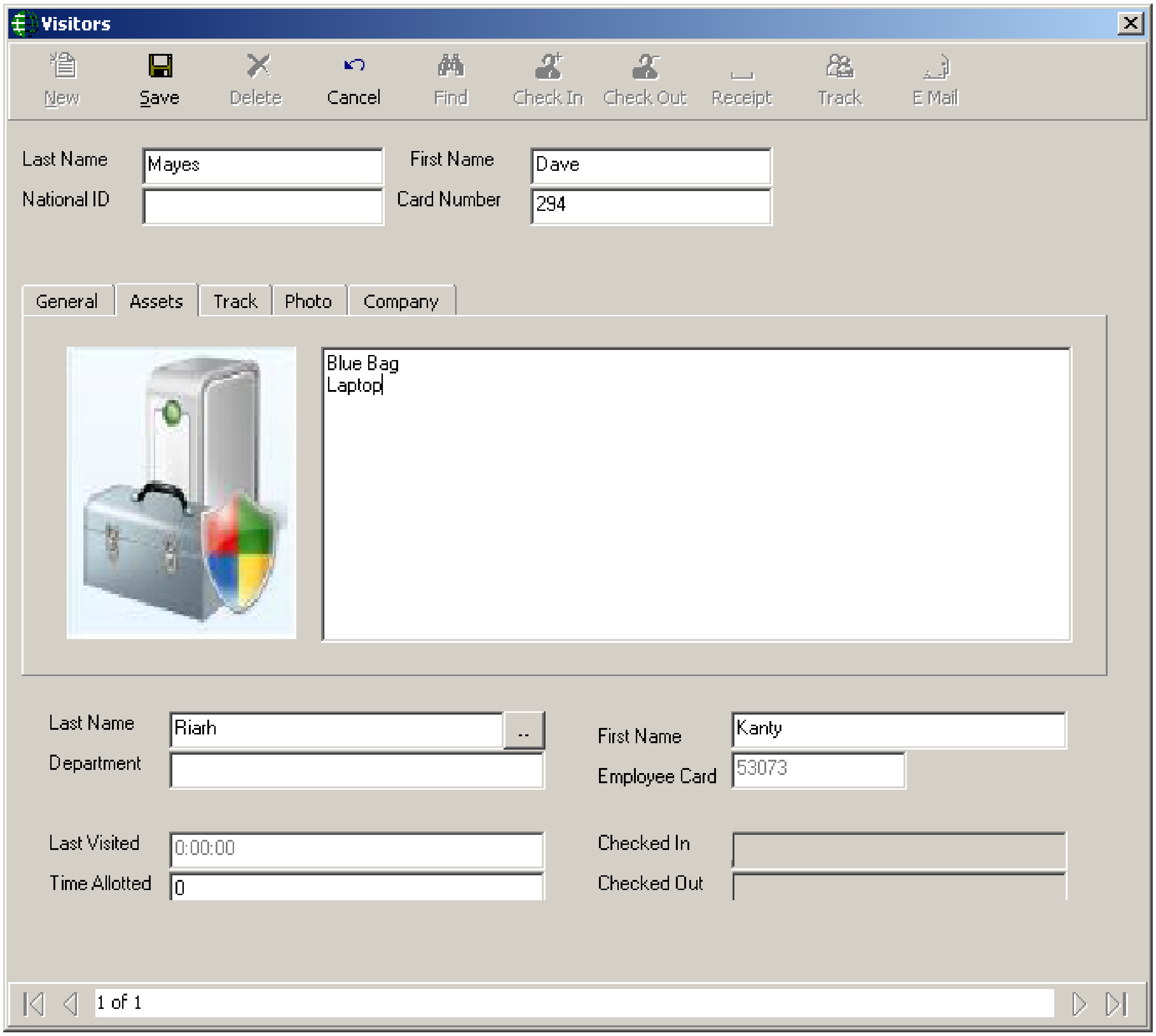
Personal Information data is optional and specific to the visitor and not to the card.

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

Last visited is also filled in by the system.

Select *Time Allotted* to create an automatic Late Alarm by system if visitor is late in checking out.

Assets



Last Name: Mayes
First Name: Dave
National ID:
Card Number: 294

Blue Bag
Laptop

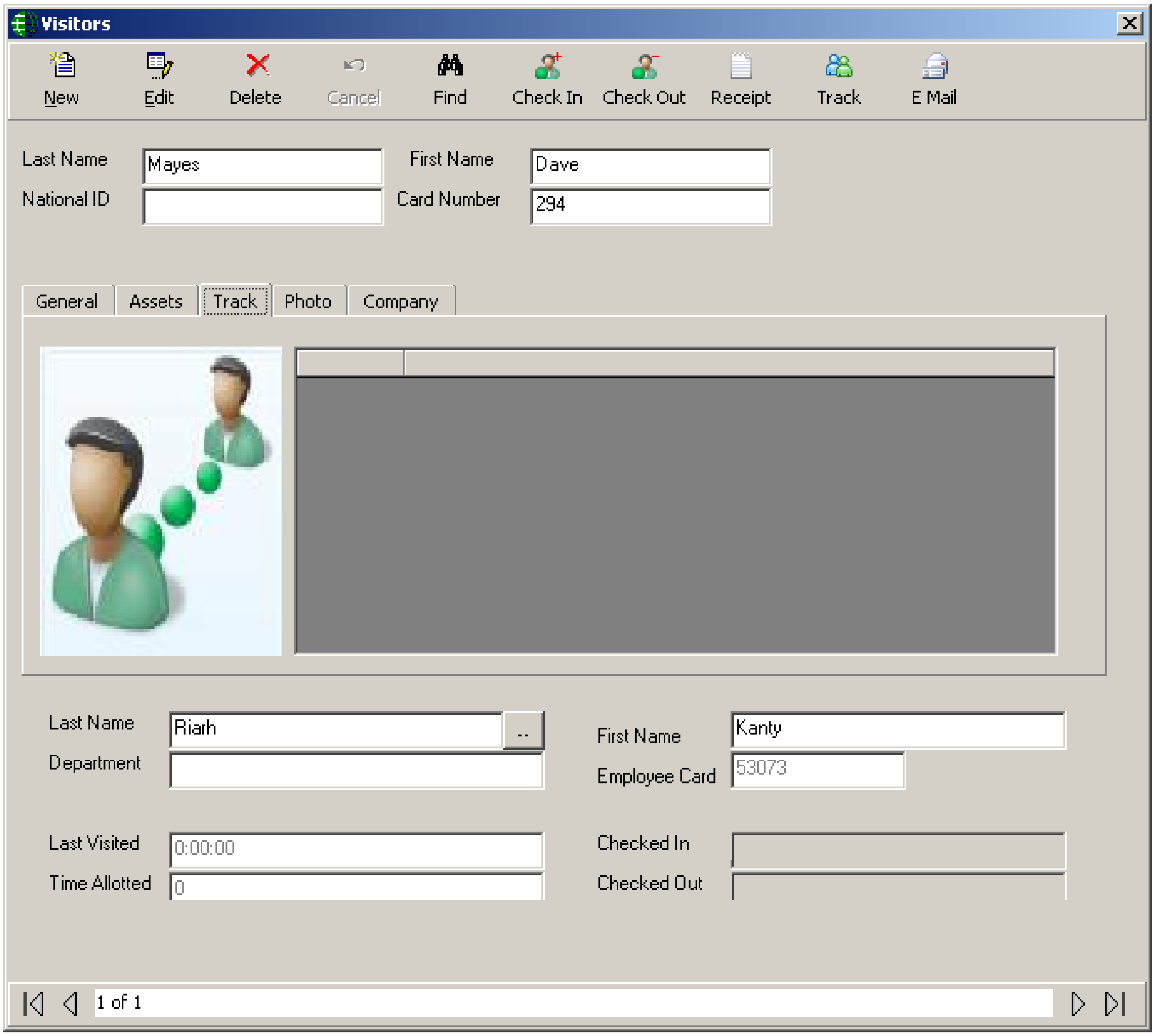
Last Name: Riarh
First Name: Kanty
Department:
Employee Card: 53073
Last Visited: 0:00:00
Checked In:
Time Allotted: 0
Checked Out:

Under the *Assets* tab, in edit mode, the operator can enter data concerning anything that the visitors 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



Last Name	Mayes	First Name	Dave
National ID		Card Number	294

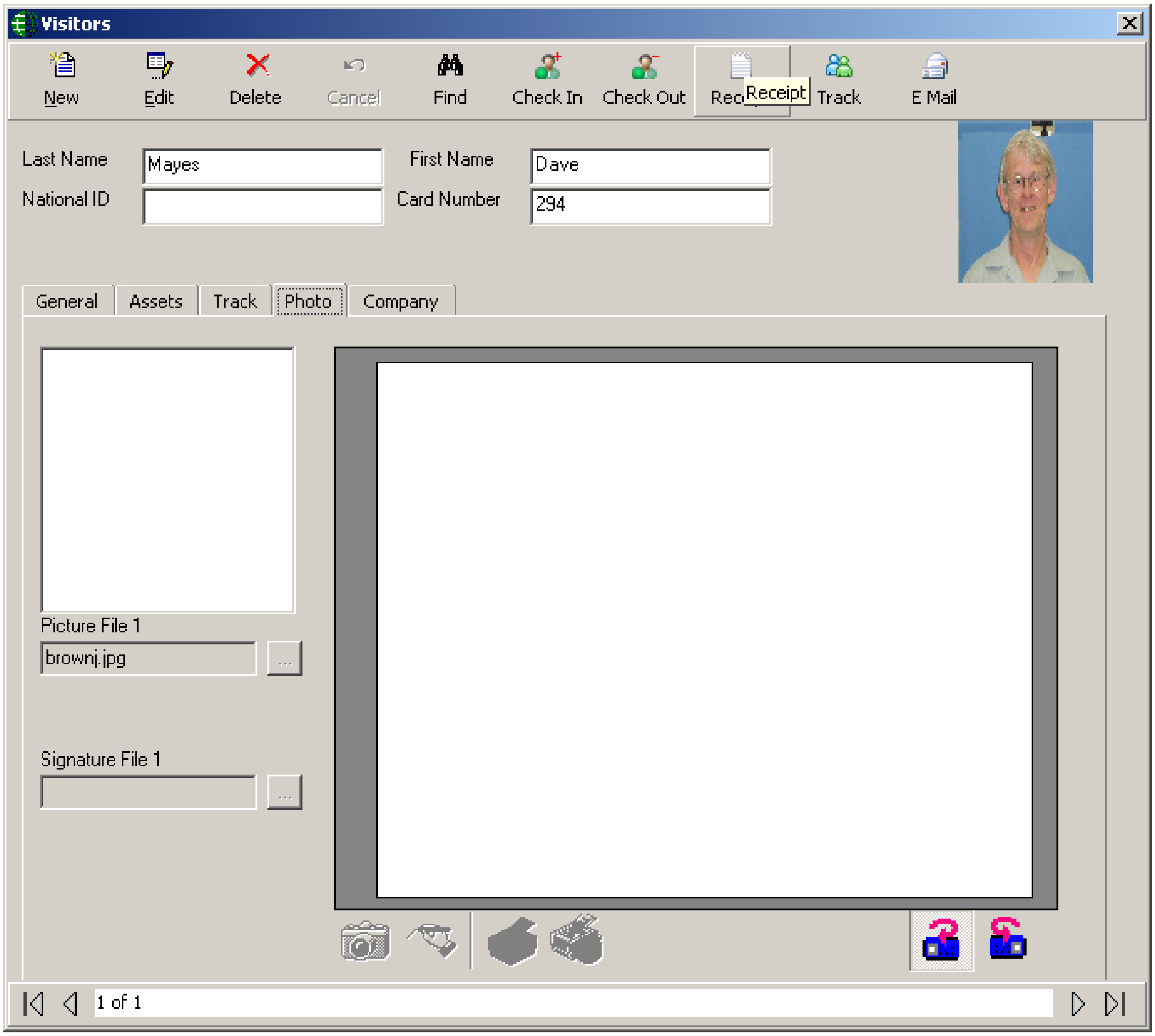
Last Name	Riarh	First Name	Kanty
Department		Employee Card	53073
Last Visited	0:00:00	Checked In	
Time Allotted	0	Checked Out	

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 to display 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 Visitors' History Report.**

Photo



Last Name: Mayes

First Name: Dave

National ID:

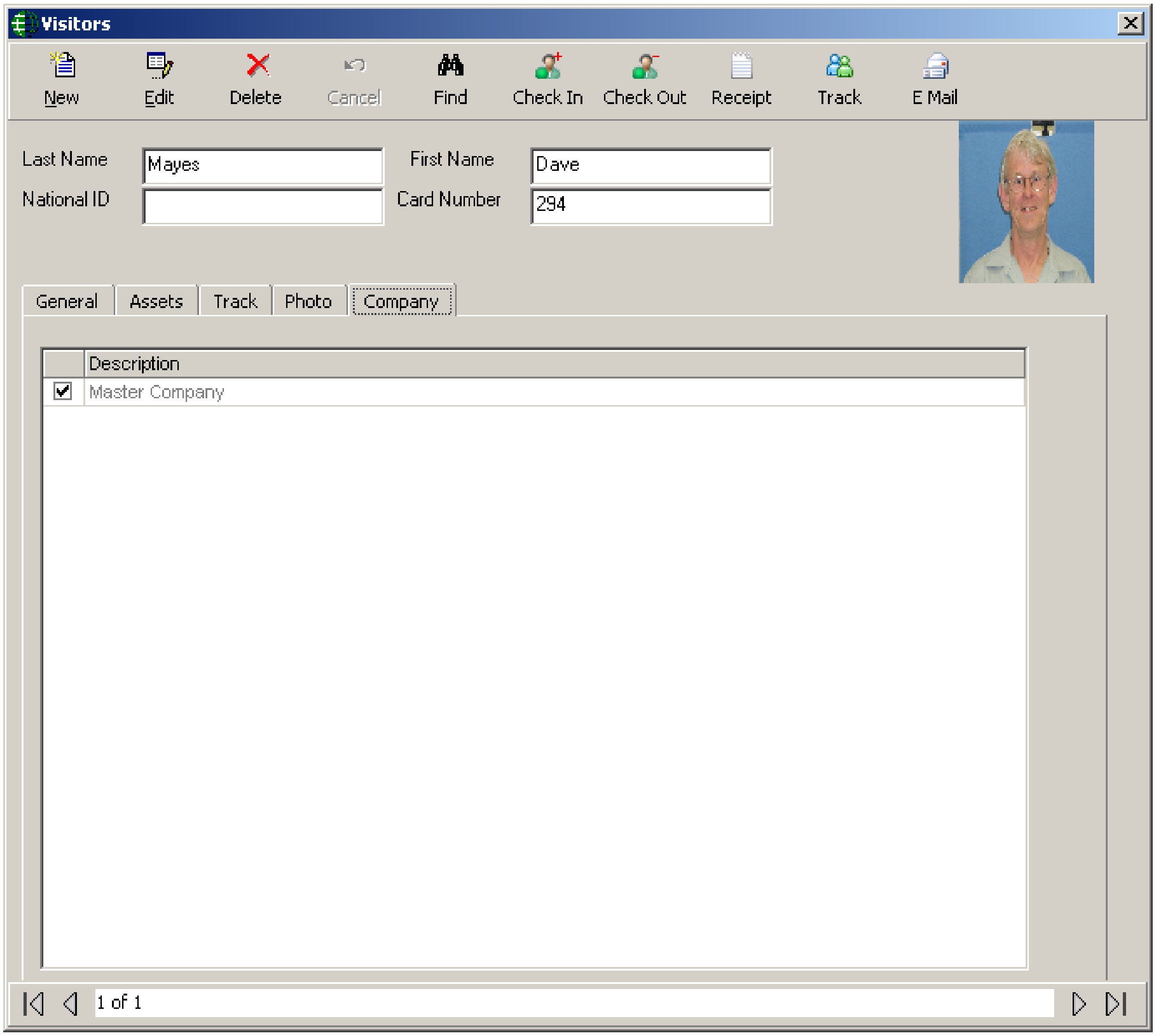
Card Number: 294

Picture File 1: brownj.jpg

Signature File 1:

The *Photo* tab shows all the templates from the visitors' badging template module. Only the fields valid for the visitor management will be selectable in visitors' badging templates module.

Company



Last Name: Mayes

First Name: Dave

National ID:

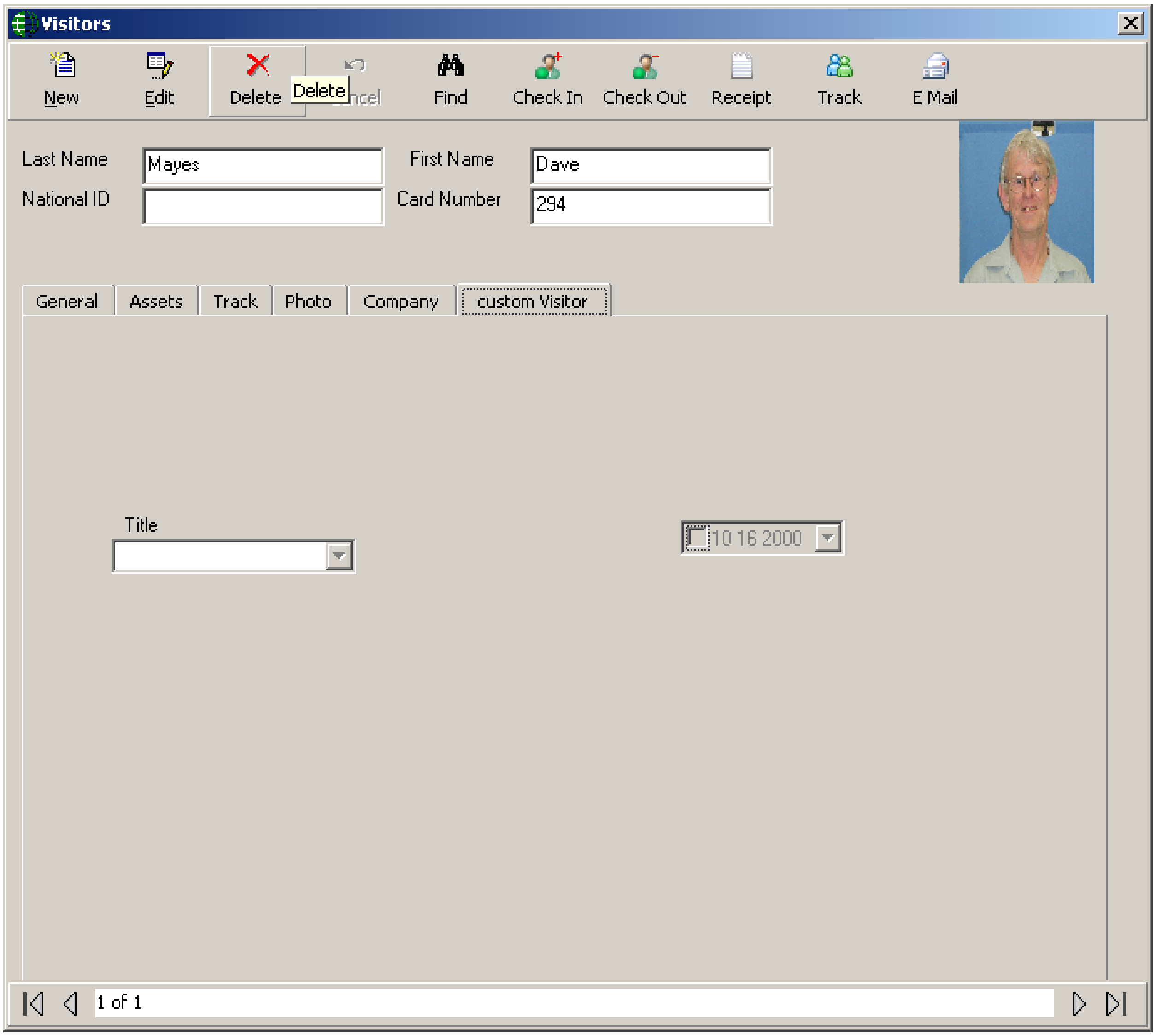
Card Number: 294

	Description
☑	Master Company

1 of 1

Company tab shows the companies assigned to the visiting visitor.

Custom Fields



Last Name: Mayes

First Name: Dave

National ID:

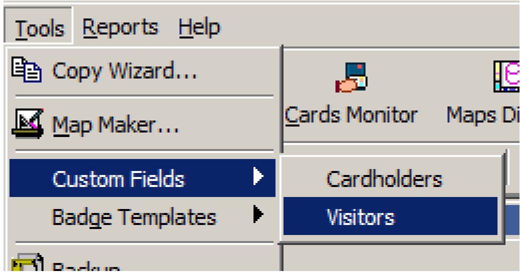
Card Number: 294

Title:

10 16 2000

1 of 1

Like cardholder, visitors' custom fields can be designed under Tools>custom fields>visitors and those fields are shown in the visitor screen as a new tab.

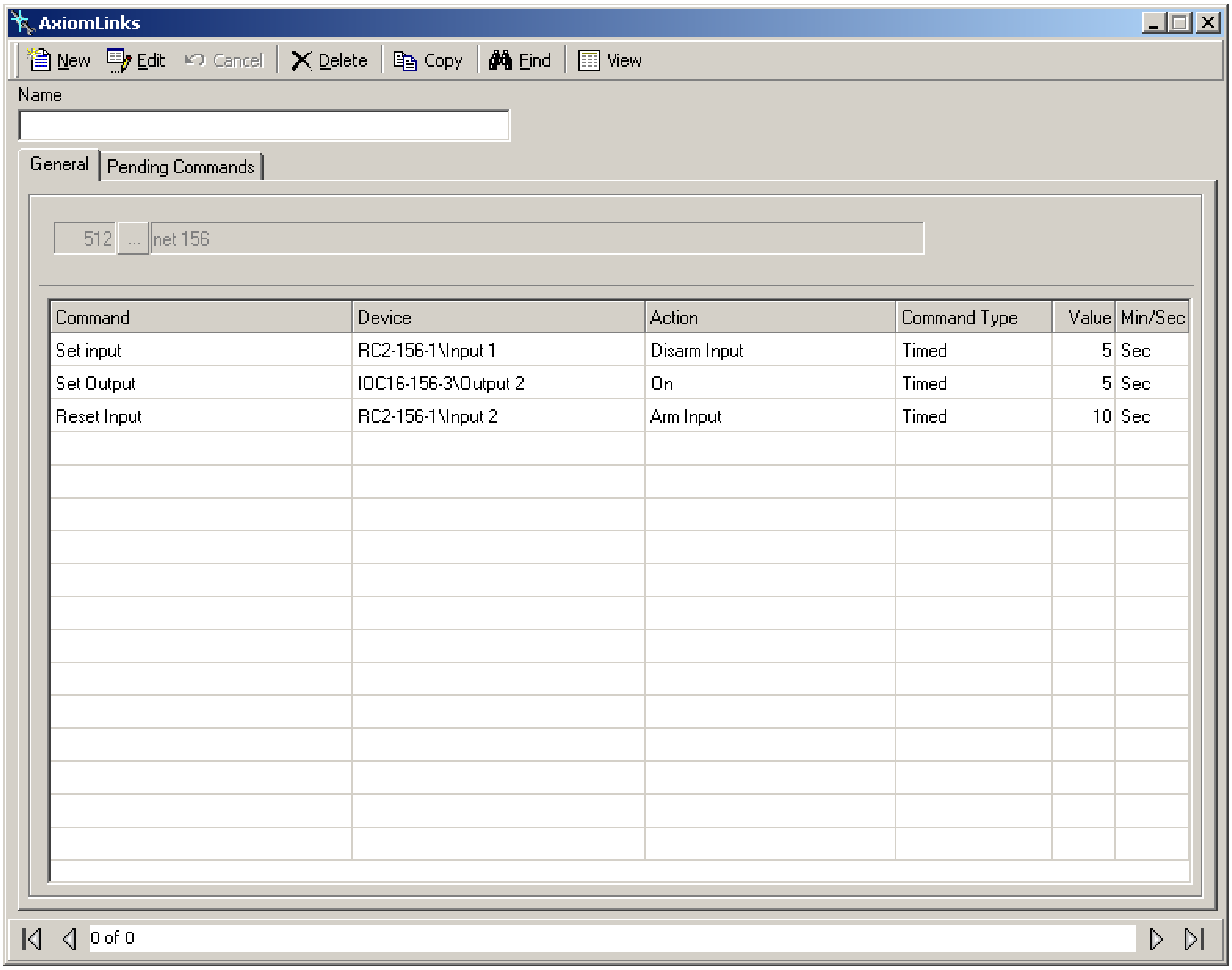


AxiomLinks™

AxiomV™ includes the *AxiomLinks*™ command script utility. *AxiomLinks*™ allows single pre-programmed events, single operator commands, complex sequences of pre-programmed events, or complex sequences of operator commands to be stored and executed later at the NC100 level without any action on the part of the operator.

Using *AxiomLinks*™ any system event or combination of events may be preprogrammed to invoke any other event or combination of events. *AxiomLinks*™ is schedulable, functions globally without the PC online and may be used to automate almost any activity in the system. Authorized system operators may execute these *AxiomLinks*™ manually from the PC as well. Links may be configured to execute once or for a specified duration ranging from 1 to 120 seconds or minutes.

Use this window to define links that may be used in *Operator Commands*, *Code Reader Linking*, Advanced Programming for Outputs, Advanced Programming for Inputs, and Advanced Programming for Access Points.



Name

512 ... net 156

Command	Device	Action	Command Type	Value	Min/Sec
Set input	RC2-156-1\Input 1	Disarm Input	Timed	5	Sec
Set Output	IOC16-156-3\Output 2	On	Timed	5	Sec
Reset Input	RC2-156-1\Input 2	Arm Input	Timed	10	Sec

Name

Up to 50 alphanumeric characters may be entered here.

General

Before creating any links select the network the link is to work on.

☞ ***AxiomLinks*™ are executed by the NC-100s and therefore only work within a network.**

Command

Click in the *command* box, and then use the drop down arrow to view the list of available commands.

- Set Access Point Feature
- Reset Access Point Feature
- Set Access Point Group Feature
- Reset Access Point Group Feature
- Grant Access
- Set Output Counter
- Set Input
- Reset Input
- Set Input Group
- Reset Input Group
- Set Output
- Reset Output
- Set Output Group
- Reset Output Group
- Initialize NC100

Device

Click in the *Device* box, and then use the drop down arrow to view the list of available devices (all or from a selected network).

Action

Click in the *Action* box, and then use the drop down arrow to view the list of available actions. The actions available will depend upon the command and device that were selected.

Command Type

Select the command type from:

- Semi-permanent: *Semi-Permanent Commands* are the most common command type. Any other command issued after a *Semi-Permanent Commands* is valid regardless of the type or source.
- Permanent: *Permanent Commands* are commands that can only be overridden by operator commands or by other permanent commands. These commands are usually used when it is important that the command is not countermanded by a schedule or a link

- Timed: *Timed Commands* are executed like *Semi-Permanent Commands* except for the timer. The timer starts at the same time the command is issued. When the timer expires the system checks the item's schedule to verify what the item's status should be, and sets the item to that status.

Value

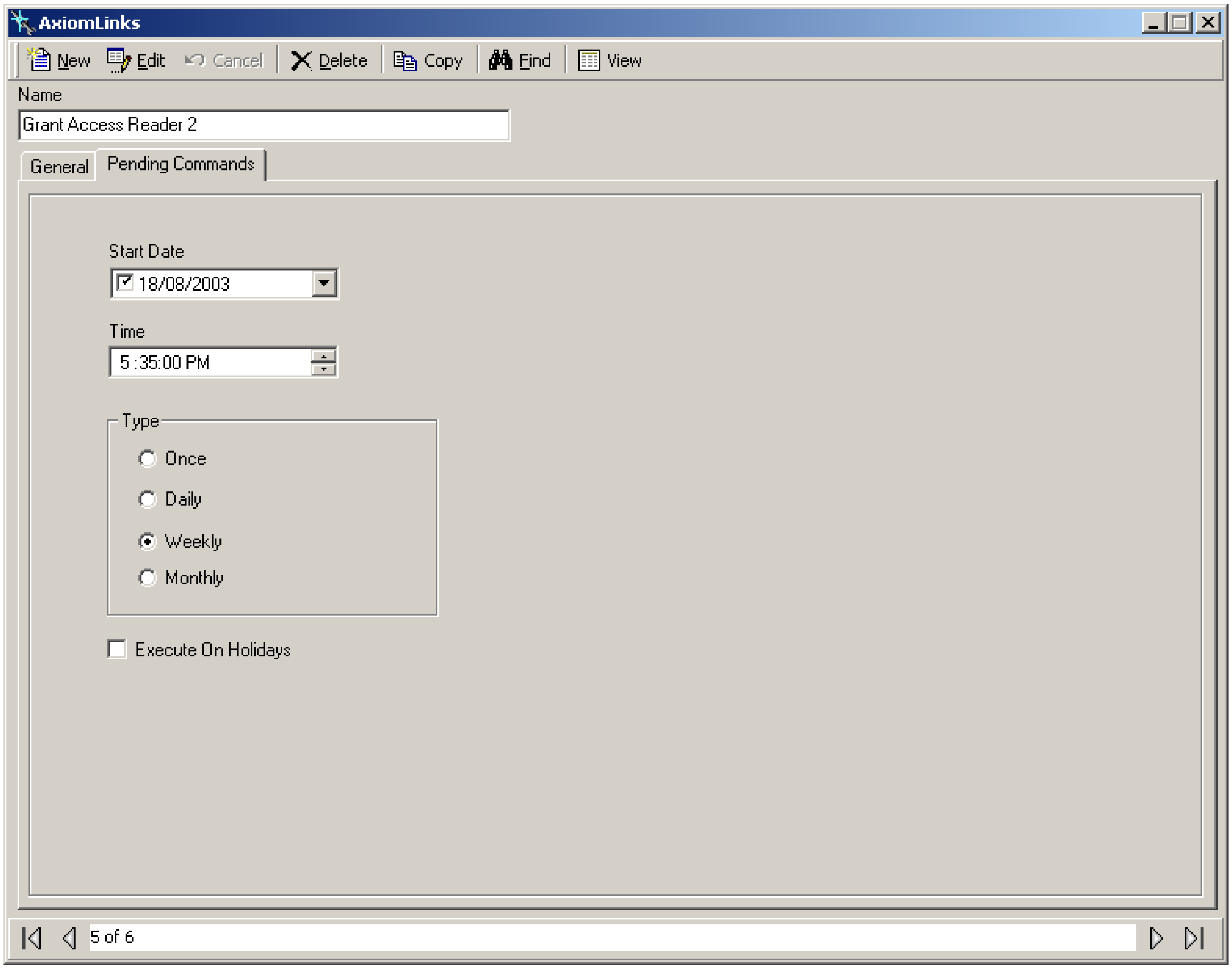
Value is number from 0 to 127 used with the seconds/minutes box to specify the time for the *Timed* command.

Min/Sec

This field indicates whether the *Value* for the *Timed* command is in minutes or seconds.

Pending Commands

Pending Commands are semi-permanent commands that may be programmed to execute an *AxiomLinks*™ Once, Daily, Weekly or monthly. Note that pending commands execute independent of any Schedule association. The *Pending Command* will execute the link that is programmed on the *General* tab.



Name: Grant Access Reader 2

Start Date: ☑ 18/08/2003

Time: 5 :35:00 PM

Type

○ Once

○ Daily

● Weekly

○ Monthly

☐ Execute On Holidays

5 of 6

Start Date

The *Start Date* is the first date that the link will be executed on. Click on the down arrow to bring up a calendar to select the date from or type in the date directly.

Time

Select the time of day the link is to be executed. Scroll up and down or type in the required time.

Type

⊙ Once: Occurs one time only at the set time and date.

⊙ Daily: Occurs each day at the set time, from start date forward.

⊙ Weekly: Occurs every seven days at the set time, beginning on the start date.

⊙ Monthly: Occurs each month on the set date and at the set time.

☑ Execute On Holiday

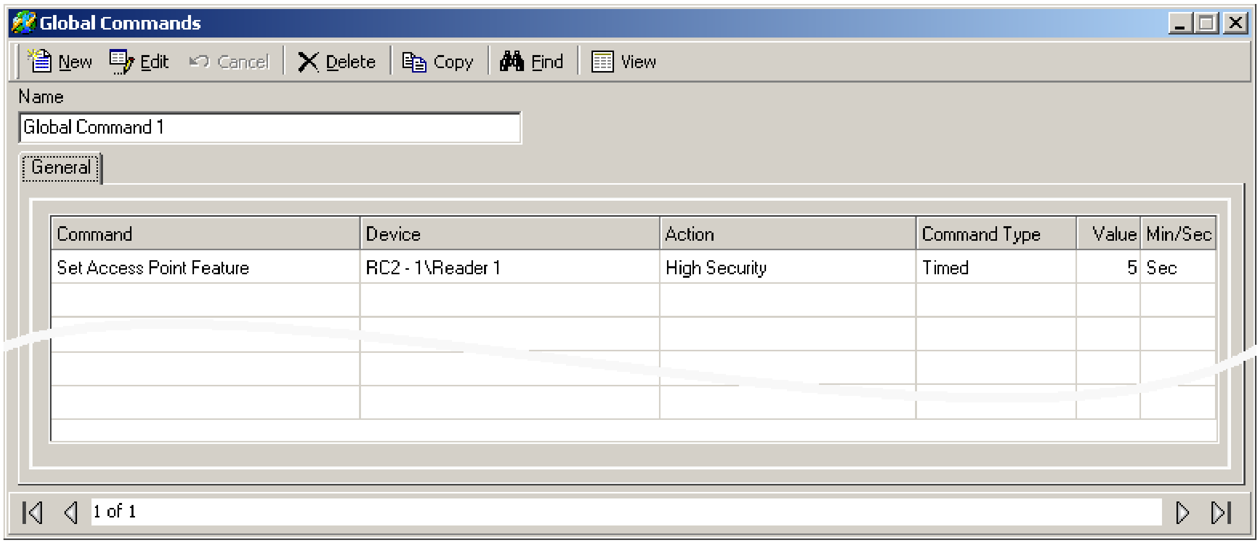
Check *Execute On Holiday* to have the system ignore the holiday day-of-the-week and verify the true day-of-the-week to see if the *Weekly Pending Command* should be executed.

AxiomLinks™ Command Summary

Input Commands	**State**	**Time**
Set Input Status Set Input Group Status	Disarm	Y
Reset Input Status Reset Input Group Status	Arm	Y
Output Commands	**State**	**Time**
Set Output Status Set Output Group Status	On	Y
Reset Output Status Reset Output Group Status	Off	Y
Preset Output Counter		N
Access Point Commands	**State**	**Time**
Grant access	-	Y
Set Access Point Feature Reset Access Point Feature	High Security Two Person Door Held Open Warning Interlock Unlock Reader Required Keypad Required Disable RTE Hard APB enabled Code Tracing Facility Code Mode Report Access Granted Report Access Granted RTE	Y
Cardholder Commands	**State**	**Time**
Activate Cardholder	-	N
Deactivate Cardholder	-	N
Reset Cardholder Area	-	N
Miscellaneous Commands	**State**	**Time**
Test battery Initialize NC100	- -	Y N
APG Feature Commands	**State**	**Time**
Set APG Feature Reset APG Feature	High Security Two Person Door Held Open Warning Interlock Unlock Reader Required Keypad Required Disable RTE Hard APB Enabled Code Tracing Facility Code Mode Report Access Granted Report Access Granted RTE	Y

Global Commands

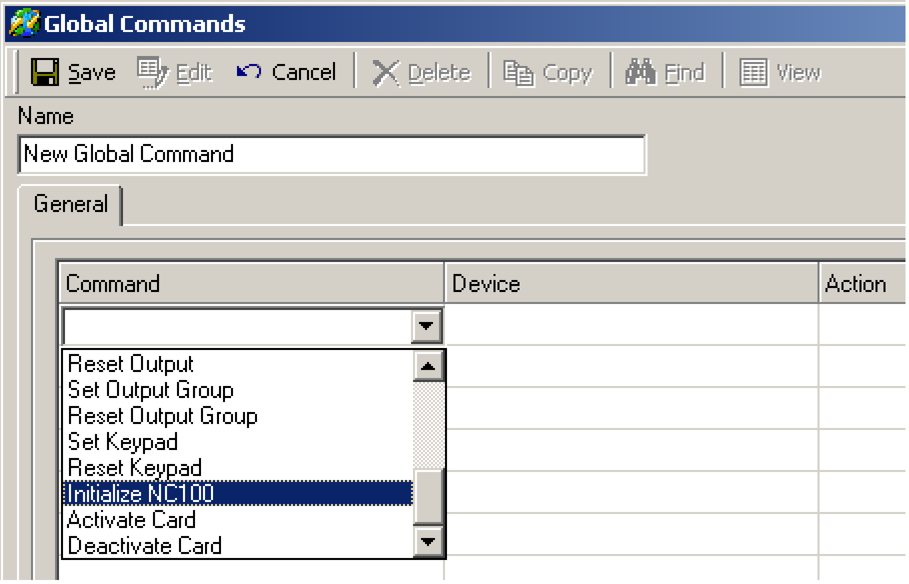
Global Commands are *AxiomLinks*™ executed by the *CommsServer*. The *CommsServer* has access to all of the system's networks. This means that an event on one network could cause a link to be executed on another network.



Name: Global Command 1

Command	Device	Action	Command Type	Value	Min/Sec
Set Access Point Feature	RC2 - 1\Reader 1	High Security	Timed	5	Sec

Global Commands are programmed the same as *AxiomLinks*™ except a network does not have to be specified. There are a few commands that are available in *Global Commands* that are not available in *AxiomLinks*™. See *AxiomLinks*™ General for more information. 'Activate Card', and 'Deactivate Card' are *Global Commands* that are not available in *AxiomLinks*™.



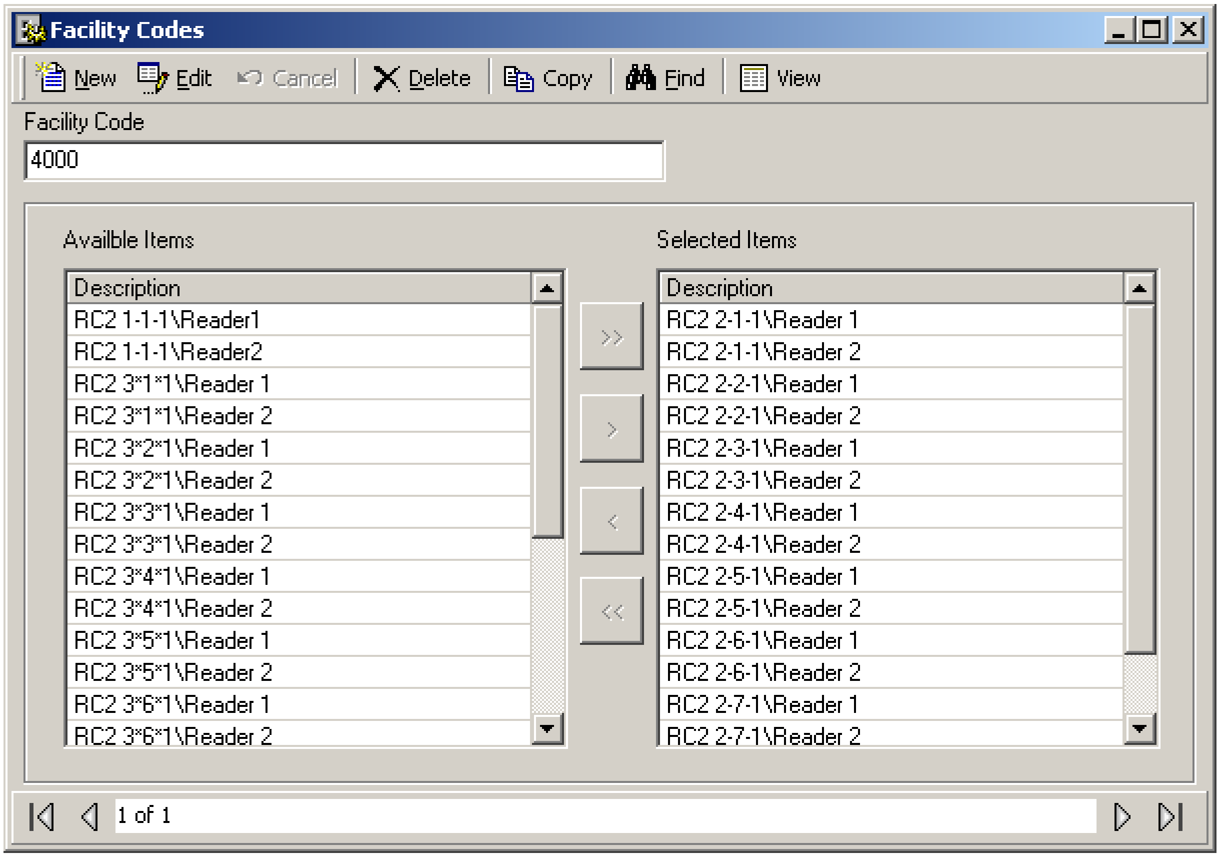
Name: New Global Command

Facility Codes

There are two sets of numbers encoded in every card. One assigns a unique access code ID number to the card and the other identifies that card as belonging to a specific facility, i.e. the *Facility Code*.

Facility Codes are used to group cards together so they only work for AxiomV™ system, which is configured with that particular facility code. There may be several cards manufactured with the same access code number. When coupled with the *Facility Code,* the cards get their unique identity. For example, two cards are both numbered 56,248. One card has a *Facility Code* of 2 and the other has a *Facility Code* of 37. A system that is set to accept only cards with a *Facility Code* of 2 will not grant access to the card with a *Facility Code* of 37. If you do not know the *Facility Code* of your cards, simply present the card to a reader and the system will display the *Facility Code*. Each reader can be assigned up to 16 *Facility Codes*.

A single site or system may be configured to accept multiple *Facility Codes*. A *Facility Code* may be assigned to work at all Access Points in the system or at specific readers only.



Facility Code: 4000

Availble Items

Description
RC2 1-1-1\Reader1
RC2 1-1-1\Reader2
RC2 3*1*1\Reader 1
RC2 3*1*1\Reader 2
RC2 3*2*1\Reader 1
RC2 3*2*1\Reader 2
RC2 3*3*1\Reader 1
RC2 3*3*1\Reader 2
RC2 3*4*1\Reader 1
RC2 3*4*1\Reader 2
RC2 3*5*1\Reader 1
RC2 3*5*1\Reader 2
RC2 3*6*1\Reader 1
RC2 3*6*1\Reader 2

Selected Items

Description
RC2 2-1-1\Reader 1
RC2 2-1-1\Reader 2
RC2 2-2-1\Reader 1
RC2 2-2-1\Reader 2
RC2 2-3-1\Reader 1
RC2 2-3-1\Reader 2
RC2 2-4-1\Reader 1
RC2 2-4-1\Reader 2
RC2 2-5-1\Reader 1
RC2 2-5-1\Reader 2
RC2 2-6-1\Reader 1
RC2 2-6-1\Reader 2
RC2 2-7-1\Reader 1
RC2 2-7-1\Reader 2

1 of 1

☞ **When using multiple *Facility Codes*, cards having the same access code, but different *Facility Code*s will be read as the same card. AxiomV™ uses only the access code to identify a cardholder, even though access may be granted based on the *Facility Code*.**

💣 **If no *Facility Code* is programmed, then <u>any</u> *Facility Code* will be accepted.**

Name

Up to 50 alphanumeric characters may be entered here.

Available Items

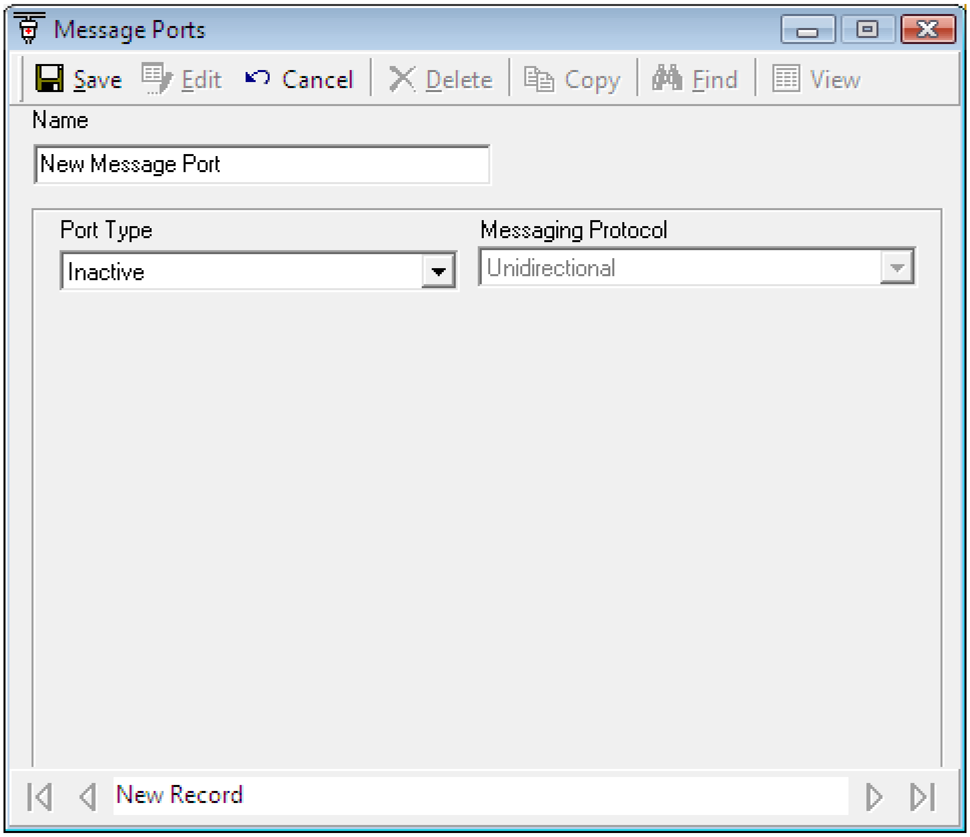
Available Items will show all of the access points in the system.

Selected Items

Selected Item lists the access points requiring that facility code.

Message Ports

Use *Message Ports* to configure the ASCII ports of your system.



Name: New Message Port

Port Type: Inactive

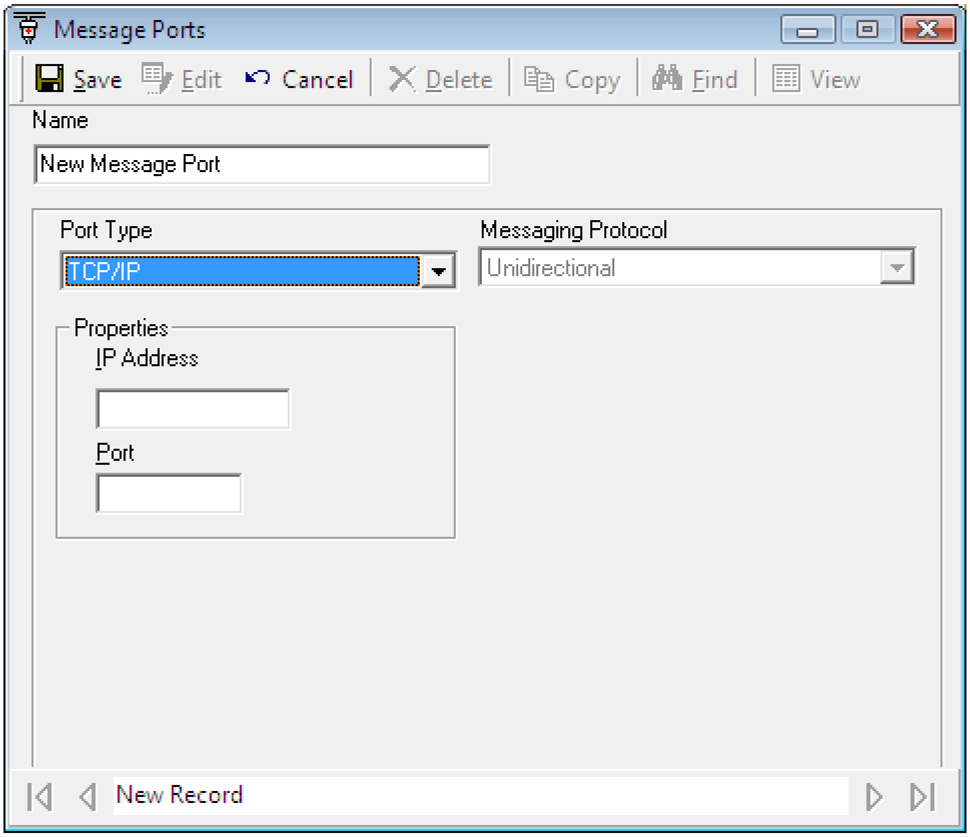
Messaging Protocol: Unidirectional

Name

Up to 50 alphanumeric characters may be entered here.

Port Type

Choose an Inactive port to disable the message, a TCP/IP port, a Direct Port, an eMail port, or a SafeSuite™ keypad port to enable.



Name

New Message Port

Port Type

TCP/IP

Messaging Protocol

Unidirectional

Properties

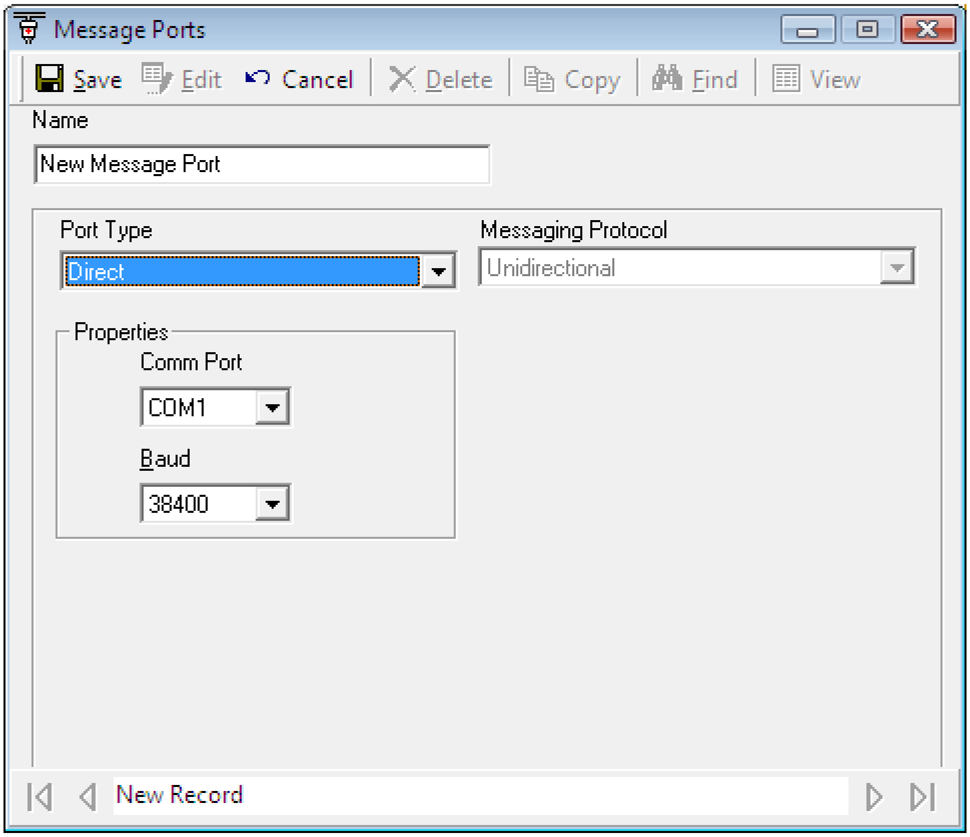
IP Address

Port

New Record

Properties

Set the port properties depending on the port type. For TCP ports set the IP address and port number. For direct ports select the comm. port and set the baud rate. eMail ports require the SMTP server, the address the message is to be sent to, the Local address and a password if required.



Name: New Message Port

Port Type: Direct

Messaging Protocol: Unidirectional

Properties

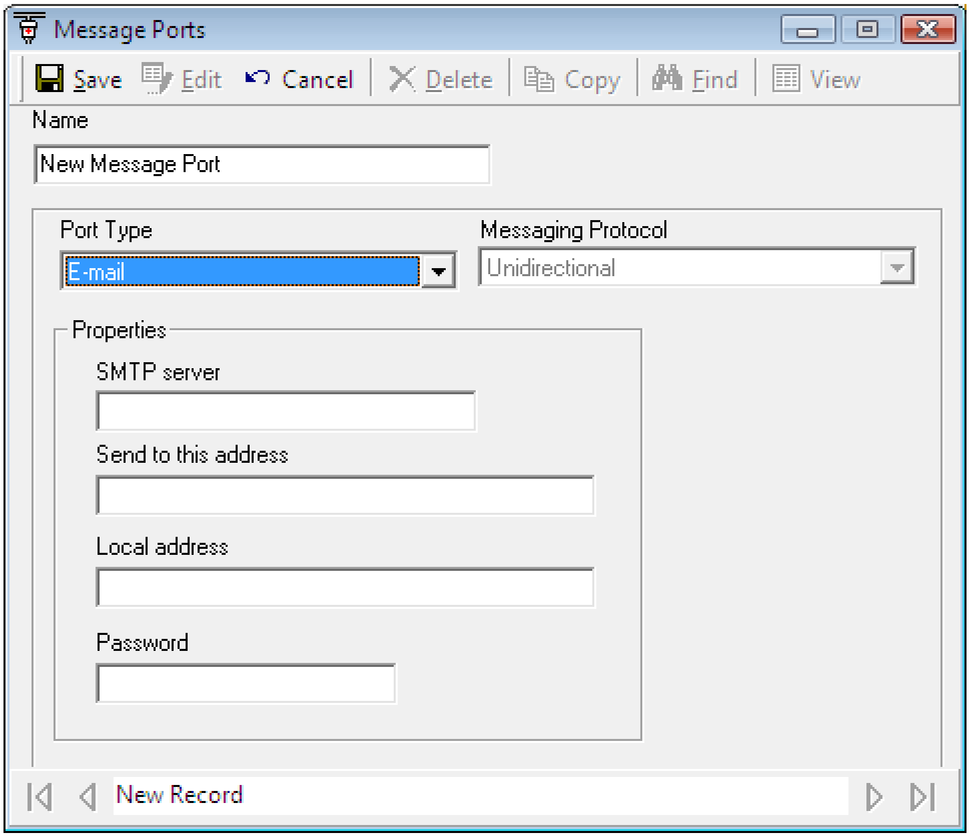
Comm Port: COM1

Baud: 38400

New Record

Messaging Protocol

Unidirectional is the only possibility at this time.



Name: New Message Port

Port Type: E-mail

Messaging Protocol: Unidirectional

Properties

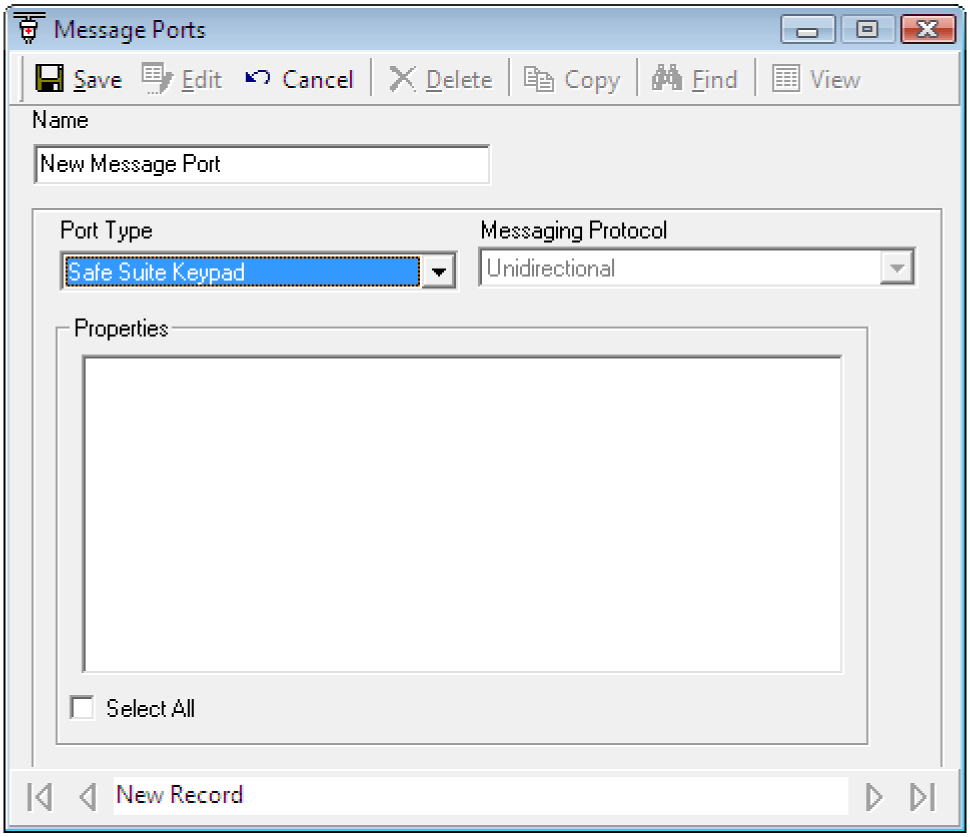
SMTP server

Send to this address

Local address

Password

New Record



Name: New Message Port

Port Type: Safe Suite Keypad

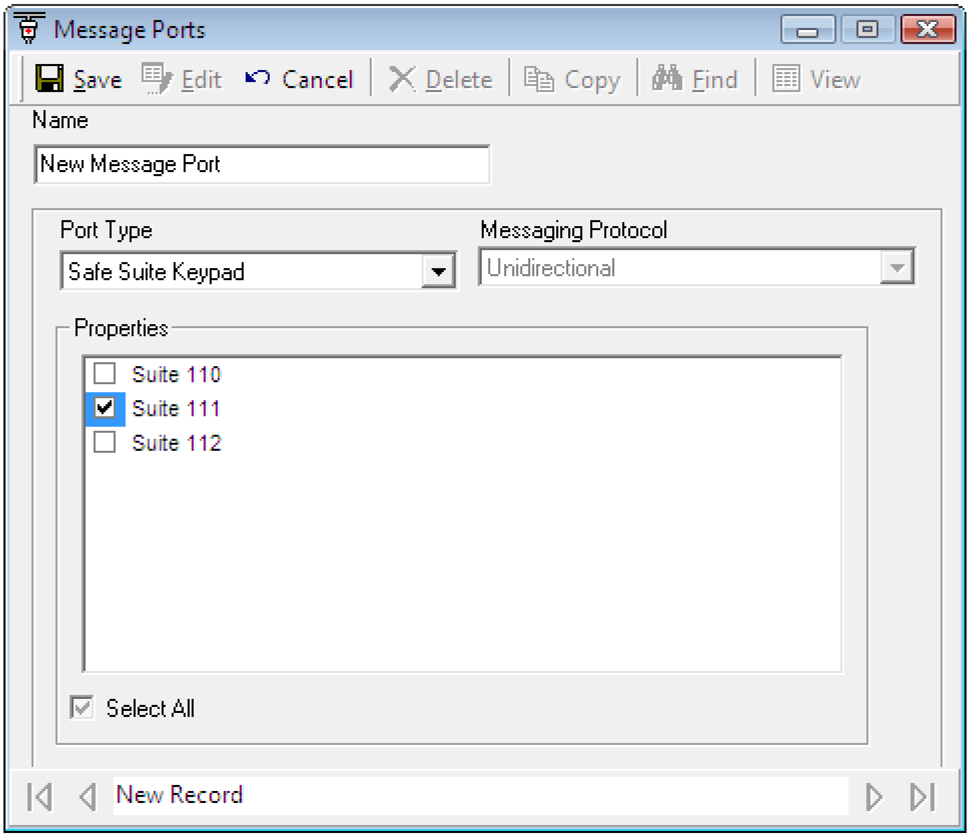
Messaging Protocol: Unidirectional

Properties

□ Select All

New Record

Select which SafeSuite™ LCD keypads are to receive the message by checking the appropriate box. The pre-created messages can be no more than two lines of sixteen characters each.



Name
New Message Port

Port Type
Safe Suite Keypad

Messaging Protocol
Unidirectional

Properties
□ Suite 110
☑ Suite 111
□ Suite 112

☑ Select All

New Record

DVR

The database selection *DVR* will call up the same connection/configuration window as the *View DVR* menu selection. (See *View DVR* on page 47 for more information.)

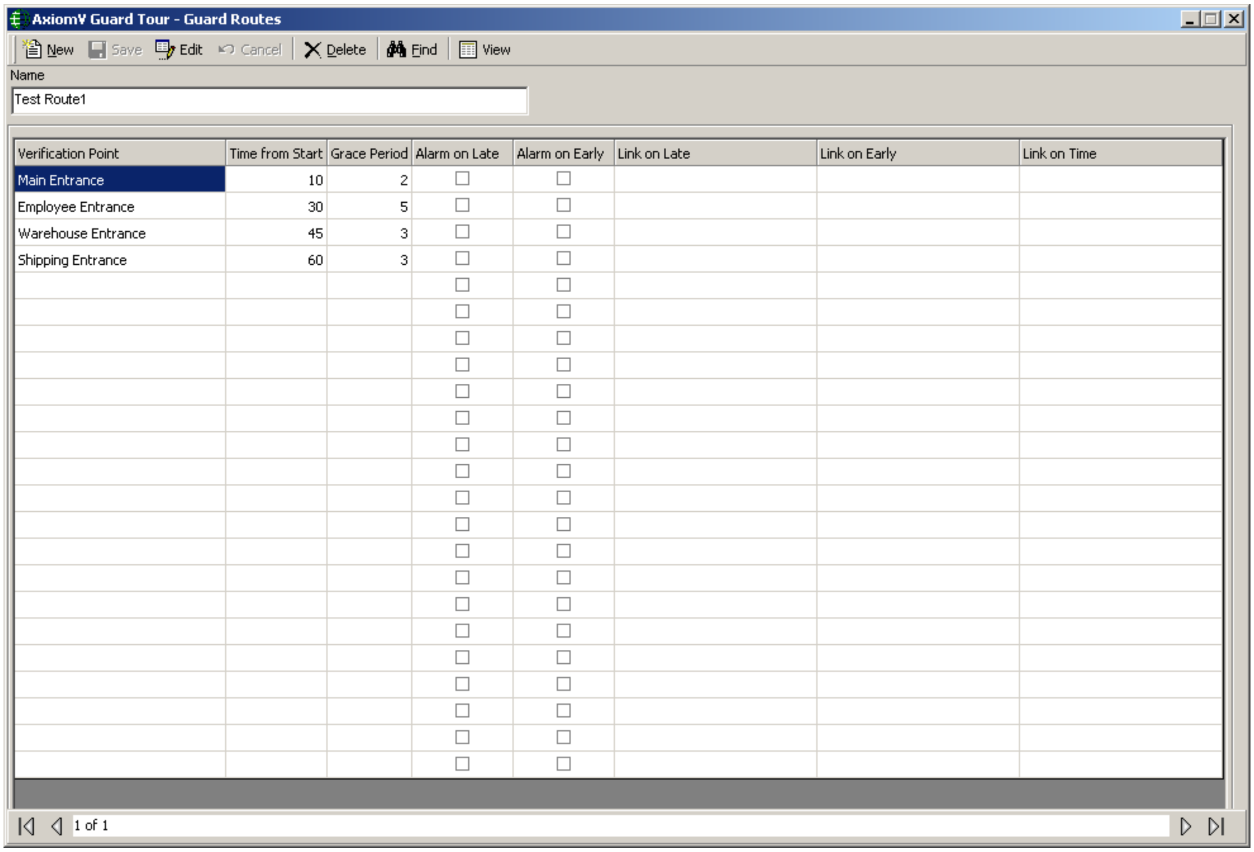
Guard Tour[15]

A Guard Tour is a set of Access Points and/or input points that a cardholder or group of cardholders read their cards at (and is granted access), and/or trigger inputs in a preset sequence, within a specified time frame.

Cardholders (guards) will move through a site verifying the safety and security of the site. They are expected to access certain doors at certain times during their inspection (tour). Alarms or links can be generated if they are late (or early) at any door. Tour can be started automatically from a schedule or manually.

The tour 'ends' when the guard accesses the last door/input. If the tour is shut down manually it is 'suspended'.

Tour Route



Name: Test Route1

Verification Point	Time from Start	Grace Period	Alarm on Late	Alarm on Early	Link on Late	Link on Early	Link on Time
Main Entrance	10	2	□	□			
Employee Entrance	30	5	□	□			
Warehouse Entrance	45	3	□	□			
Shipping Entrance	60	3	□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			
			□	□			

1 of 1

Verification Point

Click on the box and select an access point and/or an input point from the pull-down list. Specify points in the order they are to be reached during the Tour.

[15] This selection is only available if the optional license for the Guard Tour Software has been purchased and installed.

Time from Start

Enter the amount of time (from the start time) that it should take to get to the access point/input point. If it takes ten minutes to get to the first access point/input point and twenty minutes to get from the first to the second access point/input point, then enter thirty for the second access point/input point.

Grace Period

The Grace Period is a before and after amount of leniency time applied to the *Time from Start* time. For example a five minute grace time on the second access point/input point means that the cardholder needs to grant access/trigger input between twenty-five and thirty-five minutes after the start time.

Alarm on Late

☑ Is arriving late at an access point/input point an Alarm Event? (Yes/No)

Alarm on Early

☑ Is arriving early at an access point/input point an Alarm Event? (Yes/No)

Link on Late

Select a link (if any) to be executed on a late arrival at the access point/input point.

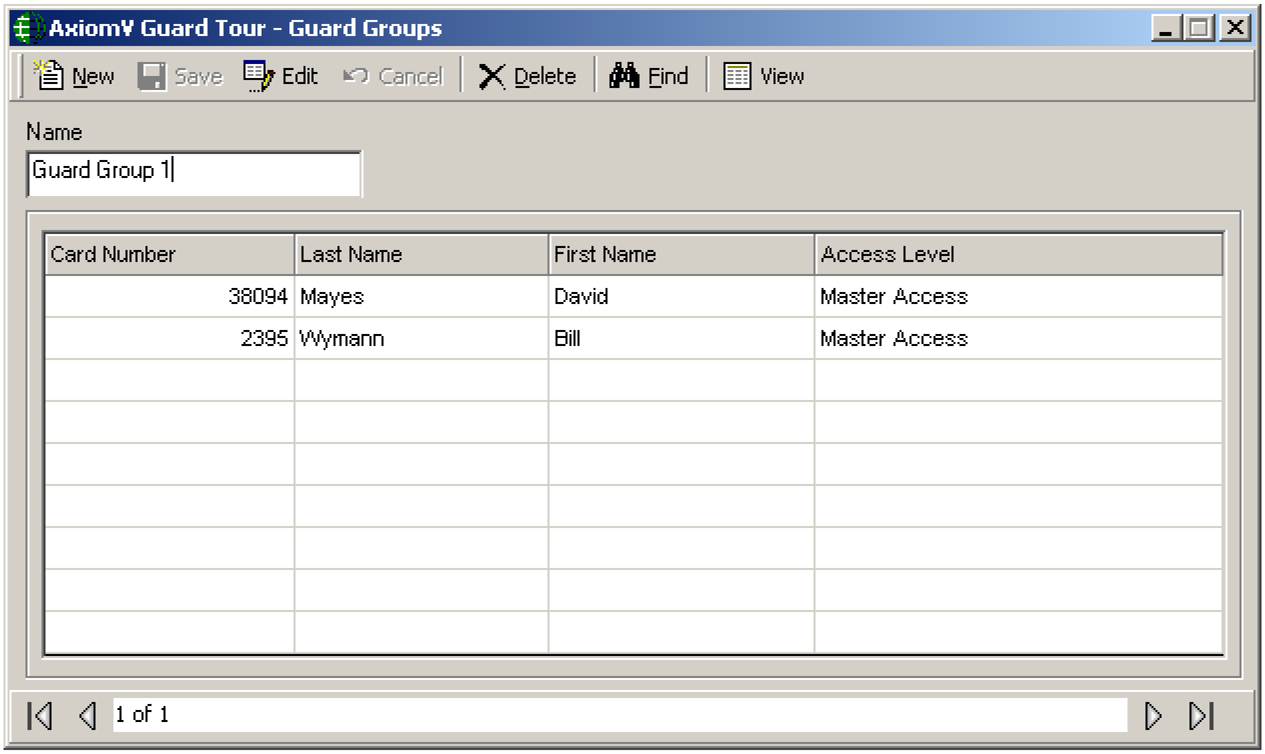
Link on Early

Select a link (if any) to be executed on an early arrival at the access point/input point.

Link on Time

Select a link (if any) to be executed on an On Time arrival at the access point/input point.

Guard Groups



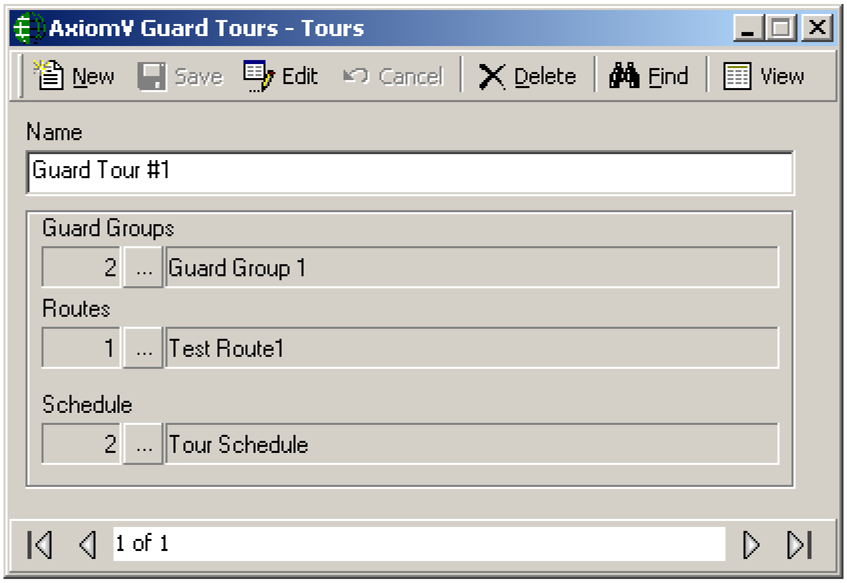
Name: Guard Group 1

Card Number	Last Name	First Name	Access Level
38094	Mayes	David	Master Access
2395	Wymann	Bill	Master Access

Create a Guard Group and give it a name. Add guards to the group by entering their card numbers. Their first name, last name, and access level will be added from the database.

While a tour is running any guard in the guard group can grant access at the scheduled access point. Therefore multiple guards can take the tour together or different guards can take the tour at different times (depending on the schedule).

Guard Tour



Name: Guard Tour #1

Guard Groups: 2 ... Guard Group 1

Routes: 1 ... Test Route1

Schedule: 2 ... Tour Schedule

1 of 1

Name

To create a Guard Tour give it a name and select a Guard Group, a Route, and a schedule (optional).

✎ **To have the tour run automatically enter a schedule, the tour will start whenever the schedule turns on. The schedule turning off is not used by the guard tour.**

💣 **Ensure that the start time on a tour's schedule (if more than one line in schedule selected) are further apart then the length of the tour. A tour will not restart if it is currently running!**

Chapter 8
Reports

☞ **Note: Even just to view the Reports, the printer driver needs be installed in Windows.**

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

There are two main programs. *Database Report* creates reports for the Network, Device configuration and other databases. *History Report* creates standard event History Reports.

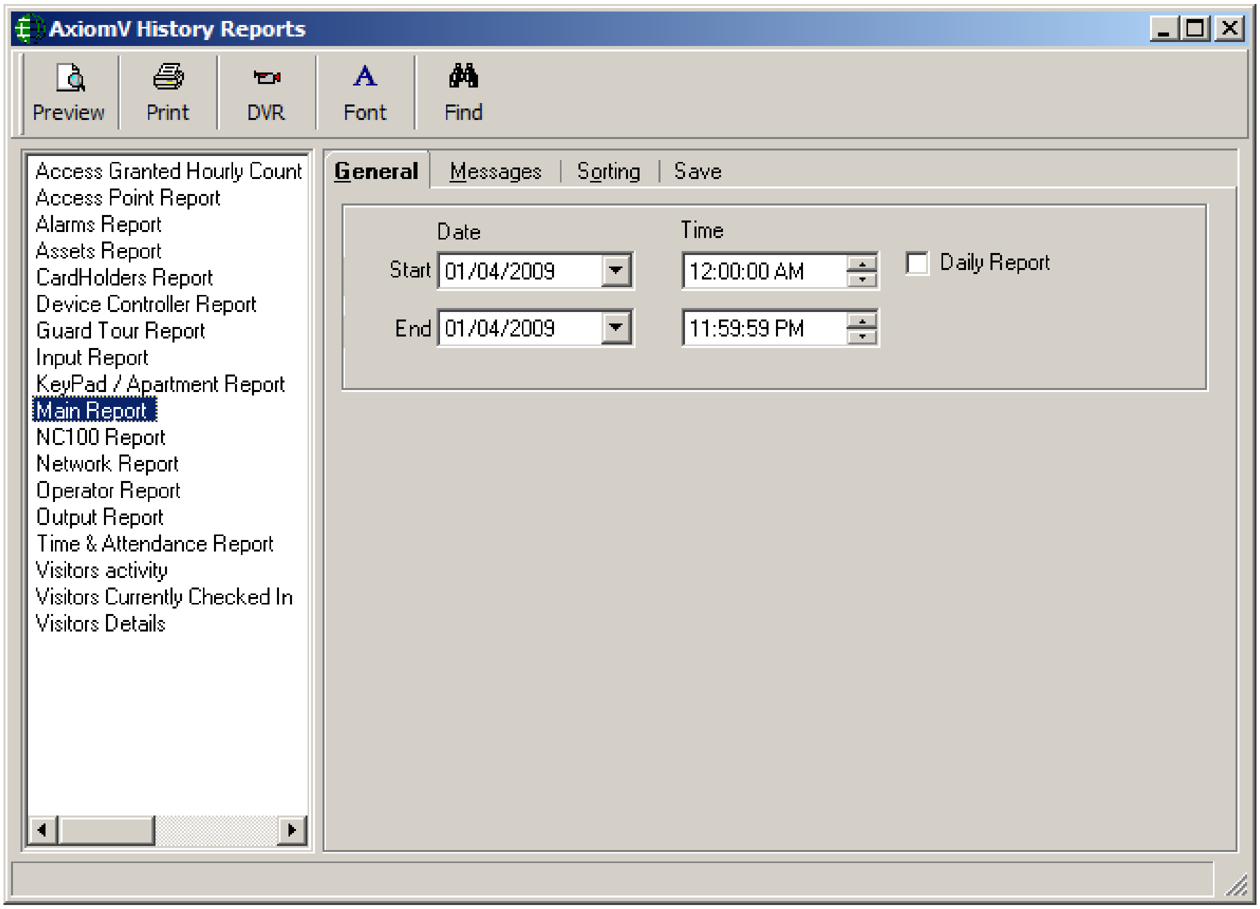
Event History Reports

Starting the History Report:

History Report can be started from the Reports menu item or from a button on the toolbar. By default, the system has the "Access Granted Hourly Count Report" report selected. The current date, from 00:00:01 a.m. through to 23:59:59 p.m. is also set by default. A number of event history report categories are available, and appear in alphabetic order in the selection list of the History Report screen.

Choose from the list to generate your report for the specific information you require. Select specific category items such as department or cardholder number to further limit your report. Use the *Date* and *Time* selector and the *Sorting* tab, to further define your report. Up to five fields can be sorted from the *Sorting* tab. Select from the list the field to be sorted, then select either alphabetical or reverse alphabetical. Finally, the report can be limited to particular messages through the *Messages* tab. From the *Messages* tab the report can be narrowed down to show only the required messages. Irrelevant messages won't be included making the report easier to read.

General



Access Granted Hourly Count
Access Point Report
Alarms Report
Assets Report
CardHolders Report
Device Controller Report
Guard Tour Report
Input Report
KeyPad / Apartment Report
Main Report
NC100 Report
Network Report
Operator Report
Output Report
Time & Attendance Report
Visitors activity
Visitors Currently Checked In
Visitors Details

	Date	Time
Start	01/04/2009	12:00:00 AM
End	01/04/2009	11:59:59 PM

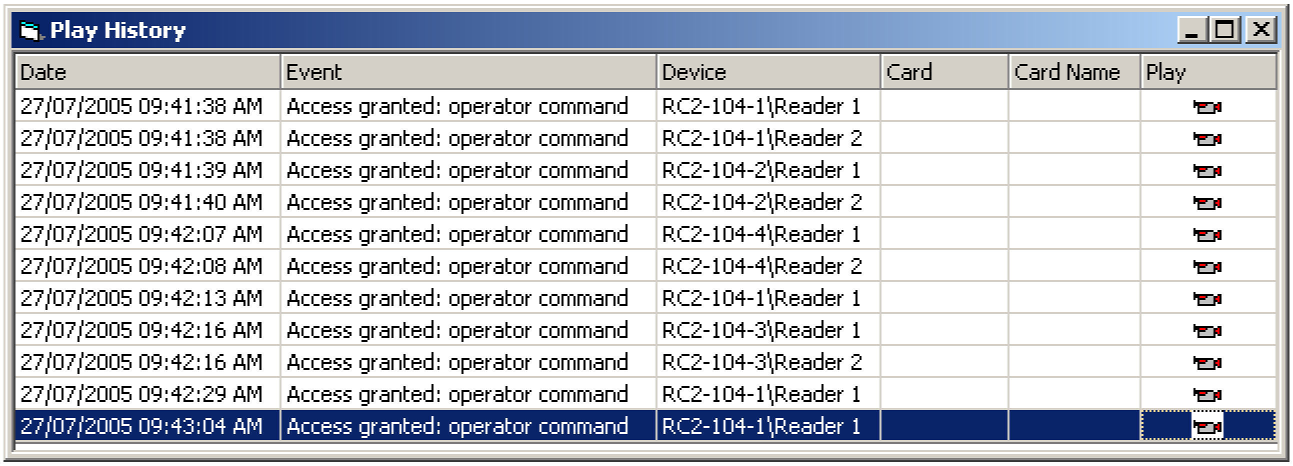
☐ Daily Report

Preview

Preview will display the report on the screen. The report can then be viewed before being printed or exported. Printing and exporting can be done from this screen.

Print

Print will send the report straight to the printer without being viewed.



Play History

Date	Event	Device	Card	Card Name	Play
27/07/2005 09:41:38 AM	Access granted: operator command	RC2-104-1\Reader 1			📹
27/07/2005 09:41:38 AM	Access granted: operator command	RC2-104-1\Reader 2			📹
27/07/2005 09:41:39 AM	Access granted: operator command	RC2-104-2\Reader 1			📹
27/07/2005 09:41:40 AM	Access granted: operator command	RC2-104-2\Reader 2			📹
27/07/2005 09:42:07 AM	Access granted: operator command	RC2-104-4\Reader 1			📹
27/07/2005 09:42:08 AM	Access granted: operator command	RC2-104-4\Reader 2			📹
27/07/2005 09:42:13 AM	Access granted: operator command	RC2-104-1\Reader 1			📹
27/07/2005 09:42:16 AM	Access granted: operator command	RC2-104-3\Reader 1			📹
27/07/2005 09:42:16 AM	Access granted: operator command	RC2-104-3\Reader 2			📹
27/07/2005 09:42:29 AM	Access granted: operator command	RC2-104-1\Reader 1			📹
27/07/2005 09:43:04 AM	Access granted: operator command	RC2-104-1\Reader 1			📹

DVR

Systems with DVRs will have items (inputs, outputs, access points) configured with associated cameras (and the IP address of the DVR that camera is being recorded by). Clicking the DVR icon in the right-hand column will send the date/time of the event in that row, and the associated camera number, to designated DVR via its IP address and playback the recorded events for that duration (configured in monitoring of device).

Font

Font is used to change the font used on the report. Simply select from the list provided. A sample of the font is shown in the area to the right. (See Fonts for more information.)

Date and Time Selector

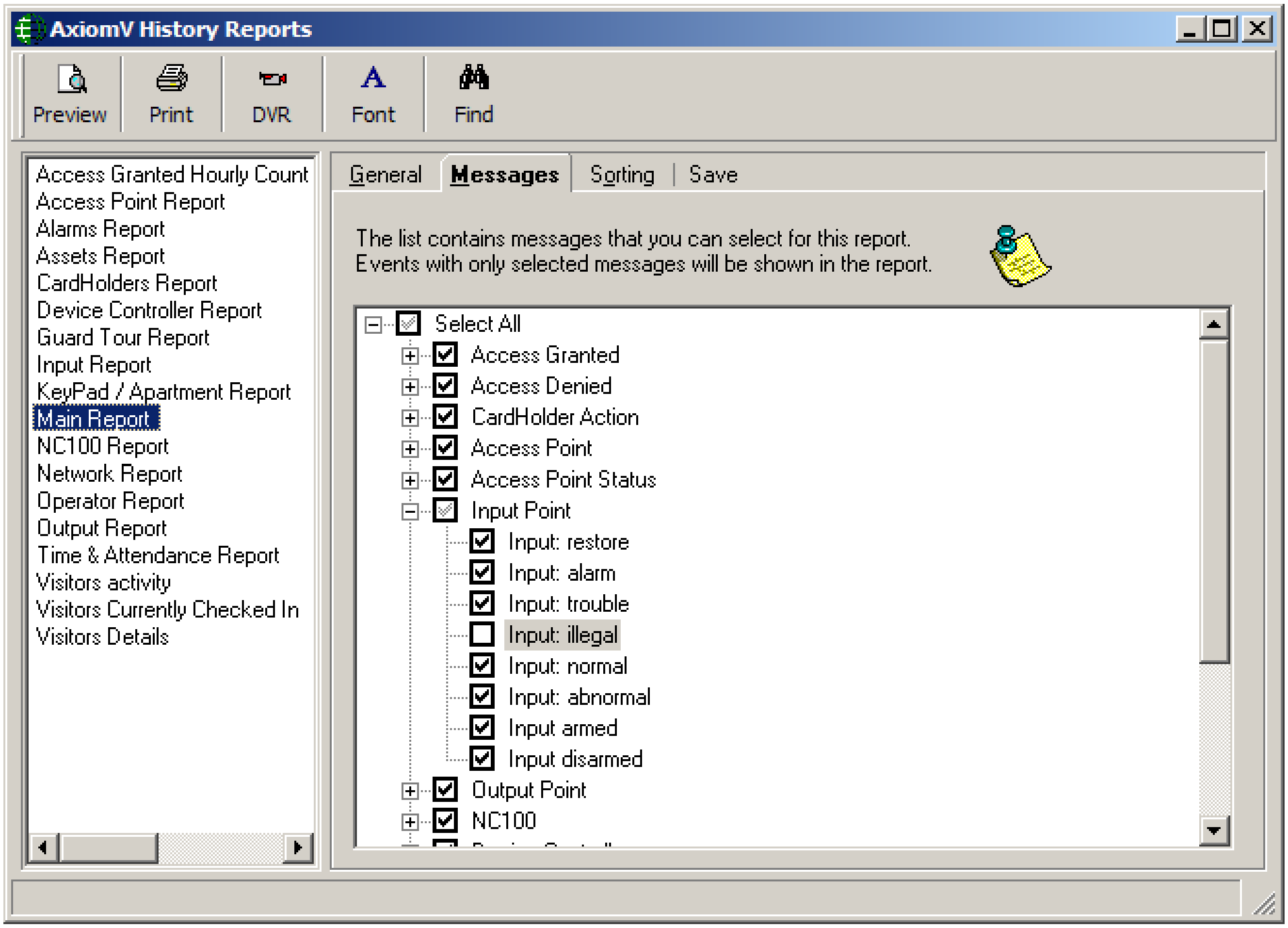
Select the *Start Date and Time* and the *End Date and Time* for the period you wish to report on, by either browsing for the required date, using the *spin* buttons to set the desired time or by keying directly into the respective date and time box.

Daily Reports

Special *Daily Report* functionality has been included to provide for reporting on a specific time period, such as 8:00:00 a.m. through 17:00:00 p.m. over a range of days such as the previous week.

Select the daily time period desired, and the Start and End dates for the desired range of days. Then check the *Daily* report option on the screen.

Messages



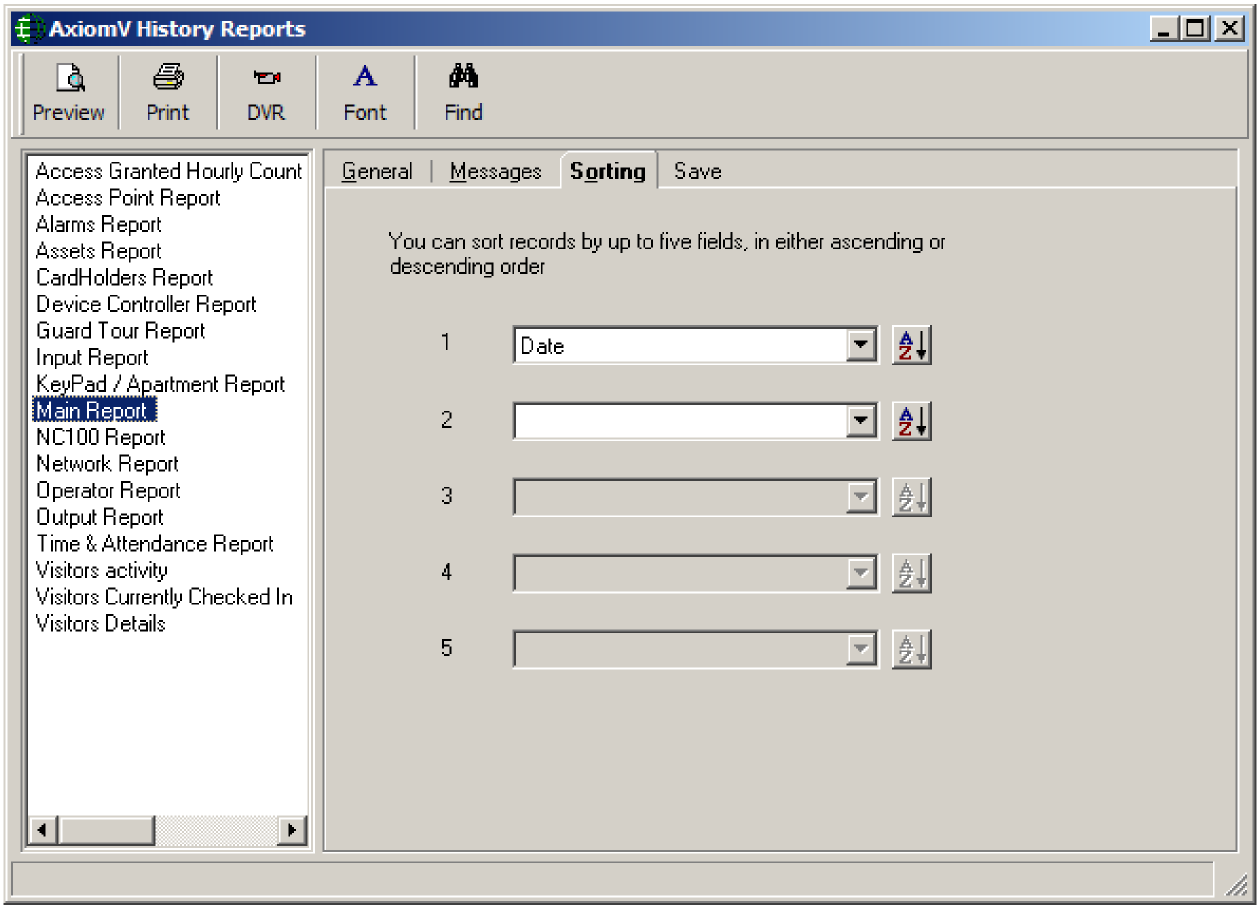
Access Granted Hourly Count
Access Point Report
Alarms Report
Assets Report
CardHolders Report
Device Controller Report
Guard Tour Report
Input Report
KeyPad / Apartment Report
Main Report
NC100 Report
Network Report
Operator Report
Output Report
Time & Attendance Report
Visitors activity
Visitors Currently Checked In
Visitors Details

The list contains messages that you can select for this report.
Events with only selected messages will be shown in the report.

- ☑ Select All
  - ☑ Access Granted
  - ☑ Access Denied
  - ☑ CardHolder Action
  - ☑ Access Point
  - ☑ Access Point Status
  - ☑ Input Point
    - ☑ Input: restore
    - ☑ Input: alarm
    - ☑ Input: trouble
    - ☐ Input: illegal
    - ☑ Input: normal
    - ☑ Input: abnormal
    - ☑ Input armed
    - ☑ Input disarmed
  - ☑ Output Point
  - ☑ NC100

As well as selecting the category and date/time parameters for your report, it can be further defined by messages. Click on the check boxes to select/deselect messages. Only events with the checked messages will appear in the report.

Sorting



You can sort records by up to five fields, in either ascending or descending order

1 Date

2

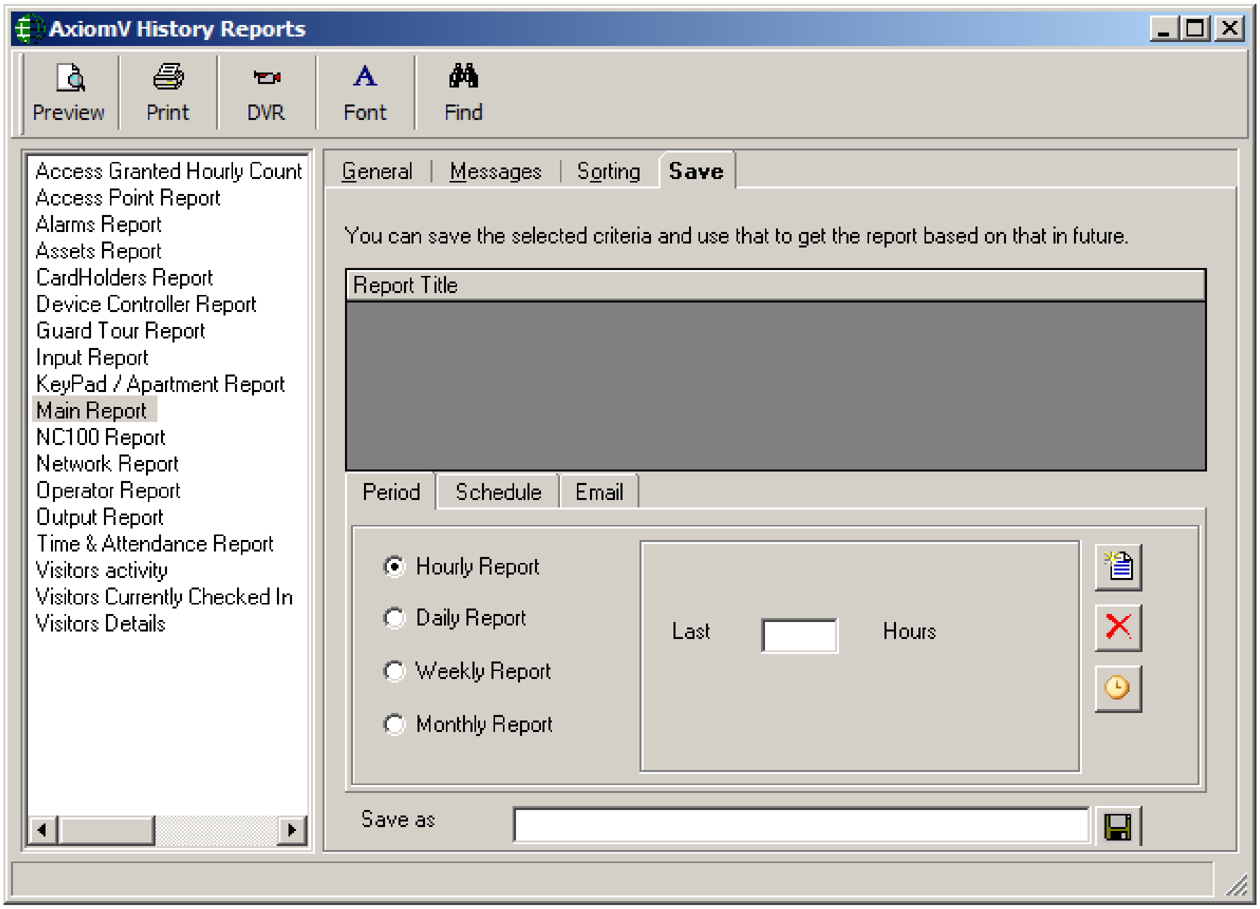
3

4

5

The *Sorting* tab provides the ability to customize the report by sorting chosen fields (either ascending or descending). Up to five fields sorts can be done for each report. The report is first sorted by sort 1 and then (if programmed) by sorts 2-5 (in order).

Save[16]Error! Bookmark not defined.Error! Bookmark not defined.



Access Granted Hourly Count
Access Point Report
Alarms Report
Assets Report
CardHolders Report
Device Controller Report
Guard Tour Report
Input Report
KeyPad / Apartment Report
Main Report
NC100 Report
Network Report
Operator Report
Output Report
Time & Attendance Report
Visitors activity
Visitors Currently Checked In
Visitors Details

You can save the selected criteria and use that to get the report based on that in future.

● Hourly Report
○ Daily Report
○ Weekly Report
○ Monthly Report

Last ____ Hours

Under the *Save* tab you can set up reports to run automatically. To accomplish this, the optional module 'Report Server' is required.

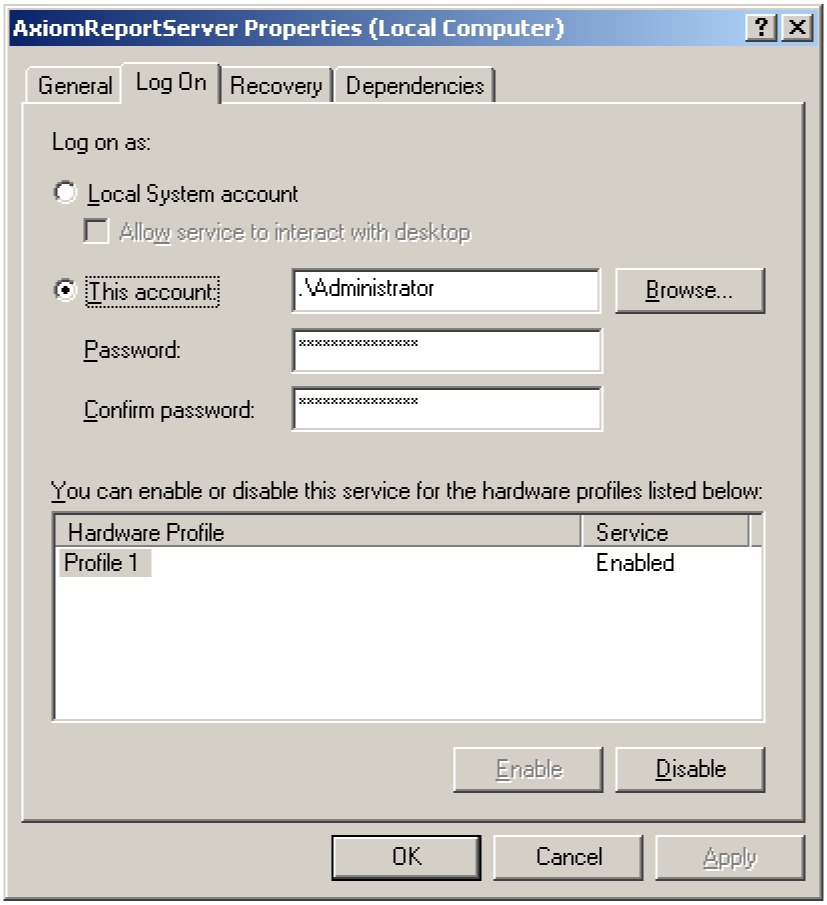
When a report is designed and saved all of the criteria (or data) to create that report is saved (the report itself is not saved). Reports will then run and print/email according to the schedule created for the report, unless the Report Server is off. If the Report Server is off at the time of a schedule print/email it of course will not print/email at that time nor will it print/email when the server is turned on. It will print/email at the next scheduled time according to the saved design criteria for the report. For example, if an Every 12 hour report is created to start on 1 January 2012 at 8:30 a.m., it will print/email at that time then at 8:30 p.m. 1January 2012, then 8:30 a.m. 2January 2012, etc. Now if the server is turned off from 6:00 a.m. 5 January 2012 until 12:45 p.m. 5 January 2012, then no report will be printed/emailed at 8:30 a.m. 5 January 2012 or at 12:45 p.m. 5 January 2012. The next report will be printed/emailed at 8:30 p.m. 5 January 2012.

Reports cannot be printed/emailed for periods that are not completely in the past. Therefore reports that are scheduled to print/email at a time within the parameters of the

[16] This selection is only available if the optional license for the History Report Scheduler Software has been purchased and installed.

period will print/email a report for the previous period. This means that if a report is scheduled for 4:00 p.m. to cover the time from 8:00 a.m. to 7:00 p.m., then the report will be printed/emailed for the previous day and not the current day. A report that covers from, *day 1* to *day* '*Last*' always prints/emails the previous month.

The AxiomV™ Report Server is an independent AxiomV™ system that allows the user to design and schedule history reports.



AxiomReportServer Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\Administrator

Password: ***************

Confirm password: ***************

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

Be sure to change the Log On property for 'Axiom Report Server' from *Local System account* to a local user account.

To create an automatic report select the type of report to run, what period the report is to cover, and then what schedule it is to run on.

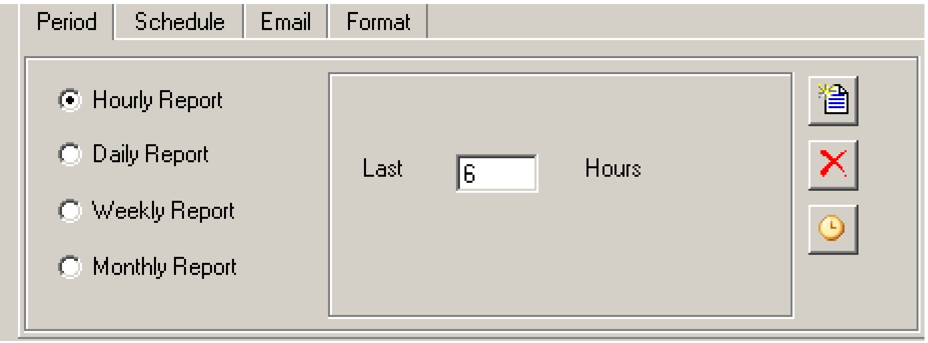
Select *New* to set up an automatic report.

Delete will remove the highlighted report from the list.

The *Schedule* button will call up the schedule tab.

Save will save the schedule created using the name typed in the white box labeled 'Save as'.

Period

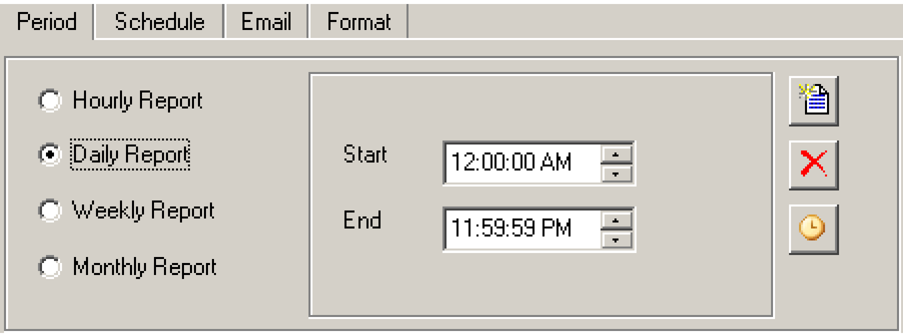


● Hourly Report
○ Daily Report
○ Weekly Report
○ Monthly Report

Last 6 Hours

Hourly

This period will cover the last ***x*** hours prior to the report being printed. The maximum time it can be set to is 99 hours (or four days and three hours).

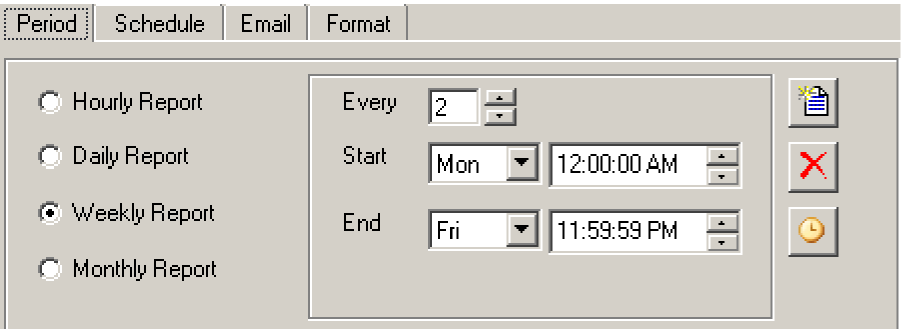


○ Hourly Report
● Daily Report
○ Weekly Report
○ Monthly Report

Start 12:00:00 AM
End 11:59:59 PM

Daily

This period will cover the specified portion of the day from Start time to End time.

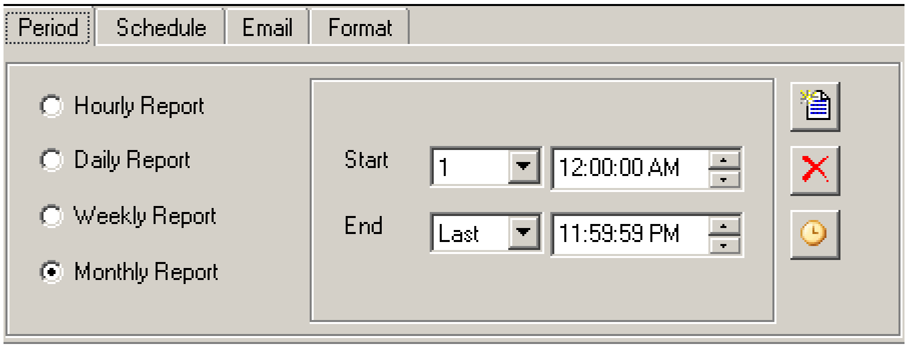


○ Hourly Report
○ Daily Report
● Weekly Report
○ Monthly Report

Every 2
Start Mon 12:00:00 AM
End Fri 11:59:59 PM

Weekly

This period can cover one or more weeks. It covers days of the week from the Start (day and time) until the End (day and time). The End can be in the current week or a succeeding week.



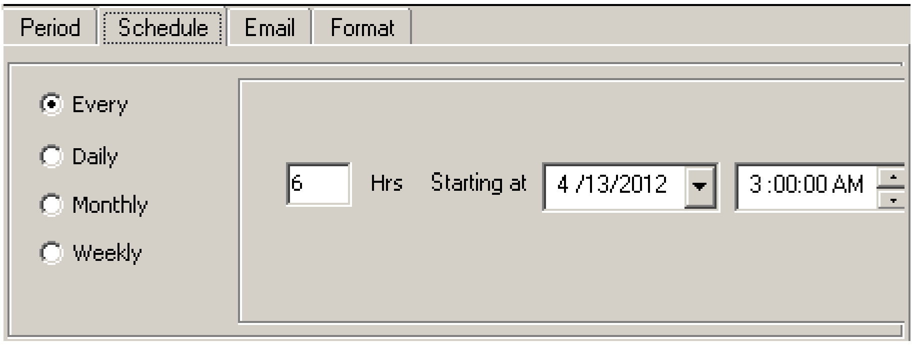
○ Hourly Report
○ Daily Report
○ Weekly Report
● Monthly Report

Start 1 12:00:00 AM
End Last 11:59:59 PM

Monthly

This period can cover up to one month. It covers the dates of the month from the Start (date and time) until the End (date and time). The End date can be a lower value then the Start date in order to span two months.

Schedule

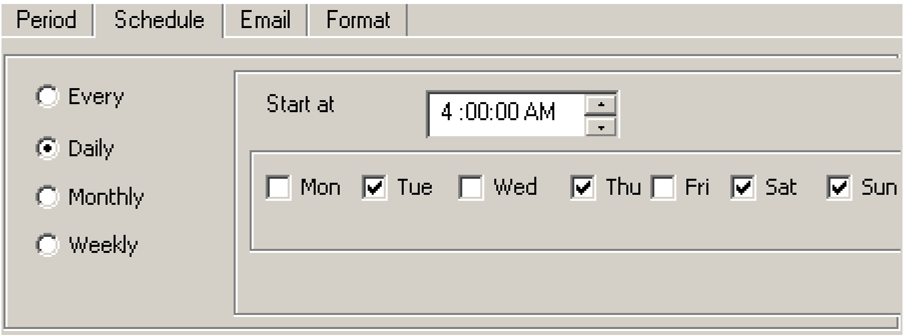


● Every
○ Daily
○ Monthly
○ Weekly

6 Hrs Starting at 4 /13/2012 3 :00:00 AM

Every

This schedule will print/email the report periodically at the set interval. The example above will print/email a report every six hours (four times a day). This interval cannot be set to more than 999 hours (or forty-one days and fifteen hours).



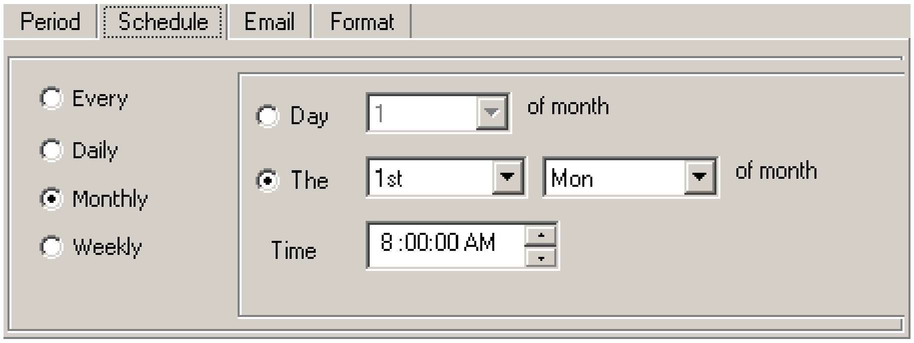
○ Every
● Daily
○ Monthly
○ Weekly

Start at 4 :00:00 AM

□ Mon ☑ Tue □ Wed ☑ Thu □ Fri ☑ Sat ☑ Sun

Daily

This schedule set which days of the week and at what time on those days that the report will be printed/emailed.

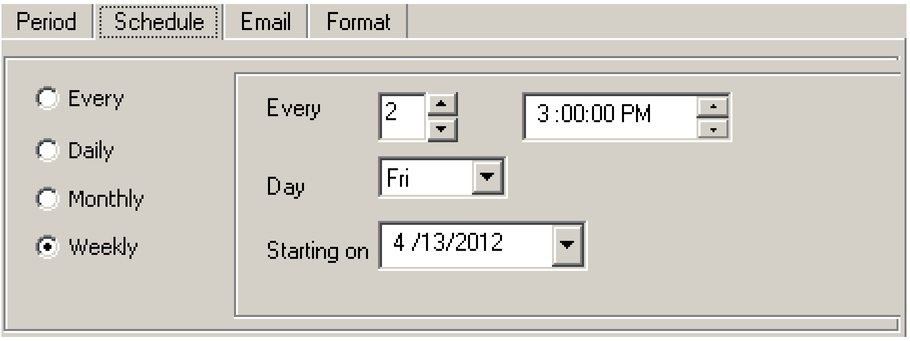


○ Every
○ Daily
● Monthly
○ Weekly

○ Day 1 of month
● The 1st Mon of month
Time 8 :00:00 AM

Monthly

This schedule can set up the report to print/email on a specific date of the month, including the Last day, or a specific day of the month like the 2nd Tuesday. Select a time on that date for the report to print/email.



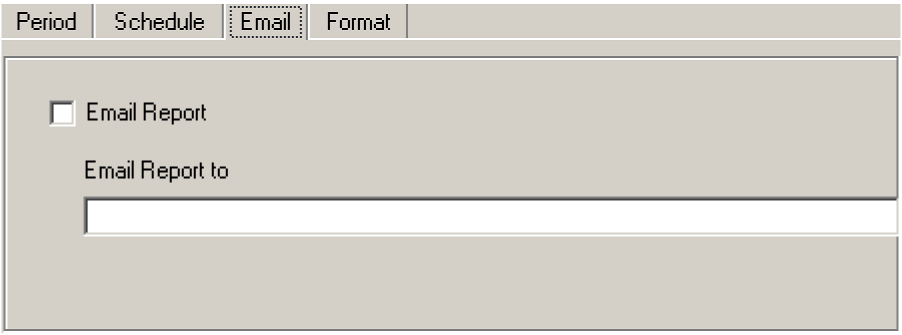
○ Every
○ Daily
○ Monthly
● Weekly

Every 2 3 :00:00 PM
Day Fri
Starting on 4 /13/2012

Weekly

This schedule will print/email the report periodically with a weekly interval. The interval could be every week, every other week, or more. Set the day of the, the time, and a date to start on.

EMail

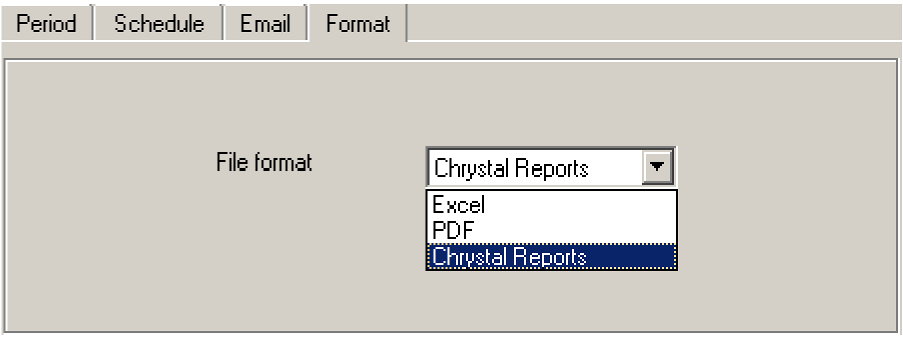


□ Email Report

Email Report to

Check the box and enter the eMail address that the periodic or scheduled report is to be sent to.

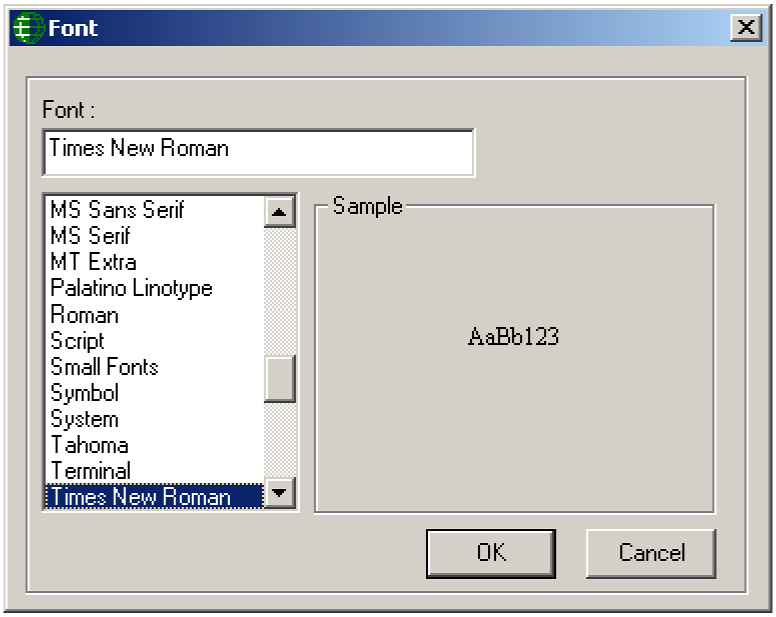
Format



File format: Chrystal Reports

Select the file format from the drop down menu (Excel, pdf, or Crystal reports) for the attached report sent through the email

Fonts



Font : Times New Roman

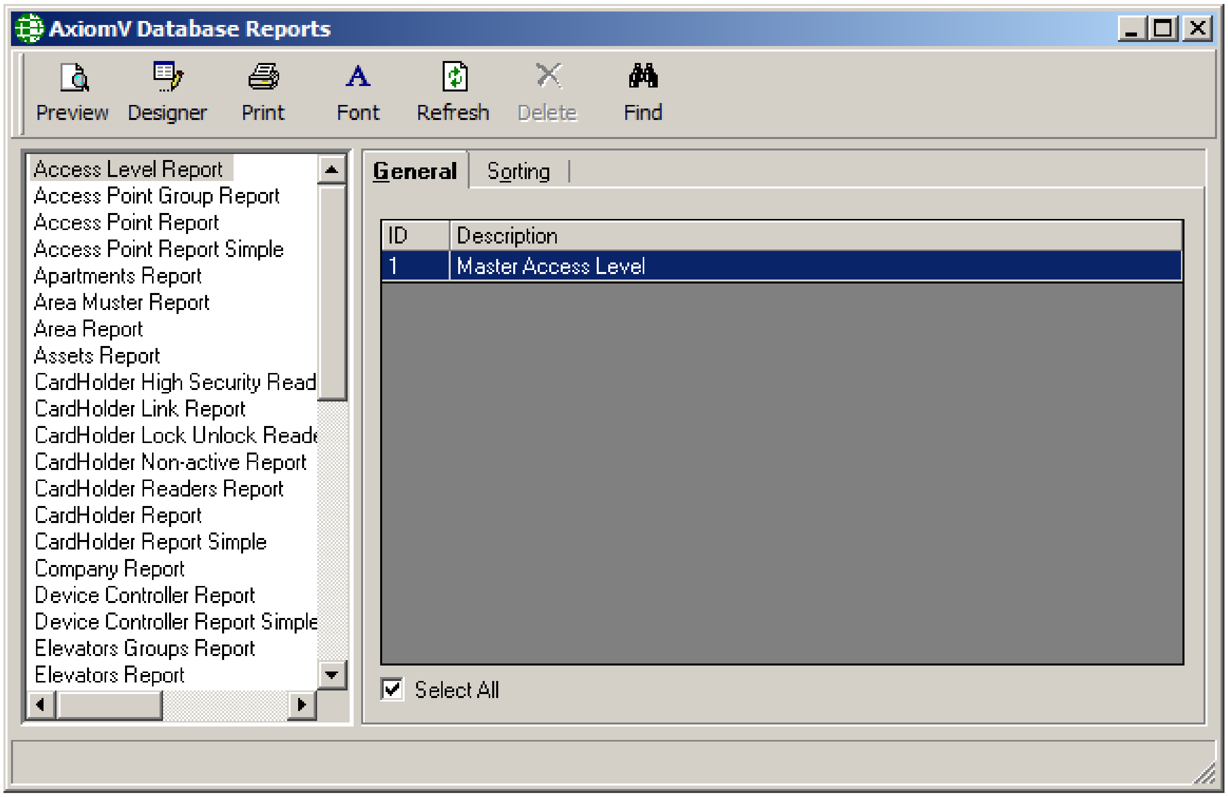
Fonts can be selected from either *Database Reports* or *Event History Reports* and applies to both. The selected font will be retained and applied to all reports, on a computer, until changed by the user. Therefore each different client machine will have its own selected font.

Database Reports

Starting Database Report

Database Report can be started from the Reports menu item or from a button on the toolbar.

General



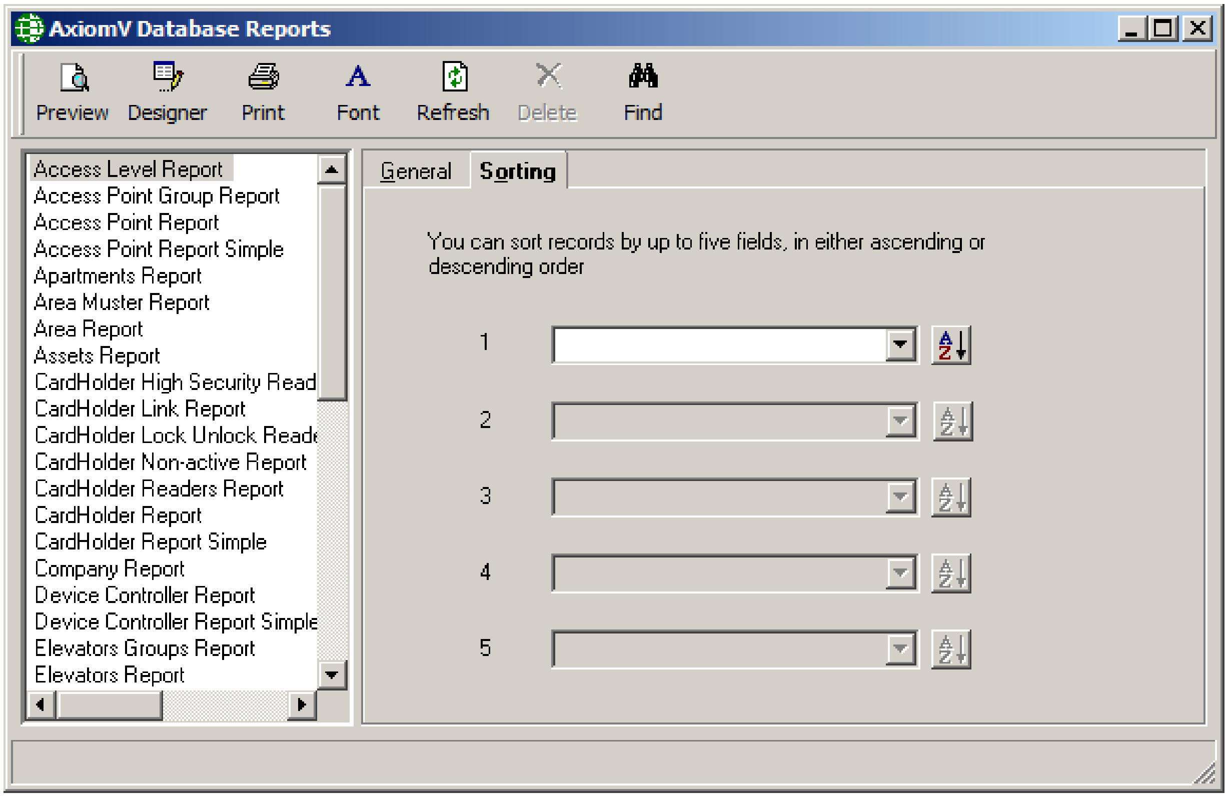
Access Level Report
Access Point Group Report
Access Point Report
Access Point Report Simple
Apartments Report
Area Muster Report
Area Report
Assets Report
CardHolder High Security Read
CardHolder Link Report
CardHolder Lock Unlock Reade
CardHolder Non-active Report
CardHolder Readers Report
CardHolder Report
CardHolder Report Simple
Company Report
Device Controller Report
Device Controller Report Simple
Elevators Groups Report
Elevators Report

ID	Description
1	Master Access Level

☑ Select All

Select from the list on the left the category (type of report) that will be the subject of the report. Then select from the list on the right the items that are to be included in the report. For example, for a cardholder report select from a list of cardholders, for an access point report select from a list of doors. Use **Click+drag**, **Shift+click** or **Ctrl+click** to select multiple items. Checking *Select All* will include all items in the report.

Sorting



You can sort records by up to five fields, in either ascending or descending order

The *Sorting* tab provides the ability to customize the report by sorting chosen fields (either ascending or descending). Up to five fields sorts can be done for each report. The report is first sorted by sort 1 and then (if programmed) by sorts 2-5 consecutively.

Preview Report

Preview Report will display the report on the screen. The report can then be viewed before being printed or exported. Printing and exporting can be done from this screen.

Report Designer

Report Designer will start the Custom Report Designer for the highlighted report. See Page 344 below for details including an example of the creation of a custom Muster Report.

Print Report

Print Report will send the report straight to the printer without being viewed.

A Font

Font is used to change the font used on the report. Simply select from the list provided. A sample of the font is shown in the area to the right. (See Fonts for more information.)

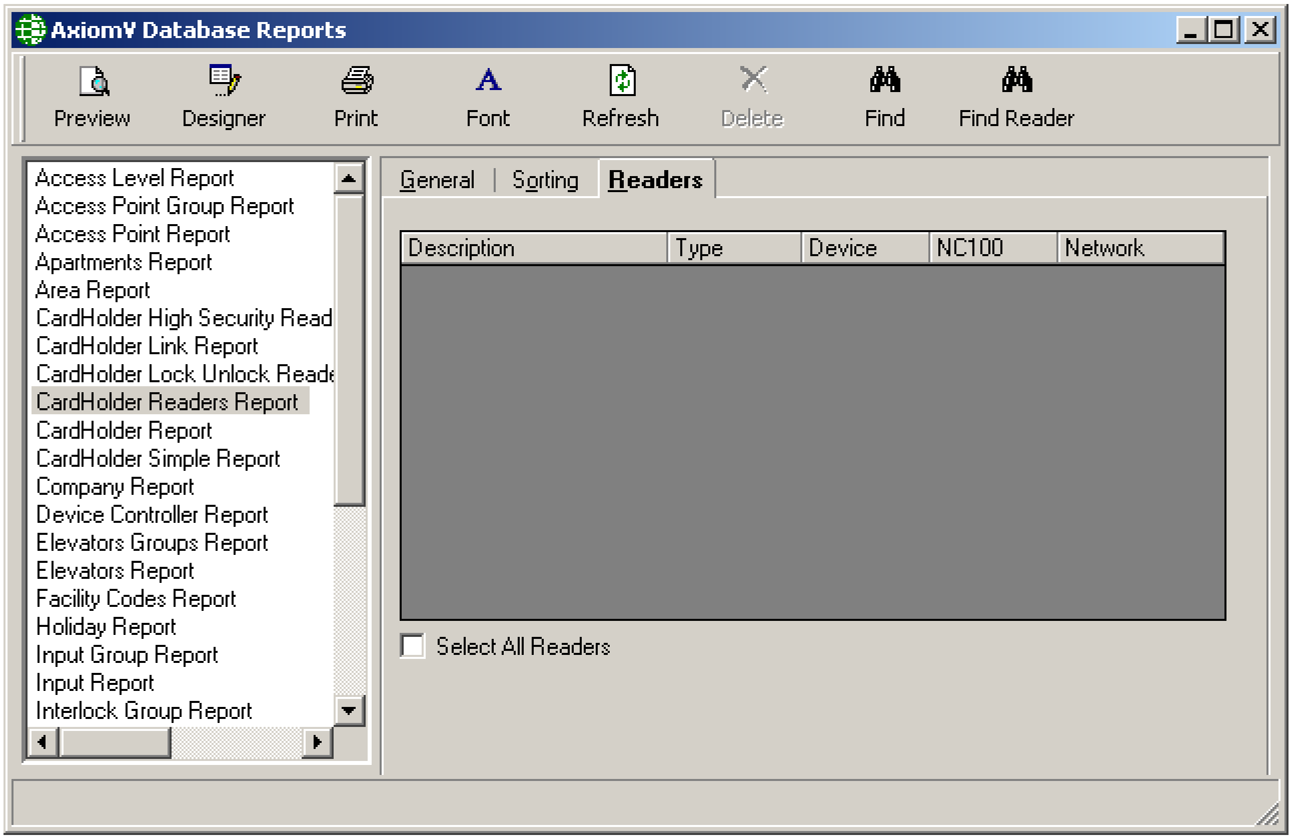
Refresh

Refresh will recompile the report list to include any newly created custom reports.

Delete

Delete is used to remove custom created report that is no longer required.

Readers



Some reports have a third tab (Readers) to further define the report. In the above example, under the general tab the cardholders are selected. Under the reader tab the access points are chosen. The resulting report will show which of the chosen readers the selected cardholder have access to.

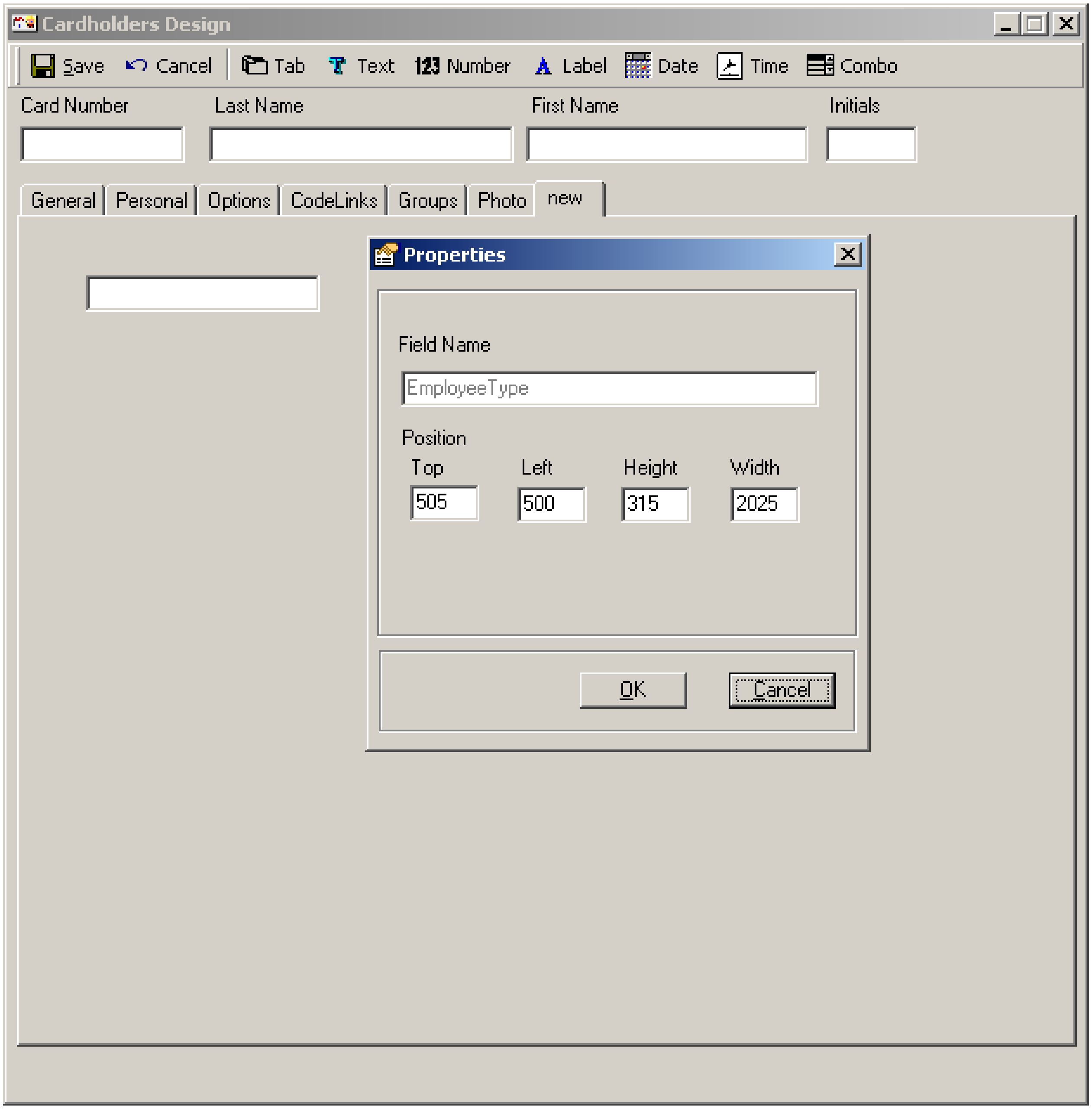
Custom Report Designer

This document will demonstrate how to create a custom design report. It will do this by for example by creating a 'Custom Muster Report'.

Any report can be customized but only by using the existing fields provided in the original report. The exception to this is the *Cardholder Reports* (*Cardholder report, Cardholder Simple report, Reader cardholder* and *Cardholder reader report*) that allows the addition of Custom Fields.RBH provides a few custom report text files for these reports to be able to add the custom fields configured in the system. For better understanding, follow the example shown below:

We want to create a custom muster report that includes fields that are not on the original report. To do this a custom report file needs to be created by RBH so that the required fields are added to the database fields' list.

For our example we want to include First Name, Last Name, and a custom field. Before starting to create the report, ensure that any custom fields that are required are available. For our example we created a custom field 'Employee Type'.



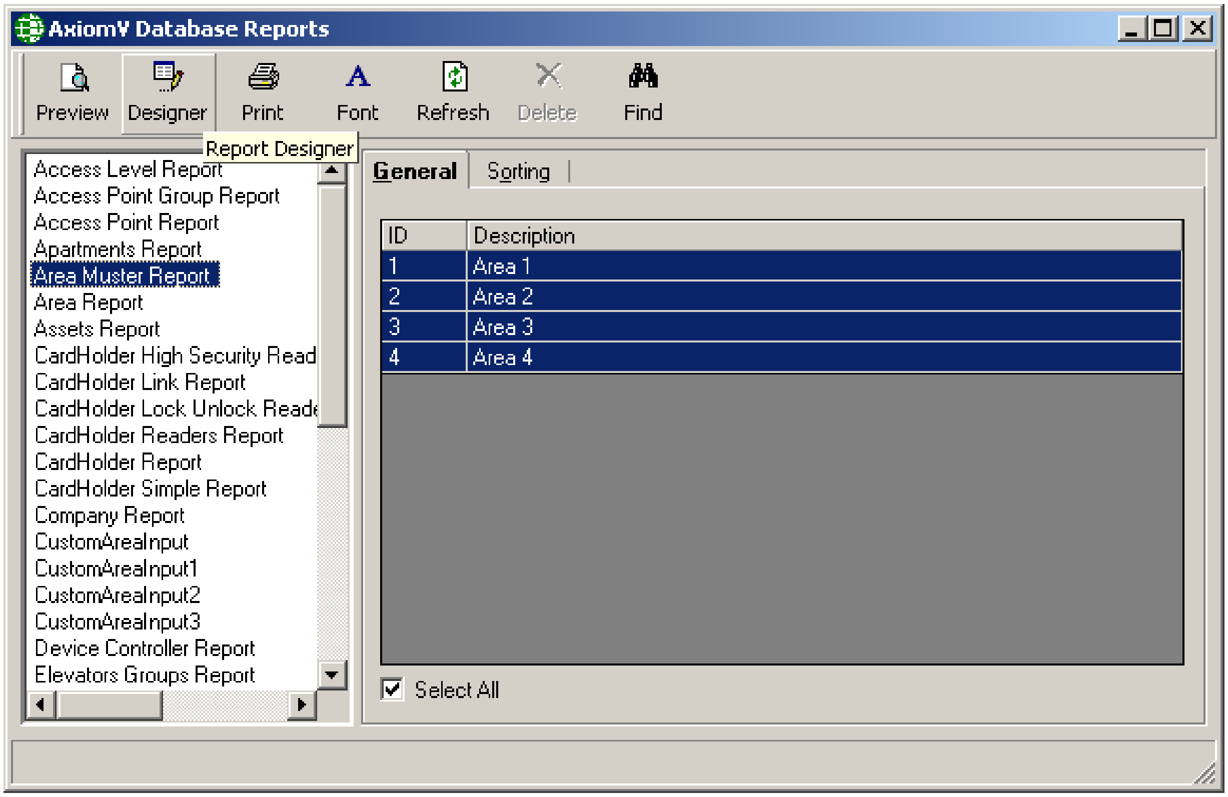
Field Name: EmployeeType

Position

Top	Left	Height	Width
505	500	315	2025

Custom Database Fields

Select the desired report (our example is a custom *Area Muster Report*) and click *Designer* to start the *Report Designer* utility.

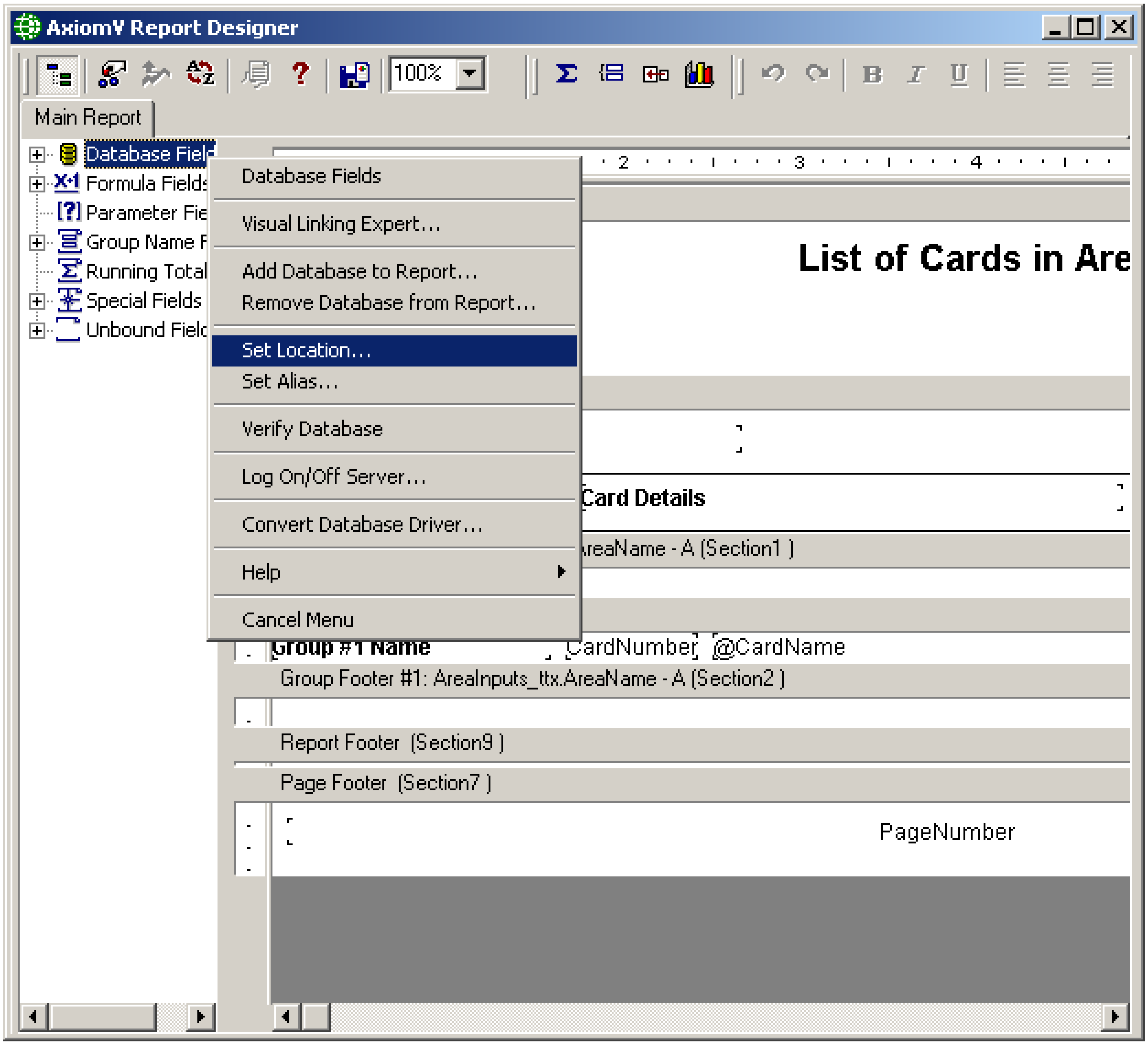


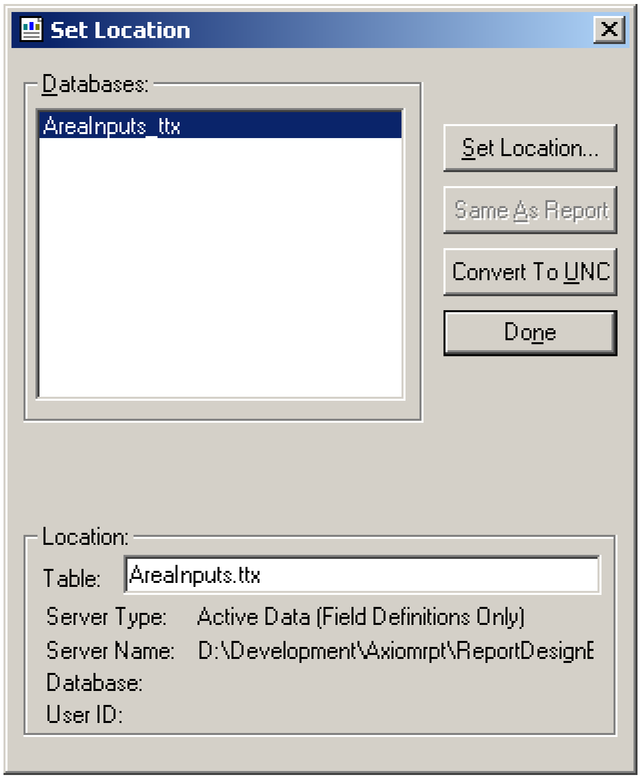
Access Level Report
Access Point Group Report
Access Point Report
Apartments Report
Area Muster Report
Area Report
Assets Report
CardHolder High Security Read
CardHolder Link Report
CardHolder Lock Unlock Reade
CardHolder Readers Report
CardHolder Report
CardHolder Simple Report
Company Report
CustomAreaInput
CustomAreaInput1
CustomAreaInput2
CustomAreaInput3
Device Controller Report
Elevators Groups Report

ID	Description
1	Area 1
2	Area 2
3	Area 3
4	Area 4

☑ Select All

To create the desired report the Database fields need to be changed. Right click on *Database Fields* and select *Set Location….* The new file provided by RBH is '*CustomAreafield.ttx'* for Area Muster report. Set this file as the new location.


AxiomV Report Designer
100%
Main Report
Database Fiel
Formula Fields
Parameter Fie
Group Name F
Running Total
Special Fields
Unbound Fielc
Database Fields
Visual Linking Expert…
Add Database to Report…
Remove Database from Report…
Set Location…
Set Alias…
Verify Database
Log On/Off Server…
Convert Database Driver…
Help
Cancel Menu
List of Cards in Are
Card Details
reaName - A (Section1)
Group #1 Name
CardNumber
@CardName
Group Footer #1: AreaInputs_ttx.AreaName - A (Section2)
Report Footer (Section9)
Page Footer (Section7)
PageNumber



Databases:

AreaInputs_ttx

Location:

Table: AreaInputs.ttx

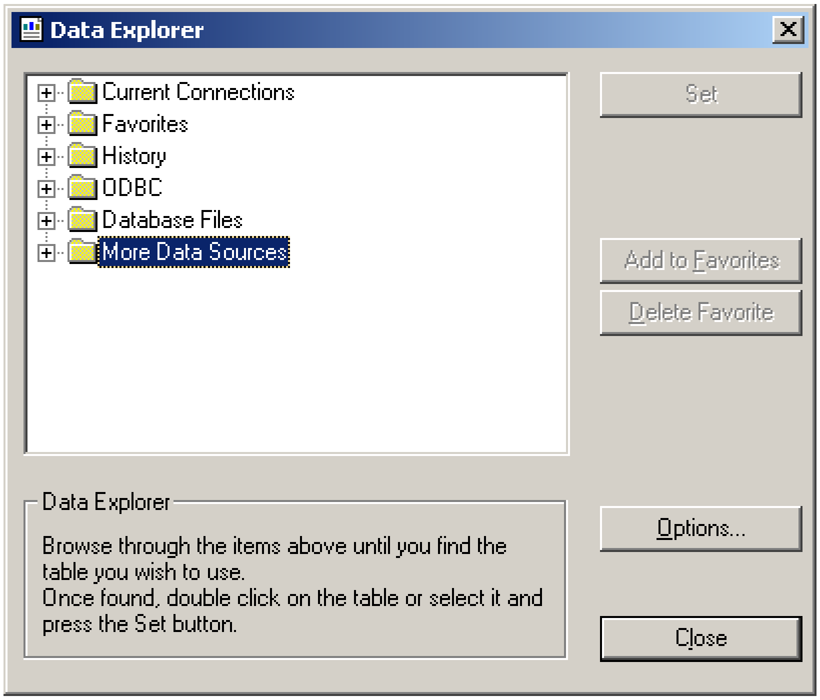
Server Type: Active Data (Field Definitions Only)

Server Name: D:\Development\Axiomrpt\ReportDesignE

Database:

User ID:

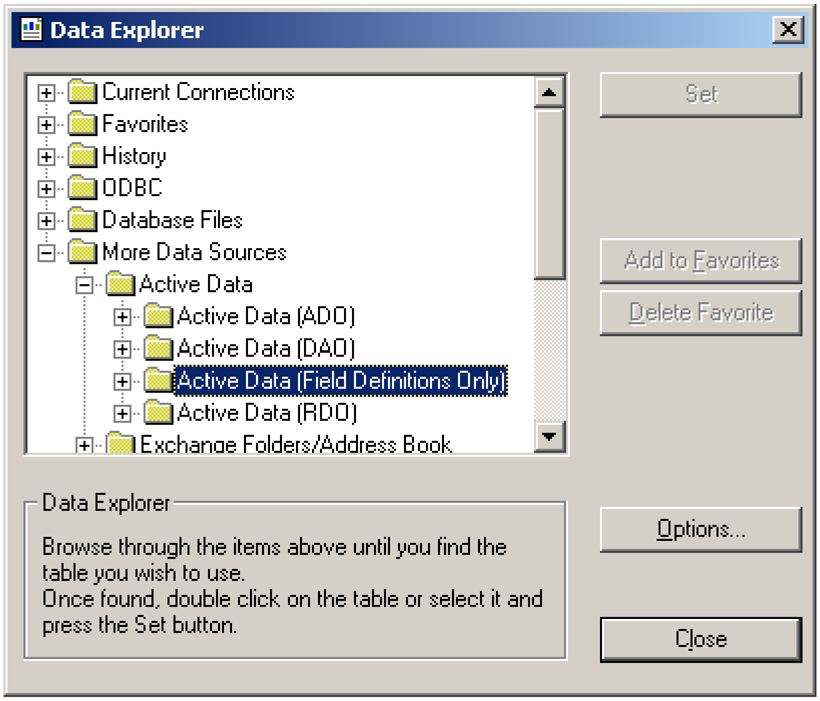
Click on the *Set Location* button to explore the Data folders in order to select the custom fields Database.



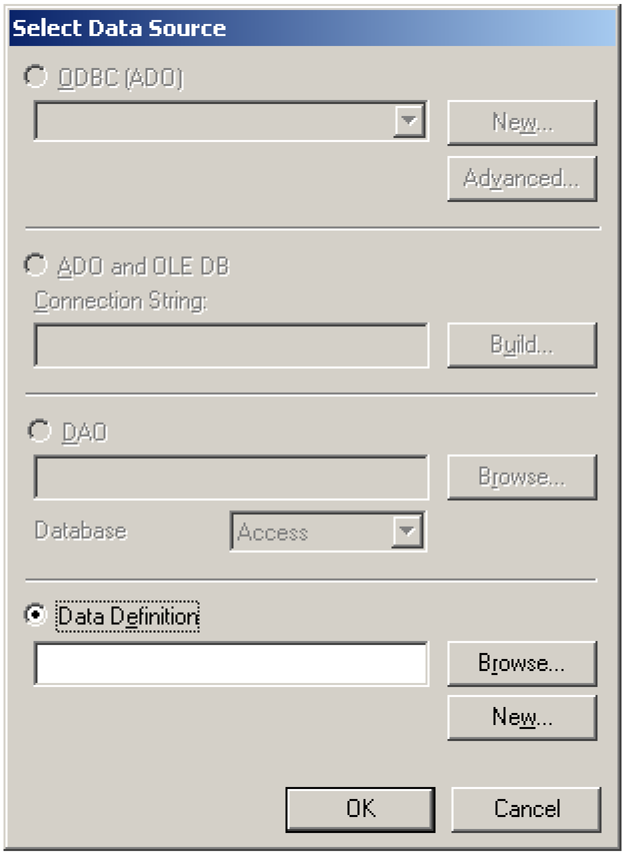
Data Explorer

Browse through the items above until you find the table you wish to use.
Once found, double click on the table or select it and press the Set button.

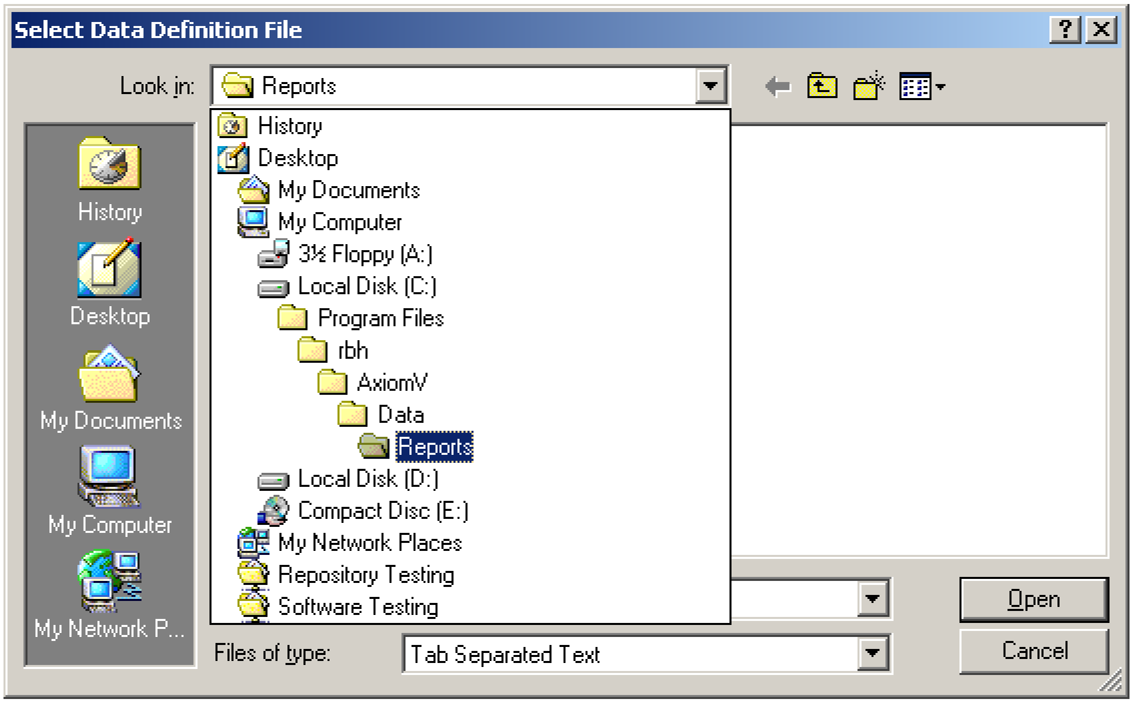
Select the path '*More Data Sources* / *Active Data* / *Active Data* (*Field Definitions Only*)' to select the *Data Source*.



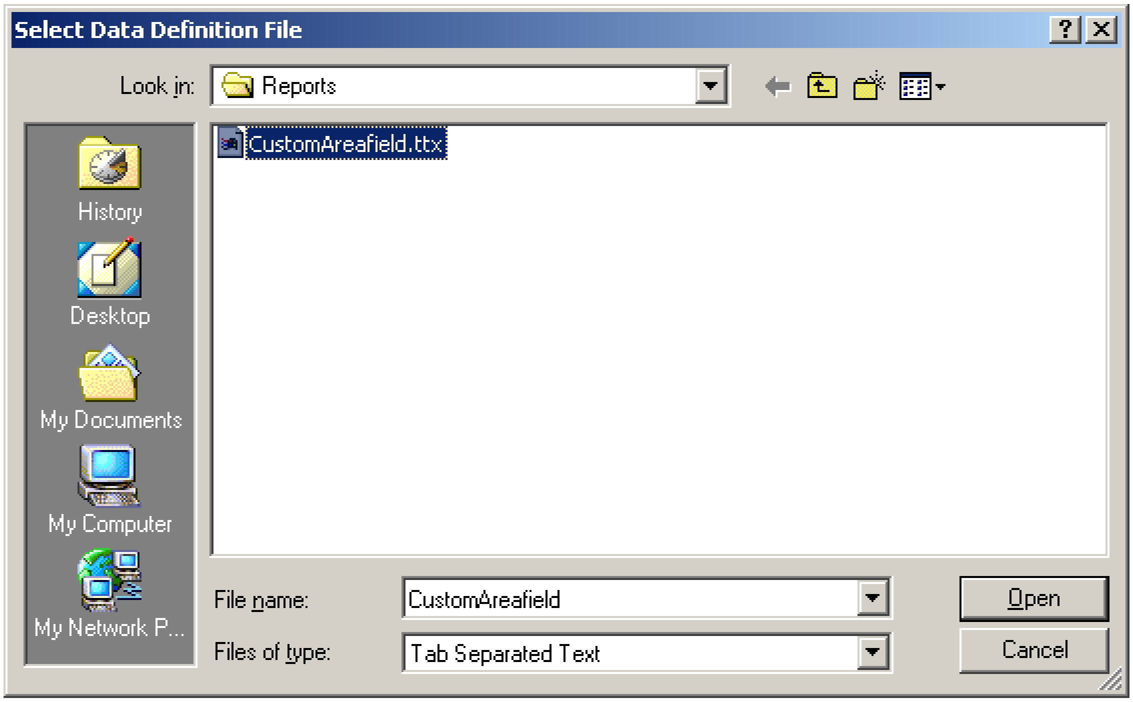
Browse through the items above until you find the table you wish to use.
Once found, double click on the table or select it and press the Set button.



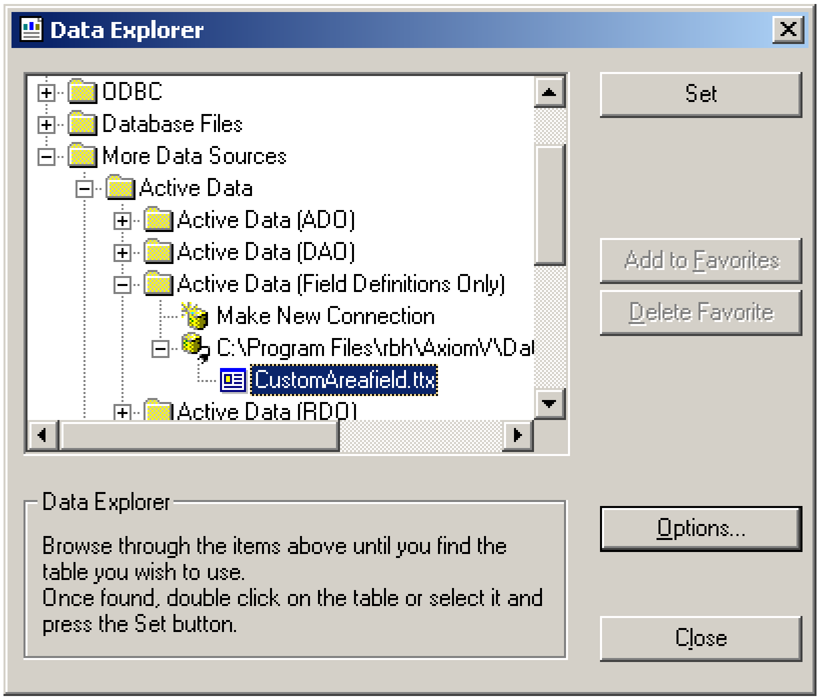
Select *Browse* and locate the *Reports* folder.



Browse the path to the provided custom file (*CustomAreafiled.ttx* in this example).



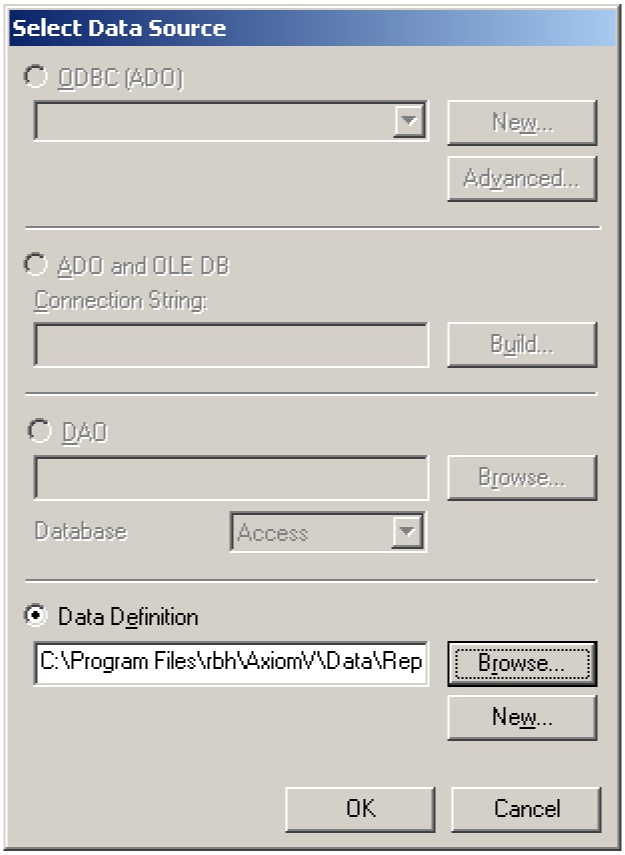
After selecting the new location file click *Open*.



Data Explorer

Browse through the items above until you find the table you wish to use.
Once found, double click on the table or select it and press the Set button.

Press *Set* to select the file.



● Data Definition
C:\Program Files\rbh\AxiomV\Data\Rep

Press *OK* to continue.

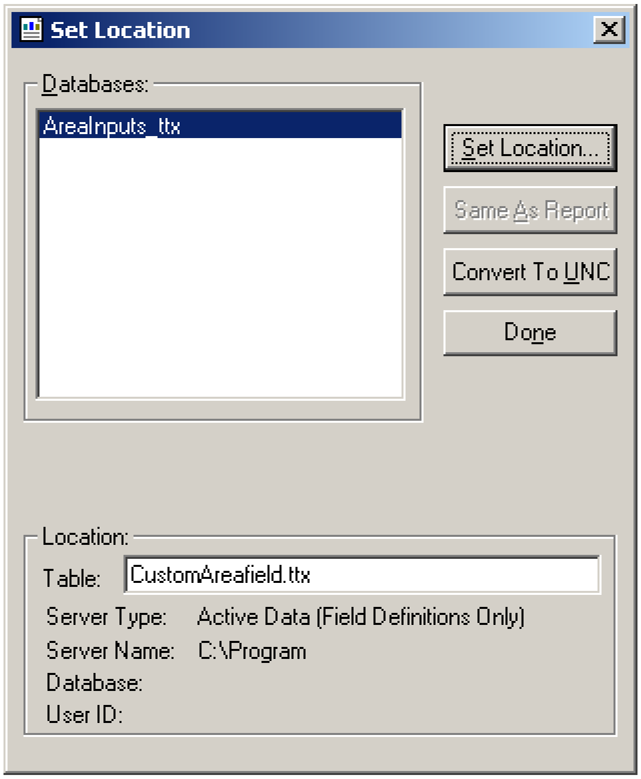
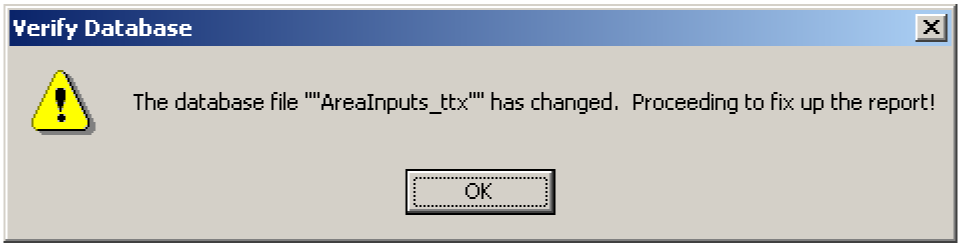


Table: CustomAreafield.ttx
Server Type: Active Data (Field Definitions Only)
Server Name: C:\Program
Database:
User ID:

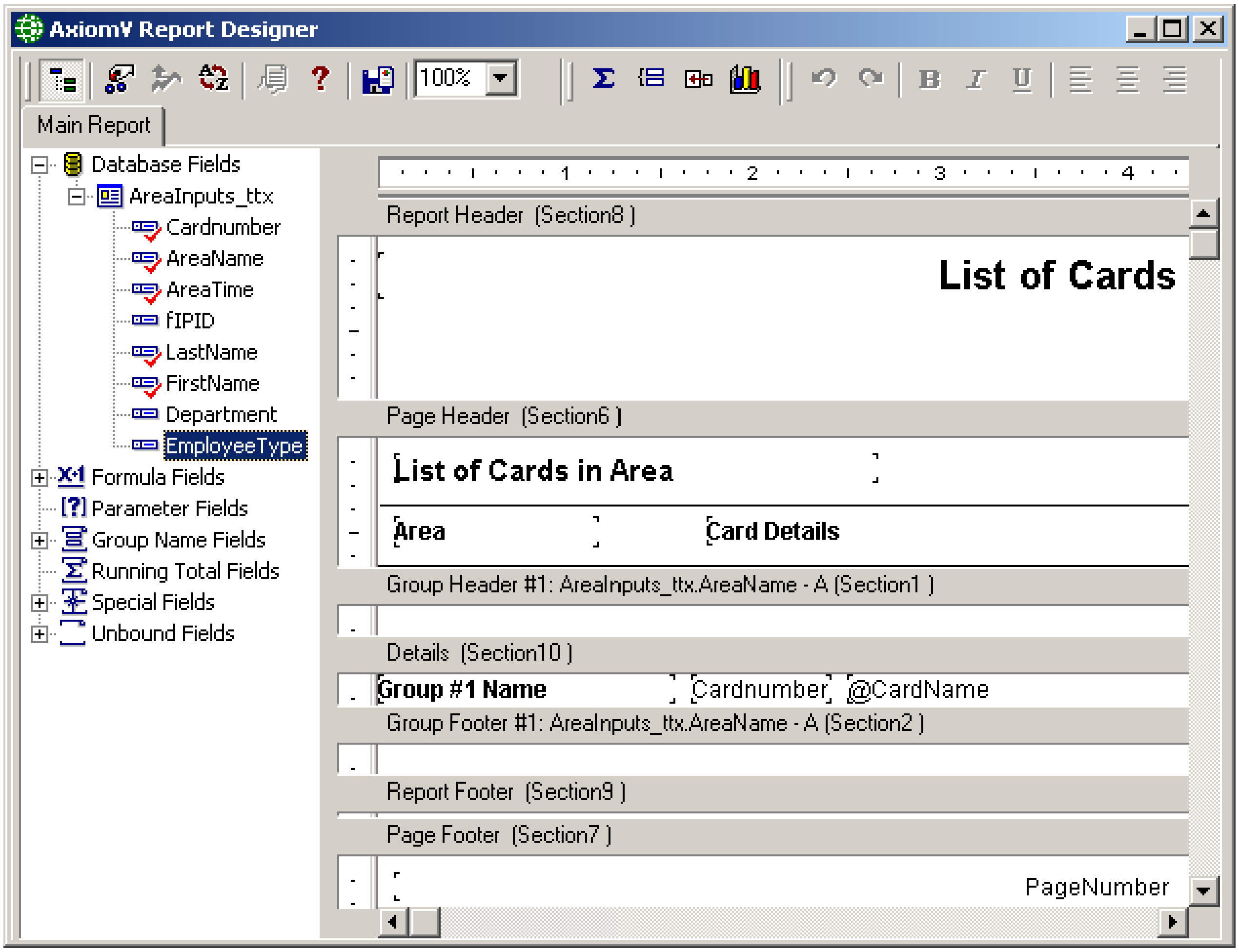
Press *Done* to complete the location selection.



The database file ""AreaInputs_ttx"" has changed. Proceeding to fix up the report!

You will get a verification of the change to the database fields. Press *OK*.

You can now see the custom fields (like Employee Type) in the field list on the left side of report.

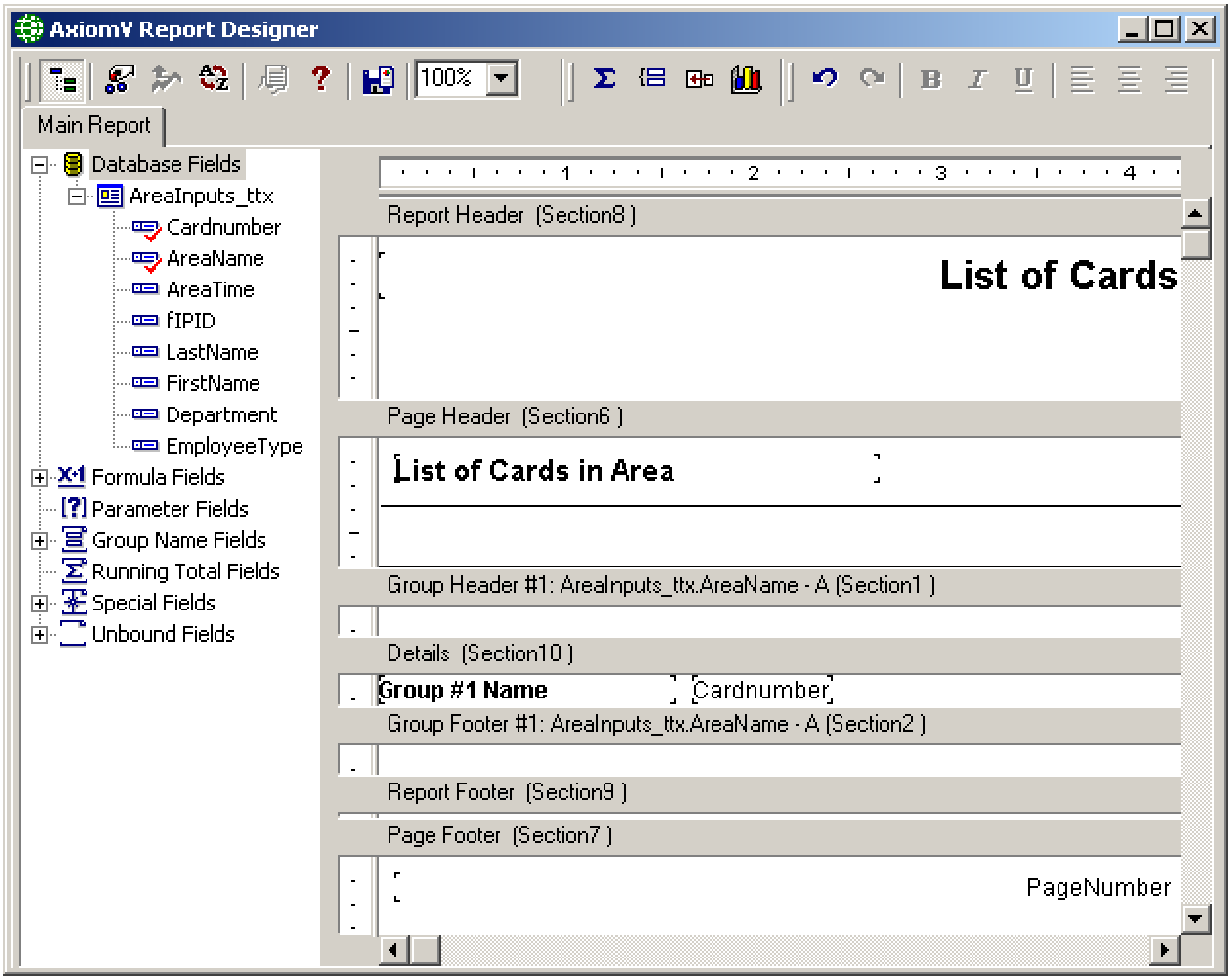


Customize Report[17]

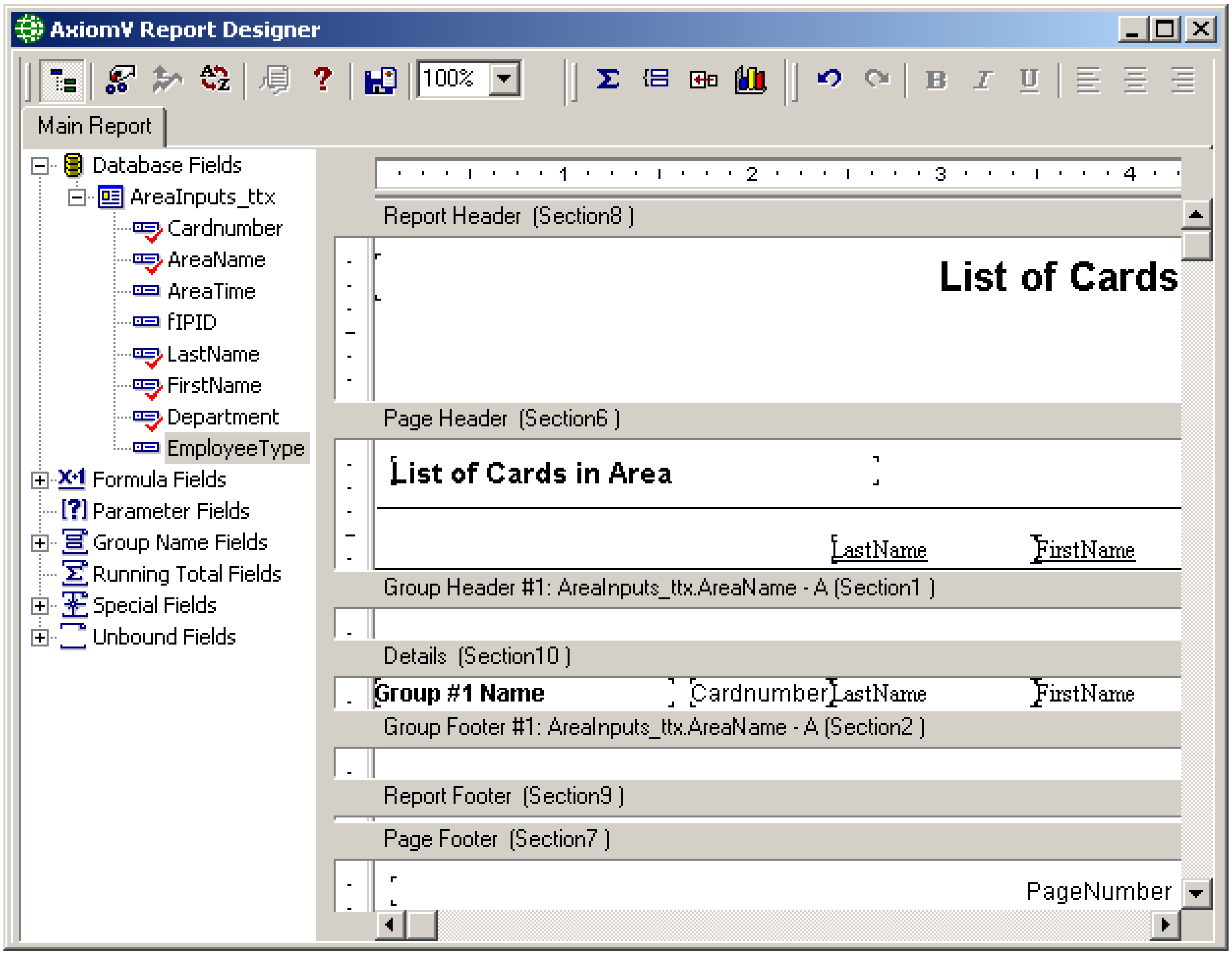
Now you can customize the report. Add and delete fields, edit text and formatting, and format formulas.

Remove Area, Card Details, and Entry Time from Section6, and remove @CardName and Area Time from Section10.

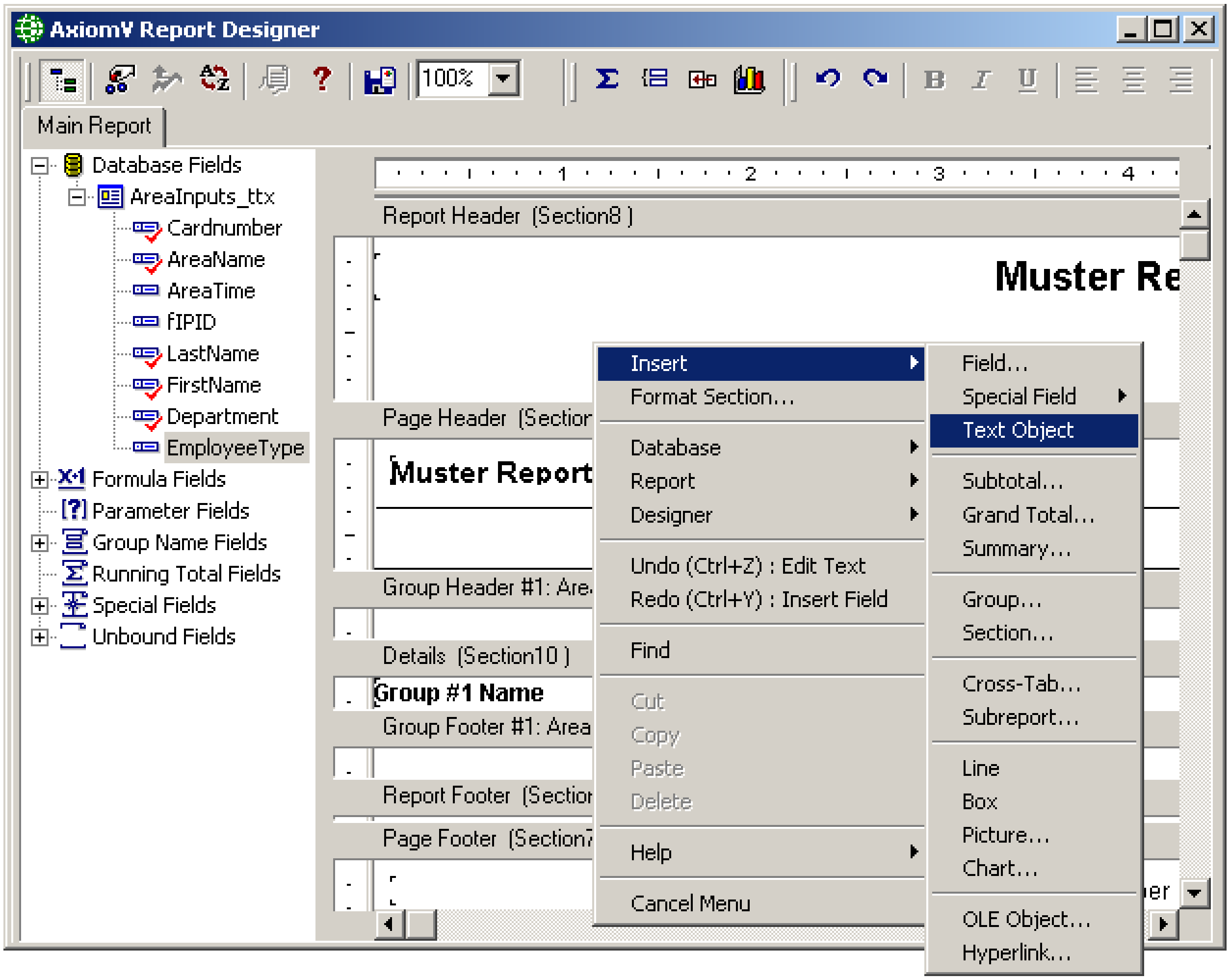
[17] This selection is only available if the optional license for the Customize Report Software has been purchased and installed.

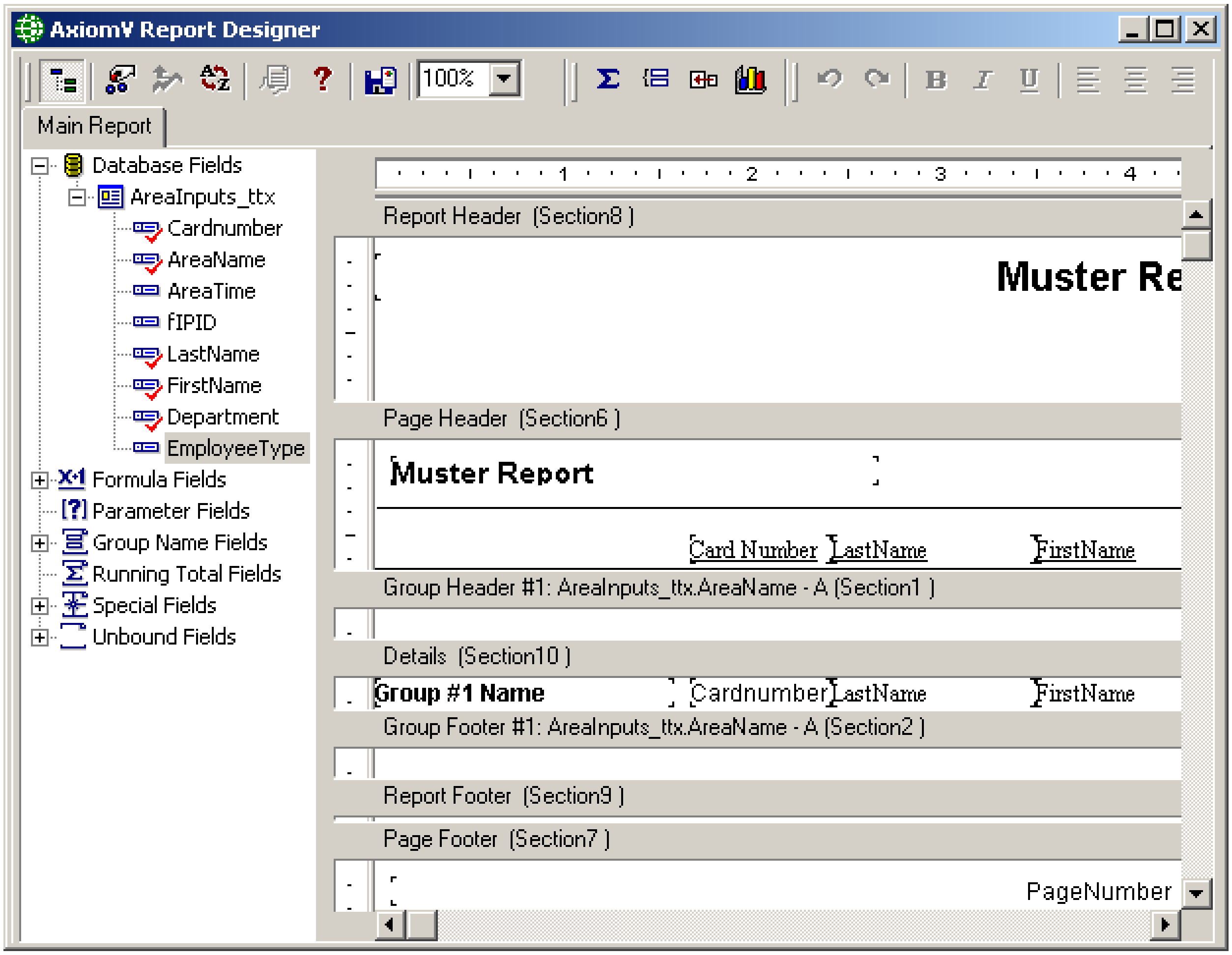


From the Database Fields List drag and drop *First Name*, *Last Name*, and *Department* into Section10. This will also create a header each one in Section6. Resize each entry for best fit in the area.

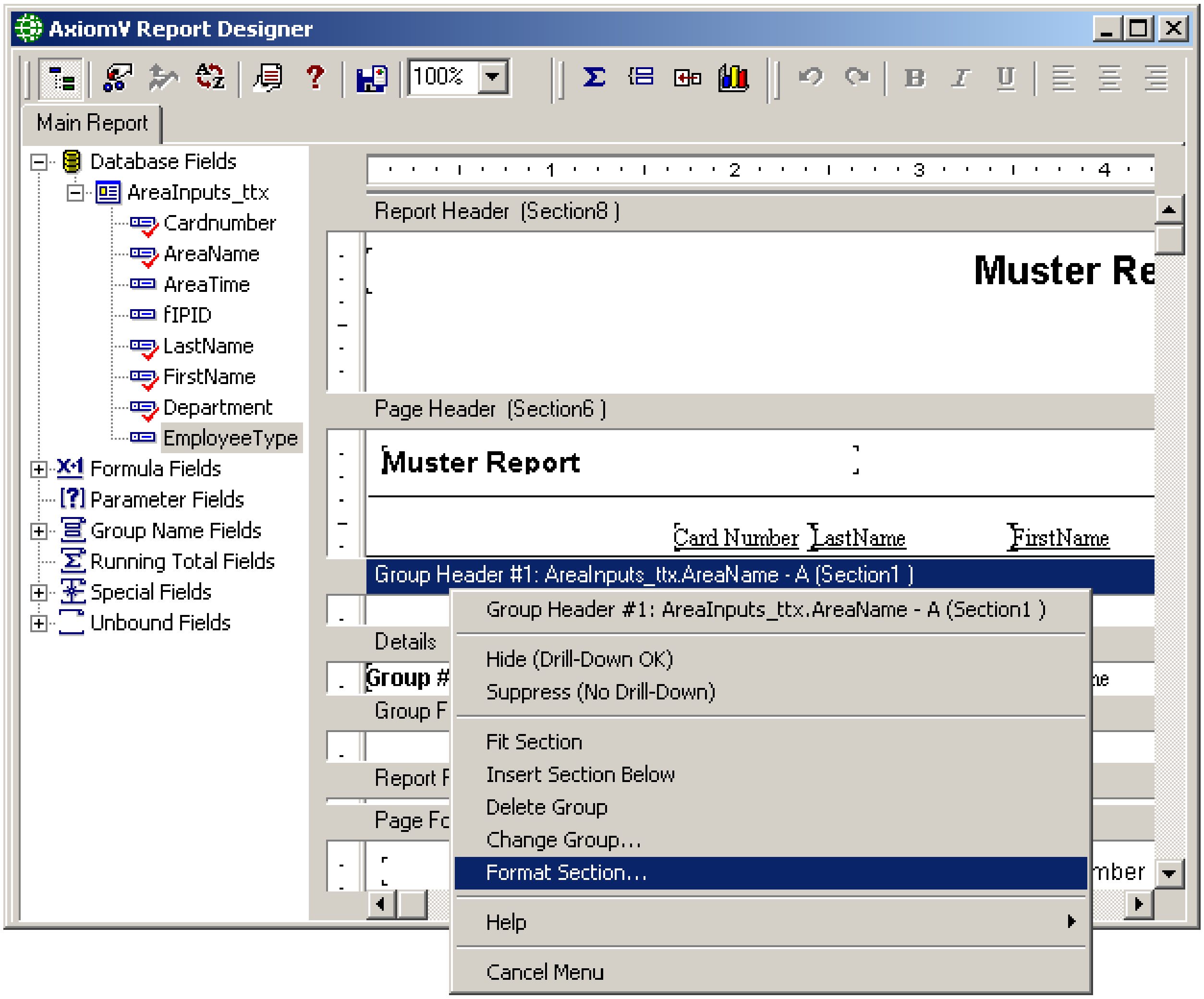


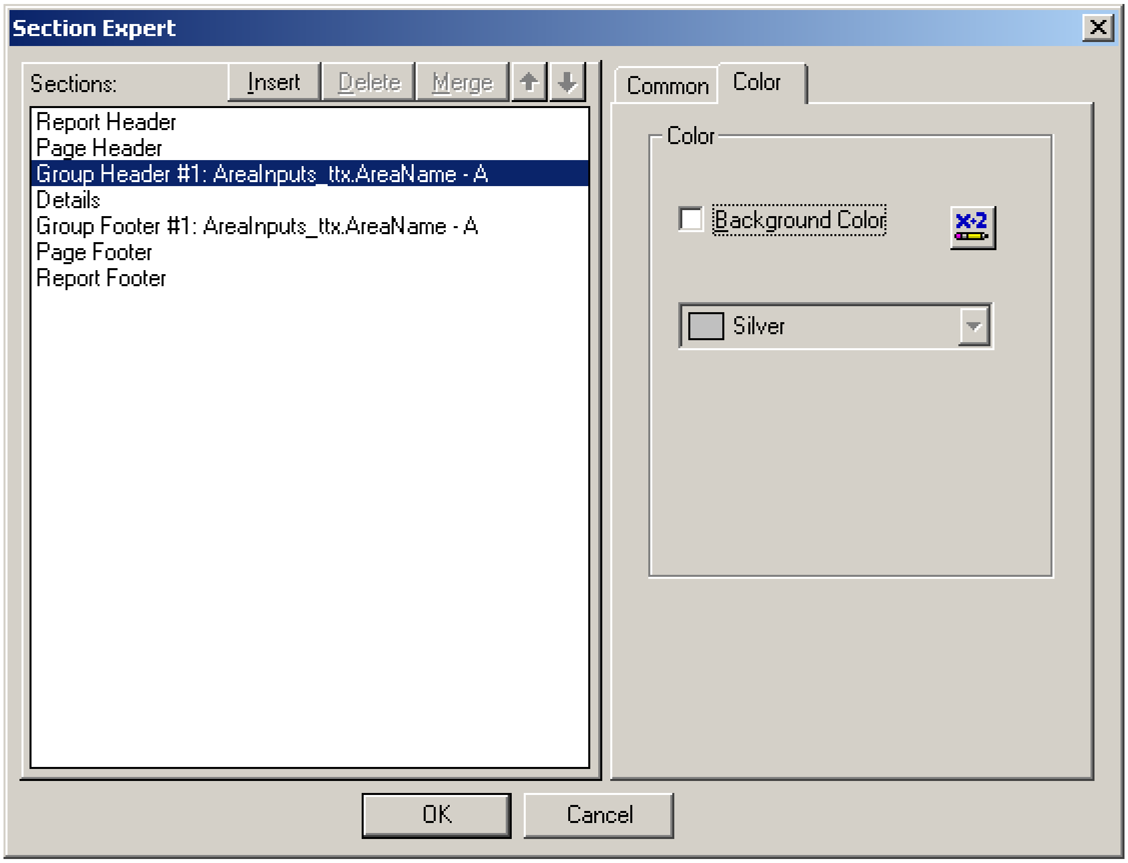
In Section6 and Section8 right click on the text fields ‘List of Card in Area’ and change them to ‘Muster Report’. Add the header ‘Card Number’ in Section6 by inserting a text object and editing it.


AxiomV Report Designer
100%
Main Report
Database Fields
AreaInputs_ttx
Cardnumber
AreaName
AreaTime
FIPID
LastName
FirstName
Department
EmployeeType
Formula Fields
Parameter Fields
Group Name Fields
Running Total Fields
Special Fields
Unbound Fields
Report Header (Section8)
Muster Re
Page Header (Sectior
Muster Report
Group Header #1: Are
Details (Section10)
Group #1 Name
Group Footer #1: Area
Report Footer (Sectior
Page Footer (Section7
Insert
Format Section...
Database
Report
Designer
Undo (Ctrl+Z) : Edit Text
Redo (Ctrl+Y) : Insert Field
Find
Cut
Copy
Paste
Delete
Help
Cancel Menu
Field...
Special Field
Text Object
Subtotal...
Grand Total...
Summary...
Group...
Section...
Cross-Tab...
Subreport...
Line
Box
Picture...
Chart...
OLE Object...
Hyperlink...



A Section Header trim is added (yellow for the muster area and red for other areas) by right clicking on the Section1 bar and selecting *Format Section*.


AxiomV Report Designer
100%
Main Report
Database Fields
AreaInputs_ttx
Cardnumber
AreaName
AreaTime
fIPID
LastName
FirstName
Department
EmployeeType
Formula Fields
Parameter Fields
Group Name Fields
Running Total Fields
Special Fields
Unbound Fields
Report Header (Section8)
Muster Re
Page Header (Section6)
Muster Report
Card Number
LastName
FirstName
Group Header #1: AreaInputs_ttx.AreaName - A (Section1)
Details
Group #
Group F
Report F
Page Fo
mber
Group Header #1: AreaInputs_ttx.AreaName - A (Section1)
Hide (Drill-Down OK)
Suppress (No Drill-Down)
Fit Section
Insert Section Below
Delete Group
Change Group…
Format Section…
Help
Cancel Menu



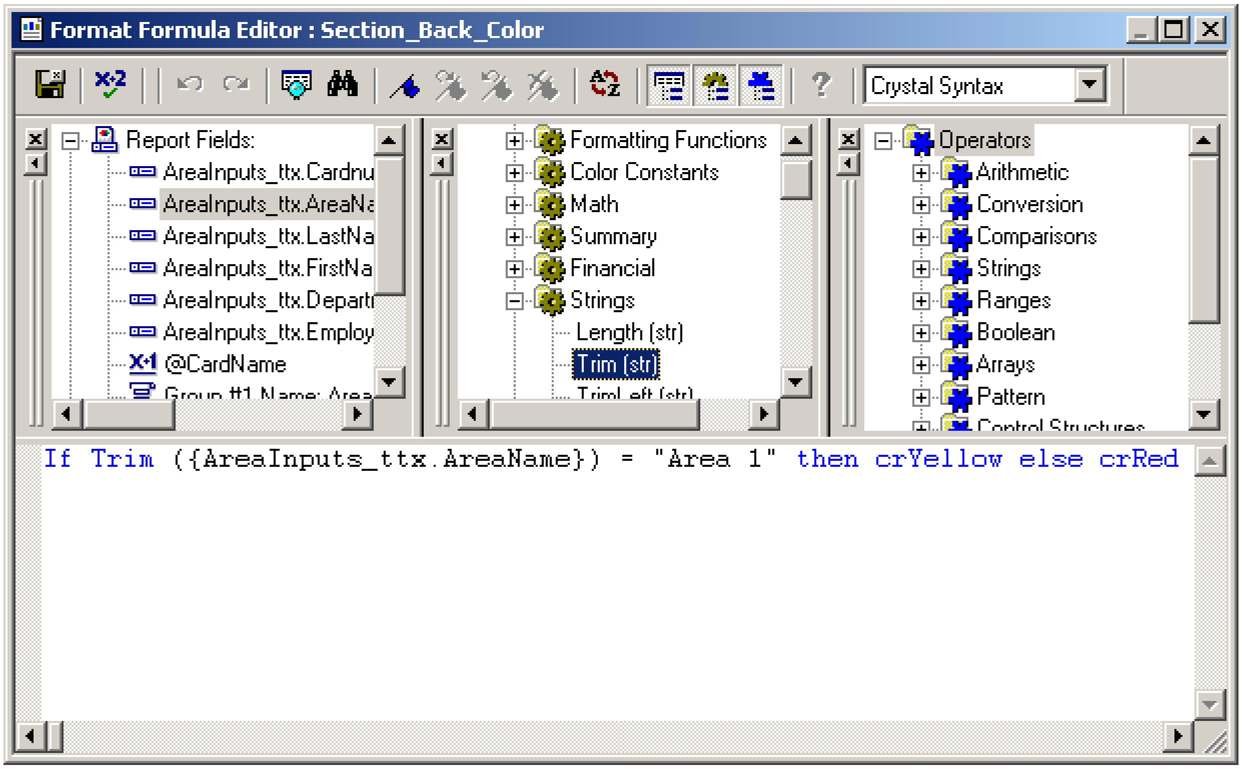
Report Header
Page Header
Group Header #1: AreaInputs_ttx.AreaName - A
Details
Group Footer #1: AreaInputs_ttx.AreaName - A
Page Footer
Report Footer

Color

□ Background Color

Silver

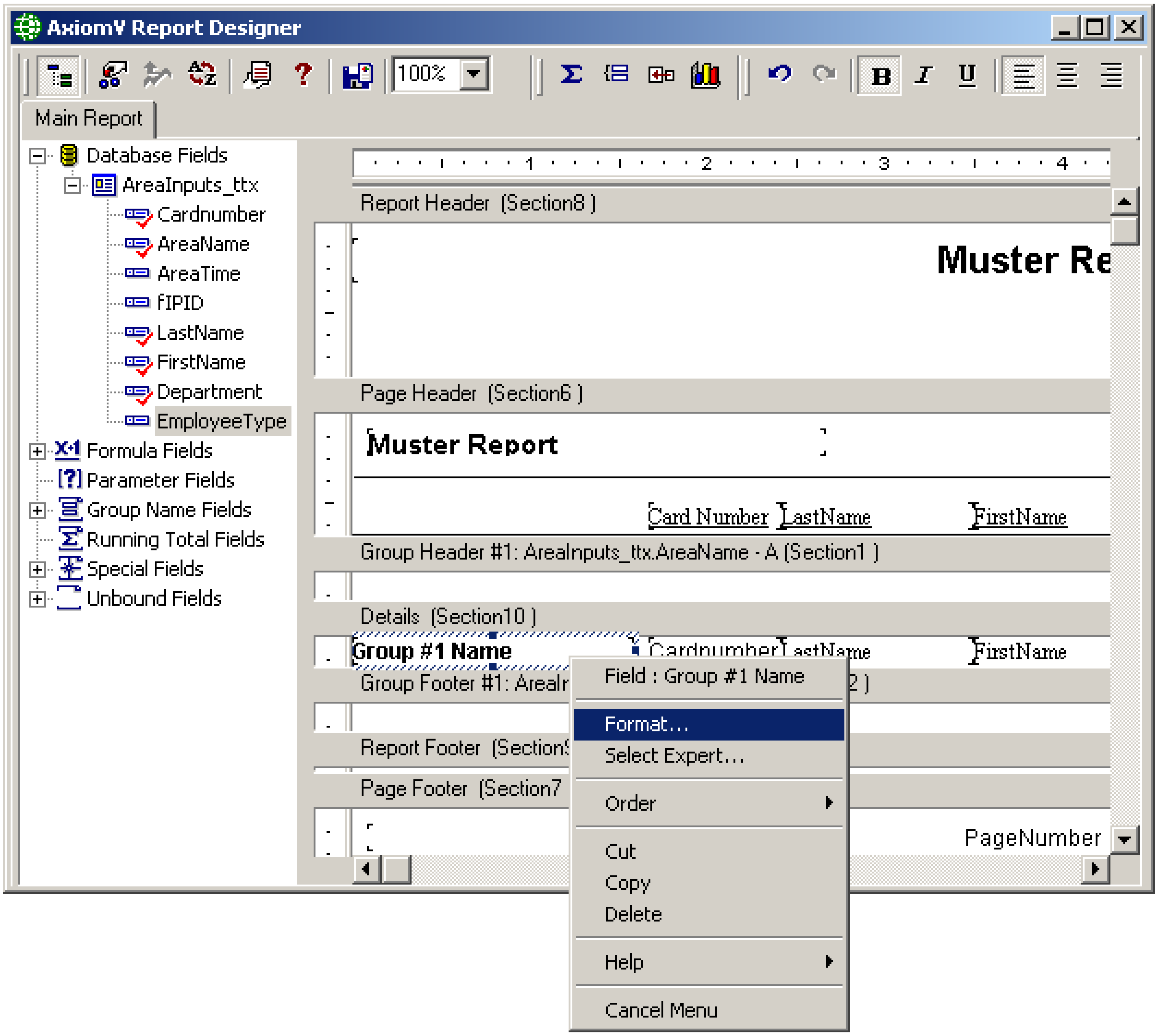
Select the *Colour* tab and press the **X+2** button.



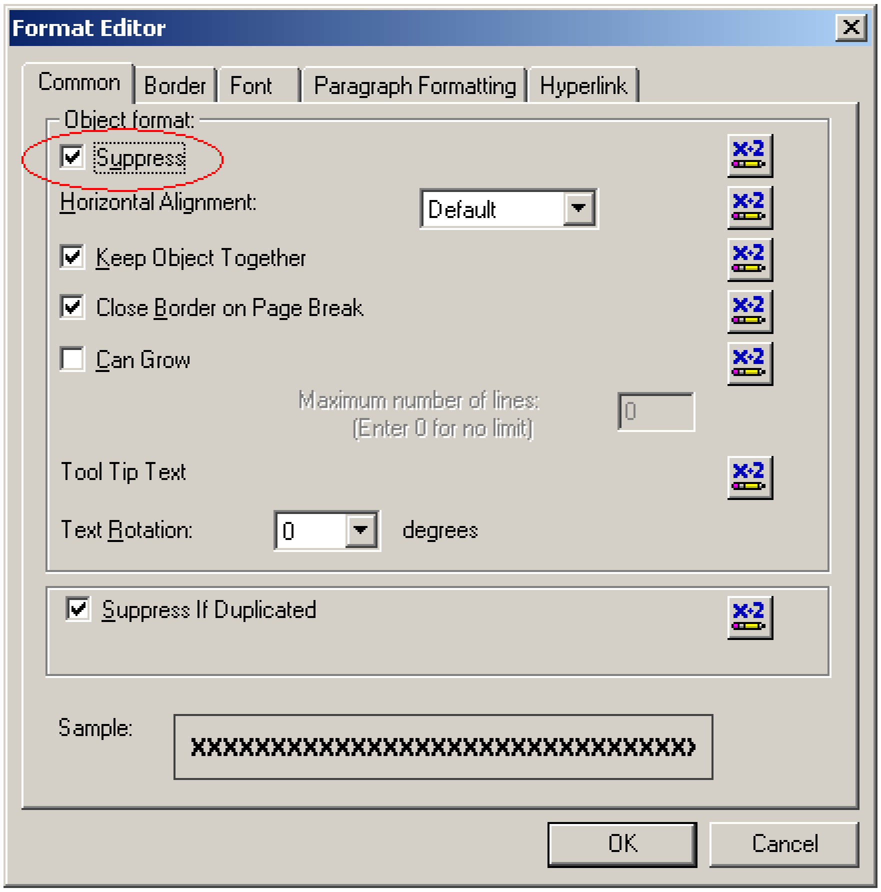
```
If Trim ({AreaInputs_ttx.AreaName}) = "Area 1" then crYellow else crRed
```

The script above will provide yellow trim for Area 1 and red for all others. Ensure that *Crystal Syntax* is selected. Save and Exit.

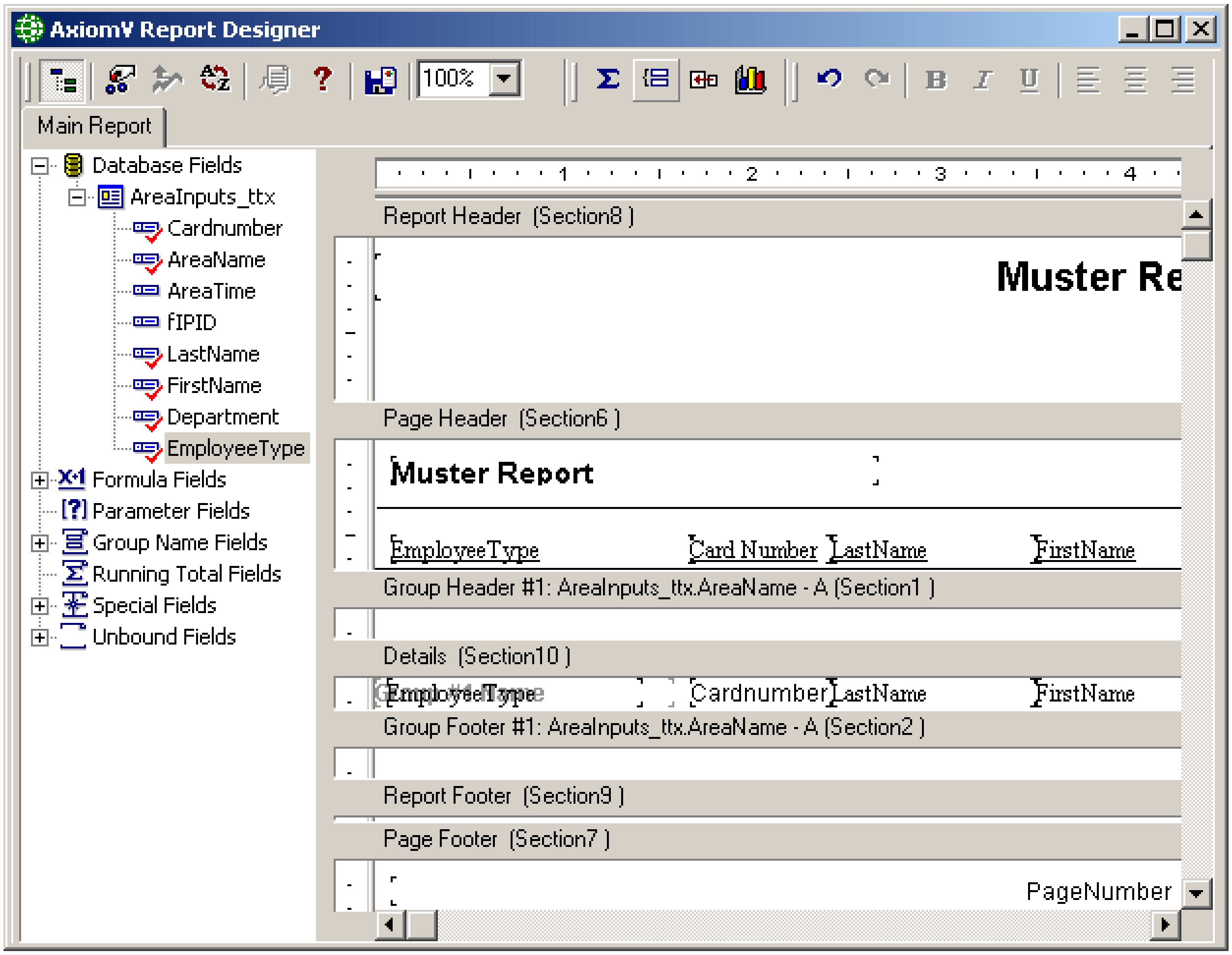
After setting up the trim hide the area names by selecting *Suppress* for the 'Group #1 Name' field. Select the field and right click. Click *Format*.



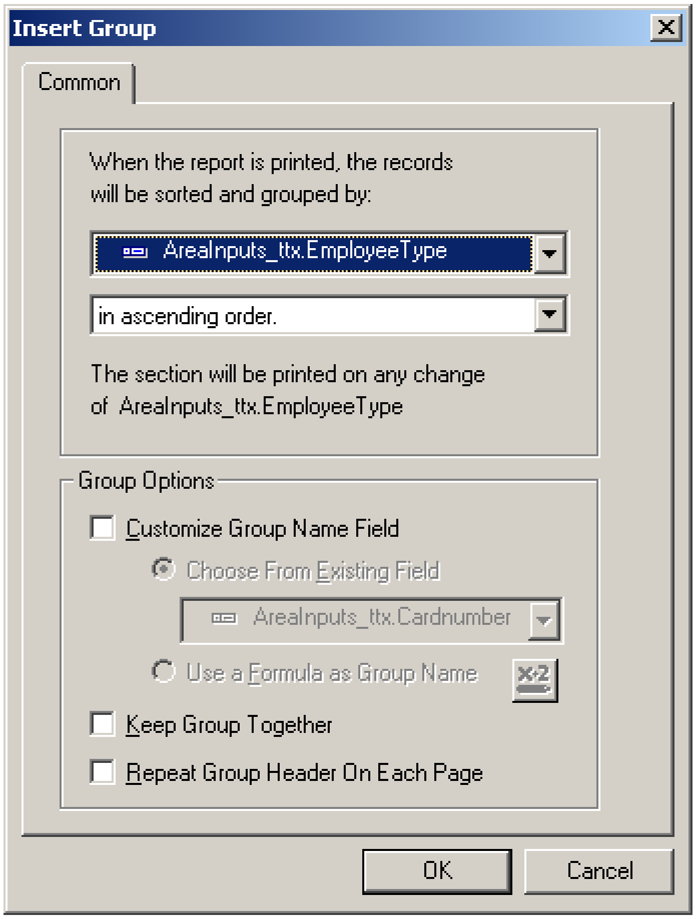
Check *Suppress* then click *OK*.



Create an *Employee Type* group. First drag and drop *Employee Type* into Section10 and edit it and its header for best fit, then click on the *Insert Group* button (⊟).


AxiomV Report Designer
100%
Main Report
Database Fields
AreaInputs_ttx
Cardnumber
AreaName
AreaTime
fIPID
LastName
FirstName
Department
EmployeeType
Formula Fields
Parameter Fields
Group Name Fields
Running Total Fields
Special Fields
Unbound Fields
1
2
3
4
Report Header (Section8)
Muster Re
Page Header (Section6)
Muster Report
EmployeeType
Card Number
LastName
FirstName
Group Header #1: AreaInputs_ttx.AreaName - A (Section1)
Details (Section10)
EmployeeType
Cardnumber
LastName
FirstName
Group Footer #1: AreaInputs_ttx.AreaName - A (Section2)
Report Footer (Section9)
Page Footer (Section7)
PageNumber

From the pull-down select *AreaInputs_ttx.Employee Type*.



When the report is printed, the records will be sorted and grouped by:

AreaInputs_ttx.EmployeeType

in ascending order.

The section will be printed on any change of AreaInputs_ttx.EmployeeType

Group Options

□ Customize Group Name Field

● Choose From Existing Field

AreaInputs_ttx.Cardnumber

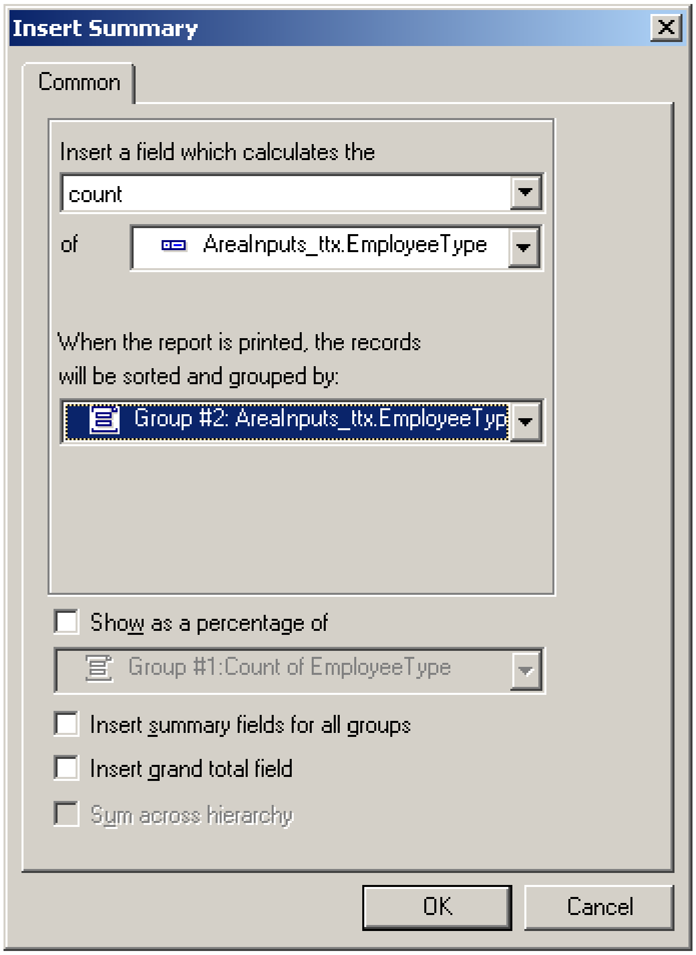
○ Use a Formula as Group Name

□ Keep Group Together

□ Repeat Group Header On Each Page

Click *OK* to create the group.

A total count of the cardholders in each area is added by clicking on the Σ (*Summary*) button. From the pull-downs select *Count* of *AreaInputs_ttx.Employee Type* and *Group #2: AreaInputs_ttx.Employee Type*. This will provide a total count for each Employee Type.



Insert a field which calculates the

count

of AreaInputs_ttx.EmployeeType

When the report is printed, the records will be sorted and grouped by:

Group #2: AreaInputs_ttx.EmployeeTyp

☐ Show as a percentage of

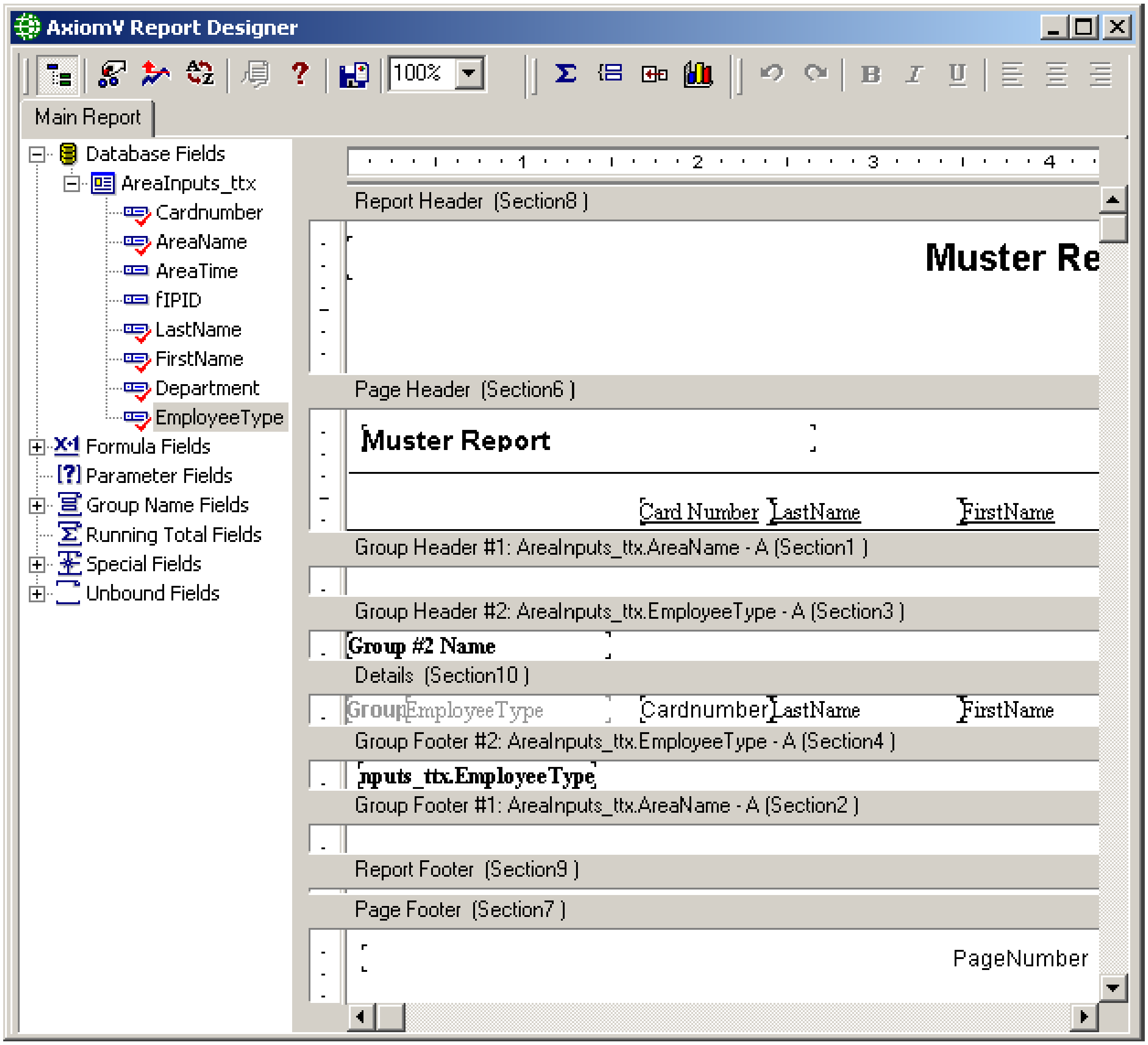
Group #1:Count of EmployeeType

☐ Insert summary fields for all groups

☐ Insert grand total field

☐ Sum across hierarchy

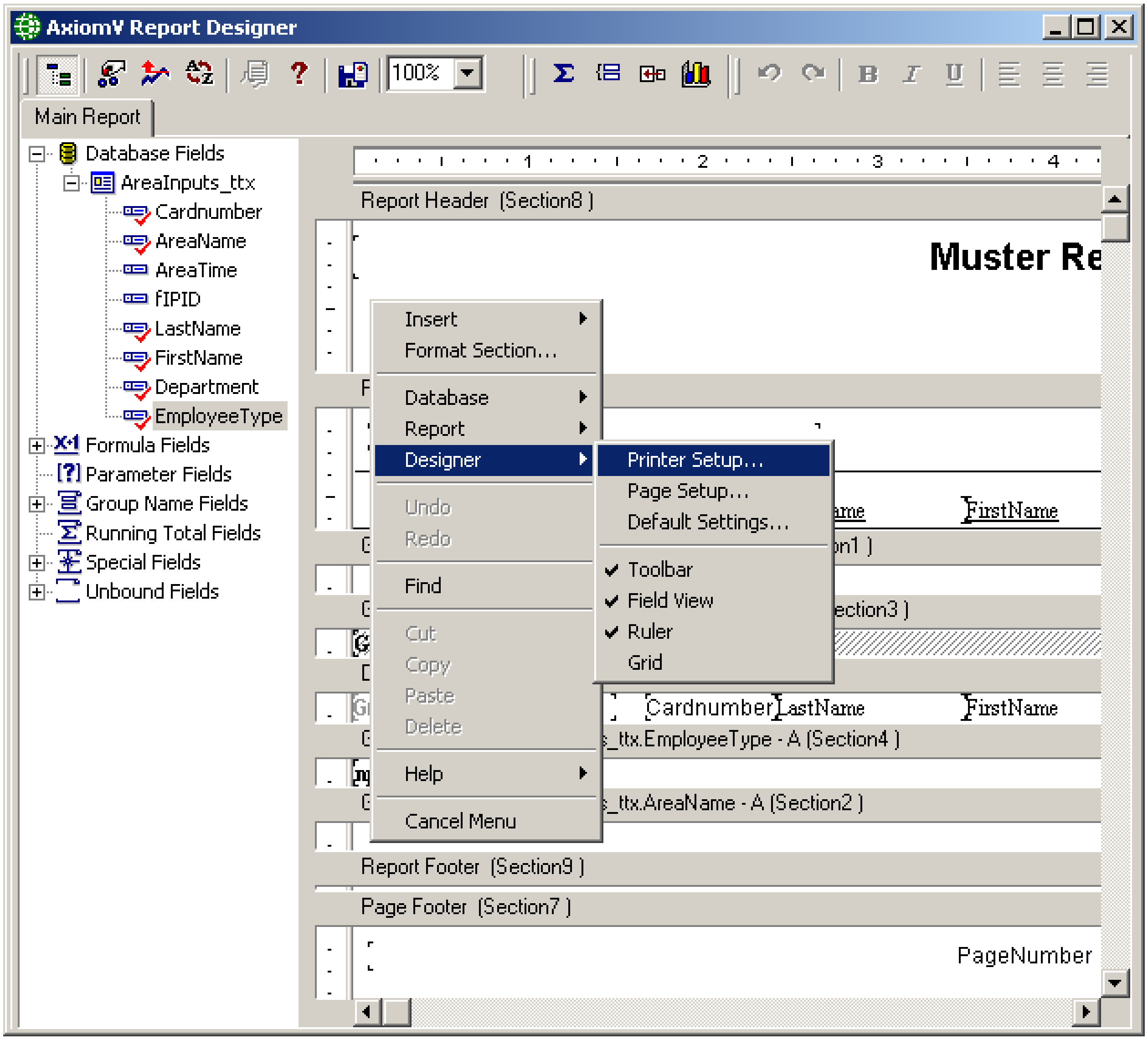
When you exit, save the report in the *Reports* folder of AxiomV™, then press *Refresh* in *Main Database Report Screen*. You'll see the report you just created.



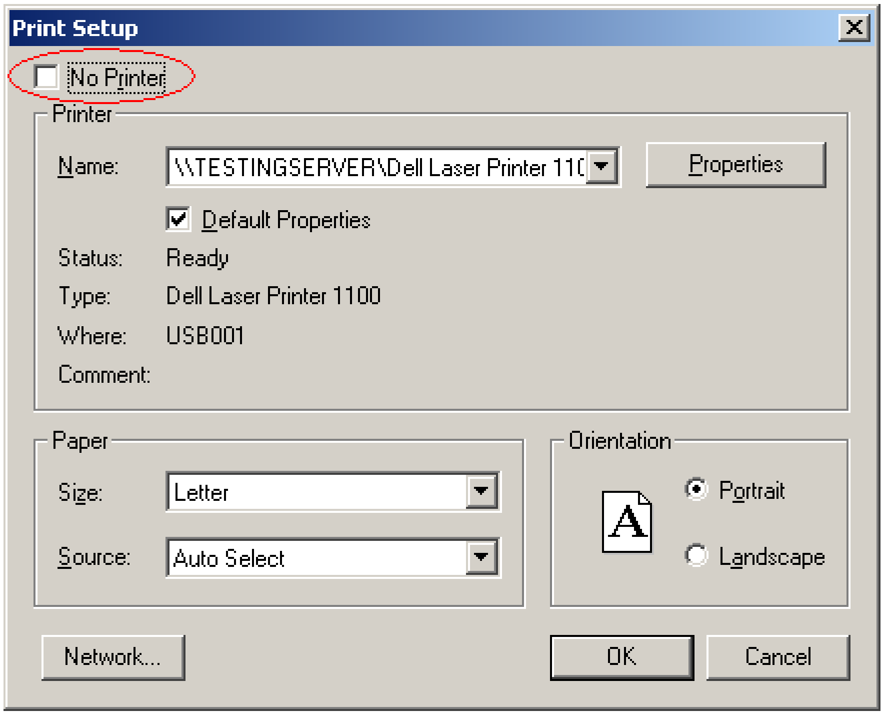
You can enhance the report by adding a text object [**Total** =] in Section4 as well as adjusting the position and size of any/all object to best display the report. Fonts can be changed, and underlines added, or bolded and/or italics.

Printer Setup

All new reports are configured without a printer selected. Right click on the report and select *Designer* / *Printer Setup* to set up a printer for your new report.



Uncheck the *No Printer* box and configure the printer settings that apply to this report on your system.



□ No Printer

Name: \\TESTINGSERVER\Dell Laser Printer 110

☑ Default Properties

Status: Ready

Type: Dell Laser Printer 1100

Where: USB001

Comment:

Size: Letter

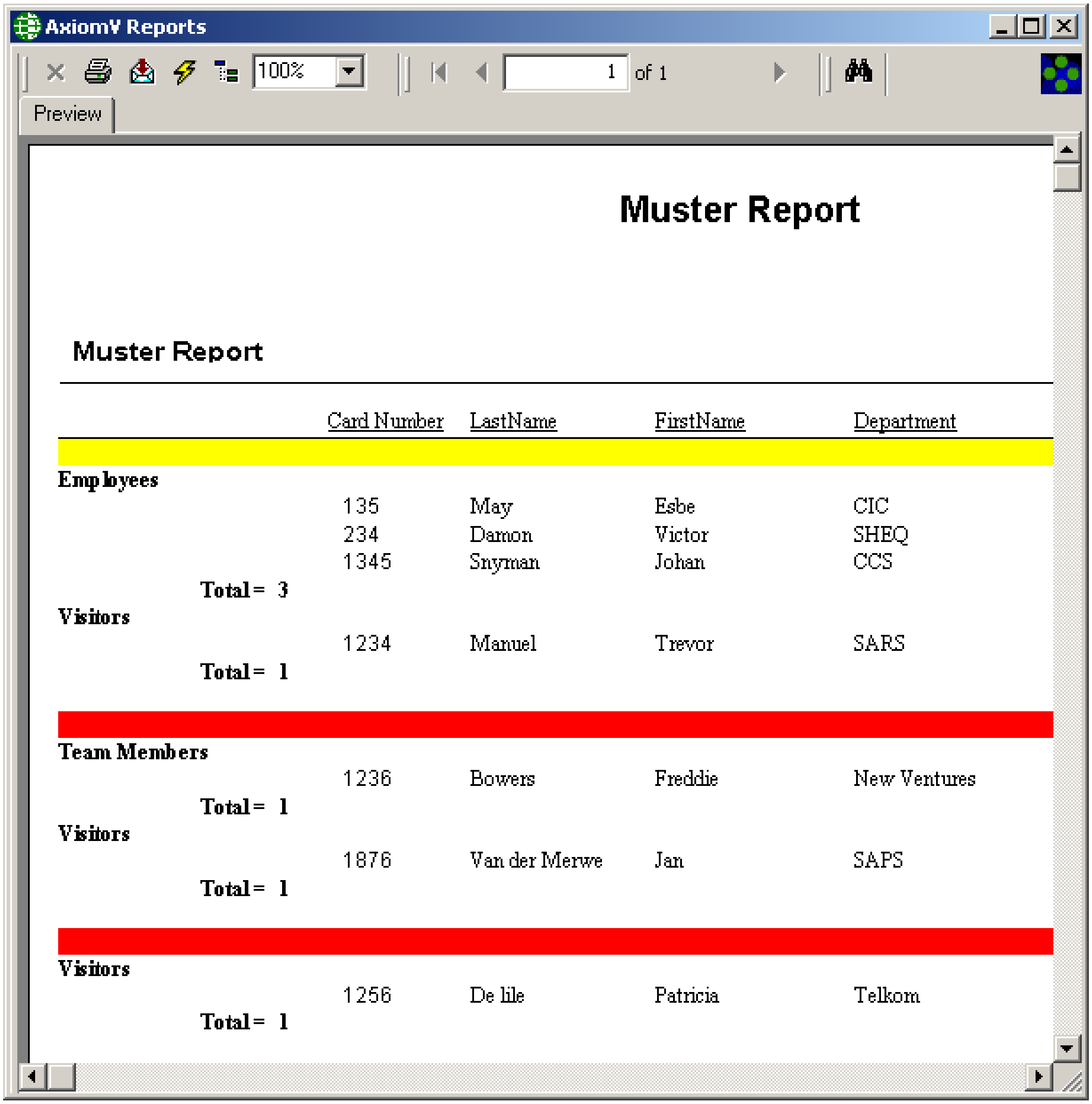
Source: Auto Select

● Portrait

○ Landscape

Sample Report

Here is a sample of the report we created.



Muster Report

Muster Report

		Card Number	LastName	FirstName	Department
Employees					
		135	May	Esbe	CIC
		234	Damon	Victor	SHEQ
		1345	Snyman	Johan	CCS
	Total = 3				
Visitors					
		1234	Manuel	Trevor	SARS
	Total = 1				
Team Members					
		1236	Bowers	Freddie	New Ventures
	Total = 1				
Visitors					
		1876	Van der Merwe	Jan	SAPS
	Total = 1				
Visitors					
		1256	De lile	Patricia	Telkom
	Total = 1				

Part 6

Appendix A

A new feature has been added to the AxiomV™ system making it possible to control the movement of assets through AxiomV™ access points. Assets will have an embedded credential readable at a distance. The position of the reader will be at a point where it will generate a signal prior to the exit point but not at the exit point. The asset reader will be connected in parallel with the access reader.

Asset Tracking[18]

An access point will be defined as an asset tracking point in order to turn on this feature. An asset will be defined in the database and will contain the information about the asset's owner. The owner will be a cardholder defined in the database.

When an asset is detected the access point will be locked for the "Asset Present Time" and the buzzer will beep three beeps per second. This is known as Asset Mode. A log message will be sent indicating the presence of the asset. If the timer times out another message will be generated indicating that the asset was not able to exit the access point. During the time period only the cardholder assigned to the asset (the owner) may exit the access point.

Operation Scenarios

Asset Tracking Normal Operation

1. The asset is detected followed by "Cardholder action: Asset at door: message.
2. The exit access point is placed into Asset Mode with the reader beeping in triplets.
3. The asset's owner is granted access "Access granted: Reader" with the owner's ID.
4. The asset is also granted access "Access granted: with asset" with the asset's ID.
5. When the access point is closed or the unlock times out the access point will be 'Locked' (even if it was previously unlocked or scheduled to be unlocked).

Asset Timeout

1. The asset is detected followed by "Cardholder action: Asset at door: message.
2. The exit access point is placed into Asset Mode with the reader beeping in triplets.
3. The asset owner fails to swipe within the Asset Present Time.
4. An alarm message "Access denied: Asset Timeout" is sent.
5. The access point is placed into High Security Mode "Cardholder action: high security ON.

[18] This selection is only available if the optional license for the Asset Tracking Software has been purchased and installed.

6. Only a supervisor or cardholder with high security privilege may be granted access after this time until the access point's High Security Mode is turned off.

Functionality

Asset Detected at Non-Asset tracking Point

At Least One 'Asset Door[19]' Defined on the NC100

If a reader that is not defined as an 'Asset Door[17]' detects an asset it will display the message "Cardholder action: Asset at Door", but no further action will be taken.

No 'Asset Doors[19]' Defined on NC100

If an asset is detected an access denied message will be logged, and no further action will be taken.

Using PIN Code

If you are using card + PIN schedule, the asset will trigger the *Asset Mode* and the user will have to enter a PIN code after swiping as usual. If PIN codes are allowed to be used instead of credentials by having card + PIN schedule off, the user will be found based upon the entered PIN.

Two Person Mode and Escort Required

Two Person Mode and *Escort Required Mode* are the only modes not allowed on an Asset Access point. All other modes are permitted.

Access Denied During Asset Mode

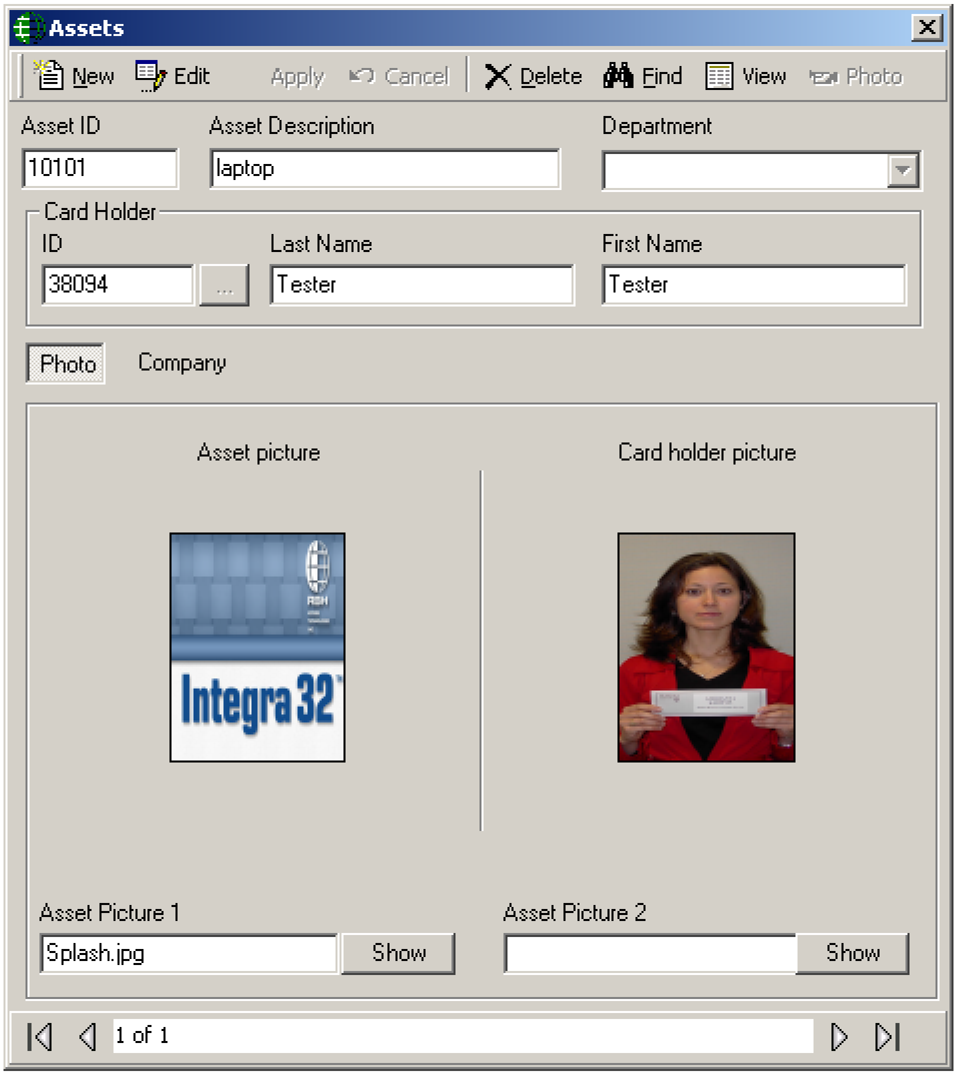
If access is denied while in Asset Mode the "Access Denied" message will be displayed and the beeper will continue. The timer will be reset to the Asset Timeout time after every wrong attempt is made. Even if the credential matches the Asset's owner, the cardholder must be granted access in order to proceed.

[19] An "Asset Door" is an Access Point of type *Asset Door* or of type *Asset Reporting*. These selections are only available if the optional license for the Asset Tracking Software has been purchased and installed.

Programming

Asset[20]

An Assets window is used for managing assets. Assets are saved as cardholders except that the card type will be Asset. The asset will not have an access level. It will be downloaded to panels, which have reader type "Asset Door" or "Asset Reporting".



Assets

Asset ID: 10101

Asset Description: laptop

Department:

Card Holder

ID: 38094

Last Name: Tester

First Name: Tester

Asset Picture 1: Splash.jpg

Asset Picture 2:

1 of 1

The Asset window has quick search on 'Asset ID', 'Asset Description', 'Cardholder ID', 'Last Name', and 'First Name' of Asset Holder.

[20] This selection is only available if the optional license for the Asset Tracking Software has been purchased and installed.

To input the owner select *Find* and search the database for the appropriate card to be the owner of the asset. The first name and last name (of the cardholder) associated with the card will be entered by the system. Company and Notes may also be added to the asset. By default the asset is assigned the same companies as its owner.

Access Point

Select the reader type as either ‘Asset Door’ or ‘Asset Reporting’ in the access point properties screen. This reader will work as a normal reader except when it detects an asset. When an asset is detected the access point will be placed into asset mode for the predefined “Asset Tracking Time”.

Appendix B

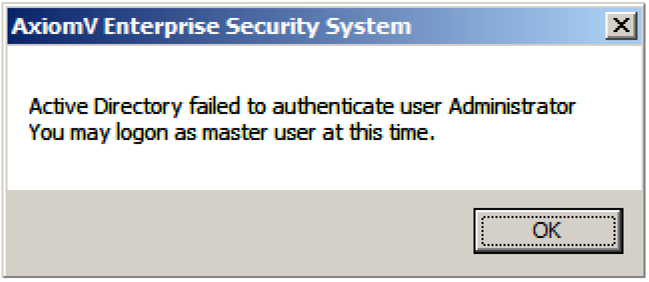
The *Active Directory* option can be added to make it quicker and easier to logon to the AxiomV™ system. Domain users can be added to the operator's list so that their Windows™ authentication can be used to logon to the AxiomV™ system.

Active Directory

Ensure that the *Active Directory* software has been installed and the license has been registered.

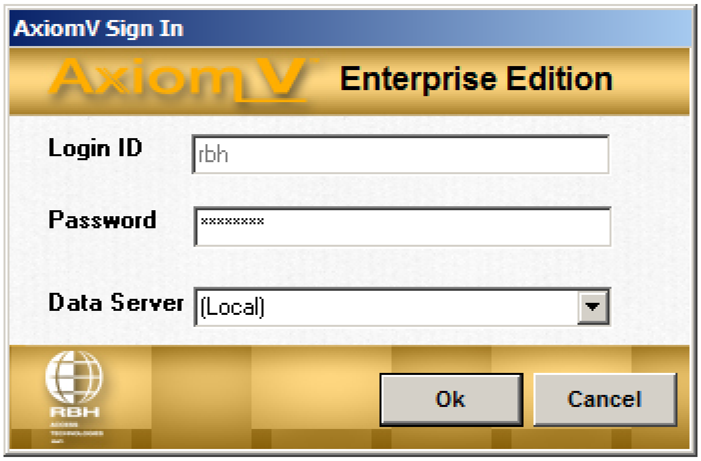
Setup

Only Windows™ users and the default 'rbh' user can logon to the AxiomV™ system. Since the current Windows™ user has not yet been added to the operator list you will have to login with the default 'rbh' user. If there are any other operators existing before the *Active Directory* option is added, these users can only be deleted. The AxiomV™ system will not allow them to be used to logon.



AxiomV Enterprise Security System

Active Directory failed to authenticate user Administrator
You may logon as master user at this time.



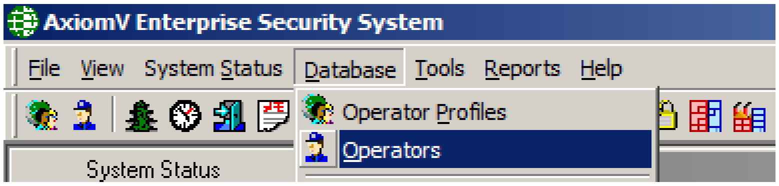
AxiomV Sign In

Login ID: rbh

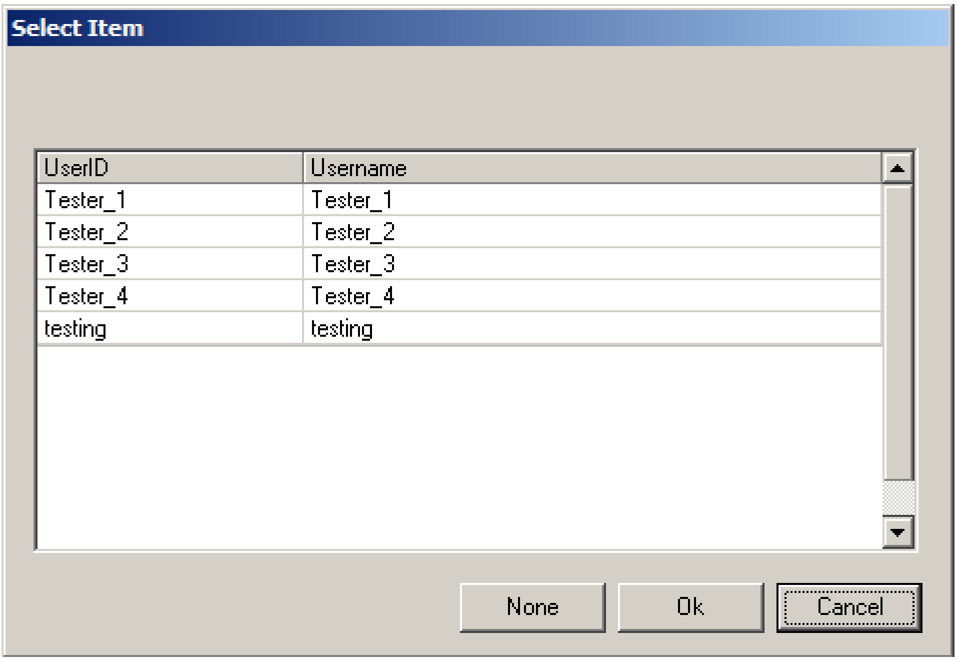
Password: *********

Data Server: (Local)

After you have logged-in go to Database\Operators to add a new operator.



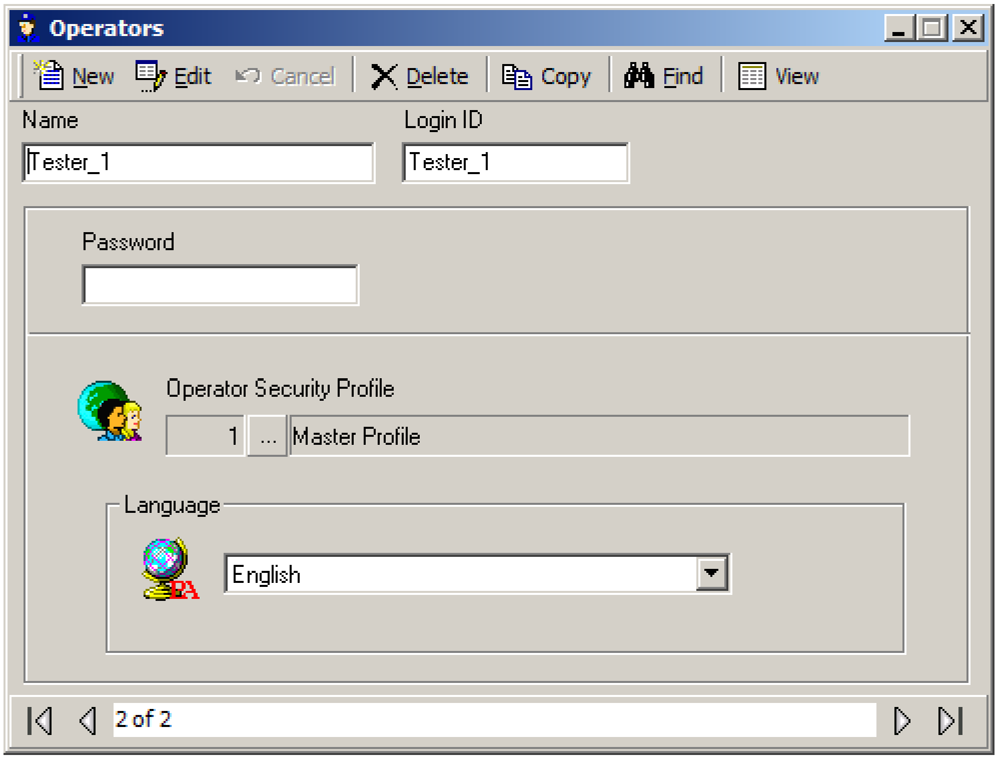
Selecting **NEW** will bring up a list of Windows™ users to be selected from.



UserID	Username
Tester_1	Tester_1
Tester_2	Tester_2
Tester_3	Tester_3
Tester_4	Tester_4
testing	testing

Login ID and Password are disabled in the AxiomV™ system since these are being taken from Window's™ users. The Log Off and Log In buttons have been removed because they are not required.

The *Active Directory* option will also disable the keyboard time feature so the system won't logout itself, the user must logout.



Name: Tester_1

Login ID: Tester_1

Password:

Operator Security Profile: 1 ... Master Profile

Language: English

2 of 2

If *Active Directory* is not available for any reason, the AxiomV™ will only allow the default 'rbh' user to logon.

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. Words that appear in Italics are also defined in this glossary.

.wav File .wav is a standard audio file format that AxiomV™ can attach to particular events thereby providing unique audio annunciation of events to operators.

Access Code Numeric data entered into a keypad to verify authorized entry into a controlled area.

Access Control A method by which you control and/or monitor entry of persons, vehicles or objects into and out of physical locations.

Access Point A point of entry or exit, for an *area* whose access is controlled and monitored by AxiomV™. (E.g. a door or parking gate.)

Alphanumeric All characters A through Z and 0 through 9 that may be used to form an Access Code.

Antipassback (APB) An Access Control feature designed to prevent improper usage of a valid card. AxiomV™ provides three types of Antipassback control: Reader Antipassback, Timed Antipassback, and Area Antipassback.

Antipassback (Reader) Reader Antipassback prevents users from sharing their card with another user and allowing them to gain access to controlled area that they are not authorized to enter. Reader Antipassback works by comparing the area the cardholder is reading into against the last APB area read into by the cardholder. If they match, then a Reader Antipassback violation has occurred.

Antipassback (Area) *Area Antipassback* is even more restrictive than *Reader Antipassback*, and prevents users from moving through a building without reading as they go. *Exit Area Antipassback* works by comparing the area the cardholder is reading out of against the last area read into by the cardholder. If they do not match, then an *Exit Area Antipassback* violation has occurred.

Antipassback (Timed) Timed Antipassback prevents a cardholder from reading at the same reader more than once within a predefined period of time.

Antipassback (Global) Antipassback tracked across multiple NC100s is called *Global Antipassback*. *Global Antipassback* must be enabled when the number of adjacent areas to be defined requires more than 8 readers.

ASCII An acronym for the American Standard Code for Information Interchange. It is a code in which the numbers from 0 to 255 represent letters, numbers, punctuation marks, and other characters. ASCII Code is standardized top facilitate transmitting text between computers or between a computer and a peripheral device.

Area A predefined physical location with borders and *Access Points* controlled and monitored by AxiomV™.

Baud Rate The speed at which data is sent through a communications cable. The baud rate is measured in bits per second (bps).

Bit The abbreviation for binary digit (0 or 1) in the binary number system.

Card Reader A device that scans or reads encoded information contained on an Access Card.

Client The client application software in an AxiomV™ system. In a stand-alone installation, both the client and server applications are run on the Host PC.

C-Net The abbreviation for Controller Network in an AxiomV™ system. The C-Net is a high-speed fault tolerant ring network that connects up to 15 NC100 controllers. Each C-Net is connected to a single communication port on the host PC via the Master Controller.

Device Any apparatus that monitors or controls an input or output point.

Device Controllers Controllers to which all input and output devices are connected in an AxiomV™ system. RC2's and IOC16's are both device controllers.

Display Language The language in which Access Control screens and messages are displayed for the user.

D-Net The abbreviation for Device Controller Network in an AxiomV™ system. A *D-Net* is a high-speed fault tolerant ring network that may connect up to 4 RC2 controllers and 16 IOC16 controllers and/or up to 255 Keypads to a NC100.

Ethernet 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.

Flash Memory Semiconductor memory that can operate as ROM, but on an activating signal, can rewrite its contents as though it was RAM. AxiomV™ NC100, RC2 and IOC16 controllers use flash memory.

Holiday Any day on which the regular weekly AxiomV™ Schedule is not appropriate. Statutory holidays and summer shut down periods are two examples. In AxiomV™, Holidays may be assigned special irregular Schedules that override the regular Schedule for that day.

Input Any field apparatus that provides information to an AxiomV™ system with respect to conditions or status of a monitored component. Examples include door contacts, thermometers etc.

Installer An employee of an RBH Authorized Dealer/Integrator, who installs, configures or services AxiomV™ systems in the field.

IP Address The abbreviation for Internet Protocol address. A 32-bit (4-byte) binary number that uniquely identifies a host computer connected to the Internet to other Internet hosts, for the purposes of communication through the transfer of packets. An IP address is expressed in “dotted quad” format, consisting of the decimal values of its four bytes, separated with periods, for example, 127.0.0.1. The first one, two, or three bytes of the IP address, assigned by InterNIC Registration Services, identify the network the host is connected to; the remaining bits identify the host itself.

Keypad Push-button numeric device used to enter a PIN code or an Access Code.

LED The abbreviation for Light Emitting Diode.

Master NC100 The NC100 controller that occupies the first position in a C-Net network and is connected to the Host PC via a serial or Ethernet connection. Communications from any controller on the C-Net must pass through the Master NC100.

Mustering An Access Control function that allows an operator to inquire on demand as to the whereabouts of all cardholders in an AxiomV™ system.

NC100 The NC100 is an intelligent communication controller in an AxiomV™ system. The NC100 manages communications between the PC and Device Controllers, and stores all configuration parameters locally. This allows all AxiomV™ systems to function fully without the Host PC online.

Operator Any individual authorized to log-on to the AxiomV™ system for purposes of data-entry or monitoring.

Output Any field apparatus that receives commands from an AxiomV™ system and executes the action specified in the command. (Examples include door locks, and lights.)

Parallel Port A parallel port sends data from device to another, in parallel lines (i.e., all bits at one time).

PIN Personal Identification Number.

RAM The abbreviation for Random Access Memory. Semiconductor-based memory that can be read and written by the CPU or other hardware devices.

ROM The abbreviation for Read Only Memory. Any semiconductor circuit serving as a memory that contains instructions or data that can be read but not modified, regardless of whether it was placed there by a manufacturer or by a programming process.

RTE Request to exit.

Serial Port An input/output location (channel) that sends and receives data to and from a computer's central processing unit or a communications device one bit at a time.

Server The server application software in an AxiomV™ system.

Schedule A Schedule (e.g. Business Hours) is a pre-defined time slot/day combination that may be assigned to Access Points, Inputs, Outputs and Cardholder Modes and Privileges, thereby governing how the AxiomV™ system operates from day to day.

Slave NC100 NC100 controllers that occupy positions 2 through 15 in a C-Net network. Communications between Slave NC100's and the Host PC must pass through the Master NC100.

System Administrator The person responsible for creating, maintaining, and controlling the AxiomV™ Database.

TAPI 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.

TCP/IP Transfer Control Protocol/Internet Protocol. TCP/IP is the protocol that networks use to communicate with each other on the Internet.

License & Warranty

Notice 1.01

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

Reader Comments