



Integrated Access Control and Security Management System

**new innovative
building security**



USER MANUAL

Copyright and Trademarks

Copyright© 2015-2019 RBH Access Technologies Inc.

All rights reserved. Printed in Canada. No part of this book may be used or reproduced, or stored in any form by any means, without the prior written consent of RBH Access Technologies Inc.

RBH constantly seeks to innovate and improve on the functionality and reliability of the AxiomXA™ 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, or damage caused or alleged to have been caused directly or indirectly by the AxiomXA™ system.

AxiomXA™ is the trademark of RBH Access Technologies Inc.

RBH ACCESS TECHNOLOGIES INC.

2 Automatic Road, Suite 108

Brampton, Ontario

CANADA

L6S 6K8

Printing Date 8 July 2019

Table of Contents

| | |
|---|----------|
| ABOUT THIS GUIDE | 1 |
| <i>Before reading this guide</i> | 1 |
| <i>Conventions in this guide</i> | 2 |
| PART 1 | 3 |
| CHAPTER 1 INTRODUCING AXIOMXA™ | 4 |
| PART 2 | 6 |
| CHAPTER 2 BEFORE INSTALLING AXIOMXA™ | 7 |
| <i>PC Requirements</i> | 7 |
| Server | 7 |
| Client | 7 |
| <i>LAN Communications</i> | 8 |
| Server to Client | 8 |
| <i>Before You Install AxiomXA™</i> | 8 |
| <i>Installing AxiomXA™ on Your Computer</i> | 8 |
| <i>License Registration</i> | 8 |
| PART 3 | 9 |
| CHAPTER 3 GETTING TO KNOW AXIOMXA™ | 10 |
| <i>Data Entry Objects</i> | 10 |
| <i>General Screen Operations</i> | 12 |
| Search Window | 14 |
| Headers | 15 |
| Command Bar | 19 |
| Commands | 20 |
| CHAPTER 4 CONCEPTS | 21 |
| <i>Access Control</i> | 21 |
| <i>Access Level</i> | 21 |
| <i>Access Point</i> | 21 |
| <i>Alarms</i> | 21 |
| <i>Antipassback (APB)</i> | 21 |
| Hard and Soft Antipassback | 22 |
| Timed Antipassback | 22 |
| Reader Antipassback | 22 |
| Area Antipassback | 22 |
| Global Antipassback | 23 |
| <i>Area</i> | 23 |
| <i>C-NET Controller Network</i> | 24 |
| <i>Connection Types</i> | 24 |
| <i>NC100 Network Controller</i> | 24 |
| <i>UNC100 Network Controller</i> | 24 |
| <i>UNC100-Keypad Network Controller</i> | 24 |
| <i>UNC500 Network Controller</i> | 25 |
| <i>D-NET Device Network</i> | 25 |
| <i>RC2/NIRC/NURC Reader Controller</i> | 25 |
| <i>IOC16 Input / Output Controller</i> | 25 |
| <i>IOC8 Input / Output Controller</i> | 25 |

| | |
|--|-----------|
| <i>Holidays</i> | 25 |
| <i>Schedules</i> | 26 |
| PART 4 | 27 |
| CHAPTER 5 MONITORING SECURITY ACCESS | 28 |
| <i>Client Log In</i> | 28 |
| Log In | 28 |
| Tile View | 30 |
| Standard View | 30 |
| Log Off | 31 |
| Selections | 32 |
| View ▼ | 32 |
| System Status ▼ | 33 |
| Database ▼ | 35 |
| Tools ▼ | 40 |
| Reports ▼ | 42 |
| System Settings ▼ | 43 |
| Themes | 43 |
| <i>Tools</i> | 45 |
| Custom Fields | 45 |
| Cardholder | 45 |
| Visitors | 47 |
| Badge Templates | 48 |
| Copy Wizard | 50 |
| Import | 52 |
| Backup | 54 |
| Restore | 58 |
| Void Cards | 61 |
| <i>System Settings</i> | 62 |
| System | 62 |
| AP Activity | 62 |
| System Settings | 63 |
| Color Settings | 65 |
| Email Configuration | 66 |
| Message Sounds | 67 |
| Badge | 68 |
| User | 70 |
| General | 70 |
| Display | 71 |
| • <i>View</i> | 72 |
| Event Viewer | 72 |
| Card Monitor | 73 |
| Area Monitor | 73 |
| Alarms Monitor | 74 |
| Access Point Activity | 78 |
| CHAPTER 6 SYSTEM STATUS | 80 |
| <i>Networks</i> | 80 |

| | |
|--------------------------------------|-----------|
| <i>Controllers</i> | 82 |
| <i>Device Controllers</i> | 85 |
| <i>Access Points</i> | 86 |
| <i>Inputs</i> | 88 |
| <i>Outputs</i> | 90 |
| <i>Apartments</i> | 92 |
| <i>Access Point Groups</i> | 94 |
| <i>Output Groups</i> | 94 |
| <i>Input Groups</i> | 94 |
| <i>Guard Tours</i> | 94 |
| PART 5 | 95 |
| CHAPTER 7 | 96 |
| <i>Database</i> | 96 |
| Operators | 96 |
| Operator Profiles | 98 |
| Holidays | 100 |
| Holiday Designation | 101 |
| Schedules | 102 |
| Schedule Tips | 103 |
| Areas | 107 |
| Facility Codes | 108 |
| Hardware Setup | 110 |
| Networks | 110 |
| Network Controllers | 114 |
| Device Controllers | 117 |
| IOC16 Input Output Controllers | 119 |
| IOC8 | 120 |
| Keypad | 121 |
| Alarm Panel | 126 |
| Access Points | 130 |
| Inputs | 138 |
| Outputs | 141 |
| Non Reader Access Points | 145 |
| Elevators | 148 |
| Elevator Floor Groups | 150 |
| Access Point Groups | 151 |
| Access Levels | 153 |
| CCTVs | 157 |
| Input Groups | 159 |
| Output Groups | 161 |
| Interlock Groups | 164 |
| Companies | 166 |
| Cardholders | 167 |
| Cardholder Properties | 168 |
| Card Properties | 173 |
| Cardholder Types | 181 |

Table of Contents

| | |
|-----------------------------------|------------|
| Assets | 182 |
| Reader Access | 184 |
| Visitors | 185 |
| Departments | 187 |
| Bio Readers | 188 |
| Axiom Links | 190 |
| AxiomLinks™ Command Summary | 193 |
| Global Commands | 194 |
| Messages | 195 |
| Message Ports | 198 |
| Maps | 199 |
| Guard Routes | 203 |
| Guard Groups | 205 |
| Guard Tours | 206 |
| CHAPTER 8 REPORTS | 207 |
| <i>History Reports</i> | 207 |
| General | 208 |
| <i>Database Reports</i> | 210 |
| General | 210 |
| PART 6 | 212 |
| GLOSSARY | 213 |
| LICENSE & WARRANTY | 218 |
| INDEX | 219 |
| NOTES | 222 |

About This Guide

This guide documents how to install and use the AxiomXA™ Integrated Access Control and Security Management System as developed by RBH Access Technologies Inc. AxiomXA™ 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 access using AxiomXA™
- A system administrator who updates AxiomXA™ databases.
- A system engineer who installs and configures AxiomXA™ 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 AxiomXA™. |
| Part 2 | Read Part 2 for information on how to install and setup AxiomXA™. Part 2 is intended for the installing Dealer. |
| Part 3 | Read Part 3 to get to know AxiomXA™. 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 AxiomXA™ 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 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**.

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 cursor changes to move to that place in the manual.



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 AxiomXA™

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

AxiomXA™ combines access control, building management, and security monitoring in a highly integrated and expandable system. AxiomXA™ runs on a standard IBM compatible PC using Windows 8.1 or higher operating Systems 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 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 and a single reader controller 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 Network Controllers 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 AxiomXA™ are extensive and are presented in the familiar Windows NT User Manager format. The system database can be separated into “logical sites(networks)” 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 AxiomXA™ 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.

AxiomXA™ 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.

AxiomXA™ 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 AxiomXA™ 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 for commands to control system inputs, outputs, and access points. A major application of AxiomLinks™ is in building management.

AxiomXA™ provides extensive elevator control features, allowing control of any building elevator setup. The elevator control board provides fail-safe operation with a fire alarm input.

Comprehensive event handling and logging combined with customizable history and system reports making recording and examining system information a simple task. The AxiomXA™ 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.

AxiomXA™ 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 alarms and which actions to take. Additionally, graphics maps display the exact location of the alarm and an on map icon shows the type of alarm. AxiomXA™ 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. The client server database is more powerful than the file database. This provides the system with even more flexibility.

Part 2

Chapter 2

Before Installing AxiomXA™

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

PC Requirements

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

Server

| Requirement | Description |
|--------------------------------------|--|
| <i>Operating system</i> ¹ | Microsoft Windows 8.1, 10, Server 2012, 2012R2, and Server 2016. |
| <i>Microprocessor</i> | Intel Core i7 3.4 GHz |
| <i>Memory</i> | 16GB (minimum), 32GB (recommended) |
| <i>Hard disk space</i> | 16GB (Installation), 200GB free space (to run) |

Client

| Requirement | Description |
|--------------------------------------|--|
| <i>Operating system</i> ¹ | Microsoft Windows 7SP1, 8.1, 10, Server 2008 R2, 2012, 2012R2, and Server 2016 |
| <i>Microprocessor</i> | Intel Core i7 3.4 GHz |
| <i>Memory</i> | 8GB (minimum), 16GB (recommended) |
| <i>Hard disk space</i> | 8GB (Installation) |

¹ Only 64 bit operating systems are supported, and 'Home' versions of operating systems are not supported. **All operating systems should be up to date with windows updates.**

LAN Communications

Server to Client

Ensure that the following services have been setup:

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

Before You Install AxiomXA™

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

1. That you have installed and connected all hardware as described in the AxiomXA™ Hardware Installation Manual.
 2. Verified that your computer meets the requirements listed in the table in *PC Requirements*.
-

Installing AxiomXA™ on Your Computer

See Technical Bulletin *AxiomXA Install-Uninstall.pdf* for installation information.

License Registration

There are optional modules for the AxiomXA™ system that require the purchase and installation of a license for them to work. They are: Alternate Master Network controllers, Asset Tracking, Badging, Bio-Reader integration, CCTV integration, Card Import Utility, Customize Report Designer, Guard Tour, and History Report Scheduler. To register and activate your license, please follow the guidelines from *AxiomXA Registration Activation.pdf*. The type and description of the license will show as the title of AxiomXA client's screen.

Part 3

Chapter 3

Getting to Know AxiomXA™

AxiomXA™ 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. Therefore AxiomXA™ can look different on other client machines, but will have the same powerful capabilities.

Data Entry Objects

This section describes Data Entry and Navigation conventions used throughout the AxiomXA™ software package. Some of these tools include: *Spin Buttons*, *Check Boxes*, *Radio Buttons*, and *Slide Bars*.

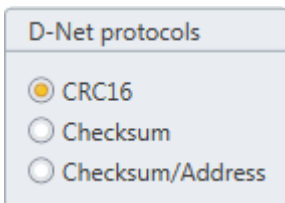


Use *Spin Buttons* to increase or decrease the value in the adjoining box.

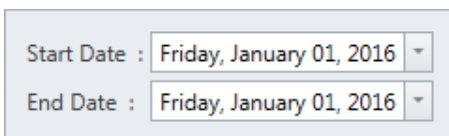
Send Email as visitors checks in :

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

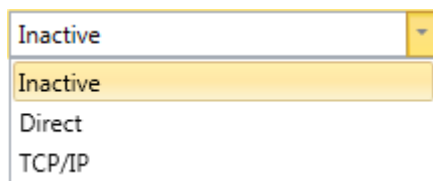
Using Exchange Server :



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.



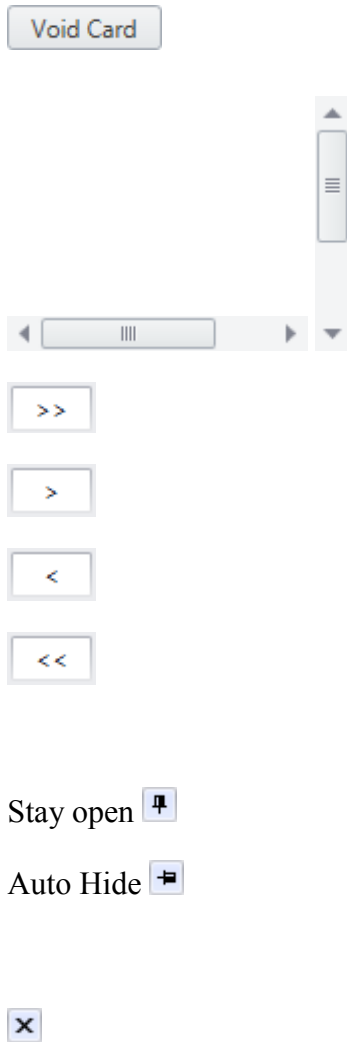
Date Field. AxiomXA™ uses the date format selected in the Windows operating system under *Control Panel – Regional Settings*. Dates can be either typed in or selected from the pull down calendar.



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.



Entry is blank, data is required (**mandatory field**).



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

Slide Bars adjusts the view of a window that is too large for the space provided for it. Click on and drag the *Slider Bars* to see the hidden portions of the window.

Select all items.

Select highlighted items

Remove highlighted items

Remove all items

Auto Hide minimizes a sub-window to a label on the edge of a window. When the cursor is moved over the label the sub-window is re-opened and closes again when the cursor is moved off. Clicking on the label will keep the sub-window open until somewhere other than the sub-window is clicked. Click on the icon again to keep the sub-window open.

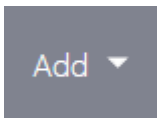
Close the window.

General Screen Operations

Windows in the system may have the following controls attached, and operate in a similar manner. Only controls appropriate to the section selected will be available. Greyed-out controls are non-functioning. This is likely due to multiple items being selected and the control only functioning with single selections. *Tile View* has associated icons for the operations while *Standard View* does not.



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



Add will add a new item. A means will be provided to select which item is to be added.



Add New adds a new record.



Edit Selected allows changes to be made to the current record.



Print?



Font?



Refresh?



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



Click *Save* after editing to save changes made.



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



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 50 of Chapter 5.



Select the ***Biometric*** button to manage a cardholder's biometric data.



Search Data bring up the search window.



Click ***Apply*** to save any changes that were made without exiting the record.



Click ***Connect to Device*** to connect to the selected item.

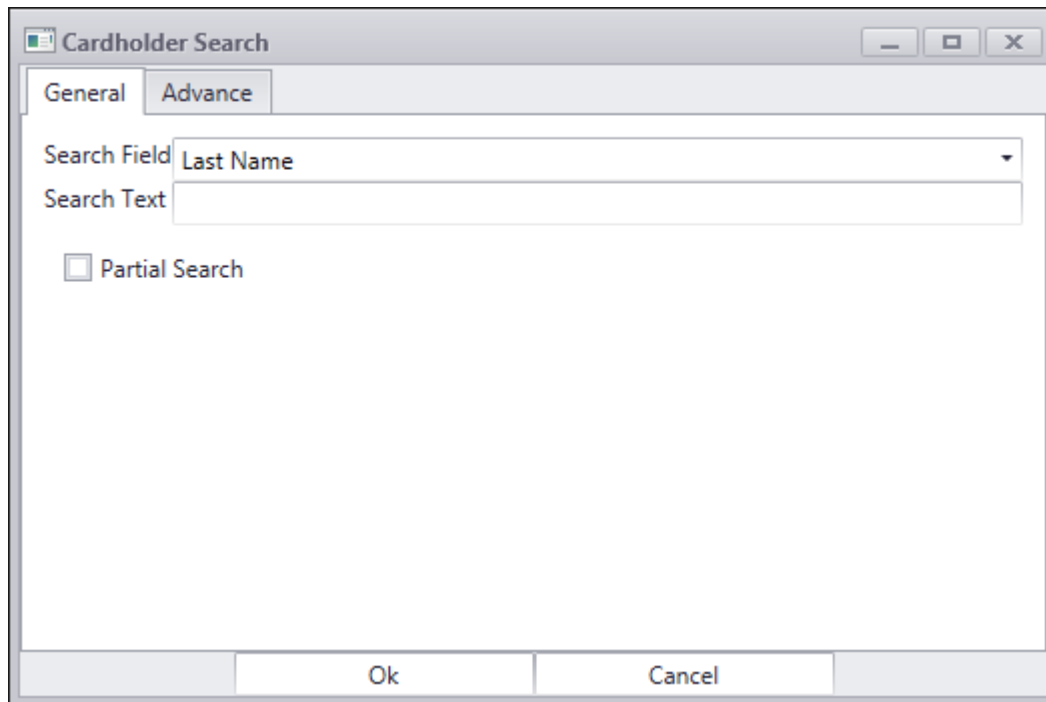


Click ***Download*** to download data to the selected item.

Search Window

The *Search Window* is only used to search for people (cardholders and visitors).

General



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 than searching under access points.

Search Text

Enter the criteria for the search in this box. Leaving the *Search Text* box empty will bring up all cardholder or visitor records.

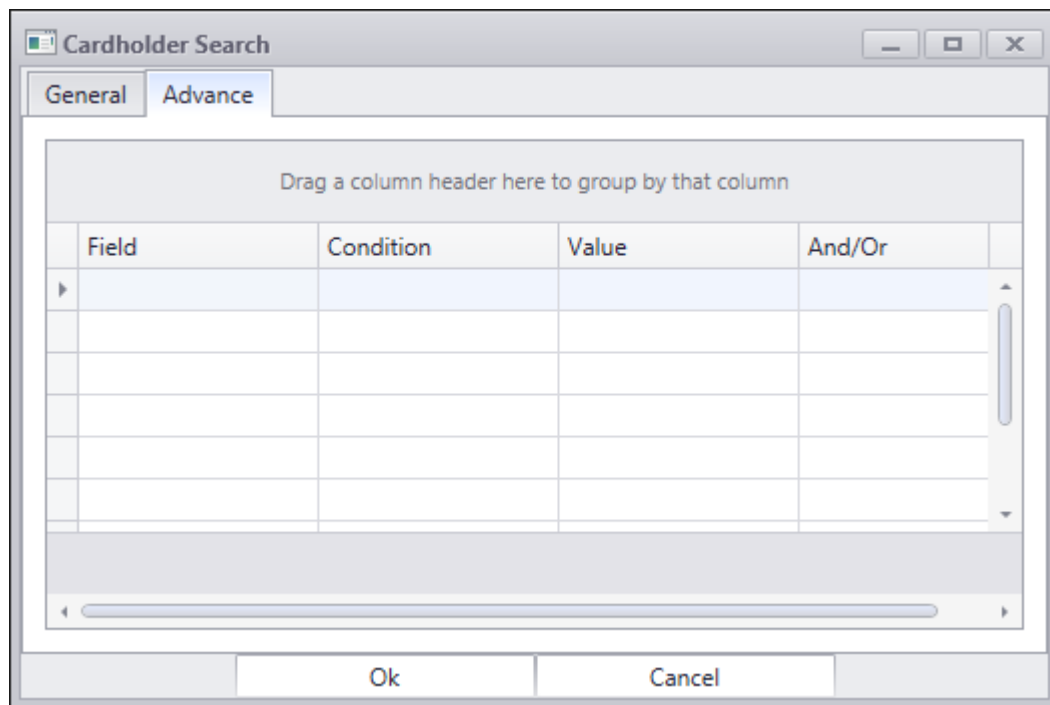
Partial Search

A partial search will look for the text anywhere within the field (e.g. “net” will find “direct network”). For an exact search don’t check *Partial Search*.

Ok

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

Advanced



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

Click on the *Field* box and pull down the list of available selections.

Under *Condition* select “=” equals, doesn’t equal “<>”, or “Like” (partial search).

Enter your desired search information under *Value*.

Finally select the conjunction for the current line to the next line (AND or OR).

Headers

Move your cursor along the headers. When the cursor is moved just right of a header’s label a filter icon (🔍) will appear, click the icon to reveal a list of filter options for that header.

Clicking a header will switch it between Sort Ascending and Sort Descending, as indicated by the triangle at the right end of the header. The display can only be sorted by one header at a time. Clicking on a different header will remove the sorting from the previous header.

Right click a header to bring out a pop-up menu. Pop-up menus will also appear when you right click on a line on the screen. The menu items will vary depending on which screen you are in. Some menu selection will have submenus.

Header Commands



Full Expand

Click on *Full Expand* to show all the lines under every grouping.



Full Collapse

Click on *Full Collapse* to hide all the lines under every grouping.



Sort Ascending

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



Sort Descending

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



Clear Sorting

Click on *Clear Sorting* to remove any sorting and return the sorting and the lines will be displayed as they were received.



Group by This Column

Click on *Group by This Column* to have the lines grouped by the currently selected column. When the *Group Panel* is shown you can drag headers on and off it instead of using the menu items. The example below shows event messages grouped by the message.

| Events | | |
|-----------|--------|------------|
| Message ▾ | | |
| Date | Device | Cardholder |

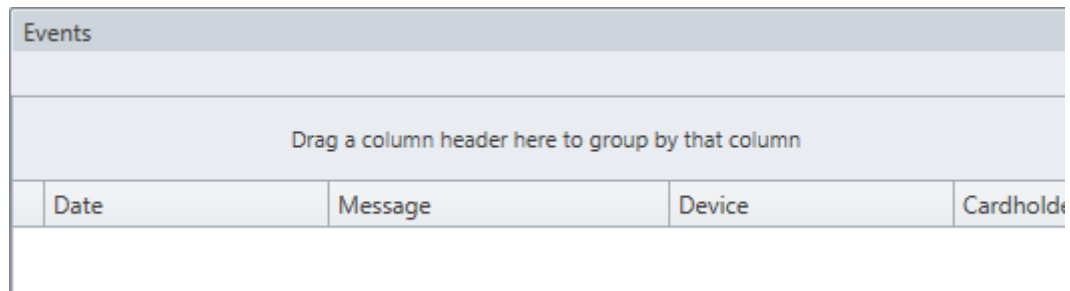


Ungroup

Click on *Ungroup* to remove the grouping.

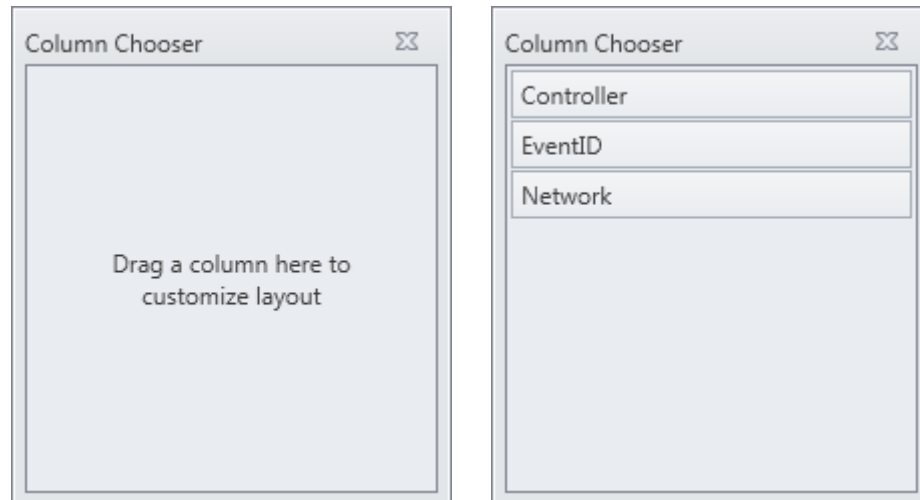
Show Group Panel / Hide Group Panel

The Group Panel is located in the space just above the headers, as shown below. When the Group Panel is shown you can drag headers onto and off it or use the menu items, Group by This Column or *Ungroup*.



Show Column Chooser

The *Column Chooser* allows you to customize the screen's display by selecting/deselecting which columns are to be included on the screen.



Drag column headers onto or off the *Column Chooser* to customize your display. At any time you can drag a header into a new position to set the headers in an order of your choosing.

Best Fit

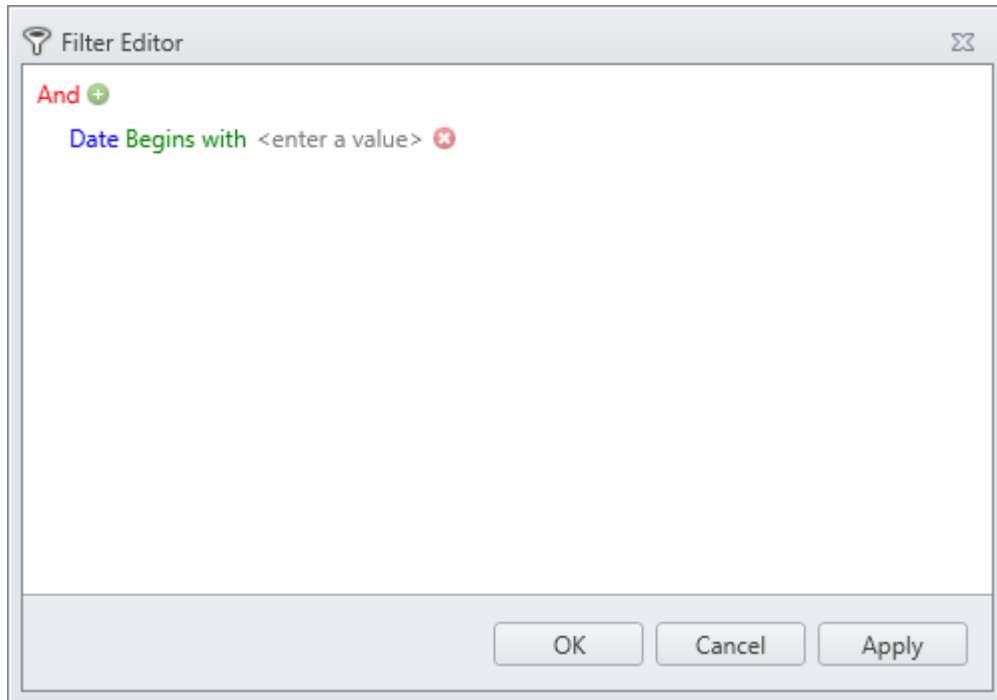
Best Fit resizes the current column to better fit the text.

Best Fit (all columns)

Best Fit (all columns) resizes all columns to better fit the text.

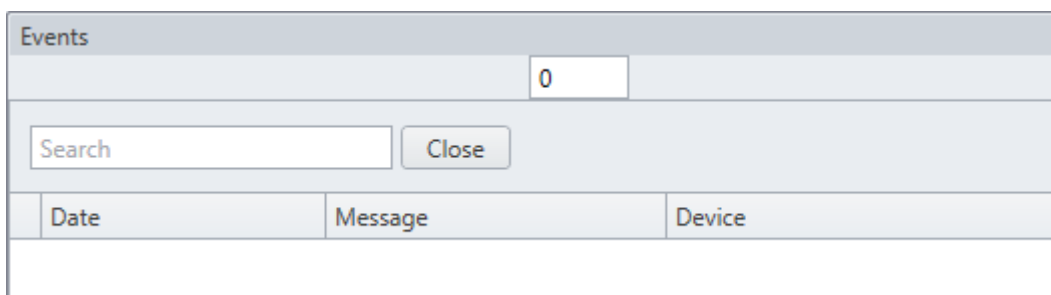
🔍 Filter Editor...

The *Filter Editor* allows for more detailed customization by limiting what data is displayed.



🔍 Show Search Panel

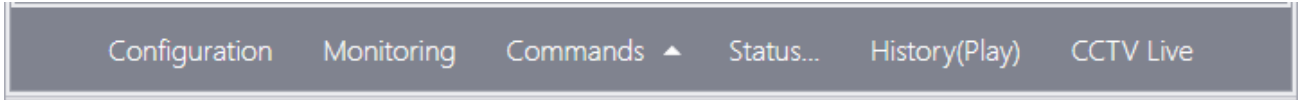
Show Search Panel will display a text box in which a search parameter can be entered.



Click *Close* to remove the *Search Panel* text box.

Command Bar

Tile View only.



Configuration

Configuration will take you to a configuration screen for the selected item.

Monitoring

Monitoring will take you to a monitoring screen for the selected item.

Commands ▼

Selecting *Commands* will provide a list of commands that can be executed on the selected item(s). See above for *Specific Commands* for the selected item(s).

Status...

Selecting *Status* will open a panel with *Status Detail*, *Events*, and *Show Alarms* for the selected item(s).

History(Play)

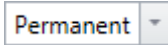
Click *History(Play)* to show last 10 transactions (history) on the selected item(s). If CCTV is configured for that device, it would show Playback button as well which will start CCTV Playback for selected event.

CCTV Live

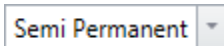
Selecting *Live* will start live play of the main camera configured for the selected item.

Commands

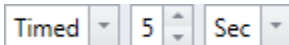
Commands can be issued by the operator (user) or by the system itself (links, schedules). There are three types of commands, Permanent, Semi-Permanent, and Timed.



Permanent 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 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 Commands are execute like *Semi-Permanent Commands* except that they are timed. 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 runs for ten minutes. When the timer expires at 5:05 p.m. the door remains locked since the unlock schedule has turned off.

This is the end of the overview for AxiomXA™ Event Viewer and System Status. Once you have read and become familiar with the general features and environment of AxiomXA™, proceed to:

[Part 4](#) for information on how to monitor security access with AxiomXA™ Monitor and System Status.

[Part 5](#)

For information on how to use and set up the AxiomXA™ Database.

Chapter 4

Concepts

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

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 from 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 AxiomXA™.

Alarms

Alarms are system messages that are important enough to require action by an operator and are not just system messages with the word ‘alarm’ in them. One Input Alarm message may be an Alarm while another Input Alarm message isn’t.

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 AxiomXA™ 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 Antipassback 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 AxiomXA™ 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 than 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.

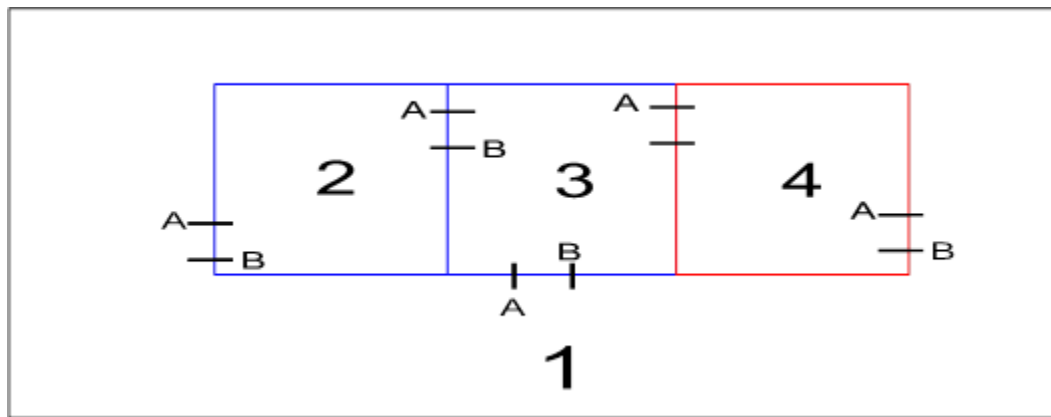
Area Antipassback not only checks to see if the cardholder is trying to enter the Area that they are already in, but also checks to see if the cardholder is trying to leave an Area that they are not in. This higher level of antipassback is mostly used in applications with Areas inside of other Areas.

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 AxiomXA™ software will control antipassback for the site and that antipassback can function across networks. This will be true as long as the AxiomXA™ server is running.

Example

In the diagram below, there are four areas numbered 1-4, all 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 AxiomXA™.

C-NET Controller Network

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

Connection Types

Direct connection – the controller network (C-NET) is connected directly to the PC serial port via RS232 or RS485.

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

NC100 Network Controller

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

UNC100 Network Controller

The UNC100 is a network controller in the system and stores all information required for local access control functions. Each UNC100 is capable of monitoring eight readers (two reader ports from a built-in-NURC and three from - RC2/NIRC/NURC device controllers) and sixteen IOC16 input/output device controllers over its D-Net.

UNC100-Keypad Network Controller

The UNC100-Keypad is a network controller in the system and stores all information required for local access control and intrusion alarm functions. Each UNC100-Keypad is capable of monitoring two readers (two reader ports from a built-in-NURC), and an intrusion alarm system (built-in-Alarm Keypad) capable of up to 8 alarm panel partitions using inputs and outputs of IOC-8 device controller over its D-net.

UNC500 Network Controller

The UNC500 is a network controller in the system and stores all information required for local access control functions. Each UNC500 is capable of monitoring eight readers (two reader ports from a built-in-RC2 and three from - RC2/NIRC/NURC controllers) and sixteen IOC16 input/output controllers over its D-Net.

D-NET Device Network

The D-Net is the communications network that links card reader controllers (RC2/NIRC/NURC) and input/output controllers (IOC16) to the network controllers in the C-NET. Up to four RC2/NIRC/NURCs and sixteen IOC16s can be connected to a single network controller.

RC2/NIRC/NURC Reader Controller

The RC2/NIRC/NURC connects to the network controller on the D-Net and supports two readers (PIN pad and/or card reader) as well as eight/four inputs and eight/four outputs.

IOC16 Input / Output Controller

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

IOC8 Input / Output Controller

The IOC8 supports eight points, which are already programmed as an input or an output, depending upon the type of IOC8 added.

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.

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.

| Name | Business Hours | | | | | | | | | | | |
|------------|----------------|-------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|
| Periods | Start | End | Sun | Mon | Tue | Wed | Thu | Fri | Sat | H 1 | H 2 | |
| Period 1: | 08:00 | 17:00 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Period 2: | 11:00 | 17:00 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 3: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 4: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 5: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 6: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 7: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 8: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 9: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 10: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 11: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 12: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 13: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 14: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 15: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 16: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

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

Part 4

Chapter 5

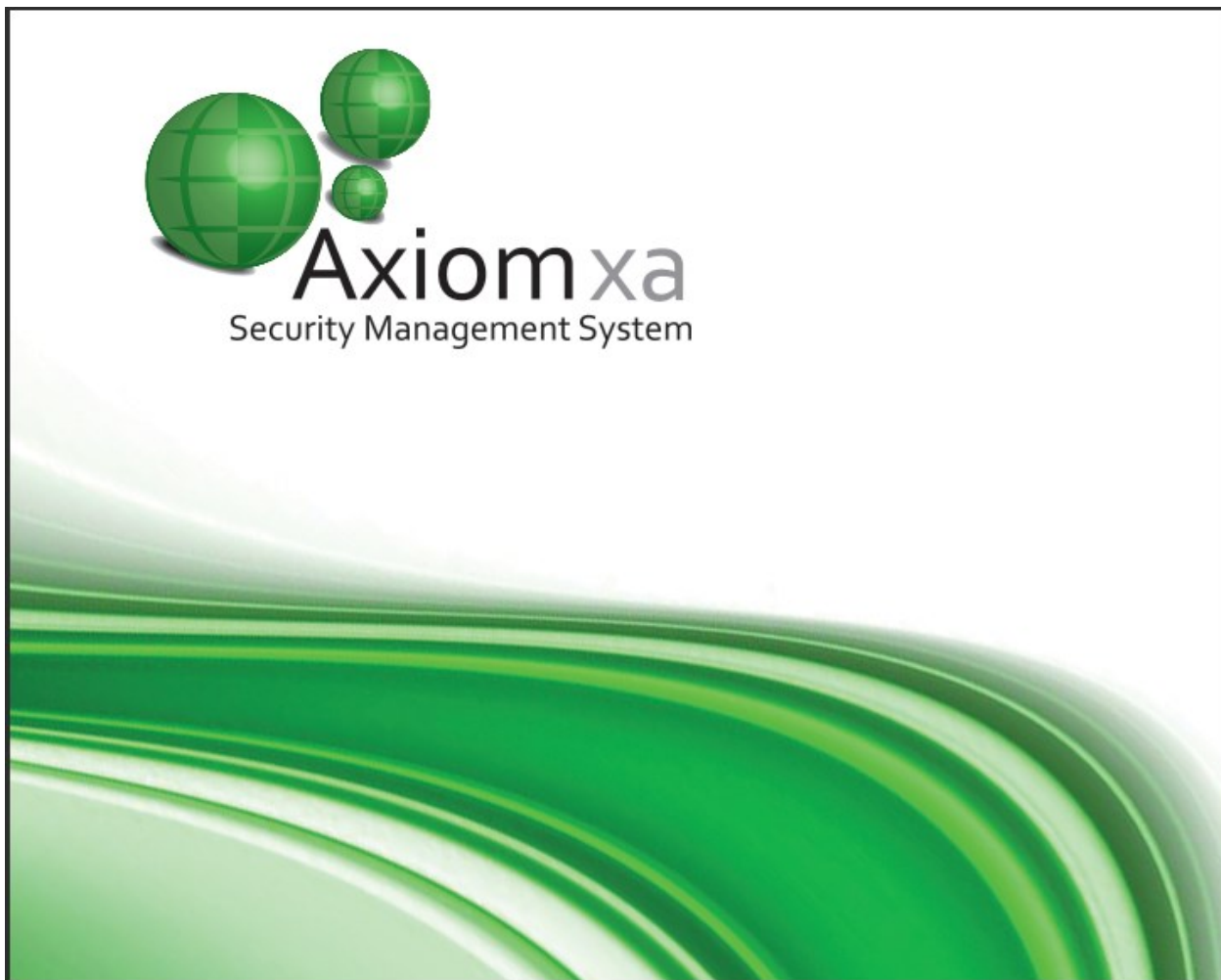
Monitoring Security Access

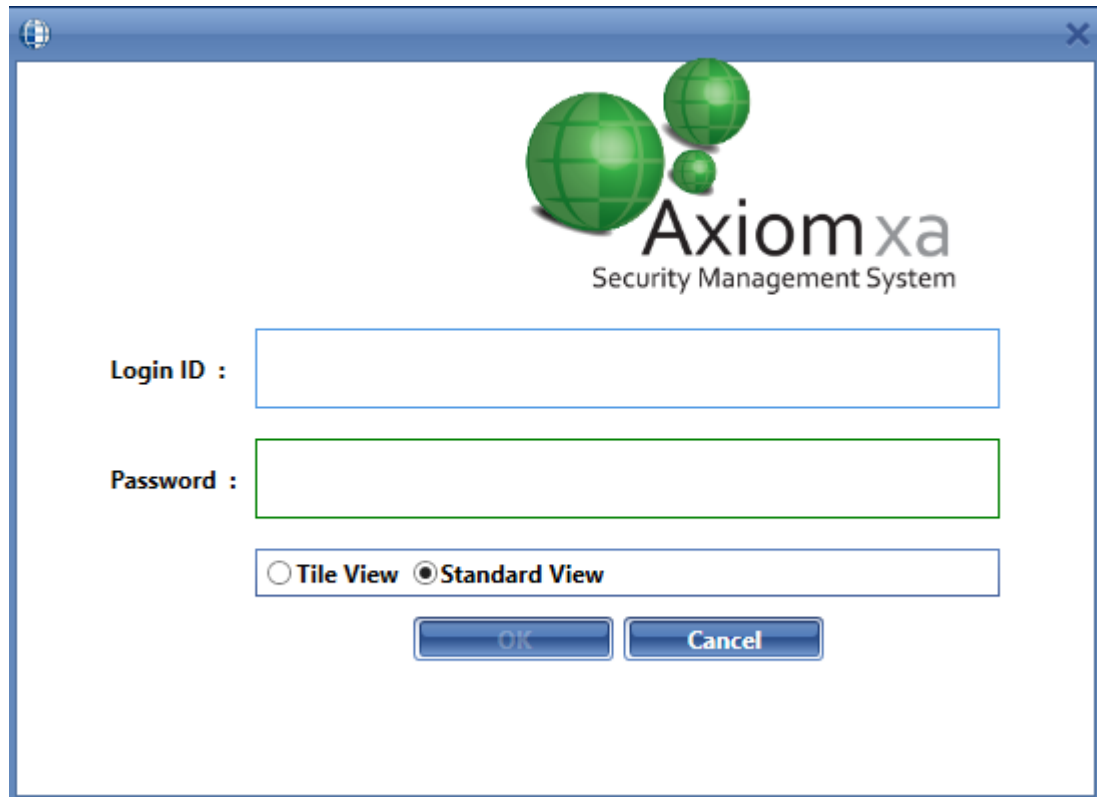
This chapter describes the operation of the AxiomXA™ client screen. All functions of the system can be performed from the client screen (as long as the operator has permission).

Client Log In

Log In

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.





The screenshot shows a login dialog box for the AxiomXA Security Management System. At the top center is the logo, which consists of three green spheres of varying sizes and the text "AxiomXA Security Management System". Below the logo are two input fields: "Login ID :" and "Password :". The "Login ID" field is a simple text box, while the "Password" field is a text box with a green border. Below these fields is a radio button group with two options: "Tile View" (unselected) and "Standard View" (selected). At the bottom of the dialog are two buttons: "OK" and "Cancel".

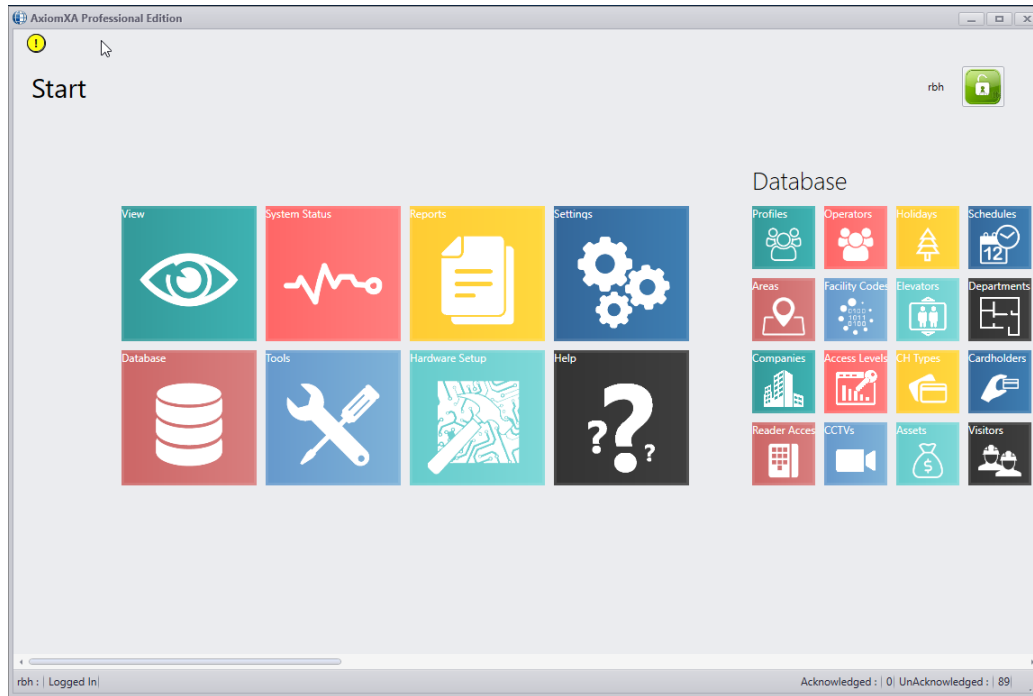
To log in, enter your user name and password. Although the “Login Name” is not case sensitive the “Password” is case sensitive.



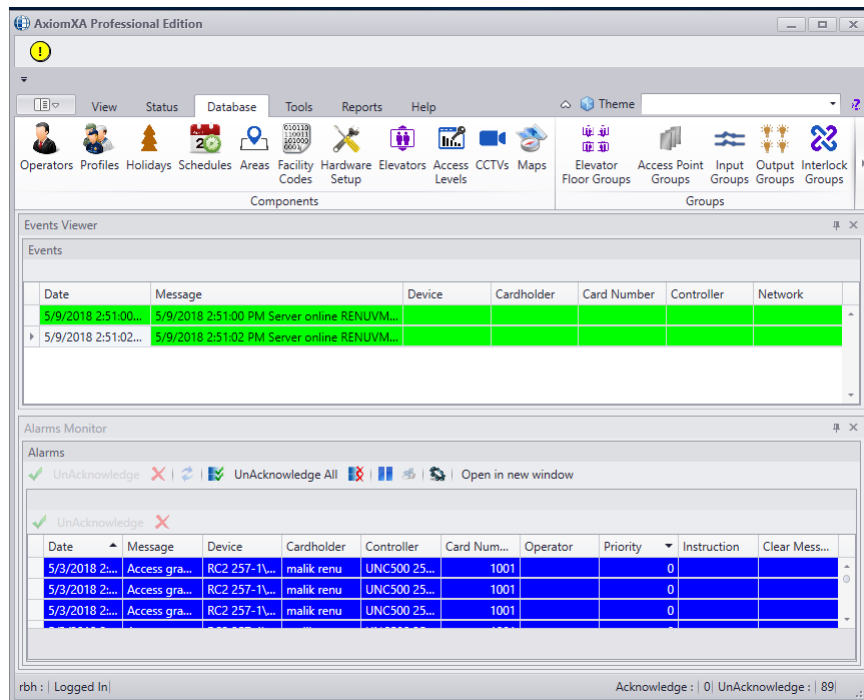
The default operator name is ‘rbh’ and the default password is ‘password’. After you have the system up and running it is recommended that you change the default password for ‘built in Administrator’ operator.

Select the *type of View* you want to log in with

Tile View

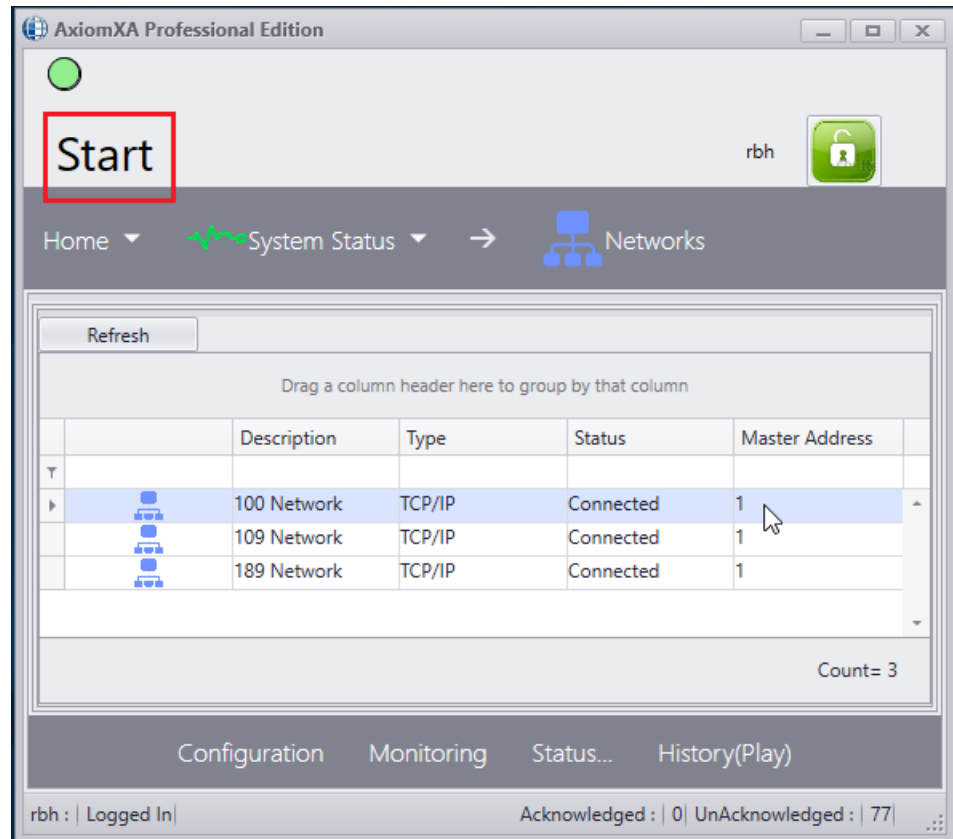


Standard View



The Client Screen displays a number of icons allowing the user to access the different portions of the system. Depending on an operator's profile only certain sections of the system may be available to an operator.

In Tile view you can return to the Main Screen from any Configuration Screen by clicking on Start. Selecting the down (▼) triangle beside a menu header will provide the operator with another level of menu selections.

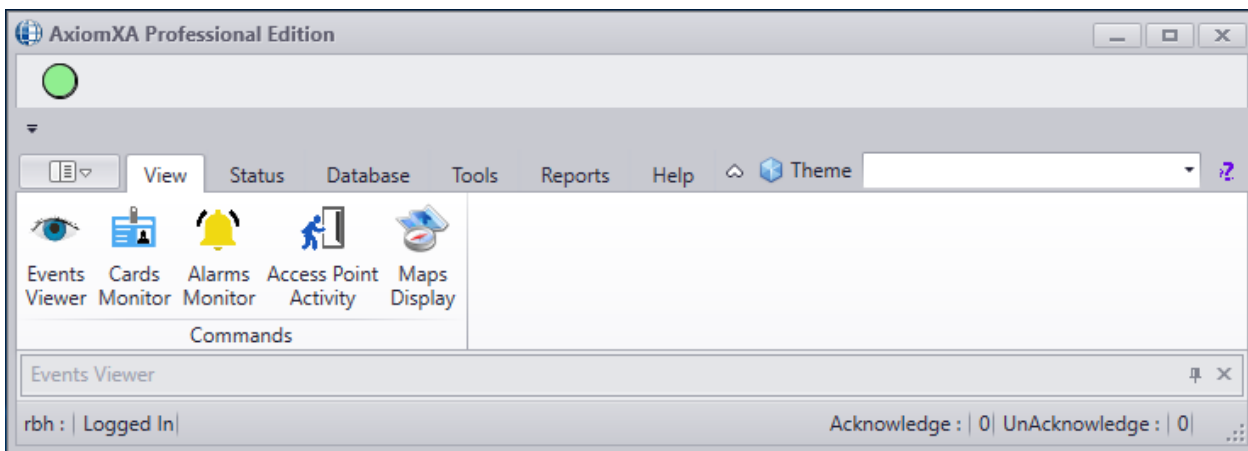
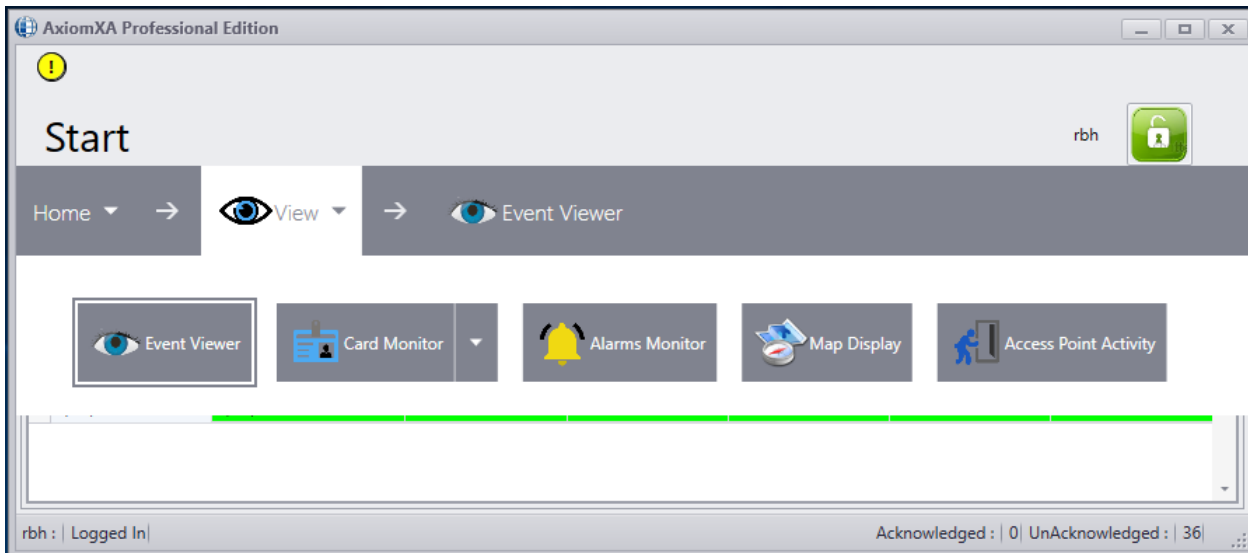


Log Off

An operator should log out when leaving the computer unattended or when finished his/her shift. To log off, simply click the appropriate button. 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. AxiomXA™ has a built-in Default Account, which activates whenever an operator logs out and forces events to be displayed and captured on the monitor screen (Standard View only). These messages will be available to the same operator only when logging in the next time.

Selections

View ▼



Event Viewer

The Event Viewer displays system and device messages. Which messages are displayed will depend on the profile 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 72 for more information on *Event Viewer*.)

Card Monitor

The *Cards Monitor* window is used to display a list of cardholders and the area they are in.

Operators can choose between displaying selected cardholders (and what area they are in) or selected areas (and which cardholders are in those areas).

Visitor and *Asset monitor* shows the list of all the visitors checked in, and assets which are accompanied by asset holders in various areas. (See page 73 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 report what was actually done for each alarm event. (See page 74 for more information on *Alarm Monitor*.)

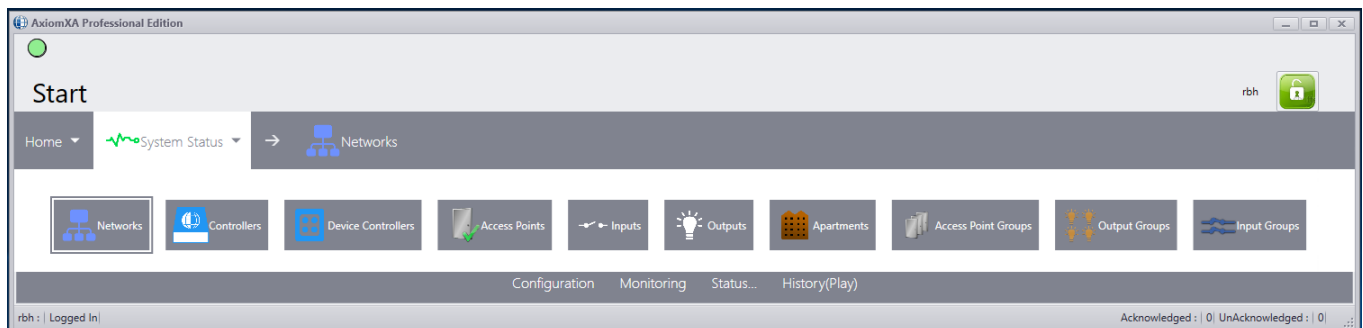
Map Display

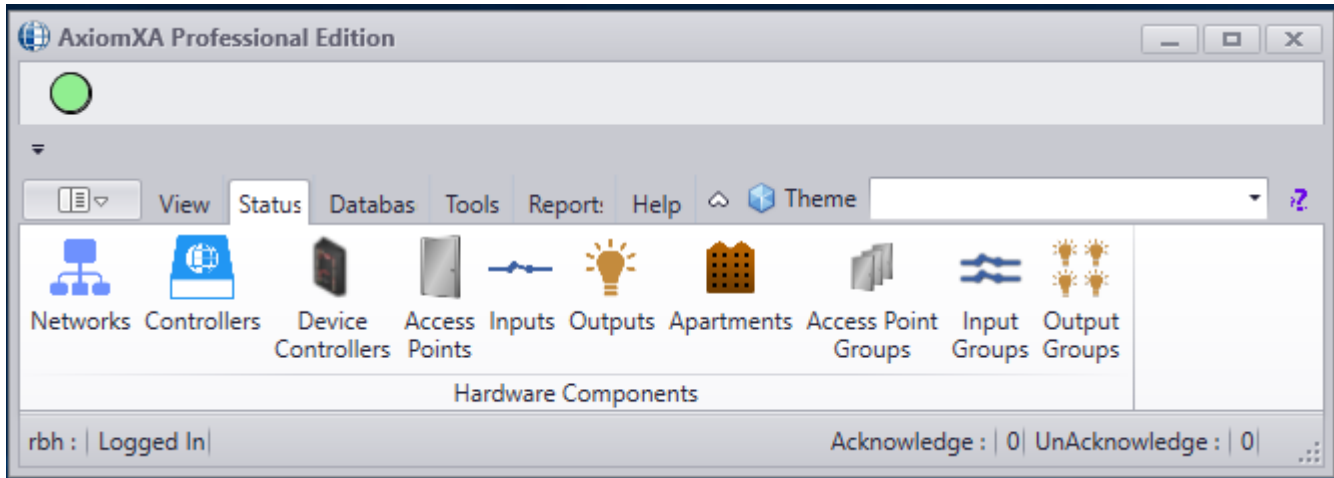
Maps Display will provide a list of maps to choose from. These maps can display the status of different types of items (like inputs, outputs, and access points) at the same time. Maps are created in the Maps module (see page 195 for more information on Maps).

Access Point Activity

The *Access Point Activity Monitor* is used to monitor multiple 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; as well up to last 999 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. (See page 78 for more information on *Access Point Activity*.)

System Status ▼





Networks

Networks will display the selected Networks. (For more information see page [80](#).)

Controllers

Controllers will display the selected Network Controller panels (NC100, UNC100, UNC100-Keypad and UNC500 panels). (For more information see page [82](#).)

Device Controllers

Device Controllers will display the selected RC2s\NIRCs\NURCs, IOC16s\IOC8 and Keypads (For more information see page [85](#).)

Access Points

Access Points will display the selected Access Points. (For more information see page [86](#).)

Inputs

Inputs will display the selected Inputs. (For more information see page [88](#).)

Outputs

Outputs will display the selected Outputs. (For more information see page [90](#).)

Apartments

Apartments will display the selected SafeSuite™ and Alarm panels with their partitions (For more information see page [92](#).)

Access Point Groups

Access Point Groups will display the selected Access Point Groups. (For more information see page [94](#).)

Output Groups

Output Groups will display the selected Output Groups. (For more information see page 94.)

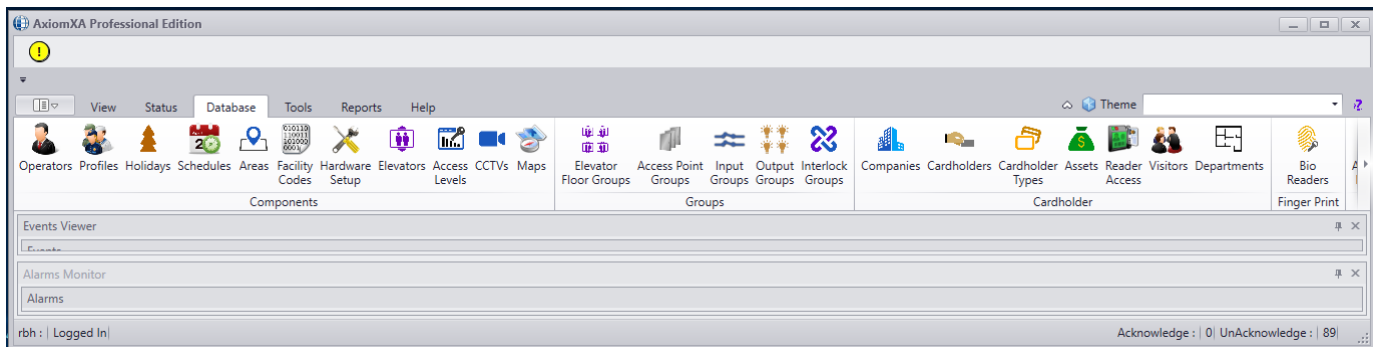
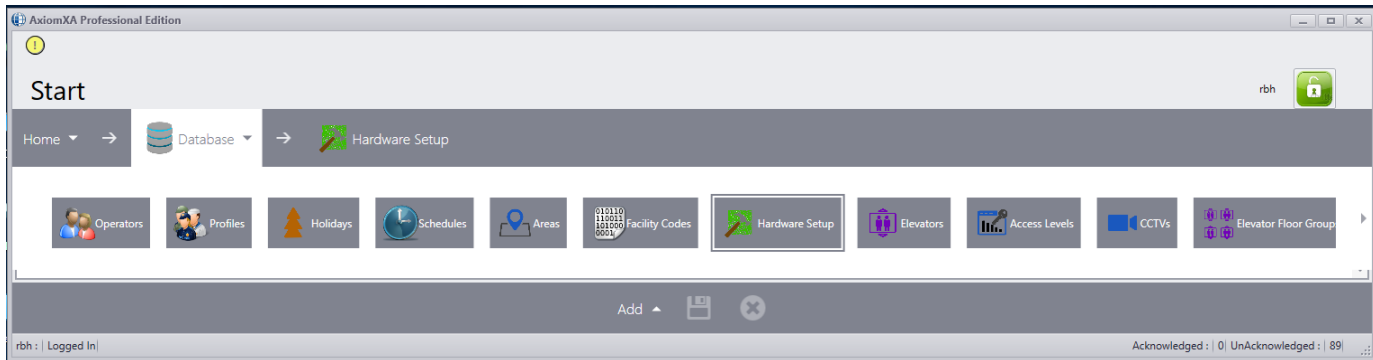
Input Groups

Input Groups will display the selected Input Groups. (For more information see page 94.)

Guard Tours

Guard Tours will display the selected Guard Tours. (For more information see page 94.)

Database ▼



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 name, password and language of the default operator may be changed it will always have full privileges. (For more information on creating see page 96.)

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 [98](#).)

Holidays

Holidays will open the *Holidays* window to create new holidays, edit or view the existing holidays. (For more information on creating *Holidays* see page [100](#).)

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 [102](#).)

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 [107](#).)

Facility Codes

Facility Codes will open the *Facility Codes* window to enter new facility codes, edit or view the existing facility codes. (For more information on creating *Facility Codes* see page [108](#).)

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, NC100/UNC500/UNC100/UNC100-Keypads, RC2/NIRC/NURCs, IOC16s, Keypads/Alarm panel and IOC8. Access Points, Non Reader 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 [110](#).)

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 [145](#).)

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 [153](#).)

CCTVs

CCTVs will open a window to configure your systems DVRs. (For more information on *CCTVs* see page [157](#).) Only Axis cameras, and RBHView integrations are supported at this time.

Elevator Floor Groups

Floor Groups will open the Elevator Floor Groups window so that combinations of elevator floors can be created for access control purposes. (For more information on *Floor Groups* see page [150](#).)

Access Point Groups

Access Point Groups allows the operator to create groups of access points. 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 [147](#).)

Input Groups

Input Groups allows the operator to create groups of inputs. 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 *Input Groups* see page [159](#).)

Output Groups

Output Groups allows the operator to create groups of 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 *Output Groups* see page [161](#).)

Interlock Groups

Interlock Groups are groups of access points grouped for a different purpose. 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 [162.](#))

Companies

Companies will open a window to create Cardholder groups. Cardholder Groups (or *Companies*) are only used in *Operator Profiles*. They are used to segregate cardholders, and limit operators in their availability to cardholders. (For more information on creating *Companies* see page [166.](#))

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 [167.](#))

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 [181.](#))

Assets

Assets will open the Asset configuration screen to add, edit, or view assets. (For more information on *Assets* see page [182.](#))

Reader Access

Reader Access will open a window to edit (add or delete) special access for cardholders. (For more information on creating *Reader Access* see page [184.](#))

Visitors

Visitors will open the *Visitors* window. (For more information on *Visitors* see page [185.](#))

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 [187.](#))

Bio Readers

Bio Readers will open the *Finger Print Readers*. (For more information on creating *Finger Print Readers* see page [188.](#))

Axiom Links

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 [190](#).)

Global Commands

Global Commands are the same as *AxiomLinks™* except that the *Comm Server* executes them instead of the Network controllers. 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 [194](#).)

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 [195](#).)

Message Ports

Message Ports will open the *Message Port* window to configure your TCP/IP, email, SQL, SafeSuite 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 [195](#).)

Maps

Map 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 devices in the chosen area.

Guard Routes

Guard Route will open the configuration window for guard route as described on page [203](#).

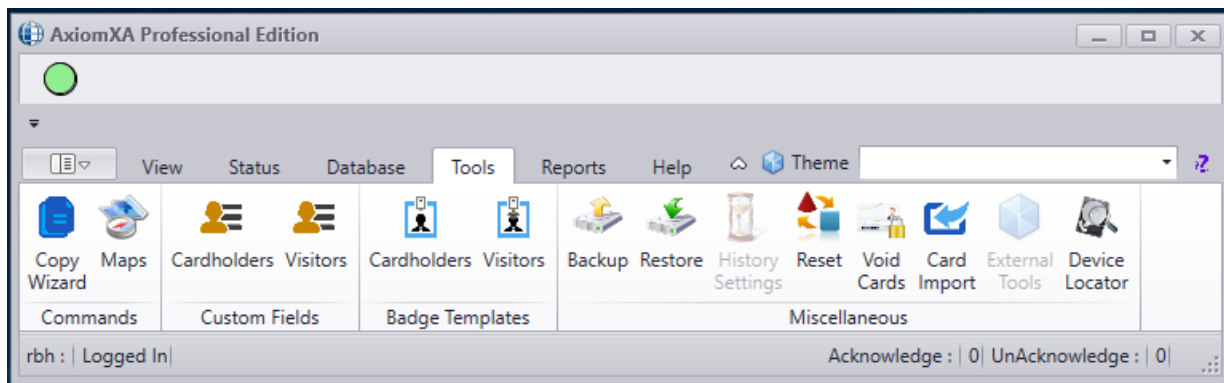
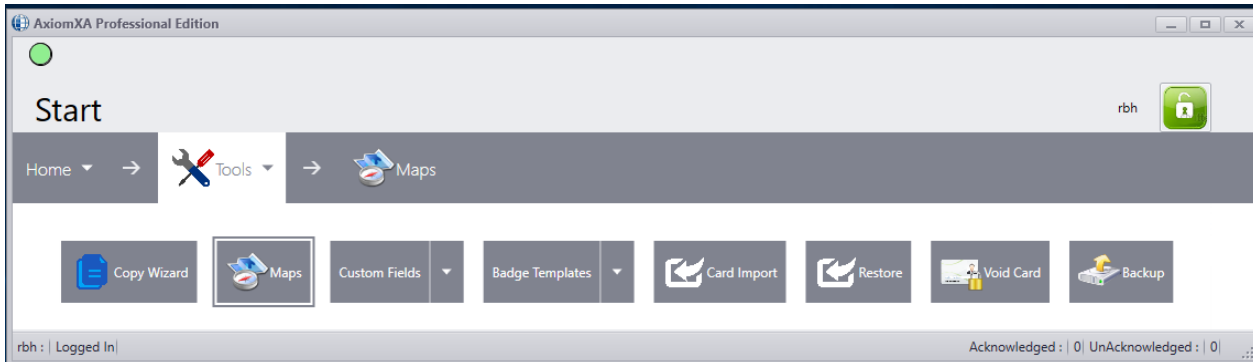
Guard Groups

Guard Groups will open the configuration window for guard group as described on page [205](#).

Guard Tours

Guard Tours will open the configuration window for guard tours as described on page [206](#).

Tools ▼



Copy Wizard

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

The *Copy Wizard* is a very versatile and quick way to program the AxiomXA™ 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. (For more information on *Copy Wizard* see page 50).

Custom Fields ▼

Cardholder

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. (For more information on *Cardholder Custom Fields* see page 45).

Visitors

This section allows additional user-defined Visitor 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. (For more information on *Visitor Custom Fields* see page 47).

Badge Templates ▼

Cardholders

This section is used to create templates for cardholder badges. The design can include data from the cardholder's record, images (e.g. a company logo or the cardholder's picture), fixed text (text common to all badges like the company's name), and other objects as well. (For more information on *Cardholder Badge Templates* see page 48).

Visitors

This section is used to create templates for visitor badges. Like the cardholder templates but meant for visitor use. (For more information on *Visitor Badge Templates* see page 48).

Import

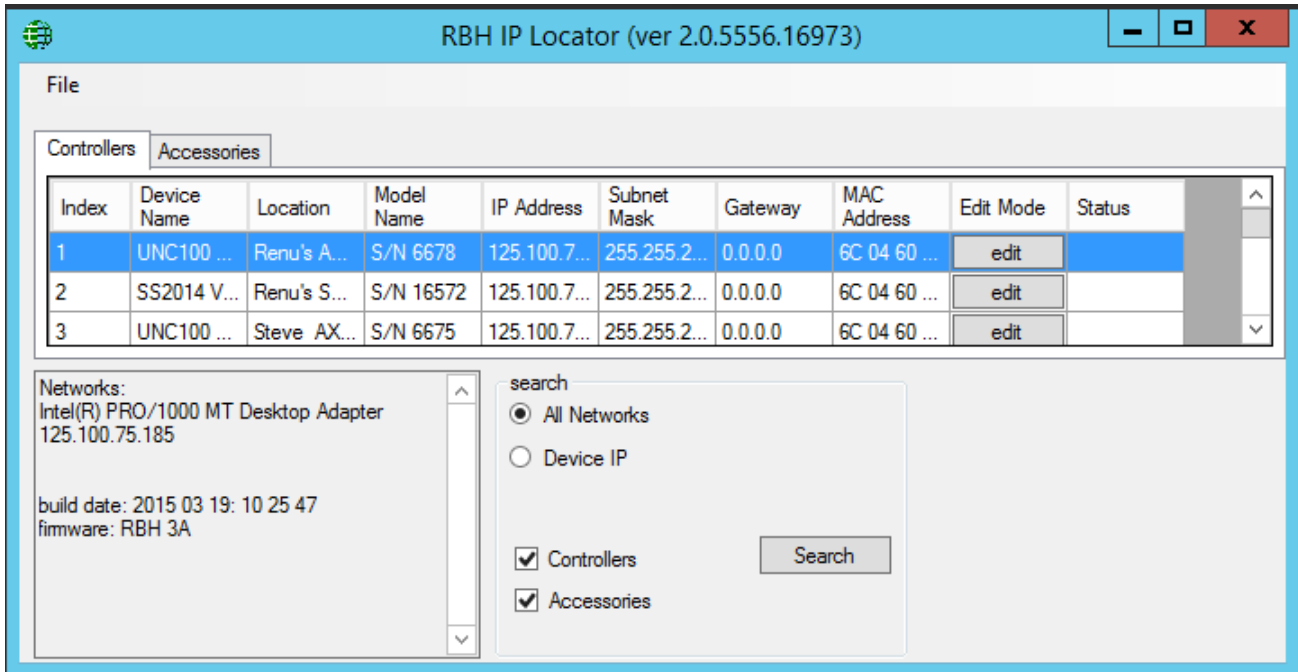
Selecting *Import* will start the Card Import utility. (For more information on *Card Import Utility* see page 52).

Void Card

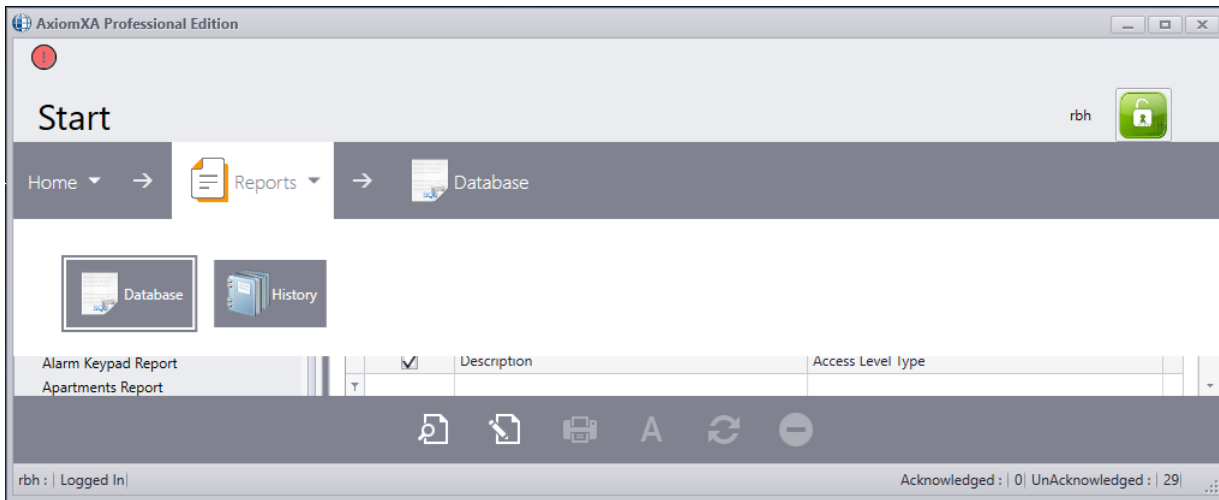
From *Void Cards* the operator can manually void (deactivate) cards that have not been used for a preset number of days. The number of days is set under the *System Setting* tab of *System settings*. If *Void Cards* is not used to manually deactivate cards, they get automatically voided as per the days configured in system settings.

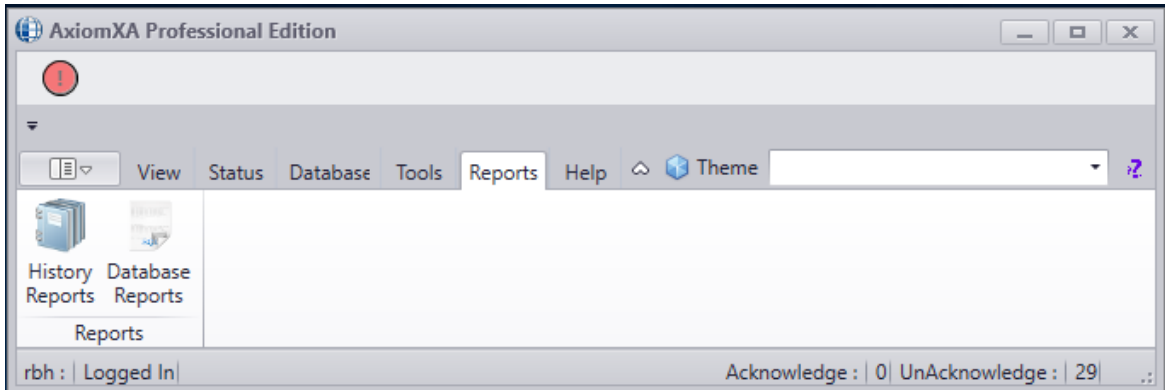
Device Locator

From *Device Locator* the installer can open the *RBH IP Locator utility* to be able to configure the UNC-500, and UNC-100 controllers.



Reports ▼





Database

This section is used to create reports using the system's data files. Details on page [210](#).

History

This section is used to generate reports from the History Logs. Details on page [207](#).

System Settings ▼

System Settings

System Settings or Settings is where system wide parameters or settings are configured. Details on page [62](#).

Themes



Themes is where the visual customization of the system's display is selected. Just pull down the list and *click* on a selection.



Tools

Custom Fields

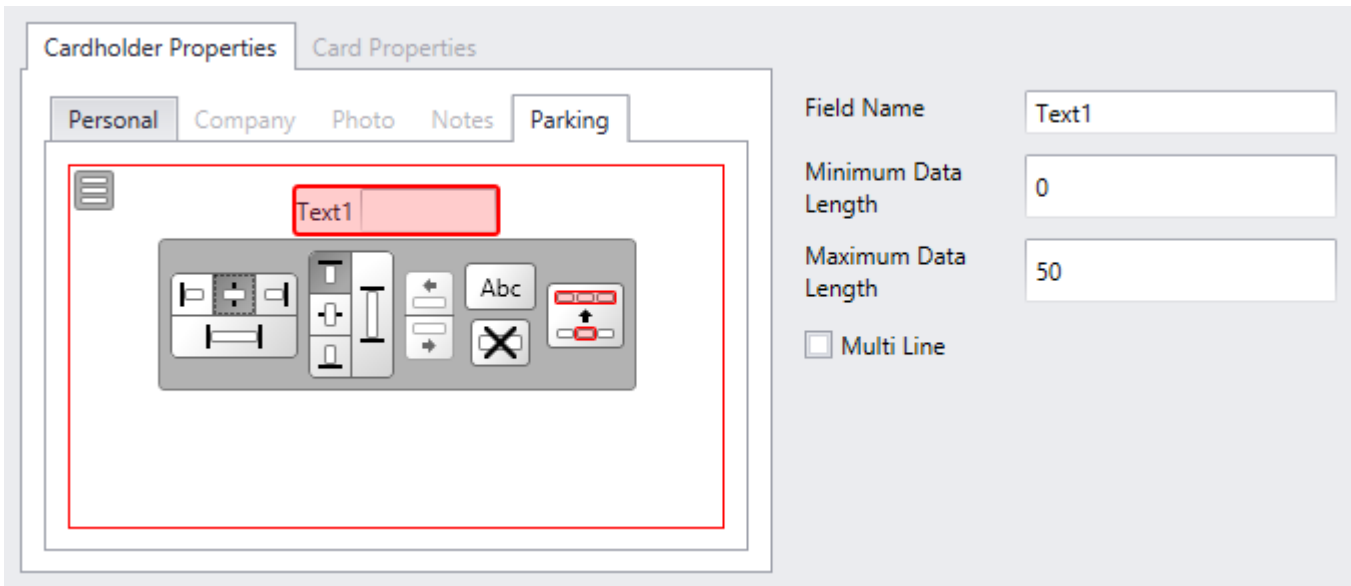
This section allows additional user-defined Cardholder\Visitor fields to be setup and given a field name. Additional fields might include, who to call in case of emergency, car license plate number, parking spot number, hiring date, tax codes, or any other information that is required for the cardholder.

Cardholder

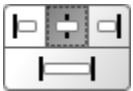
The screenshot shows a web-based form for editing cardholder information. At the top, there is a menu bar with options: Edit, Cancel, Save, Tab, Text, Number, Password, Label, Date, Time, Combo, Image. Below the menu, there are input fields for 'First Name', 'Last Name', 'Initials', and a dropdown for 'Cardholder Type'. A main container has two tabs: 'Cardholder Properties' (selected) and 'Card Properties'. Under 'Cardholder Properties', there are sub-tabs: 'Personal', 'Company', 'Photo', and 'Notes'. The 'Personal' sub-tab is active, showing a form with the following fields: 'Street Address' (text input), 'City' (text input), 'State/Province' (dropdown), 'Country' (dropdown), 'Zip/Postal' (text input), 'Phone' (text input), 'Ext.' (text input), 'Email' (text input), 'Department' (dropdown), 'Department 1' (dropdown), and 'Department 2' (dropdown).

New fields that are added will be available for all cardholder records.

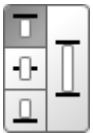
Select *Edit* to add a new tab to the cardholder screen. New fields can only be added to new tabs you create. Text, number, date, time, combo, and image box when added have their own labels so you don't have to include one yourself. Each box has its own set of parameters appropriate to its function.



Each box has a relative position and size, and not a specific one because of resizing issues.



Set the relative horizontal position left, center (shown), right, or full length.



Set the relative vertical position upper (shown), center, lower, or full height.



Change the order of boxes by shifting the selected box left or right.



Select this control to edit the label of a box.



Delete a box.



Field Name: Name or label for the field being created.

Minimum Data Length: Any value other than zero will the filed mandatory.

Maximum Data length: You can limit the amount of data entered into the field.

Visitors

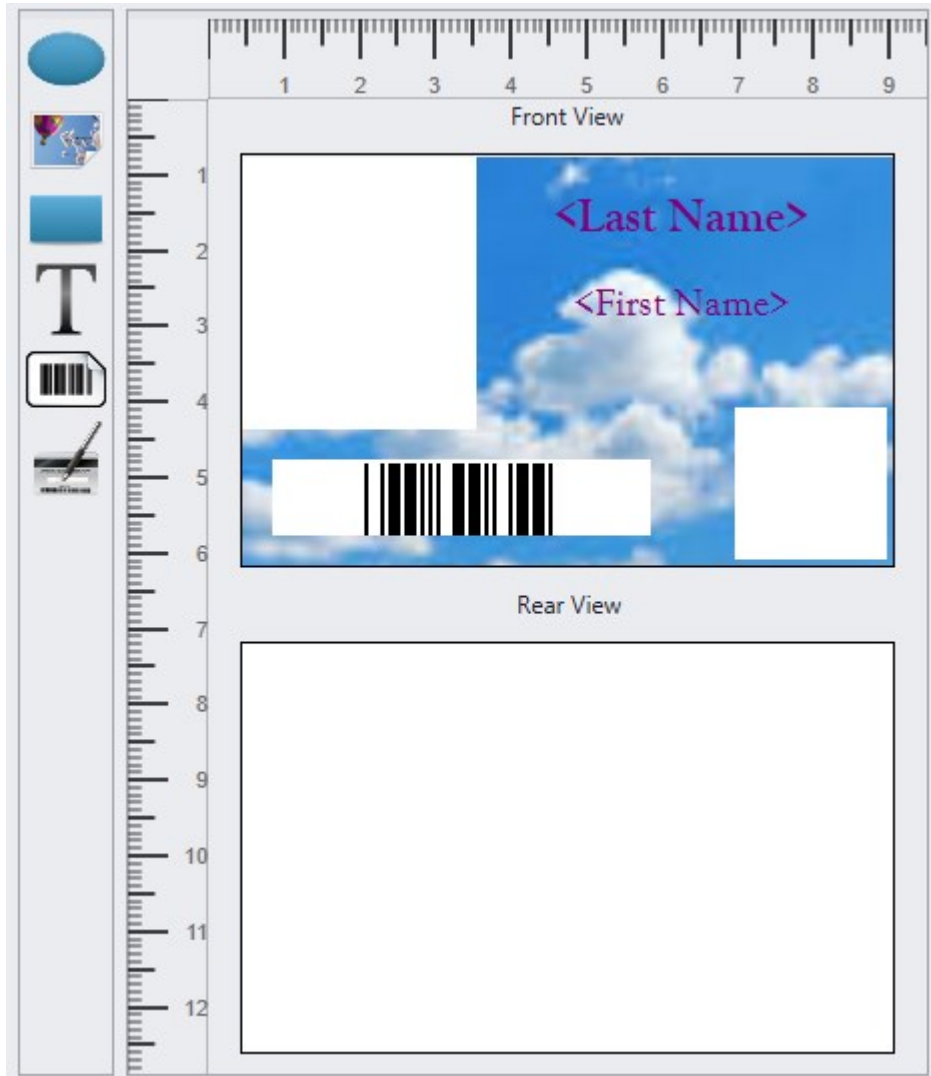
The Visitor Custom Fields function the same way as the Cardholder Custom Fields do. Any new field added will be available for all visitor records.

The screenshot shows a web-based form for editing visitor information. At the top, there is a toolbar with buttons: Edit, Cancel, Save, Tab, Text, Number, Password, Label, Date, Time, Combo, and Image. Below the toolbar, the form is divided into several sections:

- Personal Information:** Fields for First Name, Last Name, National ID, and Number.
- Navigation Tabs:** General (selected), Asset, Track, Photo, and Company.
- General Information:** A grid of fields including Reason for Visit (dropdown), Address, Date of Birth (dropdown), City, Phone, State, Email, Country, Employer, and Postal Code.
- Employee Information:** Fields for Last Name (dropdown), First Name, Department, Employee Card, Last Visited, Checked In, Time Allotted, and Checked Out.

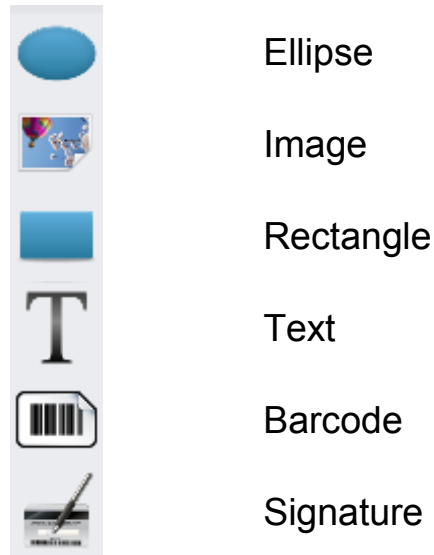
Badge Templates

Cardholder Badge Template and *Visitor Badge Template* are separate items, but are created in the same way.



Click *New/Add New* and select *New Horizontal*, *New Vertical*, *New Horizontal Id*, *New Vertical Id*, or *Custom*.

Add boxes to the template by double-clicking on the appropriate icon.



Selected boxes can be removed with the *Delete* key on your keyboard.

Properties

Each box has its own set of parameters for size, position, border, and color. Some boxes have parameters that can take fields like the cardholder's picture or a company's logo or insignia. Each template can have either an image or a solid color for its background. Use the ellipsis (...) button and search for an image for the background. The path to the image file will be displayed under *Image Path*. If an image is select its appearance can be; *none* (there is no change made to the image, it is inserted as is), *fill* (the image is stretched to fill the space completely), *uniform* (the image is stretched to fit the space while keeping its aspect ratio, some of the space might not be covered), or *uniform to fill* (the image is stretched to fill the space while keeping its aspect ratio, some of the image may be truncated so that the whole space will be completely filled).

Boxes can be dragged into position and stretched with the mouse, or size and position can be entered into the appropriate parameter in the properties (height, width, margin left, and margin top).

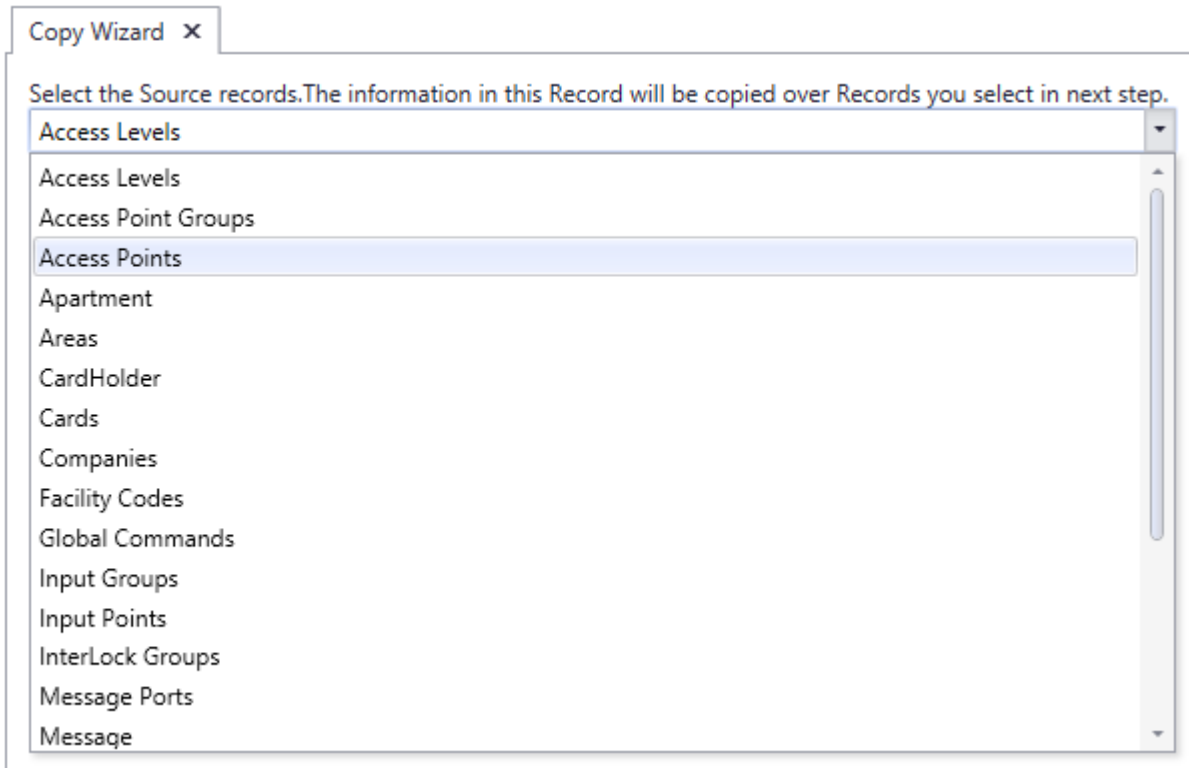
Border width and color can be set. The interior color can also be set, including being transparent.

Image size selected as *Photo* will be set a height of 36 and a width of 31. The custom selection will allow you to change these values.

The text can be static (the same on every card) or from a database field (different for each card). Font type, font color, font size, text alignment, rotate angle, italic, bold, and under line can also be configured for each text box individually.

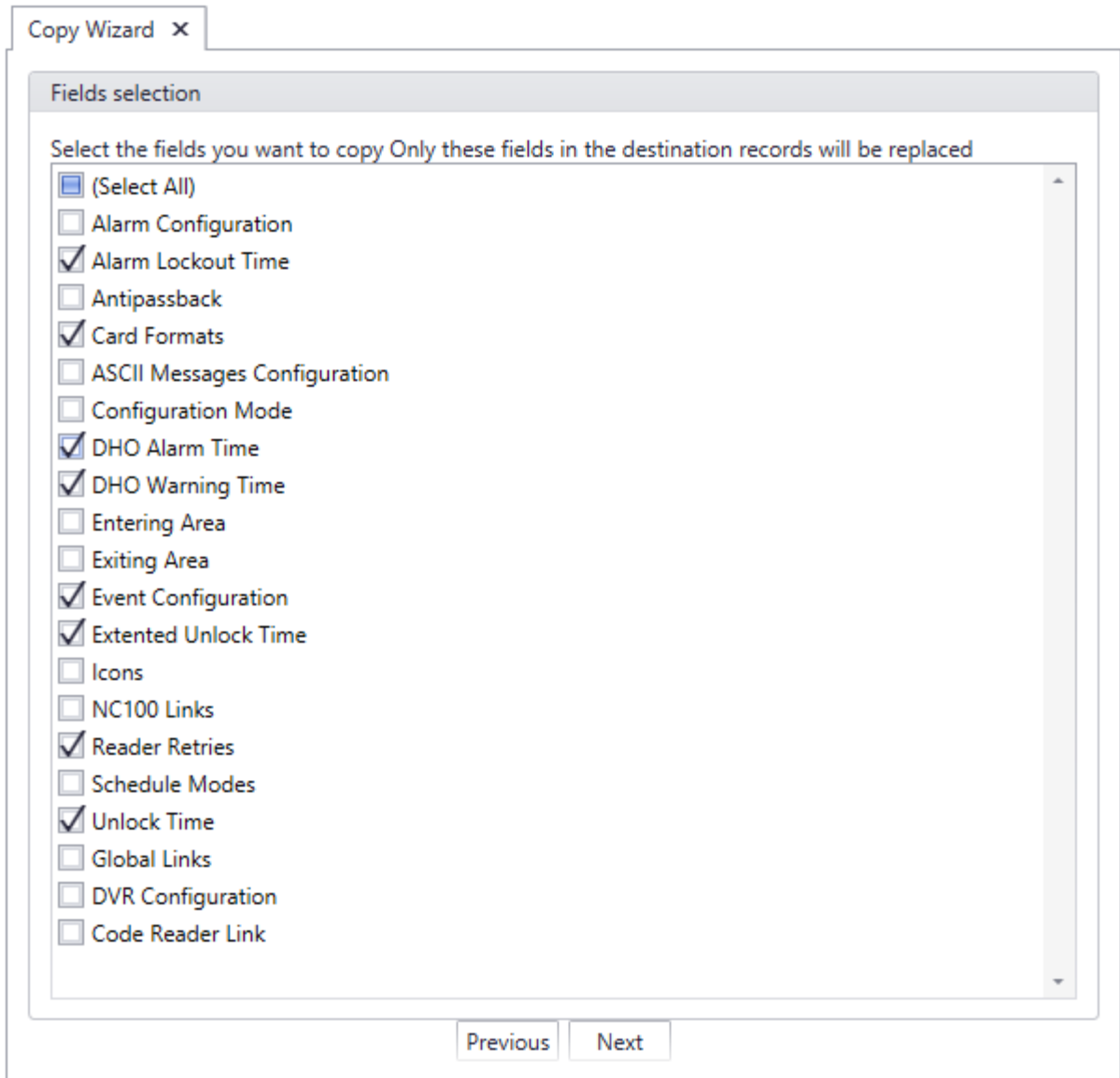
Copy Wizard

Through the *Copy Wizard* the operator can copy selected data from one item to multiple like items.

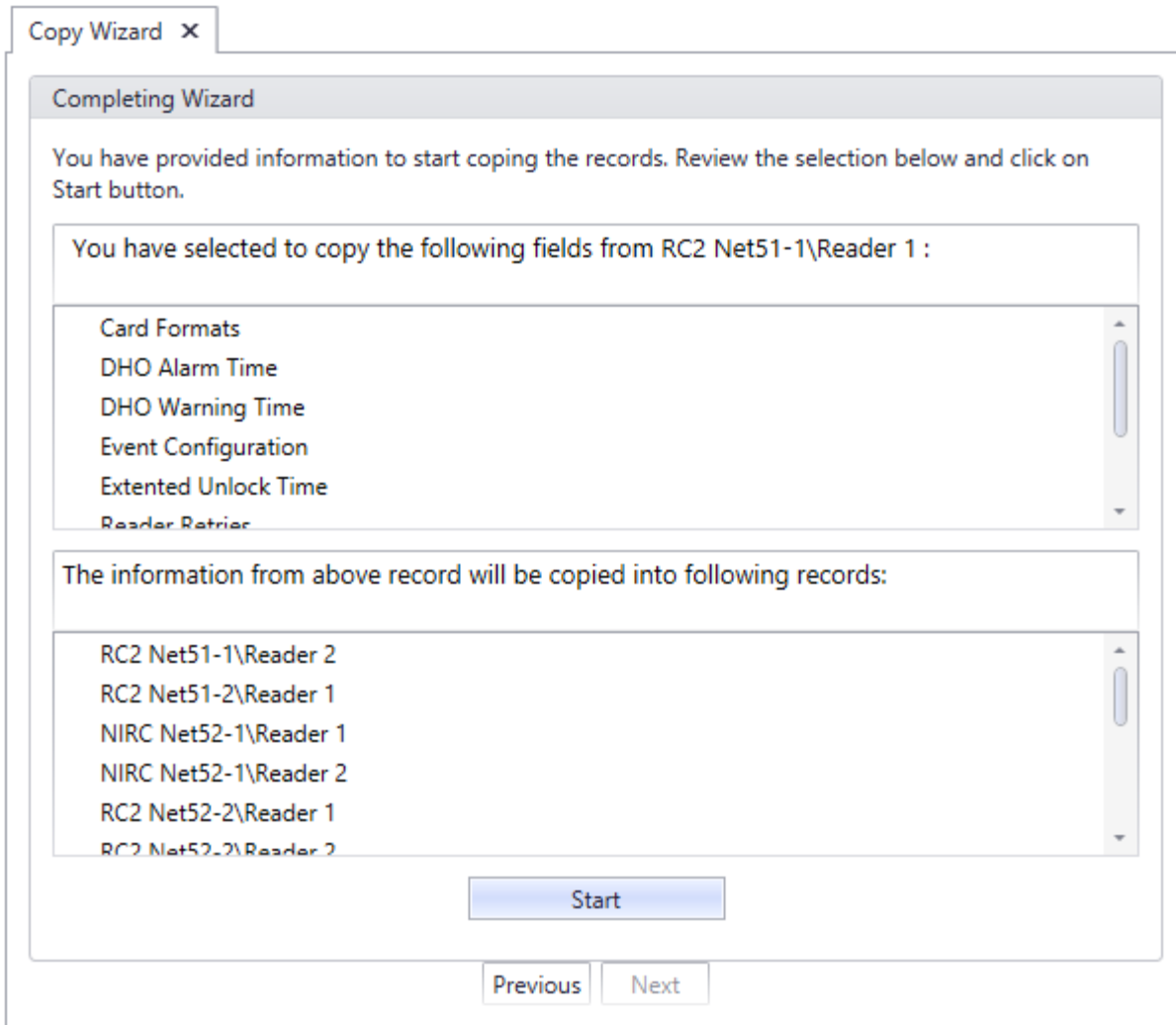


The *Copy Wizard* is a very versatile and quick way to program the AxiomXA™ system. After programming one item, that item can be used as a template to program all of the other items of the same type. For example if one access point was programmed then all the other access points could be programmed from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

To copy data from one item to another start the *Copy Wizard*. Then select a category from the pull down list. Next choose the source record to be copied from. Now select all of the destination records that are to be programmed.



Next select the fields to be copied.

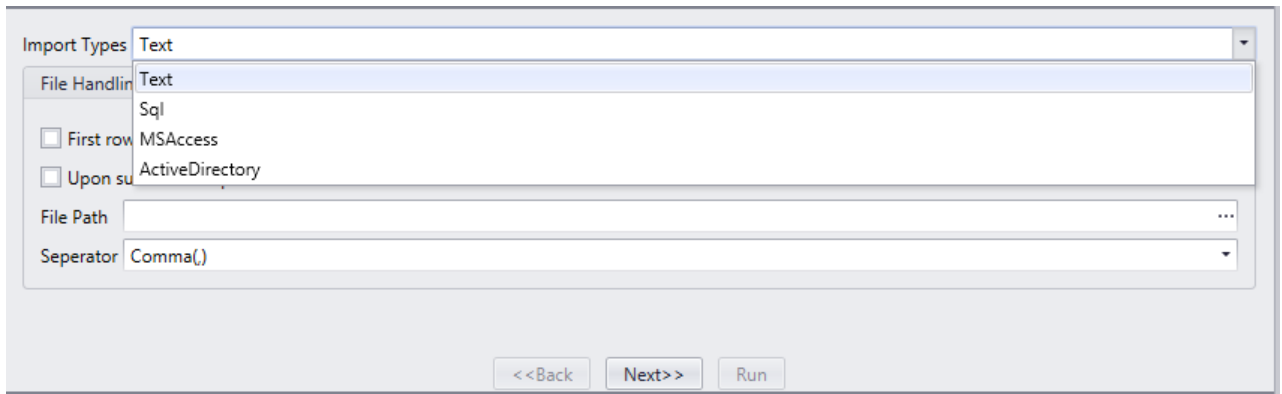


Verify your copy parameters and then click *Start* to execute the copy.

After copying you can use the *Previous* button to go back and set up another copy.

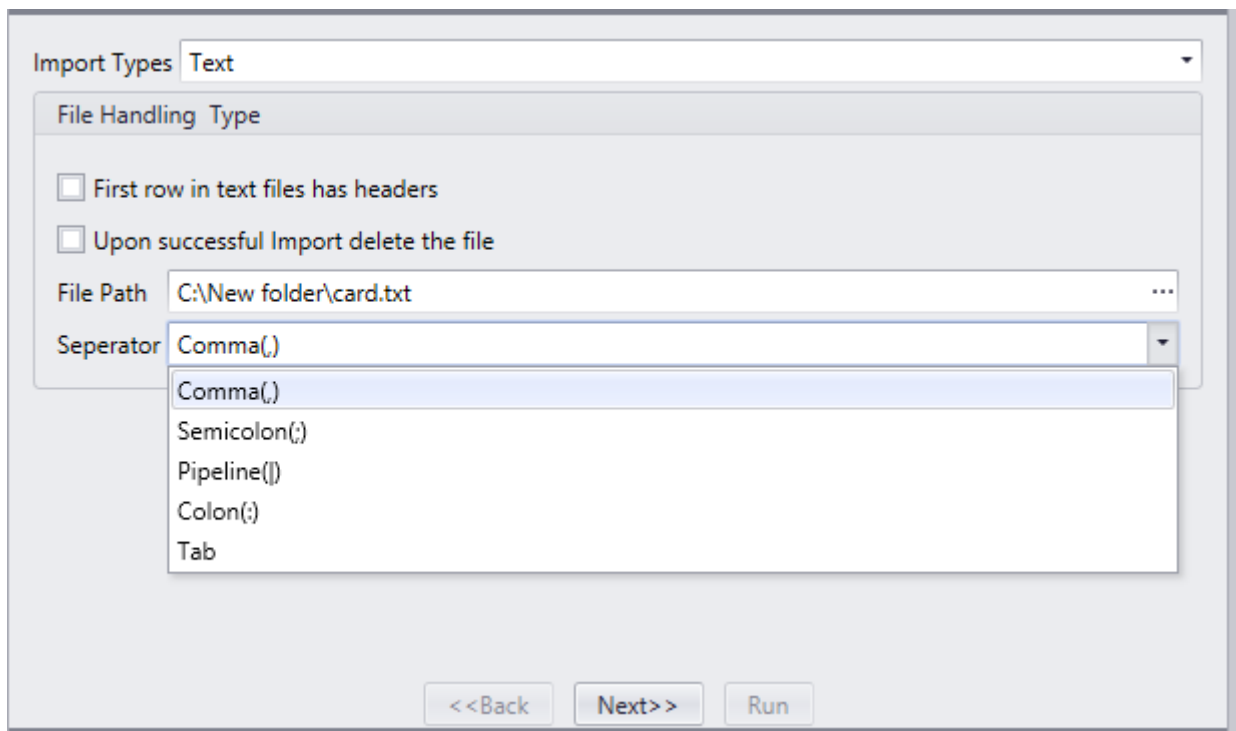
Import

AxiomXA™ Card Import Wizard is used to import cardholder information from other sources into AxiomXA™ system.



Select one of the four available *Import Types* to be imported (the file or database with the cardholder data) and then click the *Next* button.

Text Type



If you selected *Text* as the *Import Type*, type the path to the file to be imported from or you can use the Browse/Ellipsis button (...) to search for the path to the required file.

Select the type of *Separator* used in the source file

Separators can be:

Comma (,)

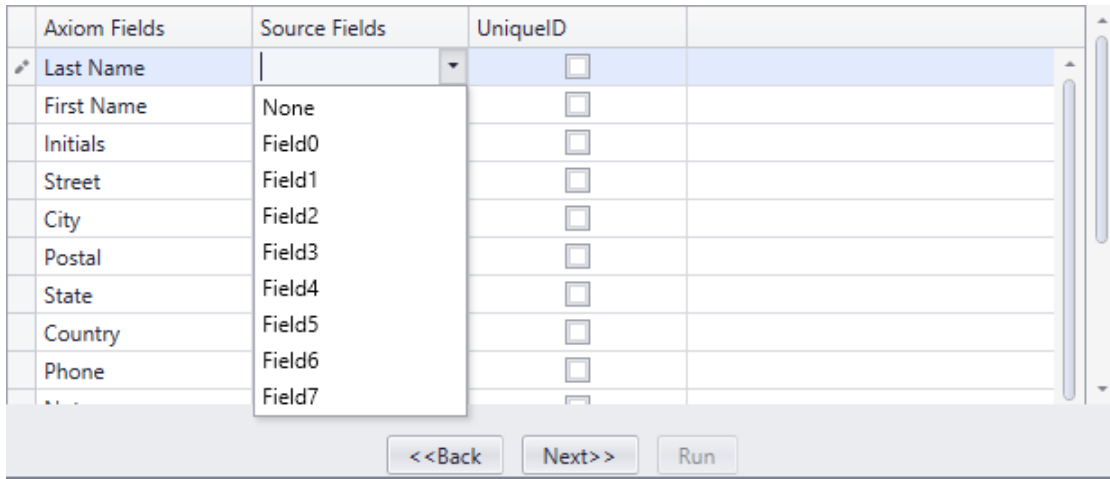
Semicolon (;)

Pipeline (|)
Colon (:)
Tab

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.

And Click *Next*.



Map the source fields to Axiom XA™ cardholder fields. Mapping the wrong fields may result in invalid cardholder data. Check the appropriate box for any Unique Fields. Click *Next* to launch the window to schedule the import.

Backup

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

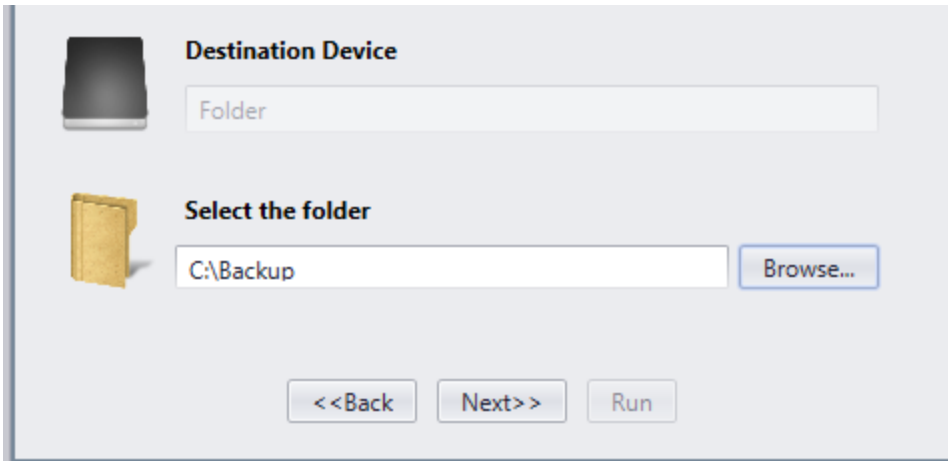
Run Now

The screenshot shows a configuration window for a backup process. At the top, there are two radio buttons: "Run Now" (selected) and "Configure Auto-backup". Below this is a "Frequency" section with three radio buttons: "Daily" (selected), "Weekly", and "Monthly". Underneath is a "Daily Frequency" section with two options: "Occurs once at:" with a time input field set to "2:47:00 PM" and "Occurs every:" with a numeric input field set to "1" and a dropdown menu set to "Hour". At the bottom, there is a "Summary" section with a "Description" label. At the very bottom of the window are three buttons: "<<Back", "Next>>", and "Run".

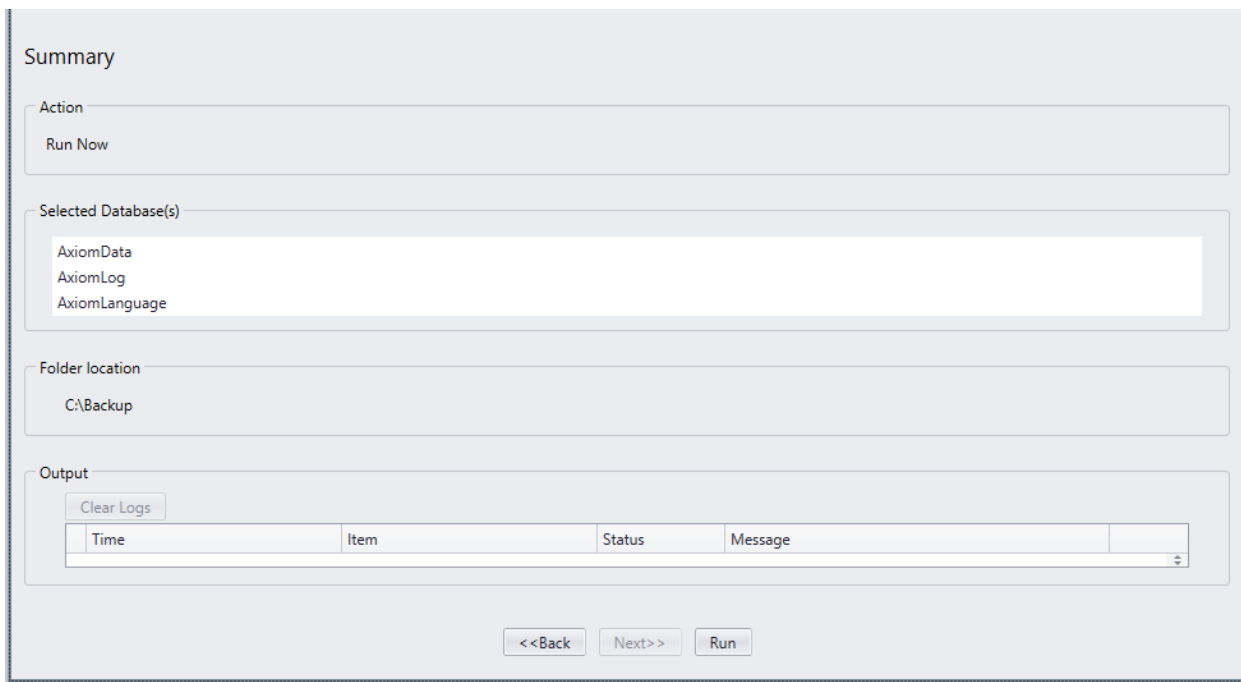
To run the backup immediately, select 'Run Now' and click *Next*.

The screenshot shows a selection interface for databases. It features a tree view with a single expanded item, "Databases", which has a small blue square icon to its left. Underneath "Databases", there are three items listed, each with a checkbox: "AxiomData" (checked), "AxiomLog" (unchecked), and "AxiomLanguage" (unchecked). At the bottom of the window are three buttons: "<<Back", "Next>>", and "Run".

Select the databases to be backed up by clicking in the box to check or uncheck the selection and click *Next*



Select the folder the backup files will be sent to.



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

Summary

Action
Run Now

Selected Database(s)
AxiomData
AxiomLog
AxiomLanguage

Folder location
C:\Backup

Output
Clear Logs

| Time | Item | Status | Message |
|----------------------|---------------|--------|----------------------|
| 10/4/2016 3:45:34 PM | AxiomData | Passed | Files at : C:\Backup |
| 10/4/2016 3:45:35 PM | AxiomLog | Passed | Files at : C:\Backup |
| 10/4/2016 3:45:36 PM | AxiomLanguage | Passed | Files at : C:\Backup |

<<Back Next>> Run

A progress bar will appear and each file will be listed under *Output* as it is backed up.

Auto Backup

Run Now Configure Auto-backup


Frequency
Occurs: Daily Weekly Monthly
Recurr every: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Daily Frequency
 Occurs once at: 4:05:00 PM
 Occurs every: 9

Summary
Description

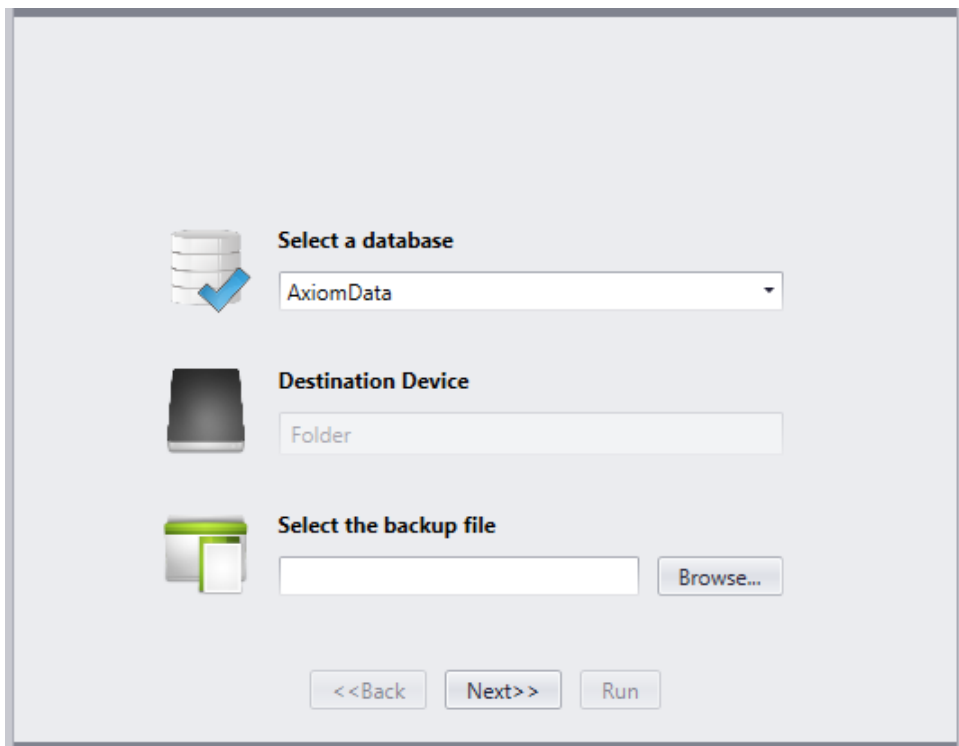
<<Back Next>> Save

Choose the *Frequency* and *Daily Frequency* of the backup is to be executed and follow the Auto Backup wizard to save the settings.

 *RBHAxiomBackupServer* service should be running for Auto Backup to work.

Restore

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



Select the *database name* you want to restore from the drop down menu and select the source *Backup file*, you want to restore from, and Click on *Next*

The screenshot shows a configuration wizard with three main sections:

- Select a database:** A database icon with a blue checkmark is on the left. To its right is the title "Select a database" and a dropdown menu containing "AxiomData".
- Destination Device:** A hard drive icon is on the left. To its right is the title "Destination Device" and a text input field containing the word "Folder".
- Select the backup file:** A folder icon is on the left. To its right is the title "Select the backup file", a text input field containing the path "C:\Backup\20170630122145043 AxiomData.bak", and a "Browse..." button.

At the bottom of the wizard are three buttons: "<<Back", "Next>>", and "Run".

Click on *Run* in the next window to restore the selected database.

The screenshot shows a 'Summary' window with the following fields:

- Action:** Restore Databases
- Selected Database(s):** AxiomData
- File location:** C:\Backup\20170630122145043_AxiomData.bak
- Output:** A table with columns 'Time' and 'Message'. A 'Clear Logs' button is located above the table.

At the bottom of the window are three buttons: '<<Back', 'Next>>', and 'Run'.

The user will see if *Restore completed* in the *Output* field of the window.

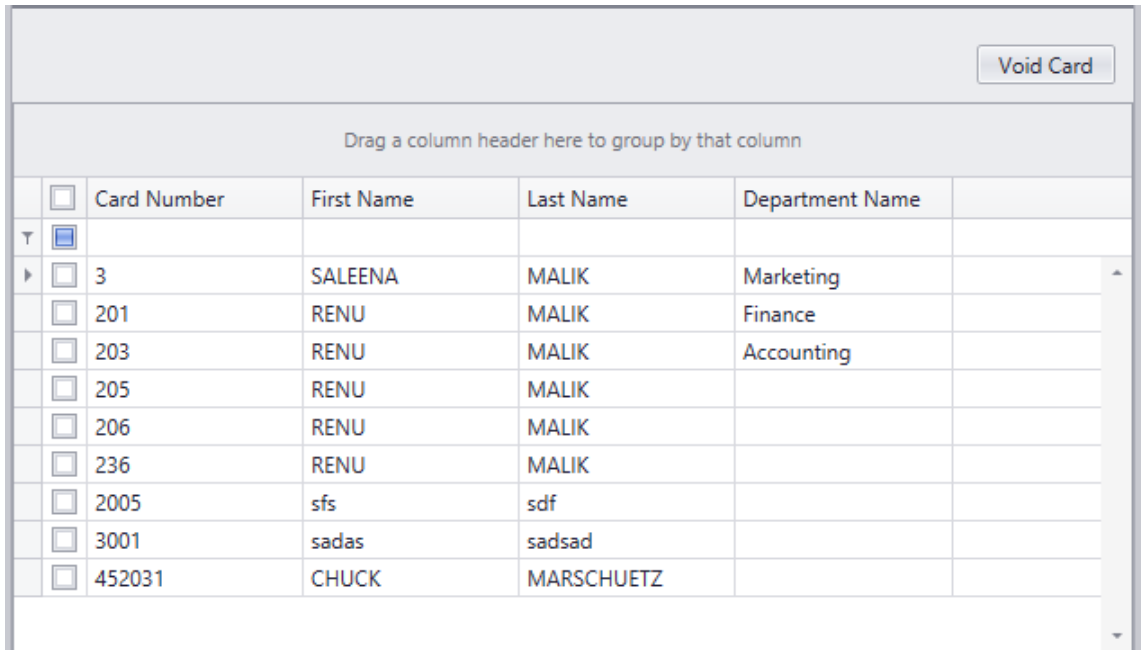
The screenshot shows the same 'Summary' window as above, but with the 'Output' table populated with a single row:

| Time | Item | Status | Message |
|----------------------|-----------|-------------------|--|
| 6/30/2017 3:25:52 PM | AxiomData | Restore Completed | From : C:\Backup\20170630122145043_AxiomData.bak |

The 'Run' button at the bottom is now disabled.

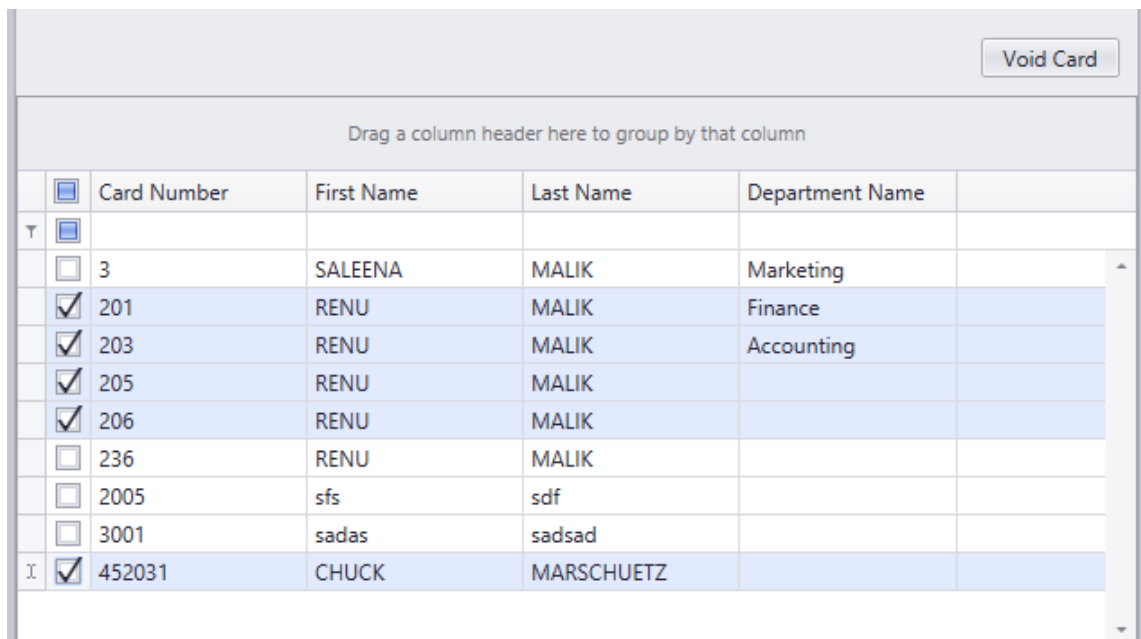
Void Cards

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 Settings* tab of *System Settings*.



| Void Card | | | | | |
|---|--------------------------|------------|-----------|-----------------|------------|
| Drag a column header here to group by that column | | | | | |
| <input type="checkbox"/> | Card Number | First Name | Last Name | Department Name | |
| T | <input type="checkbox"/> | | | | |
| | <input type="checkbox"/> | 3 | SALEENA | MALIK | Marketing |
| | <input type="checkbox"/> | 201 | RENU | MALIK | Finance |
| | <input type="checkbox"/> | 203 | RENU | MALIK | Accounting |
| | <input type="checkbox"/> | 205 | RENU | MALIK | |
| | <input type="checkbox"/> | 206 | RENU | MALIK | |
| | <input type="checkbox"/> | 236 | RENU | MALIK | |
| | <input type="checkbox"/> | 2005 | sfs | sdf | |
| | <input type="checkbox"/> | 3001 | sadas | sadsad | |
| | <input type="checkbox"/> | 452031 | CHUCK | MARSCHUETZ | |

Select the cards that you want to void manually. Clicking on *Void Card* at the top of window will immediately deactivate the selected cards.



| Void Card | | | | | |
|---|-------------------------------------|------------|-----------|-----------------|------------|
| Drag a column header here to group by that column | | | | | |
| <input type="checkbox"/> | Card Number | First Name | Last Name | Department Name | |
| T | <input type="checkbox"/> | | | | |
| | <input type="checkbox"/> | 3 | SALEENA | MALIK | Marketing |
| | <input checked="" type="checkbox"/> | 201 | RENU | MALIK | Finance |
| | <input checked="" type="checkbox"/> | 203 | RENU | MALIK | Accounting |
| | <input checked="" type="checkbox"/> | 205 | RENU | MALIK | |
| | <input checked="" type="checkbox"/> | 206 | RENU | MALIK | |
| | <input type="checkbox"/> | 236 | RENU | MALIK | |
| | <input type="checkbox"/> | 2005 | sfs | sdf | |
| | <input type="checkbox"/> | 3001 | sadas | sadsad | |
| I | <input checked="" type="checkbox"/> | 452031 | CHUCK | MARSCHUETZ | |

System Settings

System

AP Activity

The screenshot shows a web interface for configuring AP Activity. At the top, there are two tabs: 'System' and 'User'. Below these, there are several sub-tabs: 'AP Activity', 'System Settings', 'Color Settings', 'Email Configuration', 'Message Sounds', and 'Badge'. The 'AP Activity' tab is selected. The main content area contains the following settings:

- A heading: "Select Extra fields to display in access point activity window"
- Five numbered dropdown menus:
 1. Access Level
 2. Usage Count
 3. Department
 4. De-Activation Date
 5. (Empty)
- A text input field: "Number of Access Point Activity" with the value "10".
- A checkbox: "Display Photo Only" which is checked.

Select from the pull down lists up to five additional fields to be displayed in the Access Point Activity Window.

Choose the maximum number of Access Point Activity panes that can be on the screen at one time. Newer activities will be displayed and older activities will be removed as newer ones are entered.

Check *Display Photo Only* to only display the cardholder's picture in the Access Point Activity window.

System Settings

System User

AP Activity System Settings Color Settings Email Configuration Message Sounds Badge

Send Clear Alarm to Message Port:

Autogenerate Card Number:

Print area Muster report on this client:

Use Cardholder Initial Field as numeric data:

Multiple Access Levels: 10

Min Data: 0

Cardholder picture size(Millimeter): Height 0 Width 0

Alarm sound delay: 0 Min

DVR:

Restrict Duplicate Card PIN:

Do not Initialize the panels:

Show Cardholder PIN Code:

GT-Check late arriving only once:

Use Cardholder Initial Field as:

Auto void cards after(days): 0

Operator password expires after(days): 0

Area status check Interval : 0 (Seconds (min recommended 60))

Partial Download File Update Time

Send Clear Alarm 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.

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:

The Initials Field in the cardholder screen will now only accept numeric data.

Multiple Access Levels:

Set here the maximum number of Multiple Access Levels that a cardholder can be assigned.

Min. Data:

Enter a value from 0-10 (default = 0). You will not be allowed to save a cardholder until the *Initials* field has the selected number of required data.

Card Holder Picture Size (Millimeters):

Enter here the desired Height and Width. This size is for the cardholder screen only and does not apply to the card templates at all.

Alarm Sounds Delay:

The sound file will be delayed being play by the amount of time selected here. This will allow the event that caused the alarm to be rectified before an alarm is actually registered.

DVR:

The user can select only one of the two options: Centralized Opening or Mantrap Entry. Both of the options have similar functionalities where the operator controls the access to the doors after verifying who is at the door, but different video integration windows. Mantrap Entry option is per workstation

Centralized Opening:

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

Mantrap Entry

Mantrap Entry is another system option where an operator controls the access as per cardholder requests after verifying the person at the door requesting the access. The operator has control over which door he wants to provide the access to first, if more than one user requests access at the same time at various access points. This option is also integrated with some DVRs

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.

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.

GT-Check Late Arriving Only Once:

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

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.

Auto Void Cards After:

At 1:00am 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.

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 a chance to change their password when logging in, if the expired password is not changed AxiomXA™ will not allow login for that user. The new password cannot match the previous password.

Area Status Check Interval:

The server check time interval for empty *Areas* (60 seconds recommended settings).

Partial Download File Update Time:

Cards aren't sorted with each partial download, but are sorted only one time which is the time under this field.

Color Settings

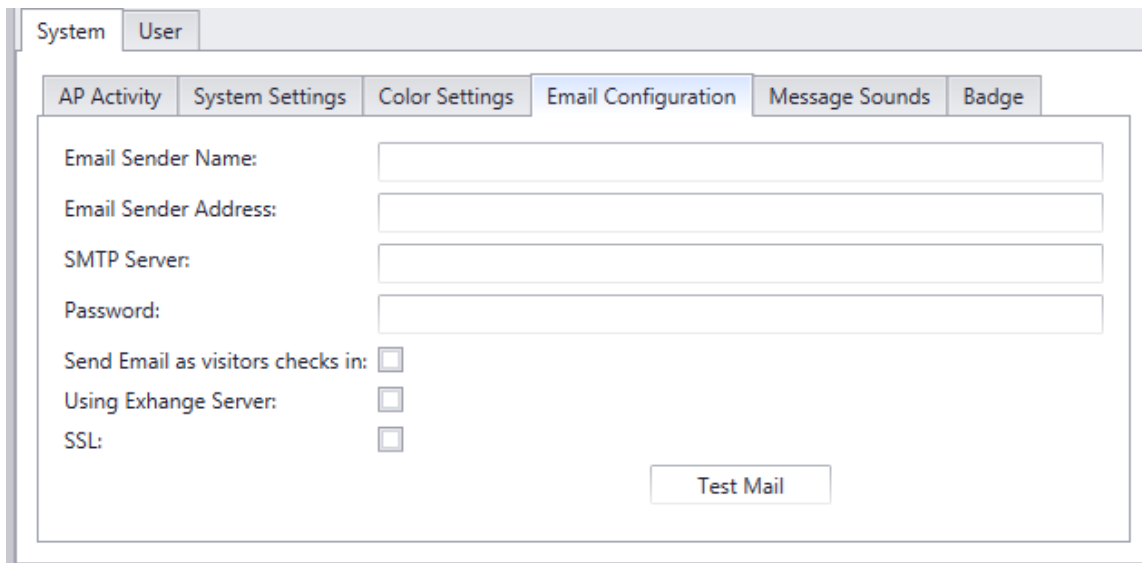
The screenshot shows the 'Color Settings' configuration window. It has a 'System' tab selected and a 'User' sub-tab. The main configuration area is titled 'Alarm' and contains a table with the following columns: Alarm Type, Background Color, Foreground Color, Bold, and Italic. There are five rows of settings for different alarm types. A 'Default Color' button is located at the bottom of the table.

| Alarm Type | Background Color | Foreground Color | Bold | Italic |
|-----------------------------|------------------|------------------|--------------------------|--------------------------|
| Default Alarm | Blue | Black | <input type="checkbox"/> | <input type="checkbox"/> |
| Acknowledge Alarm | #FF00FF00 | Black | <input type="checkbox"/> | <input type="checkbox"/> |
| Acknowledge Restore Alarm | #FF00FF00 | Black | <input type="checkbox"/> | <input type="checkbox"/> |
| UnAcknowledge Alarm | Red | White | <input type="checkbox"/> | <input type="checkbox"/> |
| UnAcknowledge Restore Alarm | Blue | White | <input type="checkbox"/> | <input type="checkbox"/> |

Default Color

You can edit the colors for the messages in the Event Viewer and the Alarms Monitor here. Select new backgrounds and font colors, as well as you can select bold and/or italic for the font.

Email Configuration



The screenshot shows a web interface with a navigation bar at the top containing 'System' and 'User' tabs. Below this is a sub-navigation bar with tabs for 'AP Activity', 'System Settings', 'Color Settings', 'Email Configuration' (which is highlighted), 'Message Sounds', and 'Badge'. The main content area contains several input fields and checkboxes: 'Email Sender Name:' with a text box, 'Email Sender Address:' with a text box, 'SMTP Server:' with a text box, 'Password:' with a text box, 'Send Email as visitors checks in:' with a checkbox, 'Using Exchange Server:' with a checkbox, and 'SSL:' with a checkbox. A 'Test Mail' button is located at the bottom right of the configuration area.

Email Sender Name:

Name of the Sender

Email Sender Address:

Sender's email address

SMTP Server:

Name of the SMTP server of Sending to' email.

Password:

Password

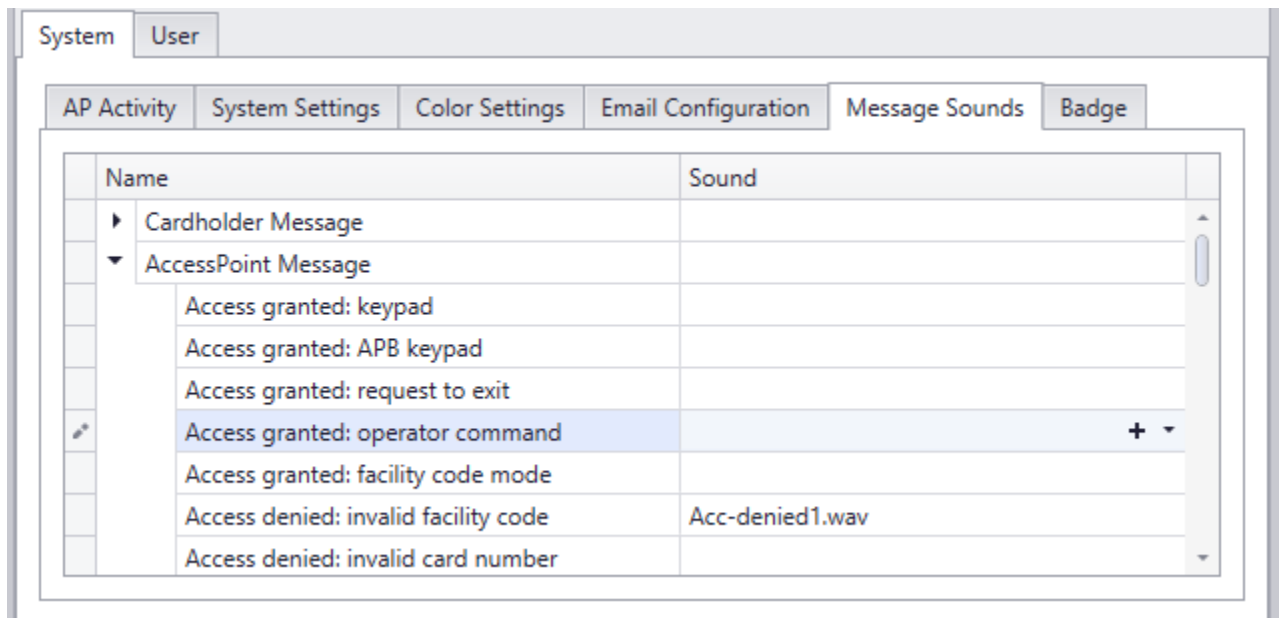
Send Email as the Visitor is Checked in:

Check this box 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 for this feature to function.

Using Exchange Server: Select if you are using Exchange Server

SSL: Select if your server requires SSL

Message Sounds



The same WAV file plays for both an event and an alarm. For an event the Wav file plays only once. On an alarm the WAV file is continuously repeated until the alarm is acknowledged.

Badge

The screenshot shows a web application interface for configuring badge settings. At the top, there are two main tabs: 'System' and 'User'. Under the 'User' tab, there are several sub-tabs: 'AP Activity', 'System Settings', 'Color Settings', 'Email Configuration', 'Message Sounds', and 'Badge'. The 'Badge' tab is currently selected. Within the 'Badge' tab, there are two sub-sections: 'Badge Settings' and 'Magnetic Encoder Setup'. The 'Badge Settings' section contains the following fields and options:

- Signature Device:** A dropdown menu.
- IP Camera**
- Camera Device:** A dropdown menu.
- IP Camera:** A text input field.
- Finger Print Device:** A dropdown menu.
- Badge Printers:** A dropdown menu.
- Duplex Badge Printing**

Under the *Badge* tab is where devices associated with creating badges are selected.

Cameras (or picture device) for acquiring the cardholder's picture are selected here.

Devices for acquiring the cardholder's signature and/or fingerprint are also selected here.

Check box is provided for selecting Duplex Badge Printing (printing on both sides of the card).

Magnetic Encoder Setup

The screenshot shows the 'Magnetic Encoder Setup' configuration page. It features a navigation menu with 'System' and 'User' tabs. Under 'User', there are sub-tabs for 'AP Activity', 'System Settings', 'Color Settings', 'Email Configuration', 'Message Sounds', and 'Badge'. The 'Badge' sub-tab is active, showing 'Badge Settings' and 'Magnetic Encoder Setup'. The 'Magnetic Encoder Setup' section includes a 'Printer Name' dropdown menu, three 'Track' tabs (Track 1, Track 2, Track 3), and a table for field configuration. The table has columns for 'Field Name', 'Length', 'Field Separator', and 'Pad Zeros'. Below the table, there are labels for 'Field Separator', 'Start Sentinel', 'End Sentinel', and 'Field Length' with a corresponding input field.

Printer Name

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

Field Name

Select the fields from 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

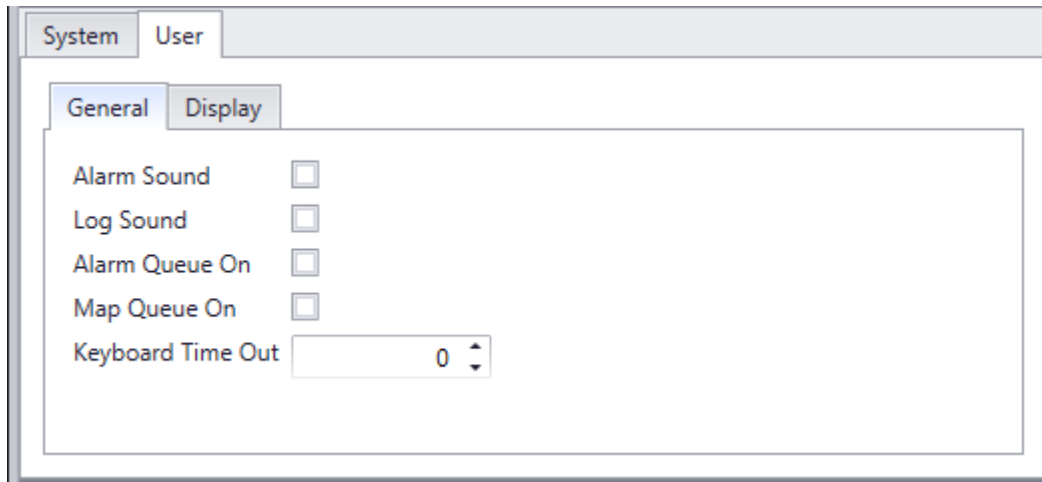
Check here to add leading zero character to numeric data to fill the field to its full length.

Field Length

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

User

General



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.

Queues:

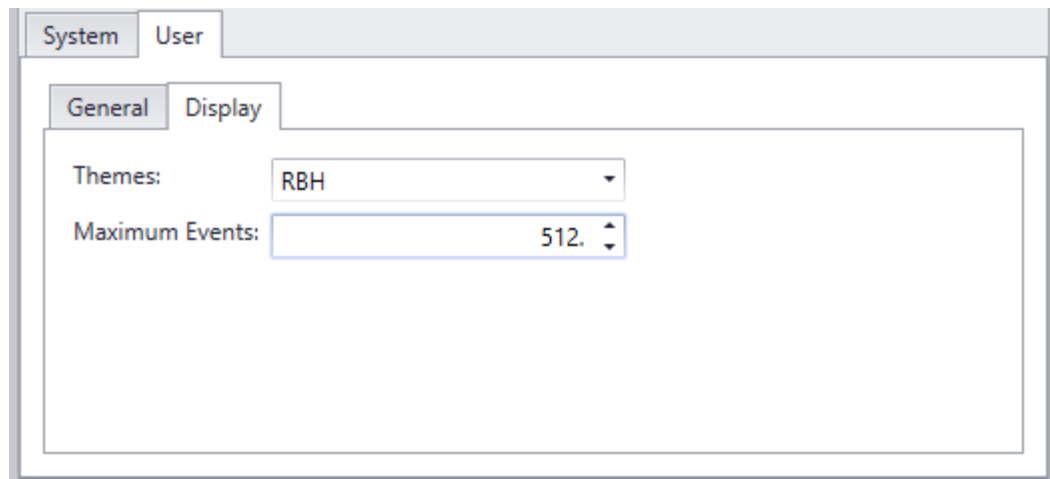
When the *Alarm Queue* is turned on the Alarm Monitor screen will be brought up whenever a new alarm comes in.

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



Themes:

Use the pull down list to select an aesthetic look for system's screens.

Maximum Events:

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

View

Under *View* the selections are *Event Viewer*, *Card Monitor*, *Alarms Monitor*, and *Access Point Activity*. *Event Viewer* comes up by default.

Event Viewer

| Date | Message | Device | Cardholder | Card N... | Controller | Netw... |
|-----------------|----------------------------------|-----------------|---------------------|-----------|------------|---------|
| 10/7/2015 8:... | D-NET CH-2 fail | IOC 16 Net52-6 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-1 fail | RC2 Net52-2 | | | NC100... | Netw... |
| 10/7/2015 8:... | Device controller: D-NET comm... | RC2 Net52-2 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-2 fail | RC2 Net52-2 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-2 fail | IOC 16Net52 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-1 normal | RC2 Net52-2 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-2 normal | RC2 Net52-2 | | | NC100... | Netw... |
| 10/7/2015 8:... | Device controller: D-NET comm... | RC2 Net52-2 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-2 normal | IOC 16Net52-5 | | | NC100... | Netw... |
| 10/7/2015 8:... | Device controller: D-NET comm... | IOC 16Net52-5 | | | NC100... | Netw... |
| 10/7/2015 8:... | D-NET CH-2 normal | IOC 16 Net52-6 | | | NC100... | Netw... |
| 10/7/2015 8:... | Device controller: D-NET comm... | IOC 16 Net52-6 | | | NC100... | Netw... |
| 10/7/2015 8:... | Access granted: reader | RC2 Net52-2... | Edward Vernon Ri... | 53071 | NC100... | Netw... |
| 10/7/2015 8:... | Access granted: reader | NIRC Net52-1... | Edward Vernon Ri... | 53071 | NC100... | Netw... |

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.

Event Viewer Commands

Right clicking on a line in the *Event Viewer* will produce a list of commands. The contents of the list will depend on the box clicked. Commands are described under System Status in [Chapter 6](#) System Status for the different items. In addition the command list will include, *Pause Display* and *Clear*.

Display Paused

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.

Card Monitor

| Area | Card Number | Last Name | First Name | Time | Reader |
|-----------|-------------|-----------|------------|---------------------|---------------|
| Main Area | 4294967295 | elevator | ee | 2017-07-04 13:23:32 | RC2 257-1\... |
| Main Area | 5 | Card | new | 2017-07-04 12:44:05 | RC2 257-1\... |
| Main Area | 1 | Shukla | Ro | 2017-07-04 12:42:01 | RC2 257-1\... |
| Main Area | 1202505 | CANNING | SA | 2017-07-04 12:09:44 | RC2 257-1\... |
| Main Area | 207 | MALIK | RE | 2017-07-04 12:08:17 | RC2 257-1\... |
| | 9 | Card | 9 | 2017-07-04 14:37:09 | RC2 258-1\... |
| | 8 | Card | 8 | 2017-07-04 14:36:31 | RC2 258-1\... |
| | 702 | issue | el | 2017-07-04 14:17:49 | RC2 258-1\... |
| | 605 | dfgdgfh | dfgdgh | 2017-07-04 13:14:32 | RC2 258-1\... |
| | 602 | delete | card | 2017-07-04 13:10:16 | RC2 258-1\... |
| | 4294967293 | bvccb | fjhgj | 2017-07-04 12:57:44 | RC2 258-1\... |

The *Card Monitor* will show the status of the selected cardholders. It will show what Area cardholders are in as well as the last access point used by a cardholder and when.



For the most effective use of this screen, customize it to your requirements. Show only the cardholder(s) you are interested in and hide any column not needed.

Area Monitor

The cardholders are sorted by Area in *Area monitor*.

| Card Number | LastName | FirstName | Time | Reader |
|-------------------|----------|-----------|---------------------|---------------------|
| ▼ Area: In Area 1 | | | | |
| 1007 | dd | nn | 2017-02-06 15:28:51 | NURC 257-3\Reader 1 |
| 1008 | sad | asd | 2017-02-06 15:28:34 | NURC 257-3\Reader 1 |
| 1010 | test crl | card | 2017-02-06 15:28:43 | NURC 257-3\Reader 1 |
| 1002 | ygh | fh | 2017-02-06 15:28:25 | NURC 257-3\Reader 1 |
| ▼ Area: Out Area | | | | |
| 4294967295 | 32 bit | Max | 2017-02-06 15:27:33 | NURC 257-3\Reader 2 |
| 1001 | Mayes | Dave | 2017-02-06 15:27:23 | NURC 257-3\Reader 2 |
| 1003 | sdasd | zAA | 15:28:59 | NURC 257-3\Reader 2 |
| 1006 | xcxz | zxc | 15:29:13 | NURC 257-3\Reader 2 |

Card/Area Monitor Commands

Activate

Activate will make an inactive card active.

Deactivate

Deactivate will make an active card inactive.

Set Area

Set Area will set the cardholder to be in a selected area.

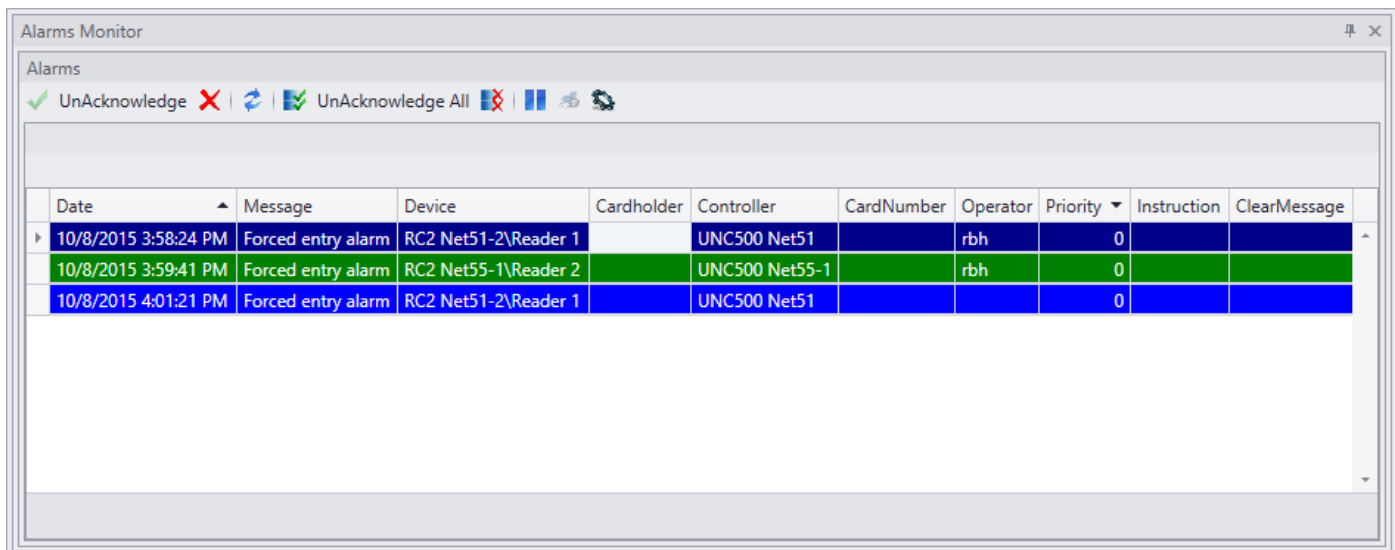
Reset area

Reset Area will set the cardholder to not be in any area.

Configuration...

Choosing *Configuration* will take you into the properties window of the selected Cardholder. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *Card /Area Monitor*.

Alarms Monitor



The screenshot shows the 'Alarms Monitor' application window. At the top, there are control buttons: a green checkmark for 'UnAcknowledge', a red 'X' for 'UnAcknowledge All', and several other icons. Below the buttons is a table with the following columns: Date, Message, Device, Cardholder, Controller, CardNumber, Operator, Priority, Instruction, and ClearMessage. The table contains three rows of data, all with a priority of 0.

| Date | Message | Device | Cardholder | Controller | CardNumber | Operator | Priority | Instruction | ClearMessage |
|----------------------|--------------------|----------------------|------------|----------------|------------|----------|----------|-------------|--------------|
| 10/8/2015 3:58:24 PM | Forced entry alarm | RC2 Net51-2\Reader 1 | | UNC500 Net51 | | rbh | 0 | | |
| 10/8/2015 3:59:41 PM | Forced entry alarm | RC2 Net55-1\Reader 2 | | UNC500 Net55-1 | | rbh | 0 | | |
| 10/8/2015 4:01:21 PM | Forced entry alarm | RC2 Net51-2\Reader 1 | | UNC500 Net51 | | | 0 | | |

The *Alarms Monitor* is used to monitor all Alarm activity. Alarms are acknowledged and cleared on this screen. Messages can be created to provide custom instructions on what needs to be done for each alarm.

Buttons



Acknowledge

Acknowledge is the first step to clearing an Alarm. An acknowledged Alarm is tied to the operator that acknowledged it. Only the acknowledging operator can clear the acknowledged Alarm.

Acknowledging an Alarm will also silence any audible associated with that Alarm.

Unacknowledge

If another operator actually actions the Alarm, the acknowledging operator can unacknowledged the Alarm so that the other operator can acknowledge it and then clear it.



Clear

Clearing an Alarm removes it from the *Alarms Monitor* screen. It **cannot** be recalled for any further action, but can be called up in a history report.



Detail

Detail will split the monitor screen. The right half of the screen provides more detailed information regarding the alarm, including instruction messages. What action was taken in regards to the Alarm can be entered on this screen as well.

The screenshot shows the 'Alarms' window with a table of alarm events and a detailed view of a selected alarm.

| Date | Mes... | Dev... | Car... | Con... | Car... | Ope... | P... | Inst... | Clea... |
|----------------------|--------|--------|--------|--------|--------|--------|------|---------|---------|
| 2/6/2017 10:21:06 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:21:14 AM | Acc... | RC2... | | UN... | | rbh | 0 | Alw... | Can... |
| 2/6/2017 10:21:19 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:21:37 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:22:16 AM | Acc... | NU... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:22:21 AM | Acc... | NU... | | UN... | | rbh | 0 | Alw... | Can... |
| 2/6/2017 10:22:37 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:22:41 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:22:56 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:23:00 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |
| 2/6/2017 10:23:06 AM | Acc... | RC2... | | UN... | | rbh | 0 | Alw... | Can... |
| 2/6/2017 10:30:45 AM | Acc... | RC2... | | UN... | | | 0 | Alw... | |

The detailed view on the right shows the following information:

- Date: 2/6/2017 10:22:21 AM
- Age: 5313
- Status: Acknowledged
- Alarm: Access granted: operator command
- Instructions: Always check cause of Alarm before Acknowledging it.
- Action Taken: [Dropdown menu]



Acknowledge All

Acknowledge All allows for the mass acknowledgement of **all** Alarms on the *Alarms Monitor* screen.

Unacknowledge All

Unacknowledge All allows for the mass unacknowledgement of **all** Alarms on the *Alarms Monitor* screen.

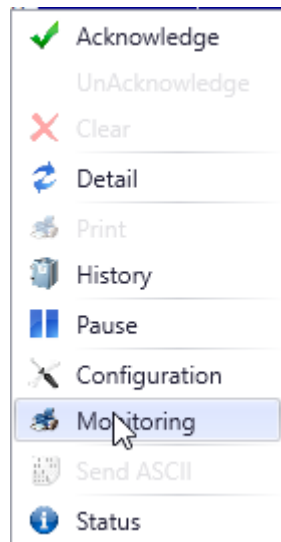
Pause

New alarms are always added to the bottom of the display, and the 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.

Color Settings

You can edit the colors for the messages in the Alarms Monitor here. Select new backgrounds and font Colors, as well as you can select bold and/or italic for the font.

Commands



Most of the commands available in right click menu are same as the buttons on the toolbar. Some extra commands in the right click menu are:

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.

Configuration

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

Monitoring

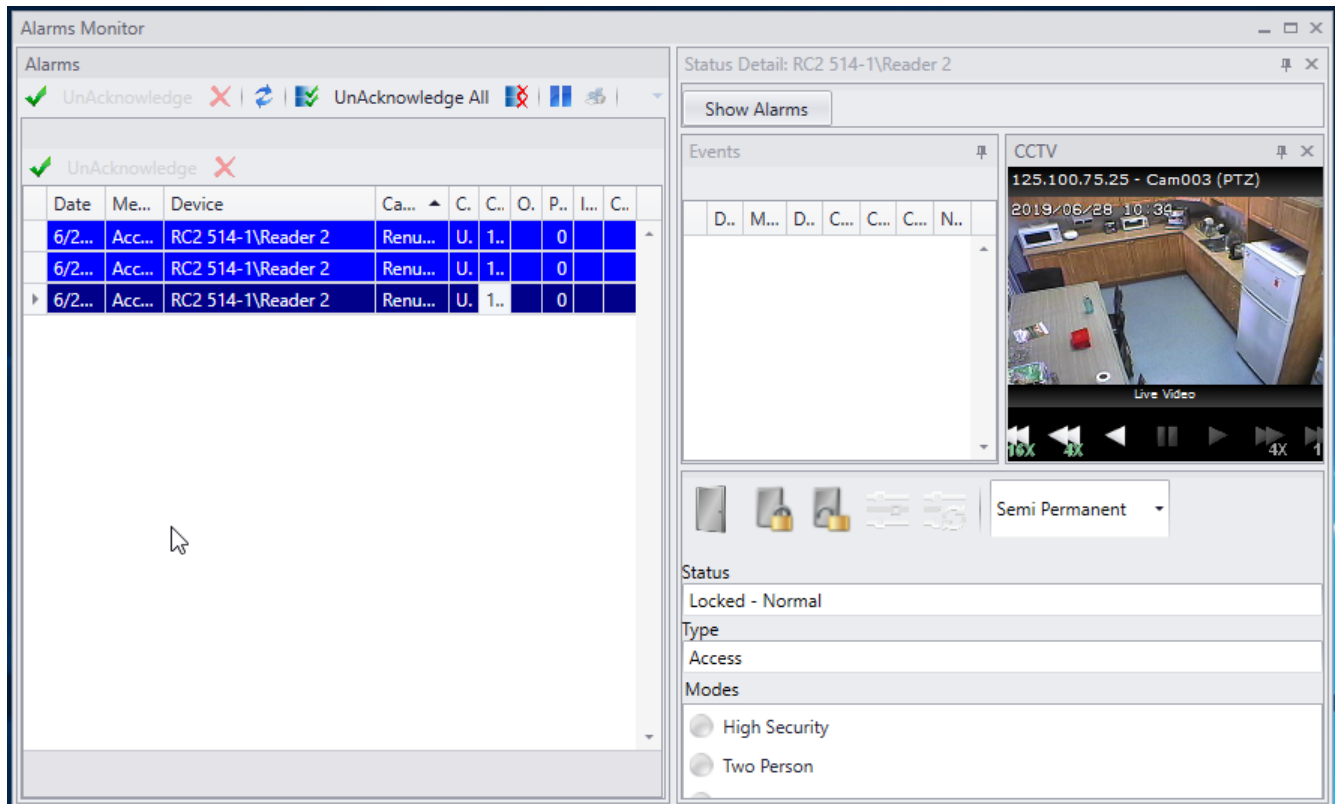
Monitoring will call up the monitoring window for the device associated with the selected alarm event.

Send ASCII

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

Status

Status will bring up a status window of the device in Alarm as it shows in System Status.



Access Point Activity

Access Point Activity is used to monitor selected access points. When an access point is accessed the information is displayed here.

The cardholder's configuration can be accessed and access point commands can be issued from this screen.

It is commonly used for video verification. The cardholders' picture will be displayed so that it can be checked against a live image of the cardholder at the door.

Access Point Activity Reader

| <input type="checkbox"/> | Name | NC100Name | Network Name | Device Name | |
|-------------------------------------|-----------------------|----------------|--------------|--------------|--|
| <input type="checkbox"/> | RC2 Net51-1\Reader 1 | UNC500 Net51 | Network 51 | RC2 Net51-1 | |
| <input type="checkbox"/> | RC2 Net51-1\Reader 2 | UNC500 Net51 | Network 51 | RC2 Net51-1 | |
| <input type="checkbox"/> | RC2 Net51-2\Reader 1 | UNC500 Net51 | Network 51 | RC2 Net51-2 | |
| <input checked="" type="checkbox"/> | NIRC Net52-1\Reader 1 | NC100 Net52-1 | Network 52 | NIRC Net52-1 | |
| <input checked="" type="checkbox"/> | NIRC Net52-1\Reader 2 | NC100 Net52-1 | Network 52 | NIRC Net52-1 | |
| <input checked="" type="checkbox"/> | RC2 Net52-2\Reader 1 | NC100 Net52-2 | Network 52 | RC2 Net52-2 | |
| <input checked="" type="checkbox"/> | RC2 Net52-2\Reader 2 | NC100 Net52-2 | Network 52 | RC2 Net52-2 | |
| <input type="checkbox"/> | NURC Net53-1\Reader 1 | UNC100 Net53-1 | Network 53 | NURC Net53-1 | |
| <input type="checkbox"/> | NURC Net53-1\Reader 2 | UNC100 Net53-1 | Network 53 | NURC Net53-1 | |
| <input type="checkbox"/> | RC2 Net54-1\Reader 1 | UNC500 Net54-1 | Network 54 | RC2 Net54-1 | |
| <input type="checkbox"/> | RC2 Net54-1\Reader 2 | UNC500 Net54-1 | Network 54 | RC2 Net54-1 | |
| <input type="checkbox"/> | RC2 Net55-1\Reader 1 | UNC500 Net55-1 | Network 55 | RC2 Net55-1 | |
| <input type="checkbox"/> | RC2 Net55-1\Reader 2 | UNC500 Net55-1 | Network 55 | RC2 Net55-1 | |
| <input type="checkbox"/> | RC2 Net51-2\Reader 2 | UNC500 Net51 | Network 51 | RC2 Net51-2 | |


Only the checked readers will be displayed in the *Access Point Activity* screen.

Each time an access point is used a new box appears on the screen.

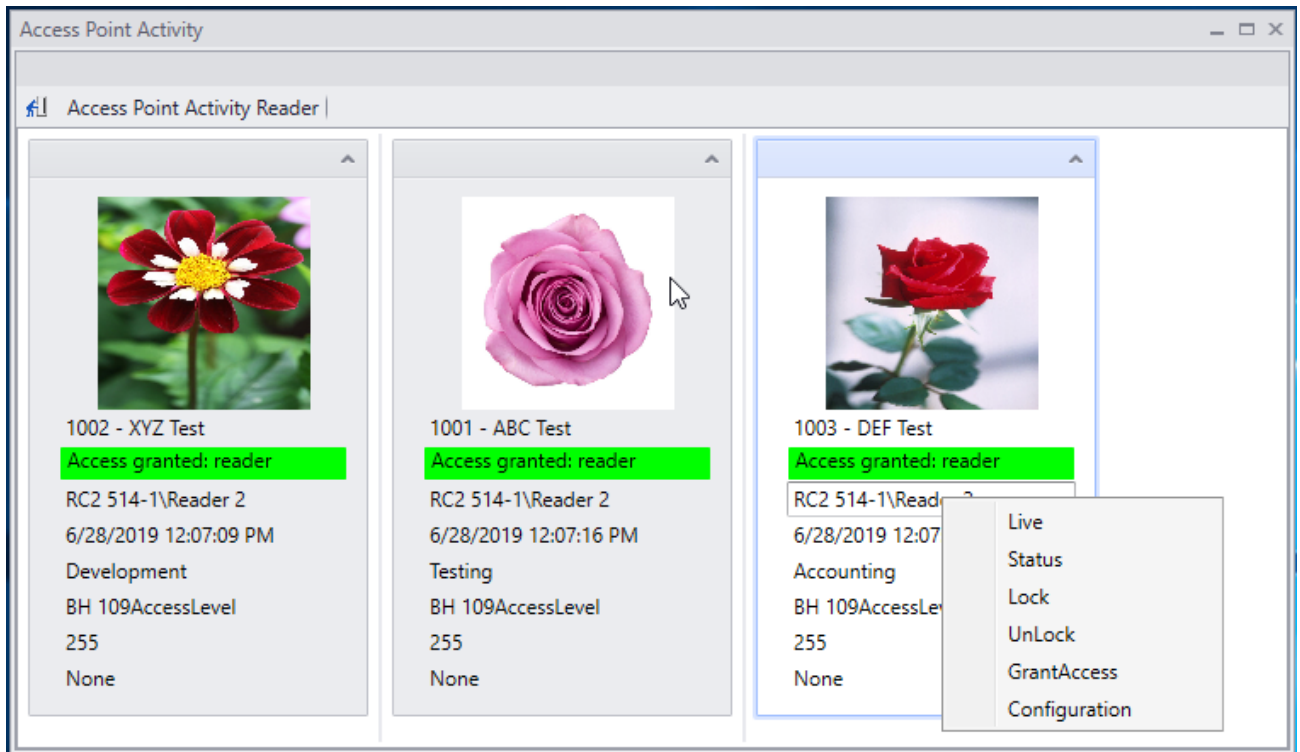
By highlighting the cardholder's name one can select *Configuration* and see the cardholder's information.

Highlight the reader in the box and you can execute the reader commands; *Status*, *Lock*, *Unlock*, or *Grant Access* on that access point.

Selecting *Live* (which will require CCTV and camera setup) will start live play of a camera configured for the selected item.

 *Access Point Activity* is often used in conjunction with CCTV cameras for video verification. The picture of the cardholder on the screen can be compared to a live video image.

The boxes can be minimized or maximized by clicking the chevron in the top right corner.



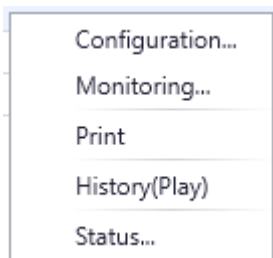
Chapter 6

System Status

The command lists will vary depending on the selection made, but will be universal throughout the system for any item selected. Meaning that access points commands are the same regardless of which view you are in or how the command list is accessed.

Networks

Networks is the default display for *System Status* and will display the status of networks in the system.



Configuration...

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System Status*.

Monitoring...

Choosing *Monitoring* will take you into the *Monitor Screen* of the selected item. In *Monitoring*, alarms can be set to trigger, messages can be blocked and/or sent out as ASCII messages, and *Global Commands* can be selected. These can be associated with any of the Network's events. Select *Cancel* or *Save* to return to the *System Status*.

Print

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

History (Play)

Clicking *History* will produce a report of up to the last ten events occurred for the selected network in its respective detailed status window

Status...

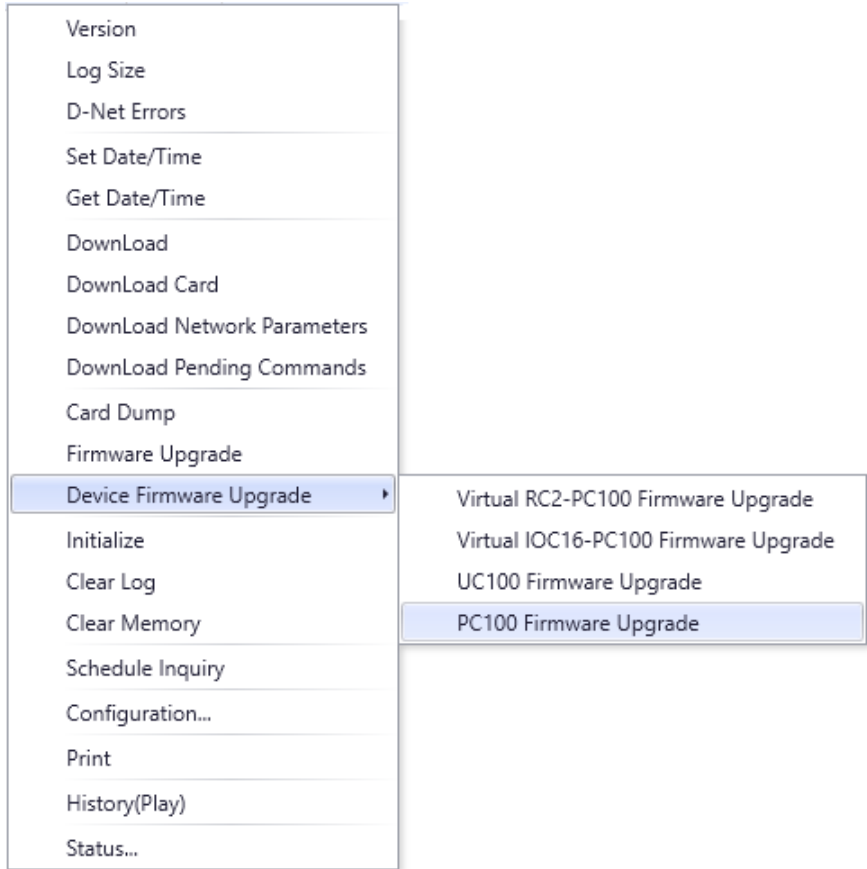
Clicking Status will open detailed status window for the network.

One can view network messages in the event viewer specific to the network(s) selected in this window.

Clicking on *Show Alarm* will open Alarm monitor window within detailed status showing last 10 Alarms for that network(s).

Controllers

Controllers will display the status of Network Controllers in the system.



Version

Version will return the firmware version of the selected Network Controllers.

Log Size

Log Size will return the amount of memory the selected Network Controllers 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 Network Controller's devices.

Set Date/Time

Set Date/Time is used to set the date and time for the selected Network Controllers.

Get Date/Time

Get Date/Time: will return the current date and time in the selected Network Controllers.

Download

Download will execute a full download to the selected Network Controllers.

Download Card

Download Card will execute a download of only the cardholder data to the selected Network Controllers.

Download Pending Commands

Download Pending commands will execute a download of only the pending command information to the selected Network Controllers.

Firmware Upgrade

Select *Firmware Upgrade* to upload a firmware file into the selected Network Controllers.

Device Firmware Upgrade

Select *Device Firmware Upgrade* to upload a firmware file into devices RC2/NURCs/NIRCs, IOC16, PC-100 panels, or SafeSuite™ panels.

Initialize

Initialize will initialize the microprocessor of the selected Network Controllers.

Clear Log

Clear Log will delete all messages from the selected Network Controllers' log buffer.

Clear Memory

Clear Memory will remove all data in the selected Network Controllers' RAM. This will include all database files and log messages.

Schedule Inquiry

Schedule Inquiry will return the status of all schedules for the selected Network Controllers.

Configuration...

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System Status*.

Print

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

History (Play)

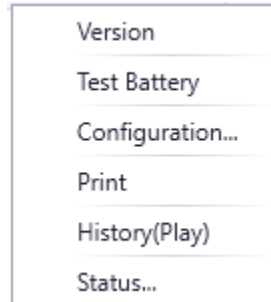
Clicking *History* will produce a report of up to the last ten events that occurred for the selected controller(s).

Status...

Selecting *Status* will split the screen and provide a *Status Detail* view of the selected Access point. Along with the *Status Detail*, an *Event Viewer* will be provided and *Alarms Monitor* with last 10 Alarms for the specific controller can be seen by Clicking *Show Alarm*. Click the *Close (X)* in the top right corner to return to the System Status.

Device Controllers

Device Controllers will display the status of device controllers in the system.



Version

Version will return the firmware version of the selected Device Controllers.

Test Battery

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

Configuration...

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System Status*.

Print

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

History (Play)

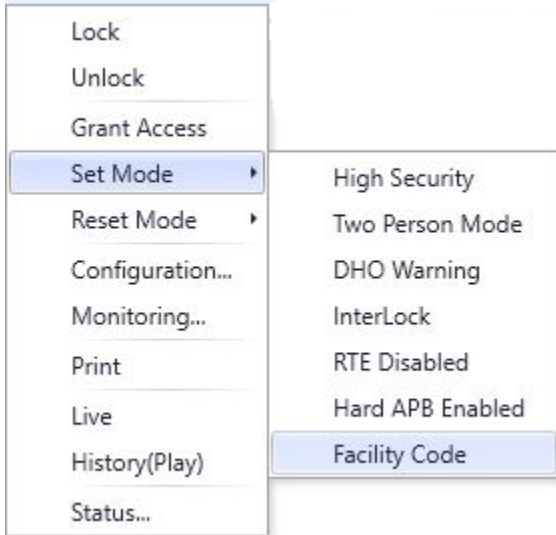
Clicking *History (Play)* will produce a report of up to the last ten events that occurred for the selected device controller(s). A *Playback* button would be available if CCTV is configured for the device.

Status...

Selecting *Status* will split the screen and provide a *Status Detail* view of the selected device. Along with the *Status Detail* an *Event Viewer* will be provided. Clicking on *Show Alarms* will open a window with last 10 alarms of selected device. Click the *Close (X)* in the top right corner to return to the *System Status*.

Access Points

Access Points will display the status of access points in the system.



Lock

Lock will lock at all selected access points.

Unlock

Unlock will unlock at all selected access points.

Grant Access

Grant Access will grant access at all selected access points.

Set Mode

Set Mode is used to turn on 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.

Reset Mode

Reset Mode is used to turn off different modes (High Security, Two Person, Door Held Open, Interlock, Request to Exit Enabled, Hard Antipassback Disabled, 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 is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System Status*.

Monitoring...

Choosing *Monitoring* will take you into the *Monitor Screen* of the selected item. In *Monitoring*, alarms can be set to trigger, messages can be blocked and/or sent out as ASCII messages, and *Global Commands* can be selected. These can be associated with any of the Access Point's events.

Associating the cameras with an Access Point is also done in *Monitoring* under CCTV. Up to 4 cameras can be selected for a device, one of which needs to be selected as *Main* camera. Select *Cancel* or *Save* to return to the *System Status*.

Print

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

Live

Selecting *Live* will start live play of the Main camera configured for the selected device.

History (Play)

Clicking *History(Play)* will produce a report of up to the last ten events that occurred for the selected access point(s)..

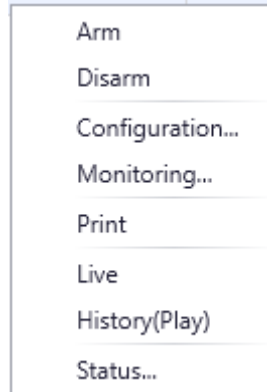
A *Playback* button is shown with the events to start CCTV playback for the selected device starting from the time stamp of the selected event. CCTV and cameras must be configured for this command to function.

Status...

Selecting *Status* will split the screen and provide a *Status Detail* view of the selected item. Along with the *Status Detail*, an *Event Viewer*, and a *CCTV* view will be provided. *Show Alarms* will open a window with last 10 Alarms for selected device(s). Click the *Close (X)* in the top right corner to return to the *System Status*.

Inputs

Inputs will display the status of inputs in the system.



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 input. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System status*.

Monitoring...

Choosing *Monitoring* will take you into the *Monitor Screen* of the selected input. In *Monitoring*, alarms can be set to trigger, messages can be blocked and/or sent out as ASCII messages, and *Global Commands* can be selected. These can be associated with any of the Input's events. Associating a camera with an Input is also done in *Monitoring*. Up to 4 cameras can be selected for same device. Select *Cancel* or *Save* to return to the *System Status*.

Print

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

Live

Selecting *Live* will start live play of the Main camera configured for the selected input.

Play History

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

A *Playback* button will be available if selected input has CCTV configured

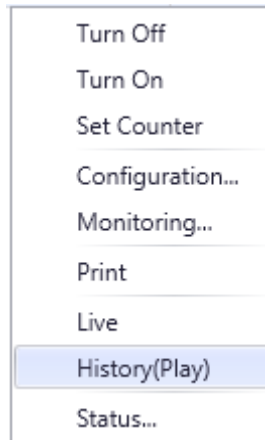
Clicking *Playback* will start CCTV playback for the selected input starting from the time stamp of the selected event. CCTV and cameras must be configured for this command to function.

Status...

Selecting *Status* will split the screen and provide a *Status Detail* view of the selected input. Along with the *Status Detail*, an *Event Viewer* and a *CCTV* view will be provided. Clicking on *Show Alarms* will bring up a window with last 10 Alarms for selected input. Click the *Close (X)* in the top right corner to return to the *System Status*.

Outputs

Outputs will display the status of outputs in the system.



Turn On

Turn On will turn all selected outputs on.

Turn Off

Turn Off will turn all selected outputs off.

Set Counter

Set Counter is used to establish the selected outputs' counter value.

Configuration...

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System Status*.

Monitoring...

Choosing *Monitoring* will take you into the *Monitor Screen* of the selected item. In *Monitoring*, alarms can be set to trigger, messages can be blocked and/or sent out as ASCII messages and *Global Commands* can be selected. These can be associated with any of the Output's events. Associating a camera with an Output is also done in *Monitoring*. Up to 4 cameras can be selected for same output. Select *Cancel* or *Save* to return to the *System Status*.

Print

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

Live

Selecting *Live* will start live play of the Main camera configured for the selected output.

Play History

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

A *Playback* button will be available if selected output has CCTV configured.

Clicking *Playback* will start CCTV playback for the selected input starting from the time stamp of the selected event. CCTV and cameras must be configured for this command to function.

Status...

Selecting *Status* will split the screen and provide a *Status Detail* view of the selected item. Along with the *Status Detail*, an *Event Viewer* and a *CCTV* view will be provided. Clicking on *Show Alarms* opens the window with last 10 Alarms for selected output. Click the *Close (X)* in the top right corner to return to the *System Status*.

Apartments

Apartments will display the status of SafeSuite™ and AlarmPanel™ devices in the system.



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 (15 for Alarm panel) are cleared.

Forced Arm

Forced Arm will arm the keypad of the selected apartments even if zones are in violation.

Arm

Arm will arm (away) the keypad of the selected apartments.

Disarm

Disarm will disarm the keypad of the selected apartments.

Configuration...

Choosing *Configuration* will take you into the properties window of the selected item. More detailed information is given in [Chapter 7 Database](#). Select *Cancel* to return to the *System Status*.

Monitoring...

Choosing *Monitoring* will take you into the *Monitor Screen* of the selected item. In *Monitoring*, alarms can be set to trigger, messages can be blocked and/or sent out as ASCII messages and *Global Commands* can be selected. These can be associated with any of the Apartment's events. Select *Cancel* or *Save* to return to the *System Status*.

History (Play)

Clicking *History (Play)* will produce a report of the last ten events that occurred for the selected apartment(s) in detailed status window.

Status...

Selecting *Status* will split the screen and will provide a *Status Detail* view of the selected item. Along with the *Status Detail* an *Event Viewer* will be provided. Clicking *Show Alarms* will bring up la t 10 alarms for selected apartment. Click the *Close (X)* in the top right corner to return to the *System Status*.

Access Point Groups

Access Point Groups will display the status of access point groups in the system.

Commands for *Access Point Groups* are the same as those for single access points. The command is applied to all access points in a group. This can be more convenient than selecting multiple access points under *Access Points*.

Output Groups

Output Groups will display the status of output groups in the system.

Commands for *Output Groups* are the same as those for single outputs. The command is applied to all outputs in a group. This can be more convenient than selecting multiple outputs under *Outputs*.

Input Groups

Input Groups will display the status of input groups in the system.

Commands for *Input Groups* are the same as those for single inputs. The command is applied to all inputs in a group. This can be more convenient than selecting multiple outputs under *Inputs*.

Guard Tours

Guard Tours will display the status of guard tours in the system. You can select *Configuration*, *Monitoring*, *Status*, *Reports*, and *CCTV* for each guard tour.

Part 5

Chapter 7

Database

Operators

From the Operators Screen the following can be done:

- Create and manage operator accounts for the AxiomXA™ 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).

| Drag a column header here to group by that column | | |
|---|---------------------------------|----------|
| | Operator Name | Login Id |
| T | | |
| ▶ | built-in administrative account | rbh |
| | John Smith | JohnS |
| | Harold Jones | Harry |

If the system is setup and licensed for the *Active Directory* option then the AxiomXA™ system can use the current domain user's authentication to login. And those users will be automatically added as operators in AxiomXA system.

The screenshot shows a web form for creating a new operator. It is divided into three main sections: 'Name', 'Password', and 'Profile'.
1. **Name**: Contains two input fields. The first is labeled 'Name :' and contains the text 'New Operator'. The second is labeled 'Login Id :'.
2. **Password**: Contains two input fields. The first is labeled 'Password :' and the second is labeled 'Confirm Password :'.
3. **Profile**: Contains two dropdown menus. The first is titled 'Operator Security Profile' and has a small box with the number '1' and a dropdown arrow showing 'Master Profile'. The second is titled 'Language' and has a dropdown arrow showing 'English'.

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 / Confirm Password

This is the log in password for the operator. It is entered twice for confirmation. *Password should contain minimum 8 characters with lowercase, uppercase, number & special character*.

Operator Security Profile

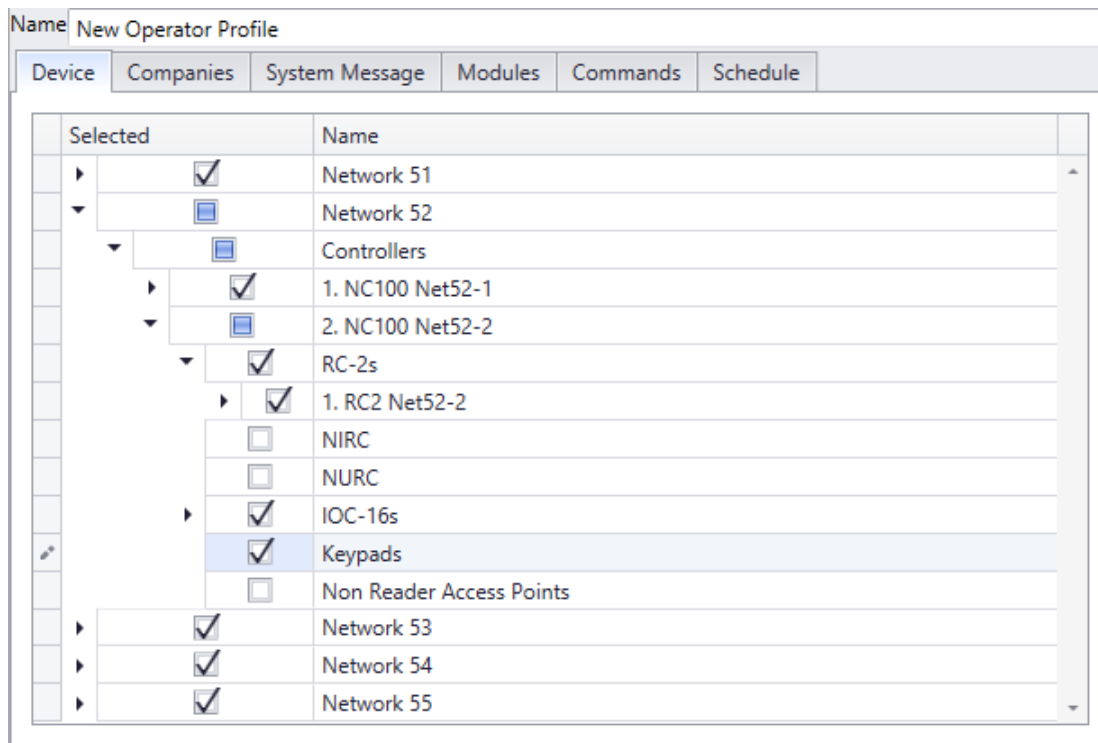
Click the *pull down* menu at the end of the list box and select a profile from the list.

Language

Click the *pull down* menu at the end of the list box and select a language from the list. When the operator logs in this language is set up in the software.

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

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 of selected Profile.

Companies

From the *Companies* 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 access to every company.

System Messages

The *System Messages* tab allows the restriction of messages the operator can see

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 various modules of the software.

Under *Cardholders* and *Devices* as module there are further sub-categories so that operator profiles can be defined accordingly.

Commands

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

Schedule

From the Schedule tab the operator can be restricted to have access to certain schedules only.

Holidays

Use the *Holidays* window to define *Holiday* dates. AxiomXA™ 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.

The screenshot shows the 'Holidays' configuration window. It has three main sections: 'Name', 'Network', and 'Holiday Type/Designation'. The 'Name' section has a text input field containing 'Labour Day'. The 'Network' section has a text input field containing '0' and a dropdown menu with '(All)'. The 'Holiday Type' section has a dropdown menu with 'Floating Date' and a 'Carry Forward' checkbox which is checked. The 'Holiday Designation' section has two radio buttons, 'Holiday 1' (selected) and 'Holiday 2'. Below this is a 'Holiday Time' section with a 'Day' field containing 'First' and 'Monday', and a 'Month' dropdown menu with 'September'.

Name

Up to 50 alphanumeric characters may be entered here.

Network

Holidays can be designated for all networks, a single network, or selections of multiple networks. 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 network selections in the holiday record.

Start Date

Start Date is the date on which the holiday begins. For single day holidays (e.g., Labour Day), select the same date for both start and end. For holidays that span several days (e.g., Christmas break) this is the first day of the holiday (e.g., Dec 23/16).

End Date

End Date is the date on which the holiday ends. 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 23/16 through Dec 30/16, select Friday December 30, 2016.

Holiday Designation

Radio buttons (*Holiday 1* or *Holiday 2*) are to 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

AxiomXA™ 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

A pull down list with *Variable Date*, *Fixed Date*, or *Floating Date* is used to select the type holiday. *Variable Date* holidays are not on the same date from year to year and therefore can't carry forward. A holiday that occurs on the same calendar date each year is a *Fixed Date* holiday. A *Floating Date* holiday isn't on the same date from year to year, but does reoccur in an easily predictable manner. E.g. Labour Day is a *Floating Date* holiday since it always occurs on the first Monday in September. New Year's Day is a *Fixed Date* holiday and Good Friday is a *Variable Date* holiday.

Carry Forward

Click on *Carry Forward* to copy holidays that have past to the next year. For example it would create the *Fixed Date* holiday 'New Year's Day – 1 Jan 2017' from the *Fixed Date* holidays 'New Year's Day – 1 Jan 2016'. *Floating Date* holiday 'Labour Day – 4 Sep 2017' would be created from *Floating Date* holiday 'Labour Day – 5 Sep 2016'.

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, 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 *Period* does not represent a continuous block of time. The start and end times are independent of one another, although AxiomXA™ 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, AxiomXA™ 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 100).

As an example, one may 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 | | | | | | | | | | | | |
|-------------|----------------|-------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|---|
| Periods | Start | End | Sun | Mon | Tue | Wed | Thu | Fri | Sat | H 1 | H 2 | | |
| ▶ Period 1: | 08:00 | 17:00 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ▲ |
| Period 2: | 11:00 | 17:00 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 3: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 4: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 5: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 6: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 7: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 8: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 9: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 10: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 11: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 12: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 13: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 14: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 15: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| Period 16: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ▼ | |

Name

Up to 50 alphanumeric characters may be entered here.

Start

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

End

End (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 Network Controller 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*, AxiomXA™ 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*.



Note that one second after 23:59:59 is 00:00:00 and not 24:00:00, therefore the time 24:00 is never actually reached, but it may be entered for the end of the day. If you want a schedule to end at midnight the closest you can get is one minute before or after (either 23:59 or 00:01).

| Name | | Night Shift | | | | | | | | | | |
|------------|-------|-------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|
| Periods | Start | End | Sun | Mon | Tue | Wed | Thu | Fri | Sat | H 1 | H 2 | |
| Period 1: | 18:00 | 24:00 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Period 2: | 00:00 | 04:00 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 3: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 4: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 5: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 6: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 7: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 8: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 9: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 10: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 11: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 12: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 13: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 14: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 15: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 16: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

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 AxiomXA™ System. 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 | | 24 Hour | | | | | | | | | | |
|------------|-------|---------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--|
| Periods | Start | End | Sun | Mon | Tue | Wed | Thu | Fri | Sat | H 1 | H 2 | |
| Period 1: | 00:00 | 24:00 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 2: | 00:00 | 00:01 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 3: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 4: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 5: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 6: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 7: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 8: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 9: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 10: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 11: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 12: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 13: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 14: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 15: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 16: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

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 | | | | | | | | | | |
|------------|-------|-----------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--|
| Periods | Start | End | Sun | Mon | Tue | Wed | Thu | Fri | Sat | H 1 | H 2 | |
| Period 1: | 08:00 | 17:00 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 2: | 12:00 | 17:00 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 3: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 4: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 5: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 6: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 7: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 8: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 9: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 10: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 11: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 12: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 13: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 14: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 15: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Period 16: | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

Areas

Areas need to be setup to control and monitor cardholder movement. They are primarily used in conjunction with Antipassback.

| | |
|--|------|
| Name | |
| New Area | |
| Reset Cardholder area Schedule | |
| 0 | |
| Input | |
| 0 | None |
| Output | |
| 0 | None |
| <input type="checkbox"/> Antipassback Area | |

Name

Up to 50 alphanumeric characters may be entered here.

Reset Cardholder Area Schedule

Pull down the list 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. The start time of the schedule selected is the time when Area will reset.

Input

Pull down the list 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

Pull down the list and select an output. When the area becomes empty (cardholder count drops to zero) the output will turn on (semi-permanently).

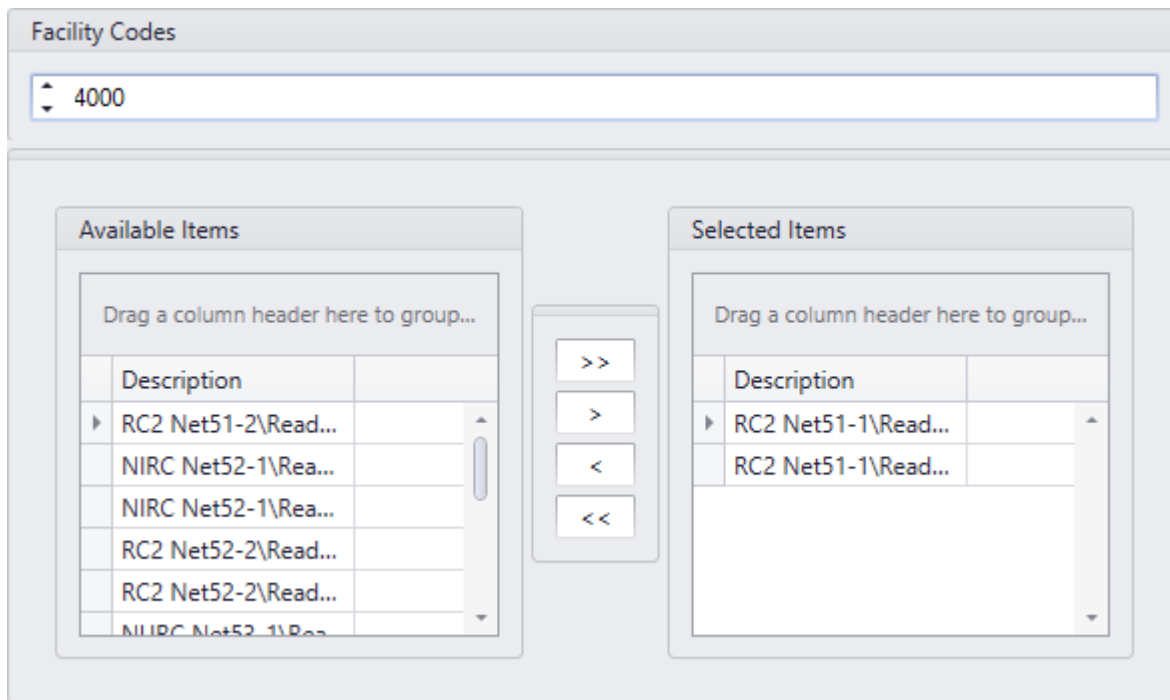
Antipassback Area

This is a check box to select if this area is an Antipassback Area. See Antipassback on page 21 for more details on antipassback.

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 one AxiomXA™ system. 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.



When using multiple *Facility Codes*, cards having the same access code, but different *Facility Codes* will be read as the same card. AxiomXA™ 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 **any** *Facility Code* will be accepted.

Facility Codes

Facility code is entered here. Use the spin button to select facility code

Available Items

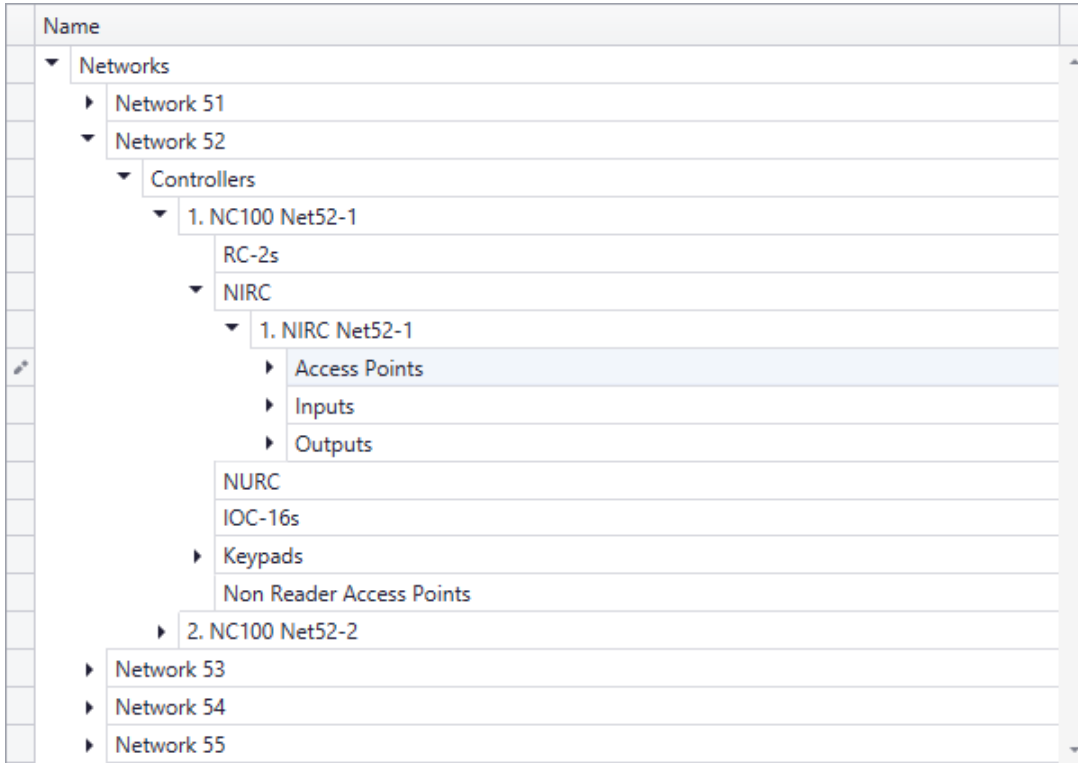
Available Items will show all of the access points in the system, (except the ones that have already been selected).

Selected Items

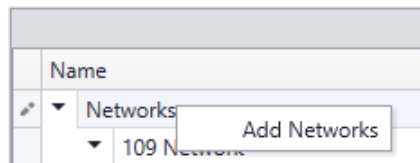
Selected Item lists the access points requiring the facility code.

Hardware Setup

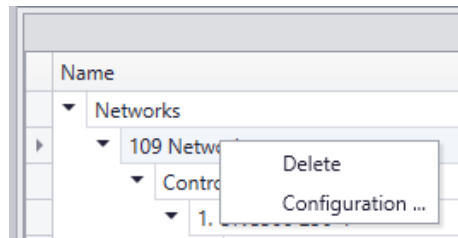
The *Hardware Setup* screen is where new hardware items are added to the system.



Networks



Right click on *Networks* or click on Add button at the bottom toolbar (available only for Tile view) to add a new network to the system. This will bring up the network configuration window to set the properties of the new network. Under the newly created Network will be an icon to add Controllers. Up to fifteen controllers can be connected on one network.



Right click on a Network or Click on the buttons at the bottom (only for Tile view) to either *Delete* that Network or to go into the Network's *Configuration* screen.

Network Name

Up to 50 alphanumeric characters may be entered here.

Server

Select from the pull down list of Servers the *Comm Server* this network is connected to.

General

Port Type

AxiomXA™ 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 address²

Use the spin buttons to select the address of the alternative or backup master Controller. If the Axiom server loses communications with the primary master Controller (address #1) it will switch to the alternate controller to resume communications with the network. This feature requires NC100 firmware version 7.40 or higher. UNC500 and UNC100 always had this feature.

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. Under a modem connection situation, this polling frequency comes into effect as soon as the modem connection has been established with the remote site.

Network Timeout

Network Timeout establishes the duration of time that must expire before the PC will declare a 'Communications Offline' condition. AxiomXA™ comes with a default timeout of 1000-milliseconds

C-Net Parameters

The C-Net parameters are for communications between the master Network Controller and slave Network Controller controllers on the C-Net. The master Network Controller does not poll the slaves. Rather, each slave Network Controller on the C-Net sends test signals to the master Network Controller 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 Network Controller on either channel A or

² This selection is only available if the optional license for the Alternate Master Network Controller Software has been purchased and installed.

channel B. Beyond this value, the master Network Controller 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.

The screenshot shows a configuration window with the following details:

- Buttons: Save, Cancel
- Network Name: 109 Network
- Server: RENUVMWINDOWS10
- General tab (selected)
- Day Light Saving time:
 - Date to move 1 Hour ahead: [Empty dropdown]
 - Date to move 1 Hour behind: [Empty dropdown]
- Battery test Interval: 24:00 HH:MM
- Time zone Difference: 00:00 HH:MM, Forward
- Card Size: 32 Bit
- Slave Protocol: C-Net
- Customer Key: [Empty text box]

Day Light Savings Time

Pull down the calendar to select a date in which the Controller will change the time of day because of Day Light Savings Time. Leave these boxes empty if Day Light Savings Time change is not required. 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 Controller (not the PC) so the dates need to be downloaded to the Controller before the change date so that controllers change time for DST even if not connected to PC.

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 cardholder database by not allowing card numbers over a preset value. Allowing larger card numbers will use more of the Network Controller's memory.

Slave Protocol

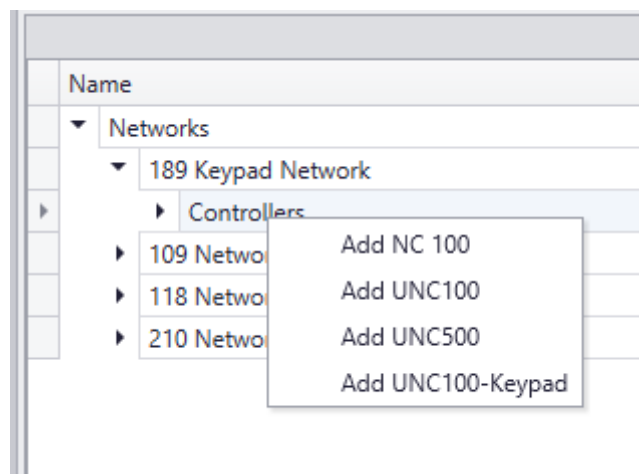
C-Net – Protocol used for NC100s to communicate with each other

E-Net – Protocol used for UNC's to communicate over TCP/IP networks.

Customer Key – Encryption/Decryption Key used with E-net Communication to Controllers.

Use Device Locator to configure Matching Encryption/Decryption Key.

Network Controllers



Type of network controller is selected at the time of adding the controller in the system. Four types of network controllers are available at this time to add in the hardware setup: NC-100, UNC500, UNC100 and UNC100-Keypad depending upon the hardware connected.

Controller Properties are set in the configuration window of controllers. The address is set when the controller is created in the system and cannot be edited later. When a UNC500 controller is added to the system an RC-2 is also added as address 1 and the UNC500 cannot be deleted without deleting the RC-2. The UNC100 works the same way with an NURC as address 1.

UNC-100-Keypad controller adds an NURC as address 1, and an Alarm Keypad as address 21.

Save Cancel

Address: 1

Controller Name: UNC500 256-1

Controller Type: UNC500

General

D-Net protocols:

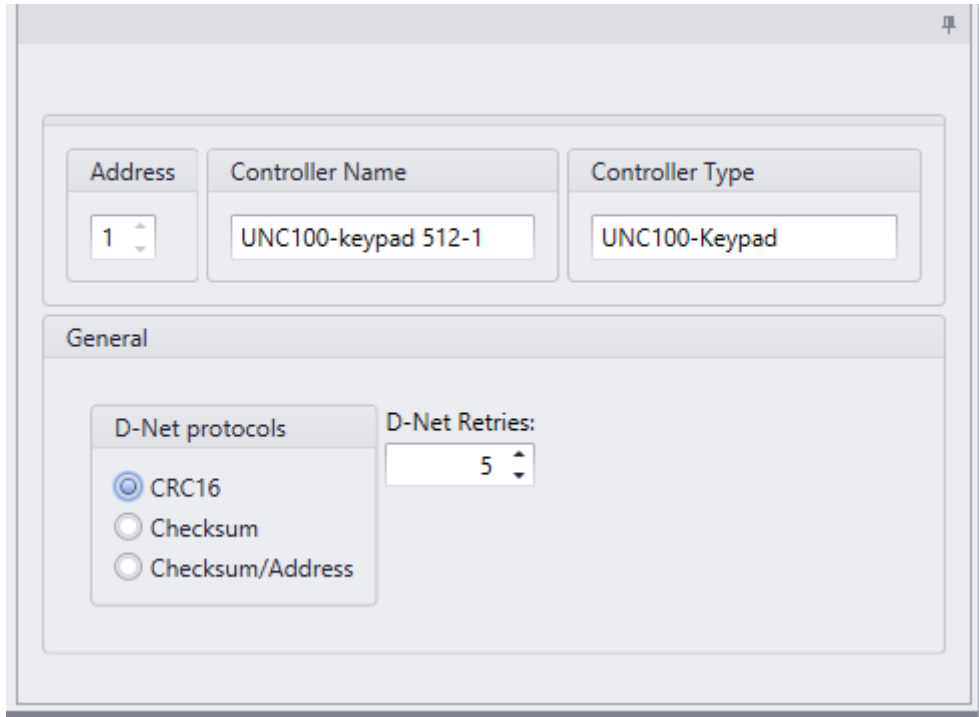
- CRC16
- Checksum
- Checksum/Address

D-Net Retries: 5

E-Net protocols:

Serial Number: 0

IP Address:



Address

Use the *Spin Buttons* to select the appropriate address for the controller being added. The lowest available address will come up by default.

Controller Name

A default name is added by the system depending upon the type of controller added, and the network ID under which controller is added. Default name can be changed and up to 50 alphanumeric characters may be entered.

Controller Type

Controller Type is added by the system depending upon the selection of controller type at the time of adding controller and cannot be changed.

General

D-Net Protocol

Select one of three protocols for the D-Net.

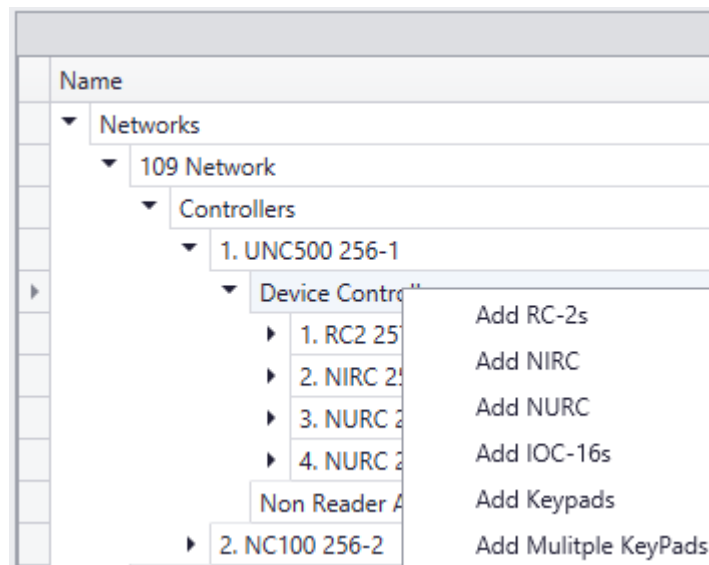
- ☉ **CRC16** is a newer more up to date protocol that is now programmed into all devices. All the current devices use CRC16 protocol.

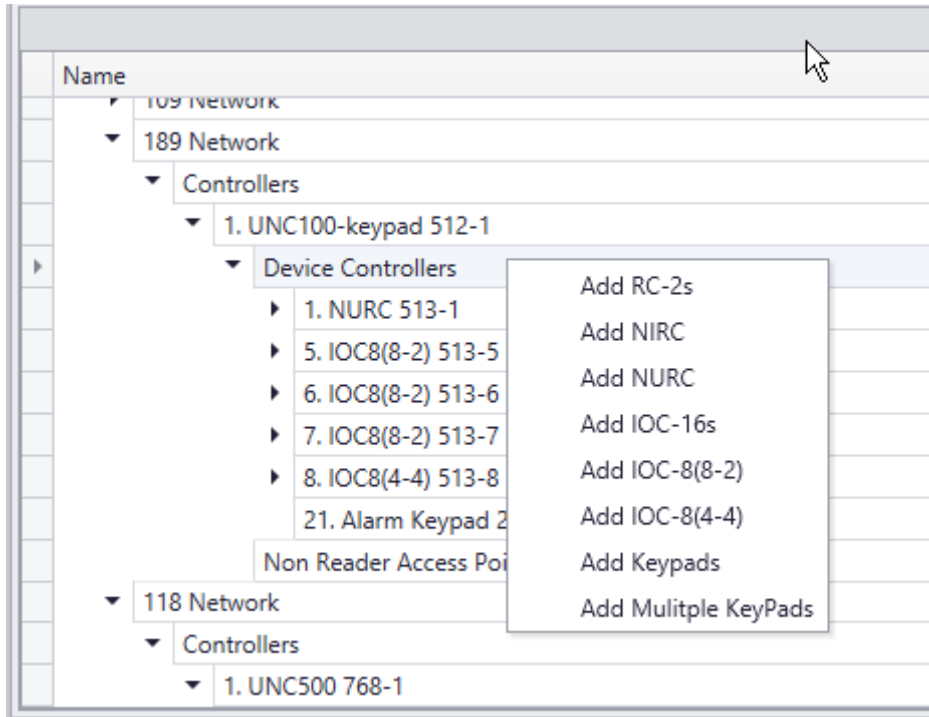
- ⦿ **Checksum** is the original protocol for the D-Net and is still included in the system for backward compatibility to original devices that are still working out in the field.
- ⦿ **Checksum/Address** was created for a special application and adds sixteen to the address of all devices in the network.

D-Net Retries

D-Net Retries specify the number of times that the Network Controller will try to communicate with the D-Net (Device Network) controllers, i.e. RC2s, NIRC, NURCs, IOC16s, Keypads and Alarm Panel before declaring and reporting an Offline condition. The default is five.

Device Controllers





Right click on *Device Controllers* or click on *Add* button at the bottom toolbar (Option available in Tile view only) to add a new device to the system.

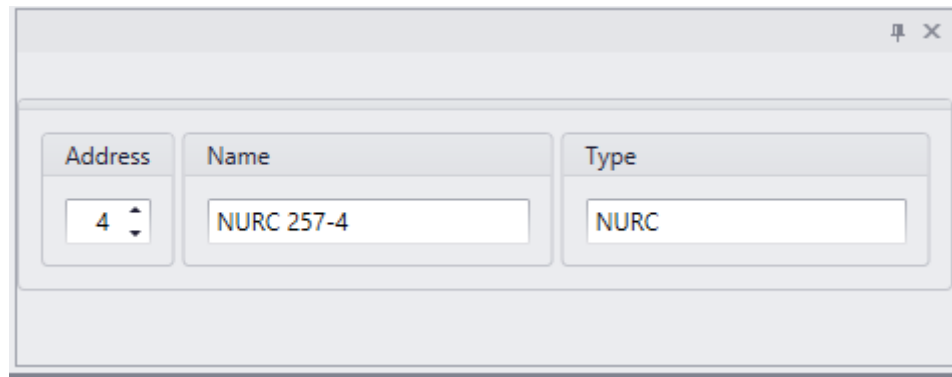
Device controllers include RC-2s, NIRCs, NURCs, IOC16s, Keypads and IOC8s for Alarm panels.

RC2, NIRC and NURC are Reader Controllers, IOC16 is an Input-Output Device controller, Keypads are Apartment device controllers and IOC8s are input-output controllers used only with Alarm panels which are added as part of UNC-100-Keypad.

Adding any device will bring up the Device Controllers configuration window to set the properties of the new device.

Adding a Reader controller will also add two access points, eight/four inputs, and eight/four outputs depending upon the device type added. The eight/four outputs and four/two of the inputs will be defaulted for the access points but can be changed to general purpose.

The address is set when the Reader Controller is added in the system and cannot be edited later.



| Address | Name | Type |
|---------|------------|------|
| 4 | NURC 257-4 | NURC |

Address

Reader controllers can only be addressed 1-4; no other addresses are valid for Reader Controllers. (Up to 8 Reader controllers can be added, for which 8RC license is required)

Name

Up to 50 alphanumeric characters may be entered here.

Type

Reader Controller Type is added by the system depending upon the selection of Reader controller type at the time of adding devices and cannot be edited later.

IOC16 Input Output Controllers

Properties for the IOC16 are set in this window. The address is set when the IOC16 is added in the system and cannot be edited later.

For each of the sixteen ports of the IOC-16 choose whether that port is to be an input or an output.

The screenshot shows a configuration window for an IOC. At the top, there are three fields: 'Address' with a dropdown menu set to '5', 'Name' with a text box containing 'IOC 16 257-5', and 'Type' with a text box containing 'IOC16'. Below these fields is a grid of 16 channels, numbered 1 through 16. Each channel has two radio buttons: 'Input' and 'Output'. Channels 1 through 8 have their 'Input' radio buttons selected. Channels 9 through 16 have their 'Output' radio buttons selected.

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.

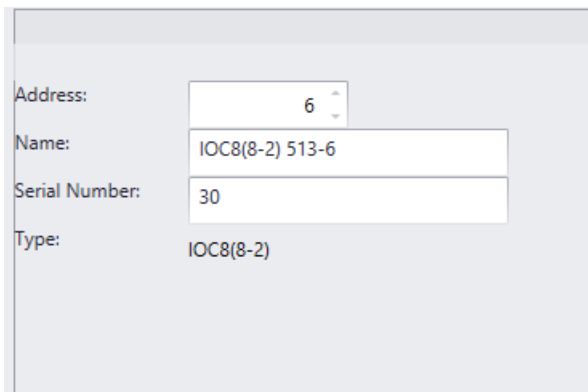
Type

Type *IOC16* is added by the system at the time of adding the input-output controller and cannot be edited later.

IOC8

The properties of the IOC8 are set at the time of adding the IOC8. Two types of IOC8s can be added:

- Add IOC-8(8-2)
- Add IOC-8(4-4)



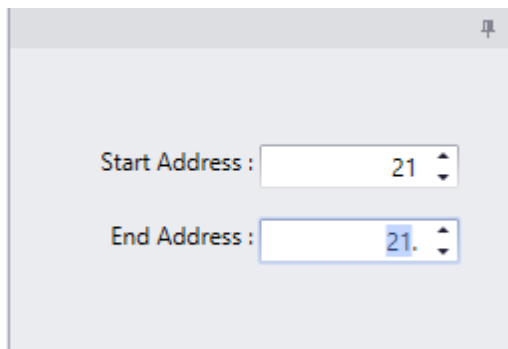
A screenshot of a configuration window with a light gray background. It contains four labeled input fields stacked vertically. The first field is labeled 'Address:' and contains the number '6'. The second field is labeled 'Name:' and contains the text 'IOC8(8-2) 513-6'. The third field is labeled 'Serial Number:' and contains the number '30'. The fourth field is labeled 'Type:' and contains the text 'IOC8(8-2)'. Each field has a small downward-pointing arrow on its right side, indicating it is a dropdown menu.

IOC8 type (8-2) adds 8 inputs and 2 outputs.

IOC8 type (4-4) adds 4 inputs and 4 outputs.

Keypad

Right click on the Device Controller or click on the Add button on bottom toolbar (Tile View) to either add one new Keypad to the system or a group of consecutively addressed Keypads.



A screenshot of a configuration window with a light gray background. It contains two labeled input fields stacked vertically. The first field is labeled 'Start Address :' and contains the number '21'. The second field is labeled 'End Address :' and contains the number '21'. Both fields have small downward-pointing arrows on their right sides, indicating they are dropdown menus.

The address is set when the Keypad is added in the system and cannot be edited later.

Address

Keypads can be addressed from 1-255. It is advisable to start addressing Keypads at 21 if future expansion can add Reader Controllers and IOC-16s.



Keypads added singly are addressed from the configuration screen while keypads added as a group are addressed as they are added.

Description

Up to 50 alphanumeric characters may be entered here.

Type

Type of Device Controller. Type Keypad is added by system at the time of adding devices as Keypad and cannot be edited later.

General

The screenshot shows a web-based configuration interface for a device. At the top, there is a header bar with 'Address' set to '6', 'Description' set to 'New Keypad', and 'Type' set to 'Keypad'. Below this is a tabbed interface with 'General' selected. The 'General' tab contains several input fields: 'Apartment Name' (with 'New Apartment' entered), 'Tenant Name', 'Contact Name', 'Emergency Phone', 'Home Phone', 'Business Phone', 'Mobile Phone', 'Parking 1', 'Parking 2', and 'Comments'. There are also 'Inputs', 'Outputs', and 'Links' tabs visible.

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: 6 Description: New Keypad Type: Keypad Refresh

General Inputs Outputs Links

| ID | Description | Zone Type | Circuit Type | Application |
|----|-------------|------------------|-----------------|-----------------------|
| 1. | Zone 1 | Entry/Exit | NC, No Resistor | Steady Siren / Buzzer |
| 2. | Zone 2 | Follower | NC, No Resistor | Steady Siren |
| 4. | Zone 3 | Exterior | NC, 1 Resistor | Steady Siren |
| 3. | Zone 4 | 24 Hours Delayed | NC, 2 Resistor | Pulse Siren / Buzzer |
| 5. | Zone 5 | General Purpose | NO, No Resistor | Steady Siren |
| 6. | Zone 6 | General Purpose | NO, No Resistor | Steady Siren |
| 7. | Zone 7 | General Purpose | NO, No Resistor | Steady Siren |
| 8. | Zone 8 | General Purpose | NO, 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

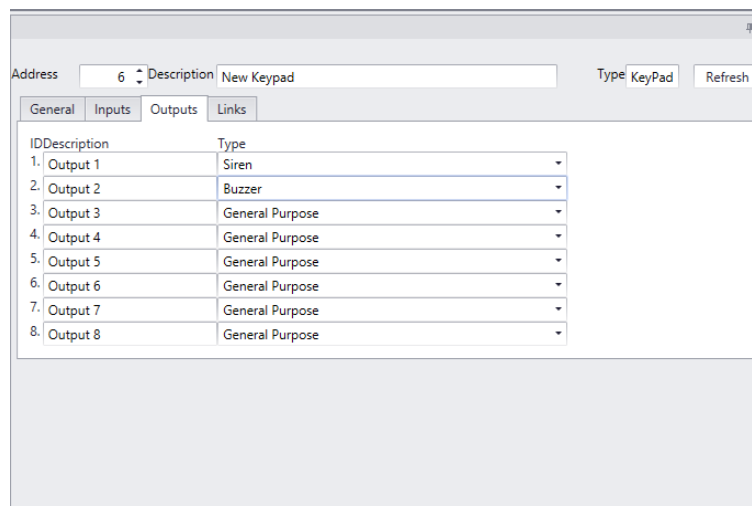
- NC, No Resistor
- NO, No Resistor
- NC, One Resistor
- NO, One Resistor
- NC, Two Resistors
- NO, Two Resistors
- NC & NO, One Resistor

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



Description

Up to 50 alphanumeric characters may be entered here.

Type

| | |
|--------------------------|--|
| <i>General Purpose:</i> | Has no predetermined function. |
| <i>Siren:</i> | Turns on to power an audible device for Alarms. |
| <i>Status LED:</i> | Turn on to indicate that the Keypad is armed. |
| <i>OK to Arm LED:</i> | Turn on to indicate that all zones are normal and the Keypad may be armed. |
| <i>Buzzer:</i> | Turns on to drive an audible that follows the Keypad's buzzer. |
| <i>Lock:</i> | This output is used to activate a door lock. |
| <i>LED1: & LED2:</i> | These outputs are used to drive the red and green LEDs of a card reader connected to the Keypad. |

Links

Address: 6 Description: New Keypad Type: Keypad Refresh

General Inputs Outputs Links

| Event | link |
|--------------|----------------|
| Zone 1 Alarm | Apartment Link |
| Zone 2 Alarm | Apartment Link |
| Zone 3 Alarm | Apartment Link |
| Zone 4 Alarm | |
| Zone 5 Alarm | |
| Zone 6 Alarm | |
| Zone 7 Alarm | |
| Zone 8 Alarm | |

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.

Beside the event you want pull down a list of links. Select the link that is to be executed when the event happens.

Alarm Panel

Alarm Keypad is added by the system at the time of adding UNC-100 Keypad as a controller. Alarm Keypad is added as an address 21 by the system.

The screenshot shows a web-based configuration interface for an Alarm Panel. At the top, there are fields for 'Address' (value: 21) and 'Description' (value: Alarm Keypad 21). To the right, there is a 'Type' dropdown menu set to 'KeyPad' and a 'Refresh' button. Below these fields are several tabs: 'General', 'Partitions', 'Inputs', 'Outputs', and 'Links'. The 'General' tab is selected and contains the following fields:

- Apartment Name: New Apartment 21
- Tenant Name: RBH
- Contact Name: Kanty
- Emergency Phone: 905-790-1515
- Home Phone: (empty)
- Business Phone: (empty)
- Mobile Phone: (empty)
- Parking 1: (empty)
- Parking 2: (empty)
- Comments: (empty)

The inputs and outputs of IOC8s are used to configure *input groups* and *output groups* which are selected as *partitions* of Alarm panel. Address 22- 32 can be added as IOC8 per UNC100-Keypad controller.

Partitions

Once input and output groups are configured for an IOC8s' inputs & outputs, they can be selected as Partitions in the Alarm Panel configuration. Up to 8 partitions can be selected here.

Address Description Type Refresh

General Partitions **Inputs** Outputs Links

Input

Partition 1

Partition 2

Partition 3

Partition 4

Partition 8

Output

Partition 1

Partition 2

Partition 3

Partition 4

Partition 5

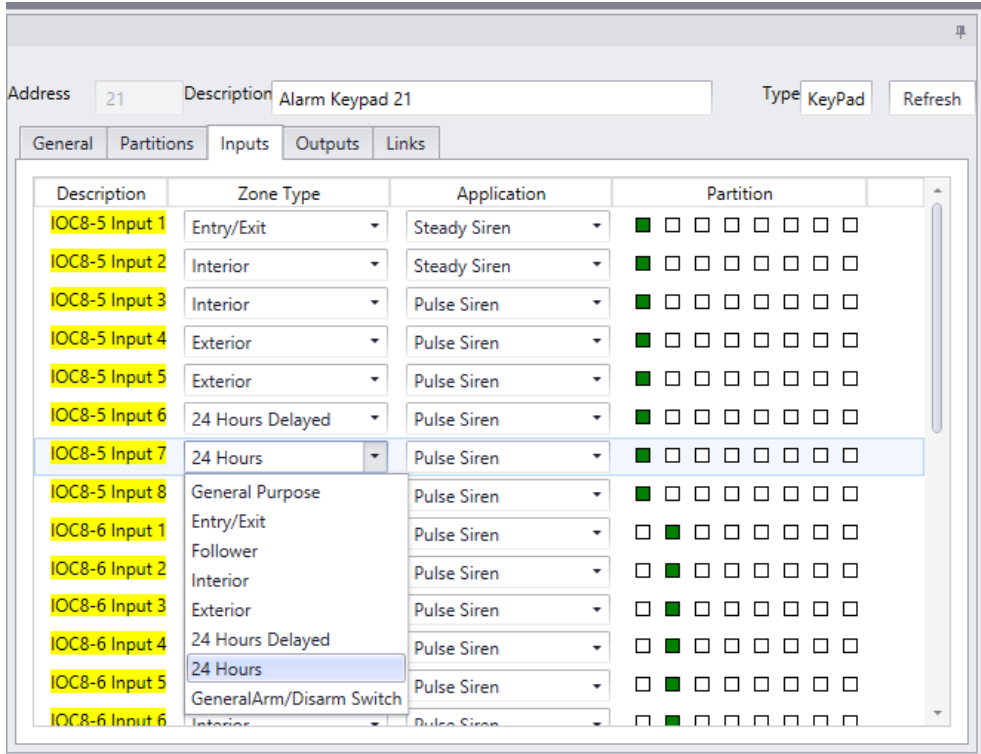
Partition 6

Partition 7

Partition 8

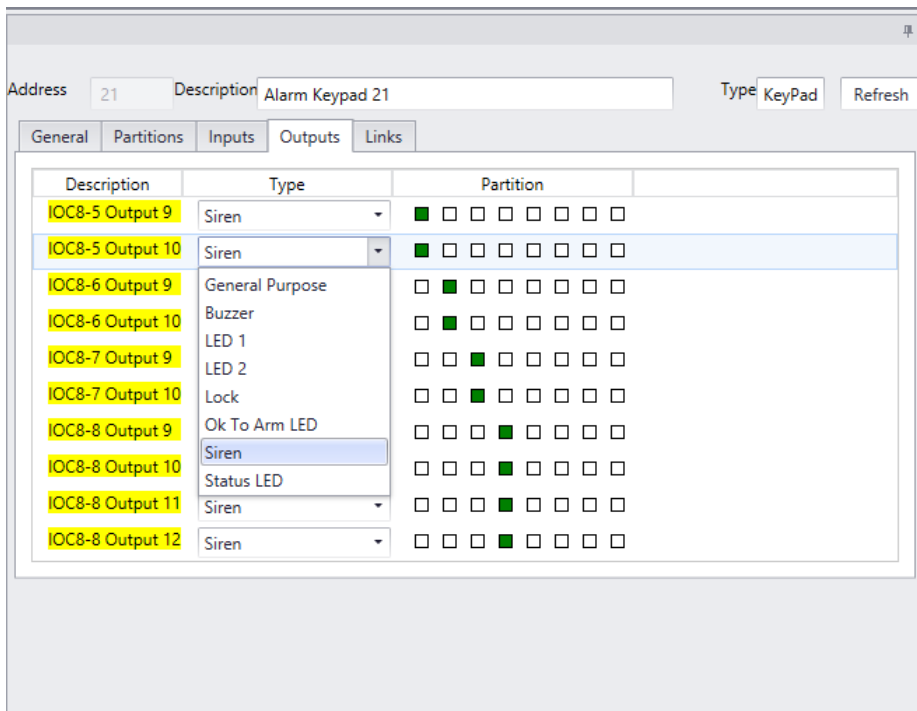
Inputs

Partitions selected here will show as *Inputs* and *Outputs* under the Alarm panels' respective tabs. Those tabs will also show if various inputs and outputs are selected in more than one partition.



Outputs

The Zone type and Application can be selected from their respective drop down list, and these can be same types as for regular Apartment Keypad explained on Page 122



Links

Link tab is to assign links with various Alarm panels' functionalities.

| Event | link |
|------------------|------|
| Keypad Panic | |
| Keypad Emergency | |
| Keypad Fire | |
| Disarm | |
| Home | |
| Evening | |
| Away | |
| Forced Armed | |
| Unlocked Door | |
| Key 01 | |
| Key 02 | |
| Key 03 | |
| Key 04 | |
| Key 05 | |
| Key 06 | |
| Key 07 | |

Access Points

Two access points are created automatically when a Reader Controller is added.

Name

Up to 50 alphanumeric characters may be entered here.

General

Name: Reader 1

General | Reader Option | Links | Code Reader Links

| | | | |
|-----------------------|-------------------------------------|----------------------|-------------------------------------|
| Type | Access | Retries | 5 |
| Auto Relock: | <input checked="" type="checkbox"/> | Unlock Time | 10 Sec |
| First Person Delay : | <input type="checkbox"/> | Extended Unlock Time | 30 Sec |
| Report Door not Open | <input checked="" type="checkbox"/> | DHO Warning | 10 Sec |
| Report unknown format | <input checked="" type="checkbox"/> | DHO Alarm | 20 Sec |
| Required PC Decision | <input type="checkbox"/> | Alarm LockOut Time | 10 Min |
| Disable force entry | <input type="checkbox"/> | Asset Present Time | 1 Sec |
| RTE bypass DC | <input type="checkbox"/> | Enabled | <input checked="" type="checkbox"/> |
| Unlock Schedule | 0 | | |
| Disable RTE | 0 | | |
| DHO Warning Schedule | 1 | Always | |

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.

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 time group, 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 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 Event viewer 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 Controller. The Controller 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.



For "Required PC Decision" feature to work, NC100 controllers must have firmware 5.09 or higher.

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 pull down list to select the *Schedule* during which this access point is to remain unlocked.

Disable Request to Exit

Use the pull down list to select the *Schedule* during which the RTE function is disabled at this access point. The system does not respond to requests to exit during this scheduled time.

DHO Warning Schedule

Use the pull down list to select the *Schedule* during which *Door Held Open (DHO)* warning is enabled for this access point.

Retries

Retries specifies the maximum number of consecutive invalid card/PIN reads permitted (1-10), 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 unlock time expires, 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 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 Option

Name: Reader 1

General Reader Option Links Code Reader Links

Card Formats
26 bit std;39 bit RBH;50 bit RBH;64 bit RBH

| | | | | |
|--------------------------|-------------------------------------|---------------|---|--------------------------|
| Deduct Usage | <input type="checkbox"/> | High Security | 0 | |
| Facility Code Fallback M | <input type="checkbox"/> | Two person | 0 | |
| Reverse Data | <input type="checkbox"/> | Card tracing | 0 | |
| In/Out Reader | <input type="checkbox"/> | Exiting Area | 0 | |
| Offline Operation Enable | <input type="checkbox"/> | Entering Area | 0 | |
| Required card and PIN | <input checked="" type="checkbox"/> | APB Enabled | | <input type="checkbox"/> |

Reader Schedule: 1 Always

Keypad Schedule: 3 Night Shift

Card Formats

This box lists all selected card reader bit formats. Readers may be configured to support up to five different card formats simultaneously. Pull down the formats list 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 174 in Chapter 7).

Facility Code Fall Back

When an access card is presented under normal conditions the Controller gets the card number and facility code from the Reader Controller and decides whether or not to grant access. If communication is lost between the Controller and the Reader Controller, the Reader Controller 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 Reader Controller 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 Reader Controller 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 Reader Controller. The exit reader is connected to the B-side of the Reader Controller. In this configuration, the B-side of the Reader Controller 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 Network Controller will download card data to the reader control. This will allow the controller to function after losing communications with the Network Controller.

Hardware Requirements

NC-100 firmware must be 8.27. An NIRC must be used with firmware version 9.1. For more detailed information check Technical Bulletin ‘TB58 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.

Reader Schedule

Use the pull down list to select a schedule for reader operation. The reader is required for access when the schedule is on.

Keypad Schedule

Use the pull down list to select a schedule for keypad operation. The keypad is required for access when the schedule is on.



When both reader and keypad schedules are on, then both card and code are required for access.



When both reader and keypad schedules are off, the access point is inactive.

High Security

Use the pull down list 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 pull down list 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.

Card Tracing

Use the pull down list 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.

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 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 pull down list 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

| Message | Link Description |
|----------------|------------------|
| Forced Entry | [Dropdown] |
| Tamper | [Dropdown] |
| Door Held Open | [Dropdown] |
| Access Granted | [Dropdown] |
| Access Denied | [Dropdown] |
| Secure | [Dropdown] |
| Patient | [Dropdown] |
| Code Tracing | [Dropdown] |
| Door not Open | [Dropdown] |

To establish a link click in the *Link Description* box beside the *Message* you want the link activated on and use the pull down list to 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

A Keypad reader is required for this functionality to work.

Name:
RC2 513-1\Reader 1 RTE

General Links

Input Type defaulted Abort Delay
 RTE 0 Sec

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 a Reader controller (RC2, NIRC and NURC) can be set as either general-purpose inputs or they can be defaulted. When defaulted, input 1 will be used as a Request-to-Exit input for the access point. Input 2 when defaulted will be used as a Door Contact input for that same access point. Side A and side B of the Reader controller 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:
Input 1

General Links

General Purpose Abort Delay
 0 Sec

Circuit type :
 NO, No Resistor Forced Arm Alarm

Disarm Schedule :

Enabled

Circuit Type

Use the pull down list 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 pull down list to select the *Schedule* during which the alarm/input is automatically disarmed by the system schedule.

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 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 two options in specifying how AxiomXA™ 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.

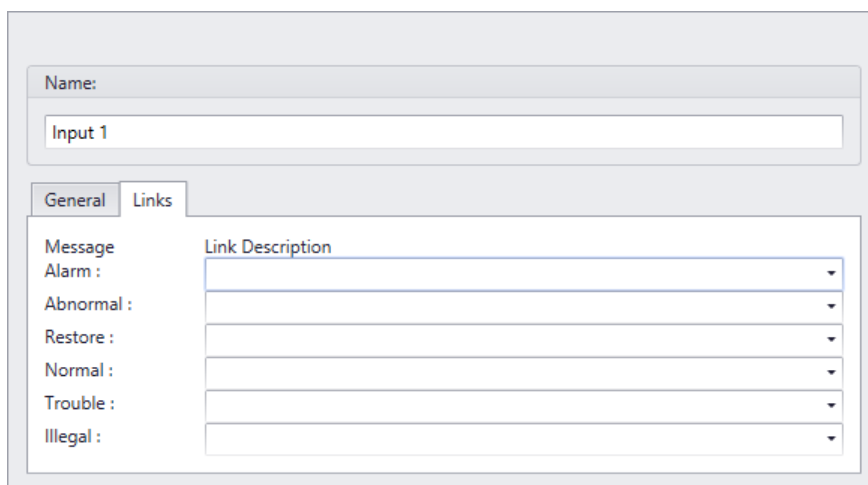
Unchecked

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



| Message | Link Description |
|------------|------------------|
| Alarm : | |
| Abnormal : | |
| Restore : | |
| Normal : | |
| Trouble : | |
| Illegal : | |

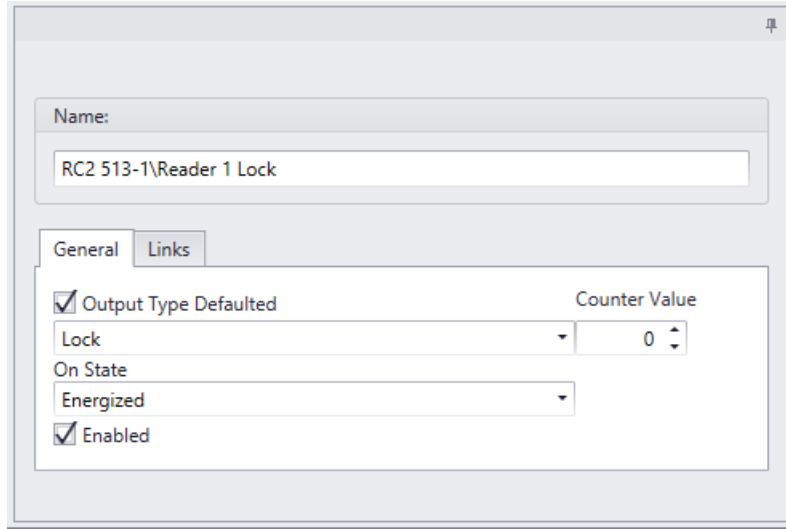
To establish a link use the pull down list in the *Link Description* box beside the *Message* you want the link activated on. Then select the desired link from the list presented. The name of the chosen link will be shown in the *Link Description* box to confirm the link programming.

Outputs

Outputs are created when adding Reader Controllers and Input Output Controllers. They can be either defaulted to an access point (Reader Controllers only) or general purpose.

Output Configuration

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.



Name

Up to 50 alphanumeric characters may be entered here.

General

Output Type Defaulted

Reader Controllers 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.

The screenshot shows a configuration window for an output device. At the top, the 'Name' field is filled with 'Output 1'. Below this, there are two tabs: 'General' and 'Links'. The 'General' tab is active and contains the following settings:

- Counter Value:** A spinner control set to 0.
- On State:** A dropdown menu set to 'Energized'.
- On Schedule:** A dropdown menu.
- Enabled:** A checked checkbox.

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

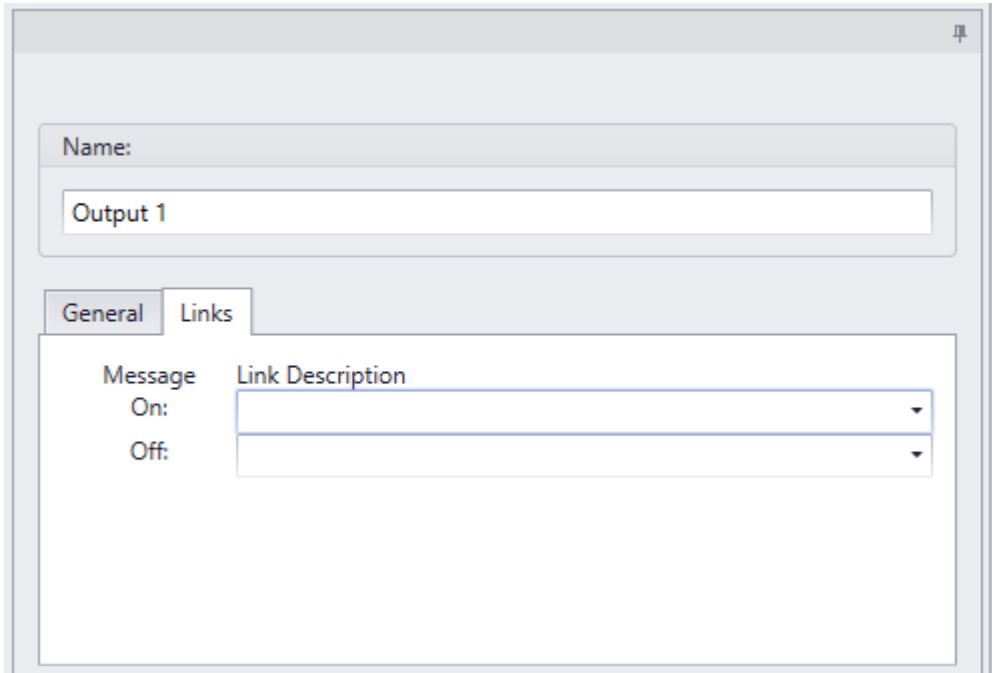
Use the pull down list to select the *Schedule* during which the output is turned 'On'.

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 is one hundred. Subsequent OFF commands will reduce the count but won't alter the Output State or execute the off link.

Links



The screenshot shows a software configuration window with a title bar and a close button. Below the title bar is a 'Name:' label followed by a text input field containing 'Output 1'. Below this is a tabbed interface with two tabs: 'General' and 'Links'. The 'Links' tab is selected. Inside the 'Links' tab, there is a table with two columns: 'Message' and 'Link Description'. The 'Message' column has two rows: 'On:' and 'Off:'. The 'Link Description' column has two corresponding dropdown menus, each with a downward-pointing arrow.

To establish a link use the pull down list in the *Link Description* box beside the *Message* you want the link activated on. Then 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 or click on *Add* button at the bottom toolbar (Tile view only) to add a new Non Reader Access Point to the system. This will bring up the Non Reader Access Point's Configuration window to set the properties of the new Non Reader Access Point.



Only General Purpose inputs and outputs on IOC16s connected to the controller should be used to create Non Reader Access Points for that controller, even though RC2s, NIRC's and NURC's general purpose inputs and outputs may be available.

Non Reader Access Point Configuration

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

The screenshot shows the configuration window for a Non Reader Access Point. The 'Name' field is set to 'Access Point'. There are three tabs: 'General', 'IO Configuration', and 'Links'. The 'General' tab is active and contains the following settings:

| | | | | |
|----------------------|--------|---|---|-----|
| Type | Access | Unlock Time | 5 | Sec |
| Unlock Schedule | 0 | DHO Warning | 20 | Sec |
| Disable RTE | 0 | DHO Alarm | 30 | Sec |
| DHO Warning Schedule | 0 | <input checked="" type="checkbox"/> Auto Relock | <input checked="" type="checkbox"/> Enabled | |

IO Configuration

The screenshot shows the 'IO Configuration' tab of the 'Access Point' configuration window. At the top, there is a 'Name' field containing 'Access Point' and a 'Refresh' button. Below this are three tabs: 'General', 'IO Configuration' (which is selected), and 'Links'. The 'IO Configuration' tab contains a table with the following rows:

| | | |
|---------------|---|---|
| Door Contract | 0 | ▼ |
| RTE | 0 | ▼ |
| Lock | 0 | ▼ |
| Forced Entry | 0 | ▼ |
| DHO Warning | 0 | ▼ |
| DHO Alarm | 0 | ▼ |

Click on pull down list to select each point: Door Contact, RTE, Lock, Forced Entry, DHO Warning, and DHO Alarm. A list of available points (input/Output) to select from will show. 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 which pulses for warning and is ON steady for alarm while Non Reader Access Points have two outputs for Door Held Open, one for DHO Warning, and one for DHO alarm.

Links

The screenshot shows the 'Links' tab of the 'Access Point' configuration window. At the top, there is a 'Name' field containing 'Access Point' and a 'Refresh' button. Below this are three tabs: 'General', 'IO Configuration', and 'Links' (which is selected). The 'Links' tab contains a table with the following rows:

| 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. Click on pull down list to select the desired link. 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.

The screenshot shows a configuration window for an elevator system. At the top, there is a 'Name' field containing 'Cab A'. Below it is a 'Reader' section with a dropdown menu showing '9' and 'RC2 258-1\Reader 1'. The main area is divided into two columns: 'Available Items' and 'Selected Items'. Each column contains a table with a 'Description' header and a list of items. The 'Available Items' table lists 'Floor 1 Cab B' through 'Floor 8 Cab B'. The 'Selected Items' table lists 'Floor 1 Cab A' through 'Floor 8 Cab A'. Between the two tables are four buttons: '>>', '>', '<', and '<<', used for moving items between the lists.

Name

Up to 50 alphanumeric characters may be entered here.

Reader

Pull down the list and select the desired elevator reader. (The Access points configured Type *Elevator* shows in the list).

Available Items & Selected Items

Only general-purpose outputs related to the Controller (which the selected elevator reader is connected to) will be listed in *Available Items*.

Shift the floor outputs between available and selected to configure the elevator cab with the proper floor outputs.



It is recommended to use only the general purpose outputs of IOC for elevators.

Elevator Floor Groups

Create Floor Groups to limit access to only the floors included in the group.

The screenshot shows a web-based configuration interface for creating an elevator floor group. It features a 'Name' field containing 'Cab A Elevator Group floors|1-4', an 'Elevator' dropdown menu set to '1 Cab A', and two side-by-side tables. The 'Available Items' table lists 'Floor 5 Cab A', 'Floor 6 Cab A', 'Floor 7 Cab A', and 'Floor 8 Cab A'. The 'Selected Items' table lists 'Floor 1 Cab A', 'Floor 2 Cab A', 'Floor 3 Cab A', and 'Floor 4 Cab A'. Between the tables are four navigation buttons: '>>', '>', '<', and '<<'.

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. Therefore cardholders can only go to the floors they have access to.

Access Point 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. Access point groups can also be used for creating Access Levels.

The screenshot shows a configuration window for an Access Point Group. At the top, the 'Name' field is set to '109 Access Point Group'. Below it, the 'Network' field is set to '256' and '109 Network'. The main area is divided into two sections: 'Available Items' and 'Selected Items'. The 'Available Items' section contains a table with a 'Description' column and a list of readers: 'NIRC 257-2\Reader...', 'NIRC 257-2\Reader...', 'NURC 257-3\Read...', 'NURC 257-3\Read...', 'RC2 258-1\Reader 1', and 'RC2 258-1\Reader 2'. The first 'NIRC 257-2\Reader...' entry is selected. The 'Selected Items' section contains a table with a 'Description' column and a list of readers: 'RC2 257-1\Reader 1' and 'RC2 257-1\Reader 2'. Between the two tables are four navigation buttons: '>>', '>', '<', and '<<'.

Name

Up to 50 alphanumeric characters may be entered here.

Network

Select a *Network* from the pull down list to select devices from. Only one network can be selected at a time.

Available Items

Available Items will show all of the access points in the network, according to the previous selection.

Selected Items

Selected Items lists the access points that are members of the Access Point 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

The screenshot shows a web-based configuration interface for an Access Level. At the top, there are three input fields: 'ID' with the value '0', 'Name' with the value 'OFFICE AccessLevel', and 'Access Level Type' with a dropdown menu set to 'Standard Access Level'. Below these are two tabs: 'General' (selected) and 'Elevator'. Under the 'General' tab, there is a 'Schedule' dropdown menu set to 'Always'. The main area contains two side-by-side tables. The left table, titled 'Available Items', has a header 'Drag a column header here to group by th...' and a list of items with a 'Description' column. The right table, titled 'Selected Items', has the same header and currently contains two items. Between the tables are four arrow buttons: '>>', '>', '<', and '<<'. The 'Available Items' table contains the following rows:

| Description |
|---------------------|
| NIRC 257-2\Reader 1 |
| NIRC 257-2\Reader 2 |
| NURC 257-3\Reader 1 |
| NURC 257-3\Reader 2 |
| RC2 258-1\Reader 1 |
| RC2 258-1\Reader 2 |
| NURC 513-1\Reader 1 |
| NURC 513-1\Reader 2 |

The 'Selected Items' table contains the following rows:

| Description |
|--------------------|
| RC2 257-1\Reader 1 |
| RC2 257-1\Reader 2 |

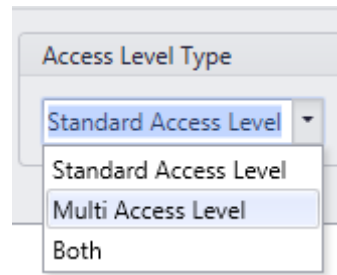
ID

ID of the Access level is system defined and shows in the window after saving an access level.

Name

Up to 50 alphanumeric characters may be entered here.

Access Level Type



Three types of Access levels are available in pull down menu:

Standard Access Level

Access level Type *Standard* are available only in the list for *Standard Access Level* of cardholders. The Elevator tab is available only for Access level Type *Standard*

Multi Access Level

Access level Type *Multi* are available only in the list for *Multiple Access Level* of cardholders.

See *Cardholder – Card Properties –*

[Multiple Access Levels](#) for information on giving these access levels to the cardholders.

Both

Access level Type *Both* are available for both *Standard Access Level* and *Multiple Access Level* of cardholders.

Schedule

Select a schedule and then 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. You do not need to use all of the schedules, nor do all of the access points need to be selected.

Elevator

Under the *Elevator* tab *Floor Groups* are tied to *Schedules*. For *Elevator Access* to work the *Elevator* reader appropriate to the selected *Floor Groups* should have been selected under the General tab.

| ID | Name | Access Level Type |
|----|--------------------|-----------------------|
| 7 | OFFICE AccessLevel | Standard Access Level |

| Floor Group Name | Schedule |
|---------------------------------|----------|
| Cab A Elevator Group floors 1-4 | Always |

When access is granted on the *Elevator* reader the system checks to see which floor associated with that reader are to be enabled. The *Floor Group* determines these floors.

View

View will display all of an access level's access points with their appropriate schedules.

| ID | Name | Access Level Type |
|----|--------------------|-----------------------|
| 7 | OFFICE AccessLevel | Standard Access Level |

| Access Point | Schedule |
|---------------------|--------------------|
| RC2 257-1\Reader 1 | Always |
| RC2 257-1\Reader 2 | Always |
| NIRC 257-2\Reader 1 | BH Schedule |
| NIRC 257-2\Reader 2 | BH Schedule |
| NURC 513-1\Reader 1 | Afternoon Schedule |
| NURC 513-1\Reader 2 | Afternoon Schedule |

The screenshot shows a configuration window with three input fields at the top: ID (containing '9'), Name (containing 'Both type Warehouse AccessLevel'), and Access Level Type (a dropdown menu set to 'Both'). Below these fields are two tabs: 'General' and 'Elevator'. The 'General' tab is active and contains a table with two columns: 'Access Point' and 'Schedule'. The table has four rows of data.

| Access Point | Schedule |
|---------------------|------------------|
| RC2 257-1\Reader 1 | BH Schedule |
| RC2 257-1\Reader 2 | BH Schedule |
| NURC 513-1\Reader 1 | Morning Schedule |
| NURC 513-1\Reader 2 | Morning Schedule |

CCTVs

| | |
|---|---------------------------------|
| Name | |
| <input type="text" value="Axis DVR"/> | |
| Make | |
| <input type="text" value="Axis Camera"/> | |
| Address | Port |
| <input type="text" value="125.100.75.213"/> | <input type="text" value="80"/> |

| | |
|--|--------------------------------|
| Name | |
| <input type="text" value="New DVR VMS"/> | |
| Make | |
| <input type="text" value="RBHView"/> | |
| Address | Port |
| <input type="text" value="128.100.1.8"/> | <input type="text" value="0"/> |

Name

Up to 50 alphanumeric characters may be entered here.

Make

From the pull down list select the manufacturer of the CCTV(The list available depends upon the License).

Address

Enter the IP Address of the CCTV here.

Port

Enter the number of the port the CCTV's uses here.

Input Groups

Input Groups is 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.

Input Groups can also be selected as *Partitions* for *Alarm panel*.

These input groups are created with *IOC8* inputs, which can be added as *Device controllers* for *UNC100-Keypad* controller.

The screenshot shows a configuration window for an Input Group. At the top, the 'Name' field is set to 'Input Group'. Below it, the 'Network' field is set to '512' and 'Network 52'. The main area is divided into two panes: 'Available Items' and 'Selected Items'. The 'Available Items' pane contains a list of inputs, with 'IOC 16Net52-5\Input 1' selected. The 'Selected Items' pane contains a list of inputs, with 'RC2 Net52-2\Input 1' through 'Input 4' selected. Navigation buttons '>>', '>', '<', and '<<' are located between the two panes.

The screenshot shows a configuration interface for an alarm panel. At the top, there is a 'Name' field containing 'Alarm Panel Apartment A'. Below it is a 'Network' section with a numeric input '512' and a dropdown menu showing '189 Network'. The main area is divided into two columns: 'Available Items' and 'Selected Items'. Each column contains a table with a 'Description' header and seven rows of input points. The 'Available Items' table lists 'IOC8-6 Input 1' through 'IOC8-6 Input 7'. The 'Selected Items' table lists 'IOC8-5 Input 1' through 'IOC8-5 Input 7'. Between the two tables are four navigation buttons: '>>', '>', '<', and '<<'. Each table also has a scroll bar on its right side.

Name

Up to 50 alphanumeric characters may be entered here.

Network

Select a *Network* from the pull down list to select devices from. Only one network can be selected at a time.

Available Items

Available Items will show all of the input points in the network, according to the previous selection.

Selected Items

Selected Items lists the input points that are members of the Input Group.

Output Groups

Output Groups is 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 a command to six individual Outputs, one command could be sent to a group of six.

The screenshot displays the configuration interface for an Output Group. At the top, there is a 'Name' field containing 'Output Group'. Below it is a 'Network' section with a dropdown menu showing '512' and 'Network 52'. The main area is divided into two columns: 'Available Items' and 'Selected Items'. Both columns have a header 'Drag a column header here to group...' and a table with a 'Description' column. In the 'Available Items' table, 'IOC 16 Net52-6\Output 8' is selected. In the 'Selected Items' table, 'IOC 16 Net52-6\Output 1' through 'Output 7' are listed. Between the columns are four arrow buttons: '>>', '>', '<', and '<<'.

Name

Up to 50 alphanumeric characters may be entered here.

Network

Select a *Network* from the pull down list to select devices from. Only one network can be selected at a time.

Available Items

Available Items will show all of the Outputs in the network, according to the previous selection.

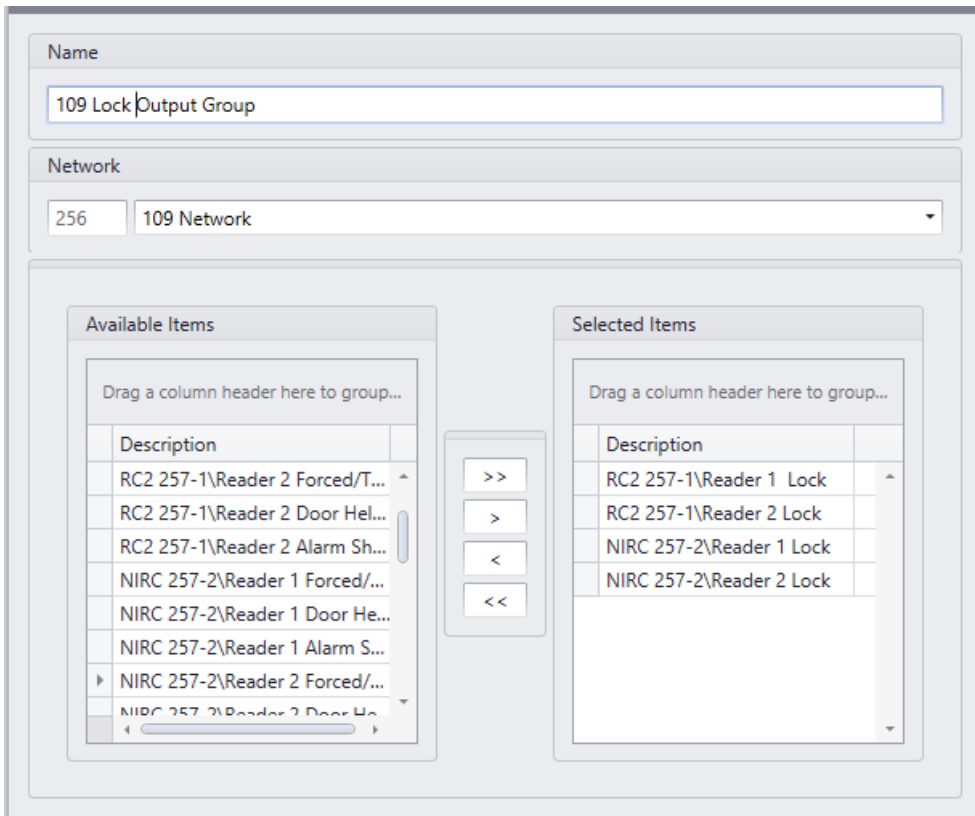
Selected Items

Selected Items lists the outputs that are members of the Output Group.

Output Groups is 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.

Output Groups can also be selected as *Partitions* for *Alarm panel*.

These Output groups are created with *IOC8* outputs, which can be added as *Device controllers* for *UNC100-Keypad* controller.



The screenshot shows a configuration window with the following sections:

- Name:** A text input field containing "Alarm Panel B outputs".
- Network:** A dropdown menu showing "512" and "189 Network".
- Available Items:** A list box containing:

| Description |
|-------------------------------|
| IOC8-7 Output 10 |
| IOC8-8 Output 9 |
| IOC8-8 Output 10 |
| IOC8-8 Output 11 |
| IOC8-8 Output 12 |
| NURC 513-1\Reader 1 Lock |
| NURC 513-1\Reader 1 Forced... |
| NURC 513-1\Reader 2 Lock |
- Selected Items:** A list box containing:

| Description |
|------------------|
| IOC8-6 Output 9 |
| IOC8-6 Output 10 |

Name

Up to 50 alphanumeric characters may be entered here.

Network

Select a *Network* from the pull down list to select devices from. Only one network can be selected at a time.

Available Items

Available Items will show all of the output points in the network, according to the previous selection.

Selected Items

Selected Items lists the output points that are members of the Onput 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 for the schedule selected for interlock group. If one of these access point grants access and/or is opened none of the other members of the group will grant access. Commonly used in mantrap applications.

The screenshot shows a configuration window for an Interlock Group. At the top, there is a text field for the group name, currently containing "Interlock Group". Below this are two sections: "Network" and "Schedule". The "Network" section has a numeric input field with "512" and a dropdown menu showing "Network 52". The "Schedule" section has a numeric input field with "2" and a dropdown menu showing "Business Hours".

Below the network and schedule settings are two main panels: "Available Items" on the left and "Selected Items" on the right. Each panel contains a table with a "Description" header and a list of items. In the "Available Items" table, two items are listed: "NIRC Net52-1\Reader 2" and "RC2 Net52-2\Reader 2". In the "Selected Items" table, two items are listed: "NIRC Net52-1\Reader 1" and "RC2 Net52-2\Reader 1". Between these two panels is a vertical stack of four navigation buttons: ">>", ">", "<", and "<<".

Name

Up to 50 alphanumeric characters may be entered here.

Network

Select a *Network* from the pull down list to select devices from. Only one network can be selected at a time.

Schedule

Select a schedule from the pull down list for the activation of the Interlock Group. When the schedule is on the Interlock Group is active and inactive when the schedule is off.

Available Items

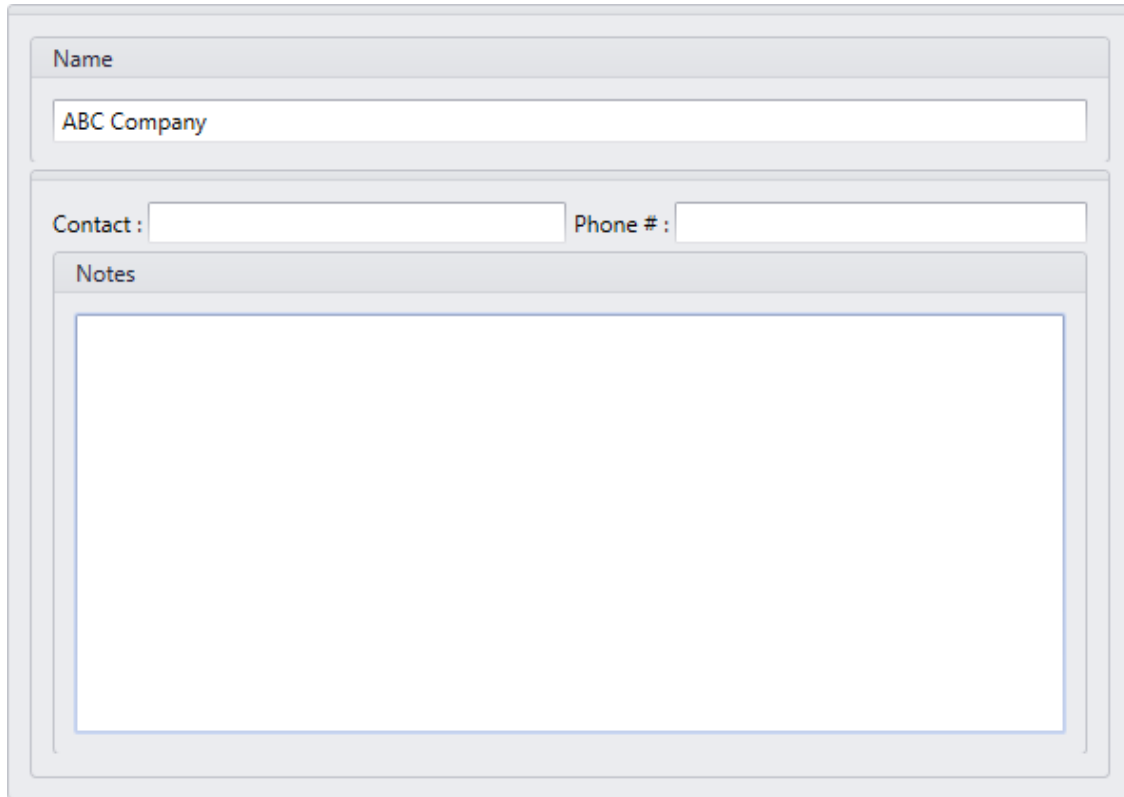
Available Items will show all of the access points in the network, according to the previous selection.

Selected Items

Selected Items lists the access points that are members of the Interlock Group.

Companies

A company is a cardholder group and is used in operator profiles.



The image shows a screenshot of a web form for creating or editing a company. The form is enclosed in a light gray border and contains the following sections:

- Name:** A text input field containing the text "ABC Company".
- Contact:** A text input field.
- Phone #:** A text input field.
- Notes:** A large, empty rectangular area for entering text.

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.

Cardholders

The *Cardholder* screen is used to manage all of the cardholders in the system.

Cardholder Screen

| List View ▾ | | | | | |
|-------------|---|----------|-----------|-------------|--|
| | | Lastname | Firstname | Card Number | |
| ▾ | | | | | |
| ▶ |  | Test | ABC | 1001 | |
| |  | Test | XYZ | 1002 | |
| |  | Test | DEF | 1003 | |
| |  | MNO | Test | 30001 | |
| |  | Test | JKL | 30002 | |
| |  | TEST | QWE | 30005 | |
| |  | ASD | TEST | 30006 | |
| |  | FGH | TEST | 50001 | |

Add

First Name

First Name is the given or common name of the cardholder.

Last Name

Last Name is the family name or surname of the cardholder. The cardholder cannot be saved if this field is left blank.

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 181.)

The screenshot shows a web form for 'Cardholder Properties'. At the top, there are four input fields: 'First Name', 'Last Name', 'Initials', and 'Cardholder Type' (a dropdown menu). Below these are two tabs: 'Cardholder Properties' (selected) and 'Card Properties'. Under the 'Cardholder Properties' tab, there are four sub-tabs: 'Personal' (selected), 'Company', 'Photo', and 'Notes'. The 'Personal' sub-tab contains several fields: 'Street Address' (a multi-line text area), 'City' (text input), 'State/Province' (dropdown menu), 'Country' (dropdown menu), 'Zip/Postal' (text input), 'Phone' (text input), 'Ext' (text input), 'Email' (text input), 'Department' (dropdown menu), 'Department 1' (dropdown menu), and 'Department 2' (dropdown menu).

Cardholder Properties

Personal

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.

Ext.

Up to 10 alphanumeric characters may be entered here.

Email

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.

Department 1

Use the pull down list to select from previously entered data under *Department* database.

Department 2

Use the pull down list to select from previously entered data under *Department* database, if a cardholder belongs to more than department.

Company

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.

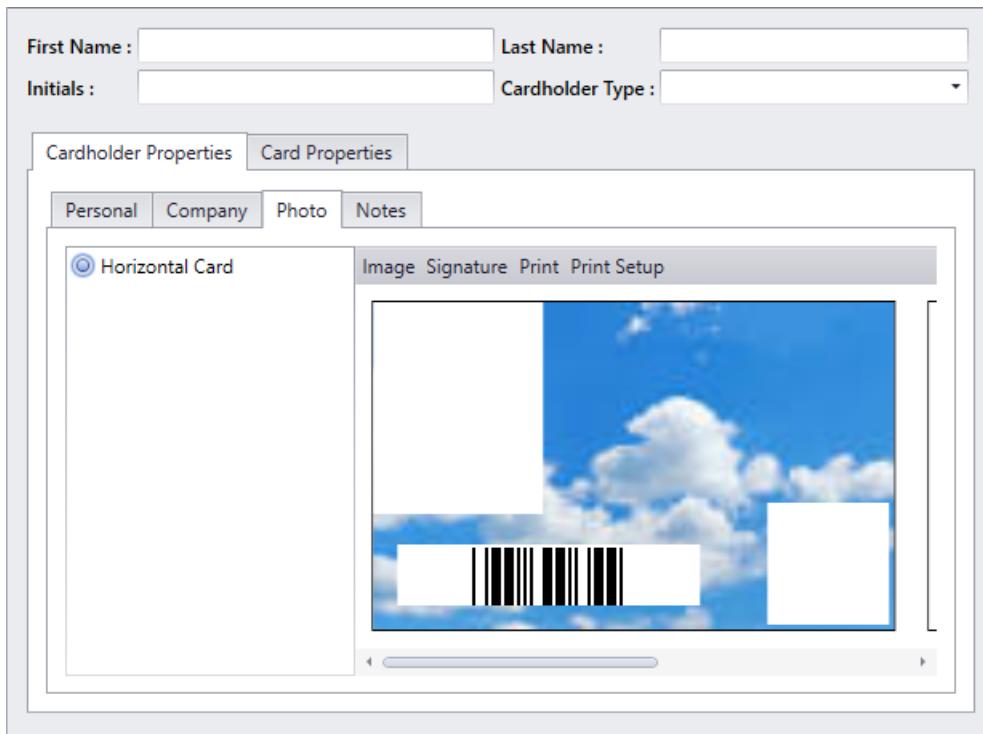
First Name : Last Name :
Initials : Cardholder Type :

Cardholder Properties | Card Properties

Personal | Company | Photo | Notes

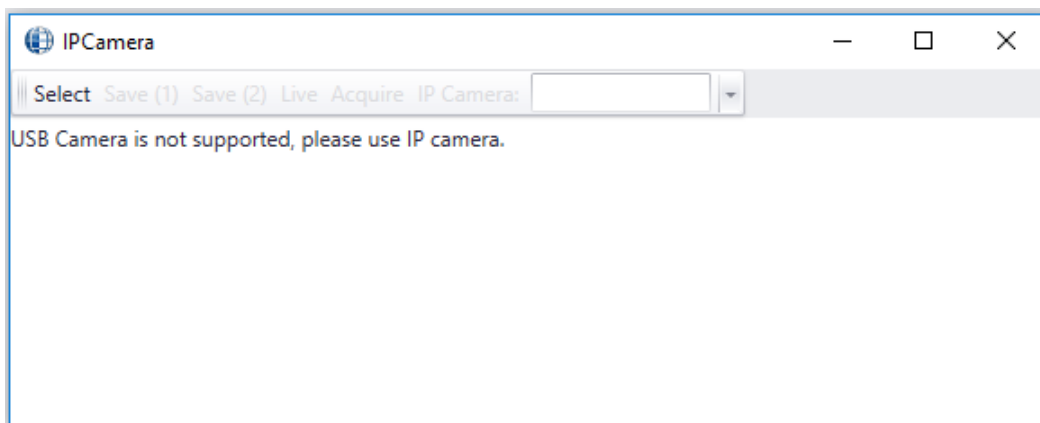
(Select All)
 Master Company

Photo



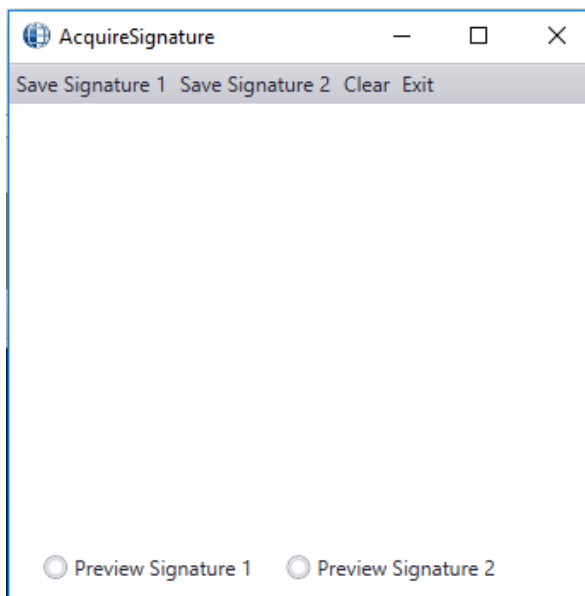
Image

Select *Image* to acquire a picture, either through a live feed or by choosing a saved file.



Signature

Signature is used to acquire a signature of the cardholder using a signature capture device.

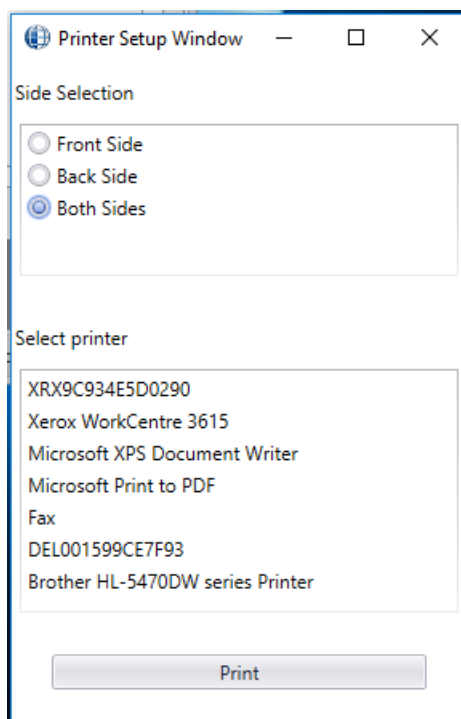


Print

Use *Print* to produce a printout of the current selected badge.

Print Setup

If you need to select different settings for a Badge, other than what is already saved in system settings, use the *Print Setup* screen to select single-sided (front or back) or double-sided printing, as well as selecting the printer the badge is to be printed on.



Notes

This tab has space available to enter any data the operator wishes. It is meant for pertinent information that doesn't fit any of the available fields.

The screenshot shows a web-based form for cardholder information. At the top, there are four input fields: "First Name :", "Last Name :", "Initials :", and "Cardholder Type :". Below these is a tabbed interface with two main tabs: "Cardholder Properties" and "Card Properties". Under "Card Properties", there are four sub-tabs: "Personal", "Company", "Photo", and "Notes". The "Notes" tab is currently selected, showing a large, empty text area with a vertical scrollbar on the right side.

Card Properties

Card Number

Card Number is the number of the card held by the cardholder. After a *Card Number* has been assigned the card number cannot be edited. All other data can be edited. To give a cardholder additional credentials click on the **+** icon.

Card Name

Card Name is a label for a particular credential. Since a cardholder can have more than one credential it may be advisable to label them for convenience.

General

Status

The status of the card: active inactive, pending (not active yet), stolen, destroyed, expired, lost suspended. Only active cards will be granted access.

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 185.)

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.



AxiomXA™ 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.

De-Activation Date

The *De-Activation Date* will specify the first date that the card will no longer work. If the *De-Activation Date* is not checked then the card will never expire.

Options

First Name: Last Name:
 Initials: Cardholder Type:

Cardholder Properties | Card Properties

Card Number + Card Name

General | Options | Code Link | Standard Access Level | Special Access Levels | Multi Access Levels

Drag a column header here to group by that column

| Description | Lock/Unlock | High Security |
|-----------------------|-------------------------------------|-------------------------------------|
| RC2 257-1\Reader 1 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| RC2 257-1\Reader 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| NIRC 257-2\Reade... | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| X NIRC 257-2\Reade... | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| NURC 257-3\Read... | <input type="checkbox"/> | <input type="checkbox"/> |
| NURC 257-3\Read... | <input type="checkbox"/> | <input type="checkbox"/> |
| RC2 258-1\Reader 1 | <input type="checkbox"/> | <input type="checkbox"/> |
| RC2 258-1\Reader 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| NURC 513-1\Read... | <input type="checkbox"/> | <input type="checkbox"/> |

Ignore High Security
 Trace this card
 Start Vacation 1
 Extend Unlock
 Ignore Antipassback
 End Vacation 1
 Escort Required
 Ignore Auto void
 Start Vacation 2
 Stealth Mode
 End Vacation 2

Description

It is the list of Access points cardholder has access to through Standard, Special and Multi Access Levels. Select from the list which access points the cardholder has *Lock/Unlock* (double swipe) privilege, and which access points the cardholder has *High Security* on/off (quadruple swipe) capability.

Ignore High Security

When checked, the cardholder is able to gain access at readers that are in high security mode

Extended Unlock

When checked, 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 checked, 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 event viewer 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. The vacation starts at the beginning of the Start Date and ends at the end of the End Date.

Start Vacation 1

Start Vacation 1 is the date (MM-DD-YYYY³) on which vacation 1 starts.

End Vacation 1

End Vacation 1 is the date (MM-DD-YYYY²) on which vacation 1 ends.

Start Vacation 2

Start Vacation 2 is the date (MM-DD-YYYY²) on which vacation 2 starts.

End Vacation 2

End Vacation 2 is the date (MM-DD-YYYY²) on which vacation 2 ends.

For example a one-day vacation on Monday, 22 August 2016 would use 08-22-2016 as the *Start Vacation* and 08-22-2016 as the *End Vacation*. Likewise a 10-day vacation starting on Tuesday 1 November 2016 would use 11-01-2016 as the *Start Vacation* and 11-10-2016 as the *End Vacation*.

³ 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.

Code Link

First Name: Last Name:
 Initials: Cardholder Type:

Cardholder Properties | Card Properties

Card Number + Card Name

General | Options | Code Link | Standard Access Level | Special Access Levels | Multi Access Levels

Drag a column header here to group by that column

| Reader Name | Link Name |
|---------------------|-----------|
| RC2 257-1\Rea... | |
| RC2 257-1\Reader 1 | |
| RC2 257-1\Reader 2 | |
| NIRC 257-2\Reader 1 | |
| NIRC 257-2\Reader 2 | |
| NURC 257-3\Reader 1 | |
| NURC 257-3\Reader 2 | |
| RC2 258-1\Reader 1 | |
| RC2 258-1\Reader 2 | |

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 pull down list. Select from the list of accessible reader, and then do the same for the link. When the cardholder is granted access at the access point the link will be executed.

Standard Access Level

Select previously defined access levels from the pull down list. Access levels determine when and where an access code is valid. Pull down list here shows all the Access levels configured as Type *Standard* and Type *Both*.

| Key | AL Name | AP Name |
|-----|----------------------------|---------|
| T | | |
| 0 | None | |
| 1 | BH AccessLevel | |
| 2 | Elv only,both AccessLevel | |
| 3 | elv standard AccessLevel | |
| 5 | one side AccessLevel | |
| 7 | OFFICE AccessLevel | |
| 8 | New AccessLevel | |
| 9 | Both type Warehouse Acc... | |
| 11 | New AccessLevel | |

Special Access Levels

Special Access Levels allows the operator to customize the cardholder’s access. This is generally used along with the Standard Access Level as an enhancement. Check all the Access points for which you want to apply same schedule, and select the schedule under *Access Schedule List* or Select an *Access Point*, then use the pull down list under Time Group to select a *Schedule* for that access point. Additional access points can be selected and schedules for them.

Access points that are part of a *Multi Access Level* will not have a check box. These access points will have the name of the *Multi Access Level* shown under *Access Level* with the appropriate schedule shown under *Time Group*.

First Name: Last Name:
 Initials: Cardholder Type:

Cardholder Properties Card Properties

Card Number + Card Name

General Options Code Link Standard Access Level Special Access Levels Multi Access Levels

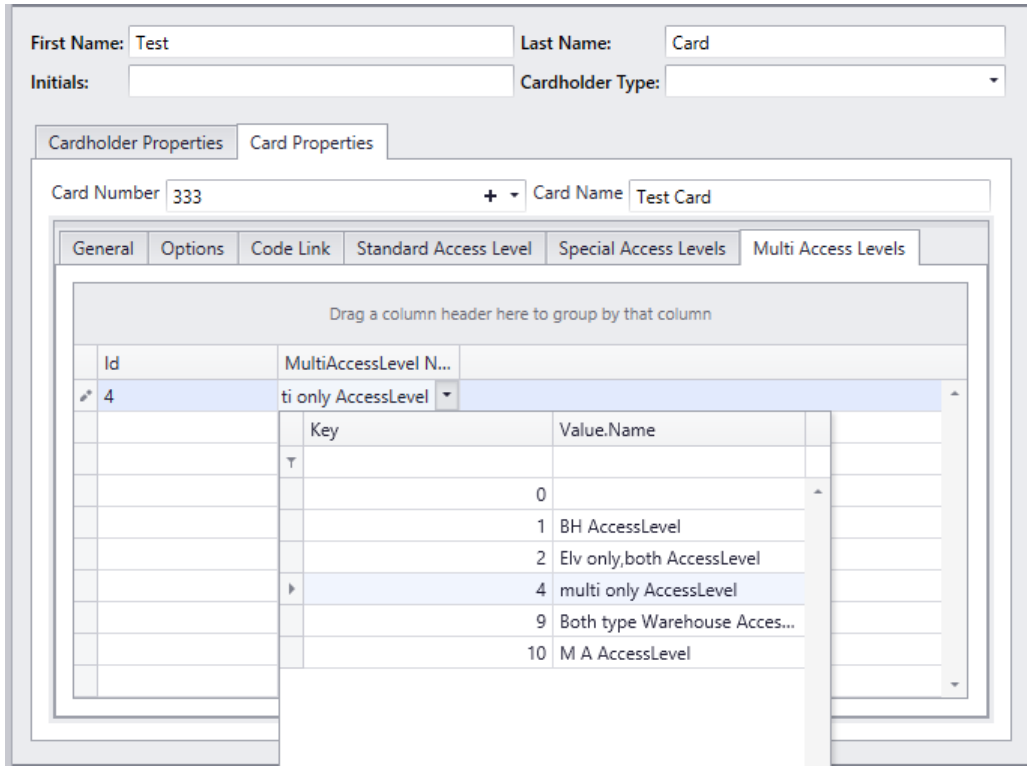
Access Schedule Afternoon Schedule

| S... | Access Point | Time Group | Access Level |
|-------------------------------------|---------------------|--------------------|--------------|
| <input checked="" type="checkbox"/> | RC2 257-1\Reader 1 | Afternoon Schedule | |
| <input checked="" type="checkbox"/> | RC2 257-1\Reader 2 | Afternoon Schedule | |
| <input checked="" type="checkbox"/> | NIRC 257-2\Reade... | Afternoon Schedule | |
| <input checked="" type="checkbox"/> | NIRC 257-2\Reade... | Afternoon Schedule | |
| <input checked="" type="checkbox"/> | NURC 257-3\Read... | Afternoon Schedule | |
| <input checked="" type="checkbox"/> | NURC 257-3\Read... | Afternoon Schedule | |
| <input checked="" type="checkbox"/> | RC2 258-1\Reader 1 | BH Schedule | |
| <input checked="" type="checkbox"/> | RC2 258-1\Reader 2 | BH Schedule | |
| <input type="checkbox"/> | NURC 513-1\Read... | | |
| <input type="checkbox"/> | NURC 513-1\Read... | | |

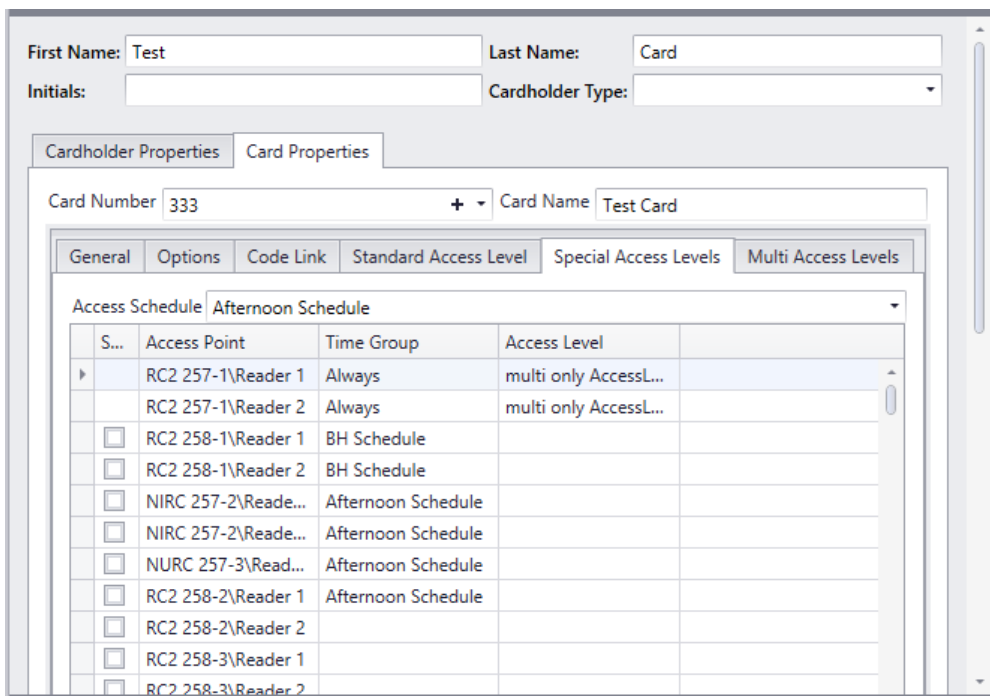
Multiple Access Levels

A cardholder can be given one standard access level and up to a specified number of Multi Access Levels. Multi Access level, in other words is a group of Special 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 have to have a standard access level; they could be given only multiple access levels. Access levels configured as Type *Both* and Type *Multi* show under the pull down list of *Multi Access Levels*.

How many Multiple Access Levels can be configured for a cardholder depends upon selection in *System Settings - System – System Settings - Multiple Access Levels*:



All the Access points selected under Special access level and Multi Access Levels can be viewed together under Special Access Levels. Access points that are part of a *Multi Access Level* will not have a check box. These access points will have the name of the *Multi Access Level* shown under *Access Level* with the appropriate schedule shown under *Time Group*.



Cardholder Types

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 (Standard) 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 include all types of Access Levels. Type: *Standard Access Levels, Both* and *Multi*.

| ID | Name |
|----|------------------------|
| 1 | Office Cardholder Type |

Access Level | Badge

Available Items

Drag a column header here to group by t...

| Description | |
|-------------------------|--|
| Elv only, both Acces... | |
| elv standard Acces... | |
| multi only AccessL... | |
| one side AccessLevel | |
| New AccessLevel | |
| Both type Warehou... | |
| M A AccessLevel | |
| New AccessLevel | |
| M AccessLevel | |
| Back AccessLevel | |
| Front AccessLevel | |

Selected Items

Drag a column header here to group by t...

| Description | |
|--------------------|--|
| BH AccessLevel | |
| OFFICE AccessLevel | |

>> > < <<

Assets

Assets are usually portable equipment or hardware that needs to be kept track of, like laptop computers or specialty metering/monitoring equipment.

The screenshot shows a web form for adding or editing an asset. At the top, there are three input fields: 'Asset Id' (containing '0'), 'Asset Description', and 'Department' (a dropdown menu). Below these is a 'Cardholder' section with three input fields: 'ID' (with a clear button 'x' and a dropdown arrow), 'Last Name', and 'First Name'. Underneath is a 'Photo' section with a 'Company' tab. It features a dropdown menu labeled 'Asset Picture 1' and two large image upload boxes labeled 'Asset Picture' and 'Cardholder Picture', each containing a placeholder image icon.

Asset ID

Up to 64 bit card size numbers may be entered here.

Asset Description

Up to 50 alphanumeric characters may be entered here.

Department

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.

Photo

Capture and save one or two pictures of the asset. The cardholder's picture will also be displayed, based on of course, the cardholder ID selected.

Company

The companies that the cardholder is associated with will be shown here.

Reader Access

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 each cardholder can be given their own personal access level.

The screenshot shows a software interface for managing reader access. At the top, there are buttons for 'Add', 'Delete', and 'Search'. Below that, the 'Access Schedule' is set to 'Morning Schedule'. The interface is divided into two main sections: 'Readers' and 'Cardholders'. The 'Readers' section has a table with columns 'Selected Accesspoi...' and 'Access Point'. The 'Cardholders' section has a table with columns 'Selected Card', 'Card Number', 'Last Name', and 'First Name'. A 'Refresh' button is located in the top right corner of the interface.

| Readers | | Cardholders | | | |
|-------------------------------------|----------------------|-------------------------------------|-------------|-----------|-------------|
| Selected Accesspoi... | Access Point | Selected Card | Card Number | Last Name | First Name |
| <input type="checkbox"/> | RC2 257-1\Reader 1 | <input checked="" type="checkbox"/> | 1001 | Renu | Malik |
| <input type="checkbox"/> | RC2 257-1\Reader 2 | <input checked="" type="checkbox"/> | 1002 | Malik | Saleena |
| <input type="checkbox"/> | NIRC 257-2\Reader... | <input checked="" type="checkbox"/> | 34294967294 | big 64 | less |
| <input checked="" type="checkbox"/> | NIRC 257-2\Reader... | <input type="checkbox"/> | 34294967295 | no64 | high |
| <input checked="" type="checkbox"/> | NURC 257-3\Read... | <input type="checkbox"/> | 10000000001 | one | one |
| <input type="checkbox"/> | RC2 258-2\Reader 1 | <input type="checkbox"/> | 34294967293 | kk | 34294967293 |
| <input type="checkbox"/> | RC2 258-2\Reader 2 | <input type="checkbox"/> | 4294967295 | big | reg |
| <input type="checkbox"/> | RC2 258-3\Reader 1 | <input type="checkbox"/> | 4294967294 | bigsa | reg |
| <input type="checkbox"/> | RC2 258-3\Reader 2 | <input type="checkbox"/> | 300000 | cc | 300000 |
| <input type="checkbox"/> | RC2 258-4\Reader 1 | <input type="checkbox"/> | 300001 | nn | 300001 |
| <input type="checkbox"/> | RC2 258-4\Reader 2 | <input type="checkbox"/> | 300002 | jj | 300002 |
| <input type="checkbox"/> | NURC 257-3\Read... | <input type="checkbox"/> | 50000 | hrr | grr |

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.



Only special access can be affected this way. Access given by a Standard and Multi Access Level cannot be changed by this method.

Visitors

The Visitors 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 *Card Type* visitor. The first thing to be done then 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. Cards may be given different Access Levels as required for your system and site. Visitor can then be assigned cards with Access Levels appropriate to their needs.

The screenshot shows a software window titled "Check In Check Out Receipt Track E-Mail". The form is divided into several sections:

- Top Section:** Fields for "First Name" (containing "Visitor"), "Last Name" (containing "One"), "National ID", and "Number".
- Navigation Tabs:** "General", "Asset", "Track", "Photo", "Company", "Notes".
- General Information Section:**
 - Reason for Visit (dropdown), Address (text), Date of Birth (text), City (text), Phone (text), State (text), Email (text), Country (text), Employer (text), Postal Code (text).
- Employee Information Section:**
 - Last Name (dropdown), First Name (text), Department (text), Employee Card (text), Last Visited (text), Checked In (text), Time Allotted (text, value "0"), Checked Out (text).



It is best to keep unassigned visitor cards deactivated until needed.

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.

General

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

Select who is being visited from the pull down list. *First Name, Last Name, 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.

Checking in will activate the visitor's card. Checking out will deactivate the visitor's card.

Assets

Under the *Assets* tab, 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

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

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.

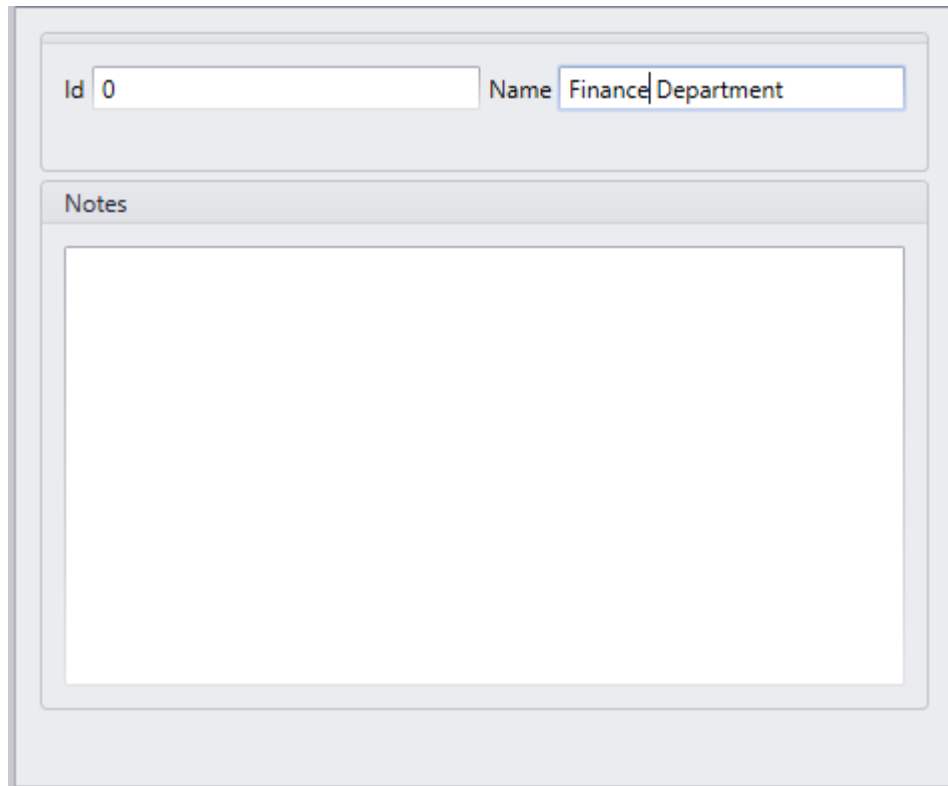
Company

Company tab shows the companies assigned to the visitor.

Notes

This tab has space available to enter any data the operator wishes. It is meant for pertinent information that doesn't fit any of the available fields.

Departments

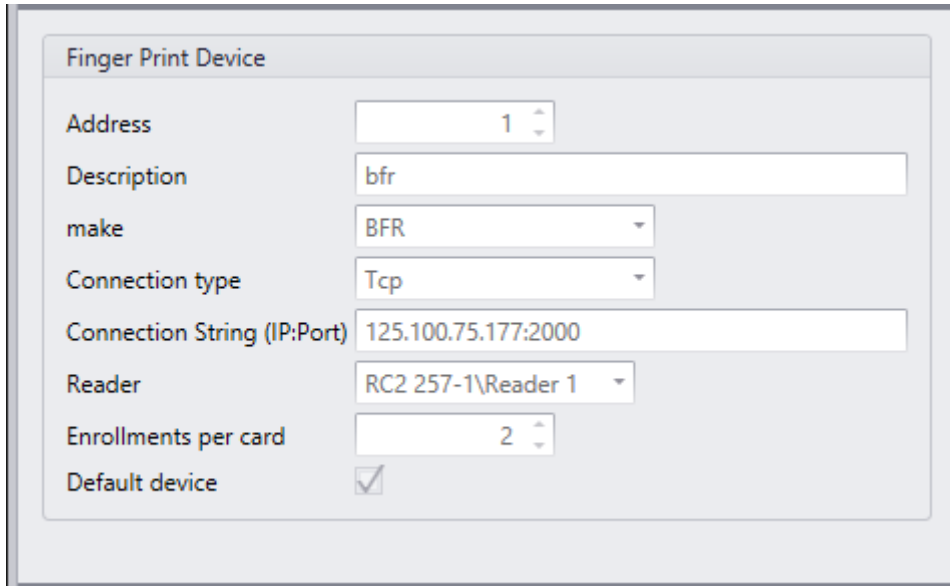


The screenshot shows a form with two main sections. The top section contains two input fields: 'Id' with the value '0' and 'Name' with the value 'Finance Department'. The bottom section is titled 'Notes' and contains a large, empty text area for entering additional information.

Here you can add the names of departments to select 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*.

Bio Readers

Before enrolling a cardholder's finger prints the reader needs to be setup.



The screenshot shows a configuration window titled "Finger Print Device". It contains the following fields and controls:

- Address:** A spinner box with the value "1".
- Description:** A text box containing "bfr".
- make:** A dropdown menu with "BFR" selected.
- Connection type:** A dropdown menu with "Tcp" selected.
- Connection String (IP:Port):** A text box containing "125.100.75.177:2000".
- Reader:** A dropdown menu with "RC2 257-1\Reader 1" selected.
- Enrollments per card:** A spinner box with the value "2".
- Default device:** A checkbox that is checked.

Address

Give each Finger Print reader a number.

Description

Up to 50 alphanumeric characters may be entered here.

Make

Select the manufacture of the Finger Print Reader from the pull down list.

Configure the reader according to the appropriate Finger Print Reader document.

Connection Type

Use the pull down list to select TCP, Serial, or USB.

Connection String

Enter the reader's IP address and port here.

Reader

Select from the pull down list which reader in the system is the Finger Print Reader.

Enrollments per Card

Choose how many fingers may be enrolled by each cardholder.

Default Device

Check the device, which will be used for finger enrollment, Bio Reader or USB enrolment scanner.

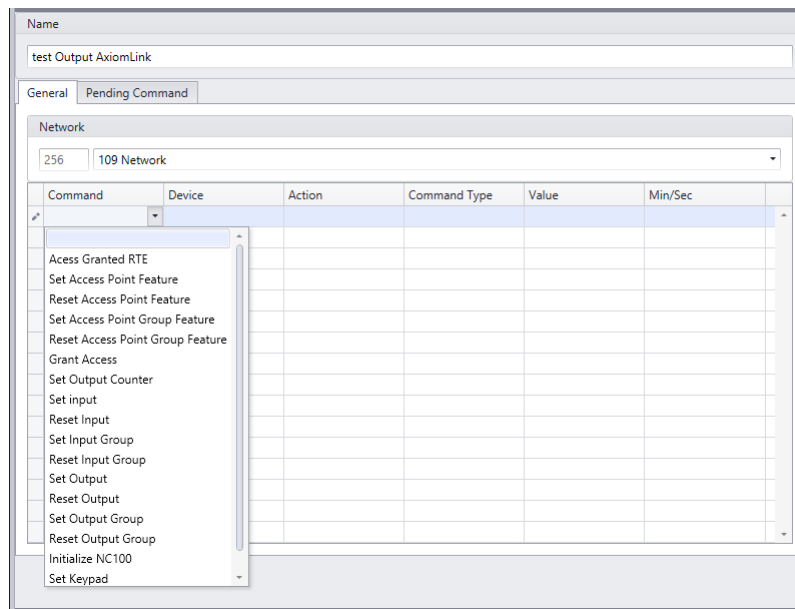
Axiom Links

AxiomXA™ 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 controller 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 and 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*.

Before you can create a link use the pull down list to select the network the link is to work on.



Name

Up to 50 alphanumeric characters may be entered here.

General



AxiomLinks™ are executed by the controllers and therefore only work within a network.

Command

Click in the empty *command* box, and then select from the drop down list of available commands.

- Access Granted RTE
- 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
- Set Keypad

Device

Click in the empty *Device* box, and then select from the drop down list of available devices.

Action

Click in the empty *Action* box, and then select from the drop down list of available actions. The actions available will depend upon the command and device that were selected.

Command Type

- Semi-permanent: Execute the command now.
- Permanent: Execute the command now; then disregard all commands except permanent commands and commands from an operator.
- Timed: Execute the command now. At the end of the specified time confirm what state the device should be in and set that state. (E.g. at the end of a 30 minute Unlock command, if the Access Point's unlocked schedule indicates that the Access Point should be unlocked, then it will remain unlocked.)

Value

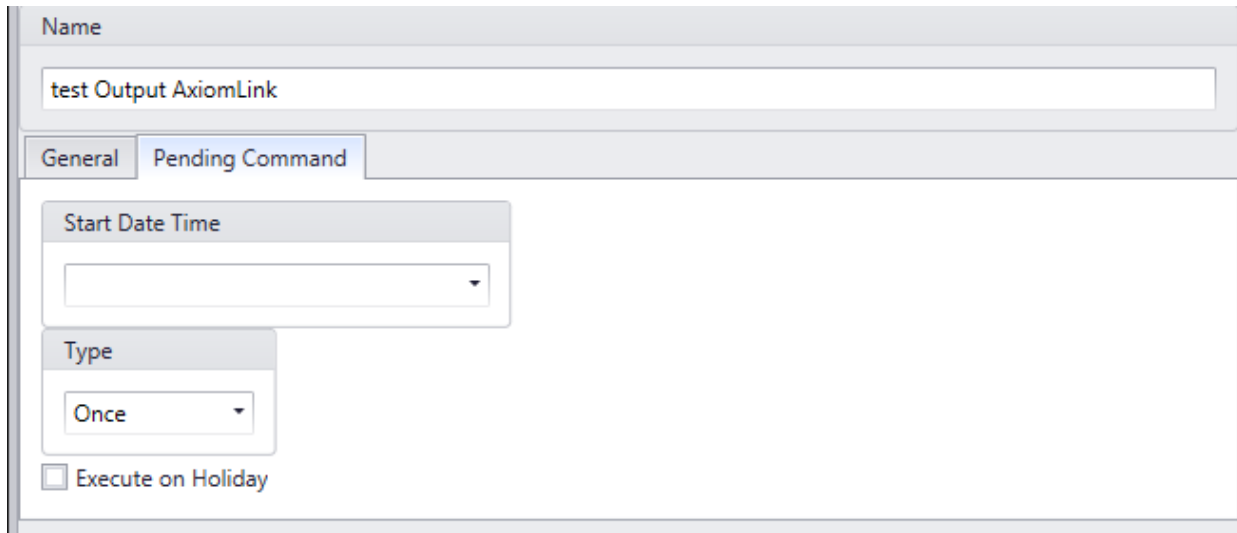
Value is number from 0 to 127 used with the *Min/Sec* box to specify the time for the *Timed Command*.

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.



The screenshot shows a web-based configuration interface for a Pending Command. At the top, there is a text input field labeled "Name" containing the text "test Output AxiomLink". Below this, there are two tabs: "General" and "Pending Command", with the latter being the active tab. Under the "Pending Command" tab, there are three main sections: 1) "Start Date Time" with a dropdown menu; 2) "Type" with a dropdown menu currently set to "Once"; and 3) "Execute on Holiday" with an unchecked checkbox.

Start Date Time

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. Then select each portion of the time of day the link is to be executed and 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

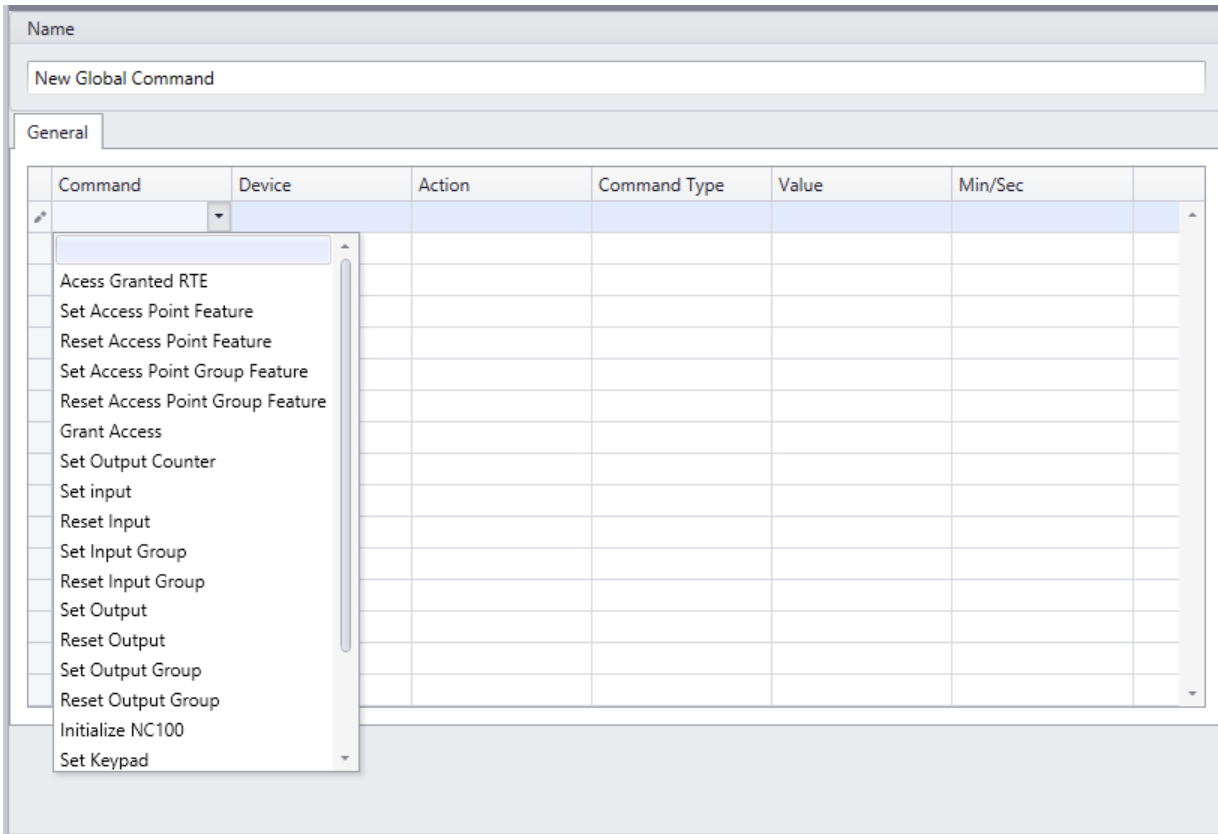
Check *Execute on Holiday* to have the system ignore the holiday day-of-the-week and verify the true day-of-the-week to see if the *Weekly Pending Command* should be executed. For example; a pending command programmed to execute every Monday won't execute on Labour Day unless *Execute on Holiday* is checked.

AxiomLinks™ Command Summary

| Access Point Commands | State | Time |
|---|---|-------------|
| Access Granted RTE | | N |
| Grant access | - | N |
| Set Access Point/APG Feature Reset Access Point/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 |
| 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 |
| Set Output Counter | | N |
| Miscellaneous Commands | State | Time |
| Initialize NC100 | - | N |
| Set Keypad | Arm | N |

Global Commands

Global Commands are *AxiomLinks™* executed by the *RBHAxiomCommsServer*. The *RBHAxiomCommsServer* 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.



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™*. These commands include 'Reset Keypad' (to disarm a SafeSuite™ panel), Activate Card, and Deactivate Card. For more information on *AxiomLinks™* see [Axiom Links](#) on page 190.

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 AxiomXA™ system. These instructions can provide information on how to respond to a specific alarm, standardized operator actions taken in response to an alarm. In this screen you can add, delete, change, or view these messages.

The screenshot shows the 'Messages' window interface. At the top, there is a title bar with the text 'Messages' and a close button (X). Below the title bar is a menu bar with buttons: 'New', 'Edit', 'Save', 'Cancel', 'Delete', 'Copy', and 'Refresh'. The main content area is divided into two sections. The top section is labeled 'Name' and contains a text input field with the text 'New Message'. The bottom section is a larger area with a vertical ellipsis on the left. On the right side of this section is a list box titled 'Message' with a dropdown arrow. The list contains the following items: NETWORKDESC, NC100ID, NC100DESC, DEVICEID, DEVICEDESC, CARDID, CARDNUMBER (highlighted in blue), and CARDHOLDERDESC. Below the list is an 'Insert' button.

Name

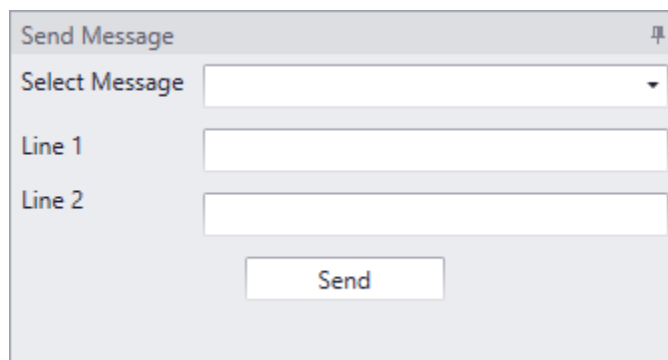
Up to 50 alphanumeric characters may be entered here.

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 responses to alarm events no matter which operator handles the alarm.

These messages can also be selected to be sent to SafeSuite™ keypads under the keypad command *Send Message*.



The image shows a software dialog box titled "Send Message". It contains a "Select Message" dropdown menu, two text input fields labeled "Line 1" and "Line 2", and a "Send" button at the bottom.

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 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 | |
| CARDNUMBER | Card number associated with the event. |
| CARDHOLDER | Name of the cardholder associated with the event. |

Any fields that have been added under Custom Fields will also be on this list.

Message Ports

Use *Message Ports* to configure the ASCII ports of your system.

The screenshot shows a software window titled "Message Ports" with a close button (X). Below the title bar is a menu bar containing "New", "Edit", "Save", "Cancel", "Delete", "Copy", and "Refresh". The main content area is organized into three sections:

- Name:** A text input field containing the text "New Message Port".
- PortType:** A dropdown menu currently showing "TCP/IP". Below it is a "Messaging Protocol" dropdown menu.
- Properties:** A section containing two text input fields: "IP Address" and "Port".

Name

Up to 50 alphanumeric characters may be entered here.

Port Type

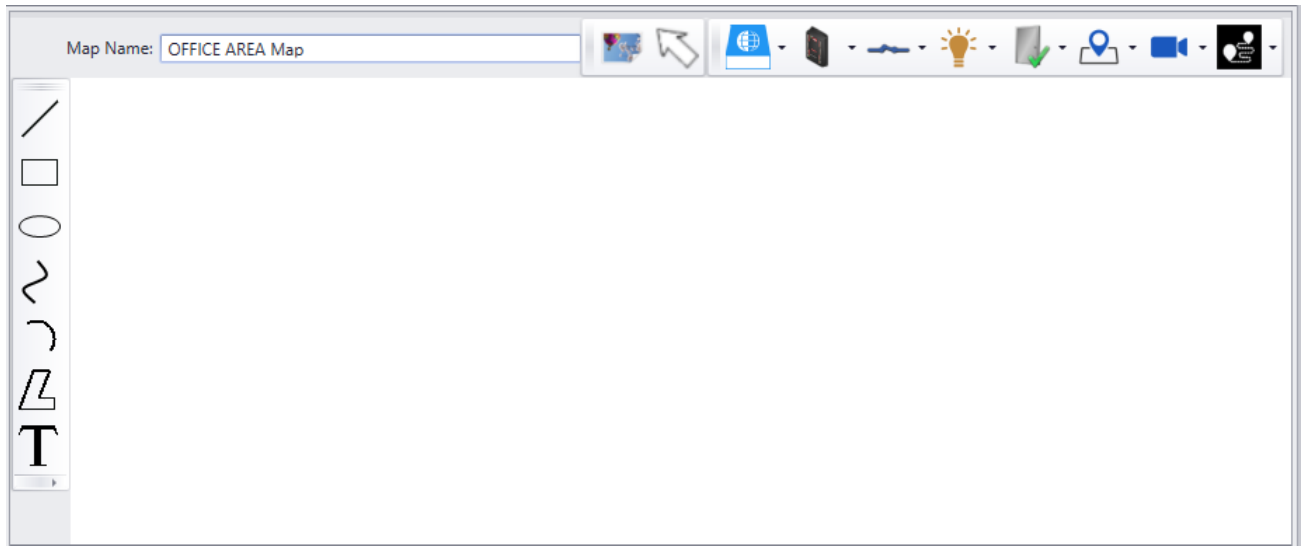
Choose an Inactive port (to disable the message port), a TCP/IP port, a Direct Port, an email port, or a SafeSuite™ keypad port.

Properties

Set the port properties depending on the port type. Direct ports require the comm. port being used and a baud rate, TCP ports need an IP address and port number, email ports require the address the message is to be sent to, and for SafeSuite™ keypads there is a list of keypads to select from.

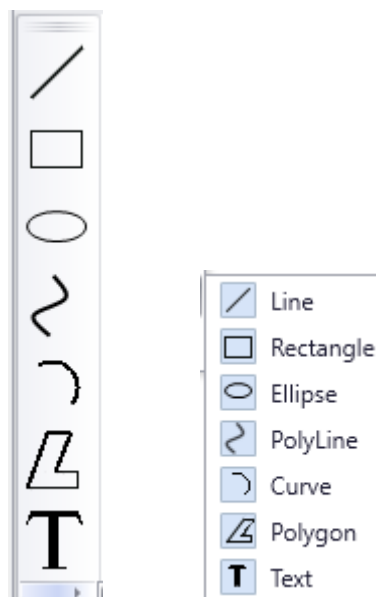
Maps

Use Maps to create graphic display of a location.

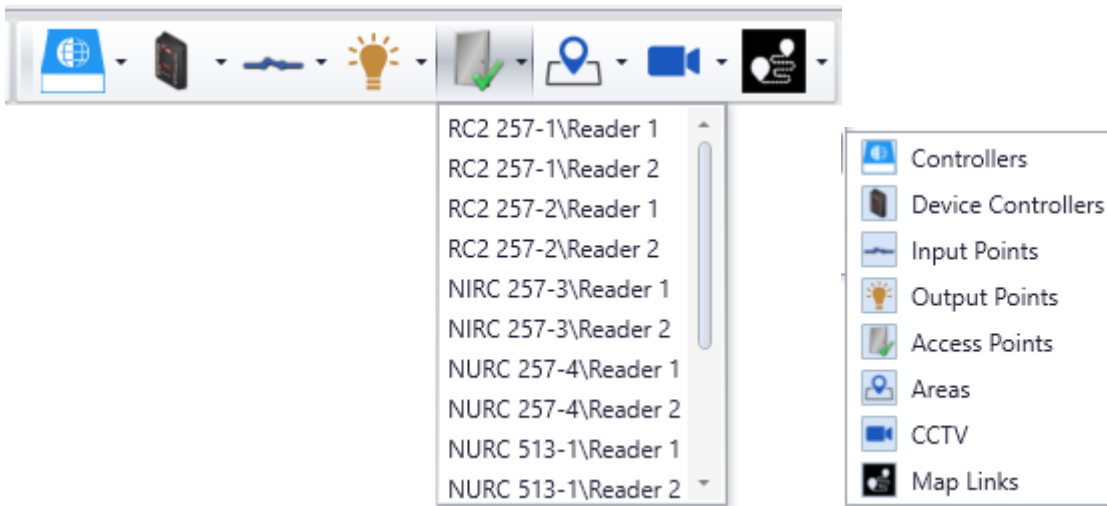


Image/Floor Plan

Use Image/Floor Plan button to select a graphics file as the background to a new map.

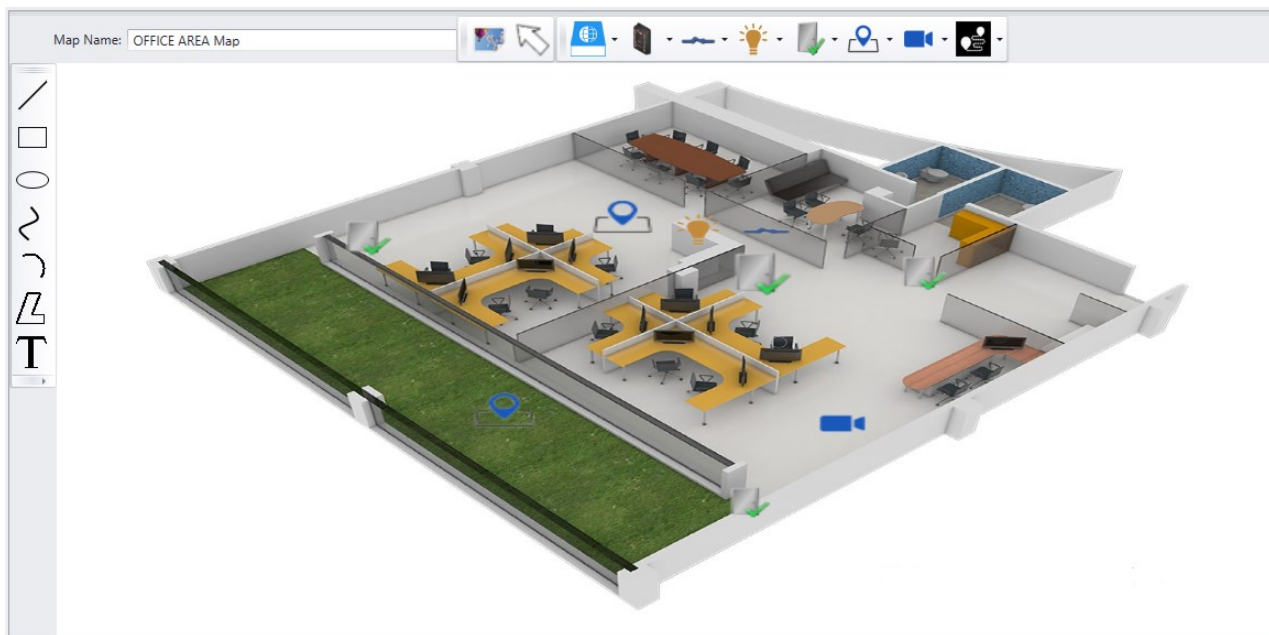


Use the *Draw* tools to enhance the map. Lines and shapes can be added to emphasize aspects of the map. Text can be added to label portions of the map for clarity.

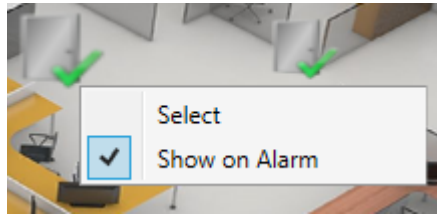


Use the *Axiom Devices* tools to add device icons to the map. The drop down menu of each device type will show the devices available to select from. These icons (*Access Points*, *Inputs*, *Outputs* etc.) will show the status of the devices when the map is displayed. *Areas* configured and *Cameras* available in CCTV integration can also be placed in these maps. The *Map Link* icon can be used to call up another map to be displayed.

A map in AxiomXA can look like:



Right click on any of the device Icon on map gives the option to *Select* the device or *Show on Alarm*



Show on Alarm, if selected for a device in a map, will pop up the Map whenever the device goes in Alarm. *Map Queue ON* option should be selected in Users' settings for this feature to work.



Alarms can be acknowledged and cleared, commands can be sent and detailed status can be seen for selected devices in map pop up.



indicates that there are outstanding Alarms on device.



indicates device's status is unknown.

Guard Routes

The screenshot shows a web application window titled 'Tour Routes'. At the top, there is a menu bar with options: New, Edit, Save, Cancel, Delete, and Refresh. Below the menu is a table with the following data:

| Verification... | Time from Start | Grace Period | Alarm on Late | Alarm on Early |
|------------------|-----------------|--------------|--------------------------|--------------------------|
| Main Entra... | 10 | 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| Maintenenc... | 20 | 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| Conference... | 30 | 5 | <input type="checkbox"/> | <input type="checkbox"/> |
| Net51\Inpu... | 45 | 5 | <input type="checkbox"/> | <input type="checkbox"/> |
| ▶ Receiving (In) | 60 | 2 | <input type="checkbox"/> | <input type="checkbox"/> |
| | | | <input type="checkbox"/> | <input type="checkbox"/> |
| | | | <input type="checkbox"/> | <input type="checkbox"/> |
| | | | <input type="checkbox"/> | <input type="checkbox"/> |
| | | | <input type="checkbox"/> | <input type="checkbox"/> |

Verification Point

Click on the box and select an access point or an input point from the pull-down list. Specify points in the order they are to be reached during the Tour.

Time from Start

Enter the amount of time (from the start time) that it should take to get to the access point. If it takes ten minutes to get to the first access point and twenty minutes to get from the first to the second access point, then enter thirty for the second access 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 means that the cardholder needs to grant access between twenty-five and thirty-five minutes after the start time.

Alarm on Late

Is arriving late at an access point an Alarm Event? (Yes/No)

Alarm on Early

Is arriving early at an access 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.

Link on Early

Select a link (if any) to be executed on an early arrival at the access point.

Link on Time

Select a link (if any) to be executed on an On Time arrival at the access point.

Guard Groups

The screenshot shows a web application window titled "Guard Groups" with a close button (X). Below the title bar is a menu bar with the following items: "New", "Edit", "Save", "Cancel", "Delete", and "Refresh". The main content area contains a form for creating a guard group. At the top of the form is a "Name" label followed by a text input field. Below this is a table with the following structure:

| Card Number | Last Name | First Name | Access Level |
|-------------|-----------------------------|------------|--------------|
| * | Click here to add a new row | | |

There are vertical scroll bars on the right side of the table area and a vertical ellipsis (three dots) on the left side of the table area.

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 Tours

A Guard Tour is a set of Access Points that a cardholder or group of cardholders read their cards at (and is granted access), in a preset sequence, within a specified period.

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. If the tour is shut down manually it is ‘suspended’.

The screenshot shows a web-based configuration window for 'Guard Tours'. At the top, there is a title bar with 'Guard Tours' and a close button. Below the title bar is a toolbar with buttons for 'New', 'Edit', 'Save', 'Cancel', 'Delete', and 'Refresh'. The main content area is divided into four sections, each with a header and a form field:

- Name:** A text input field containing 'Nightshift Guard Tour'.
- Guard Groups:** A numeric input field containing '0' and a dropdown menu.
- Routes:** A numeric input field containing '1' and a dropdown menu containing 'Guard Tour Route'.
- Schedule:** A numeric input field containing '3' and a dropdown menu containing 'Night Shift'.

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 are further apart than the length of the tour. A tour will not restart if it is currently running!

Chapter 8 Reports

The AxiomXA™ 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 Designer* creates reports for the Network and Device configuration. *History Report Maker* creates event History Reports.

History Reports

The screenshot shows the History Report Maker interface. On the left is a sidebar with a list of report categories: Access Granted Count Report, Access Point Report, Alarms Report, Assets Report, Card Holder Late Report, Card Holders Report, Controller Report, Device Controller Report, Exceptions Report, Guard Tour Report, Input Report, Keypad/Apartment Report, Main Report, Network Report, Operator Report, Output Report, Time & Attendance Report, Visitor Details, Visitors Activity, and Visitors Currently Checked In. The main area has a 'Date' section with 'Start' and 'End' dropdowns set to 4/10/2017, and a 'Time' section with 'Start' and 'End' dropdowns set to 00:00:00 and 23:59:59 respectively. There is a 'Daily Report' checkbox. Below this are tabs for 'Readers', 'Messages', and 'Schedule'. The 'Readers' tab is active, showing a table with columns: Description, Access Point T..., Device Name, NC100 Name, and Network Name. The table contains 14 rows of access events. At the bottom, there is a 'Select All Readers' checkbox and an 'Activate Windows' watermark.

| Description | Access Point T... | Device Name | NC100 Name | Network Name |
|-----------------------|-------------------|-------------------|---------------------|--------------------|
| ▶ NURC 257-1\Reader 1 | Access | NURC 257-1 keypad | UNC100-keypad 256-1 | 189 Keypad Network |
| NURC 257-1\Reader 2 | Access | NURC 257-1 keypad | UNC100-keypad 256-1 | 189 Keypad Network |
| RC2 513-1\Reader 1 | Access | RC2 513-1 | UNC500 512-1 | 109 Network |
| RC2 513-1\Reader 2 | Access | RC2 513-1 | UNC500 512-1 | 109 Network |
| NIRC 513-2\Reader 1 | Access | NIRC 513-2 | UNC500 512-1 | 109 Network |
| NIRC 513-2\Reader 2 | Access | NIRC 513-2 | UNC500 512-1 | 109 Network |
| NURC 513-3\Reader 1 | Access | NURC 513-3ddd | UNC500 512-1 | 109 Network |
| NURC 513-3\Reader 2 | Access | NURC 513-3ddd | UNC500 512-1 | 109 Network |
| RC2 514-1\Reader 1 | Access | RC2 514-1 | NC100 512-2 | 109 Network |
| RC2 514-1\Reader 2 | Access | RC2 514-1 | NC100 512-2 | 109 Network |
| NURC 1025-1\Reader 1 | Access | NURC 1025-1 | UNC100 1024-1 | 210 Network |

Choose from the list to generate your report for the specific information you require. Select specific category items such as department or card number to further limit your report. Use the *Date* and *Time* selector to further define your report. 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.

Schedule tab of History reports is used for automatic printing/emailing of the predefined reports.

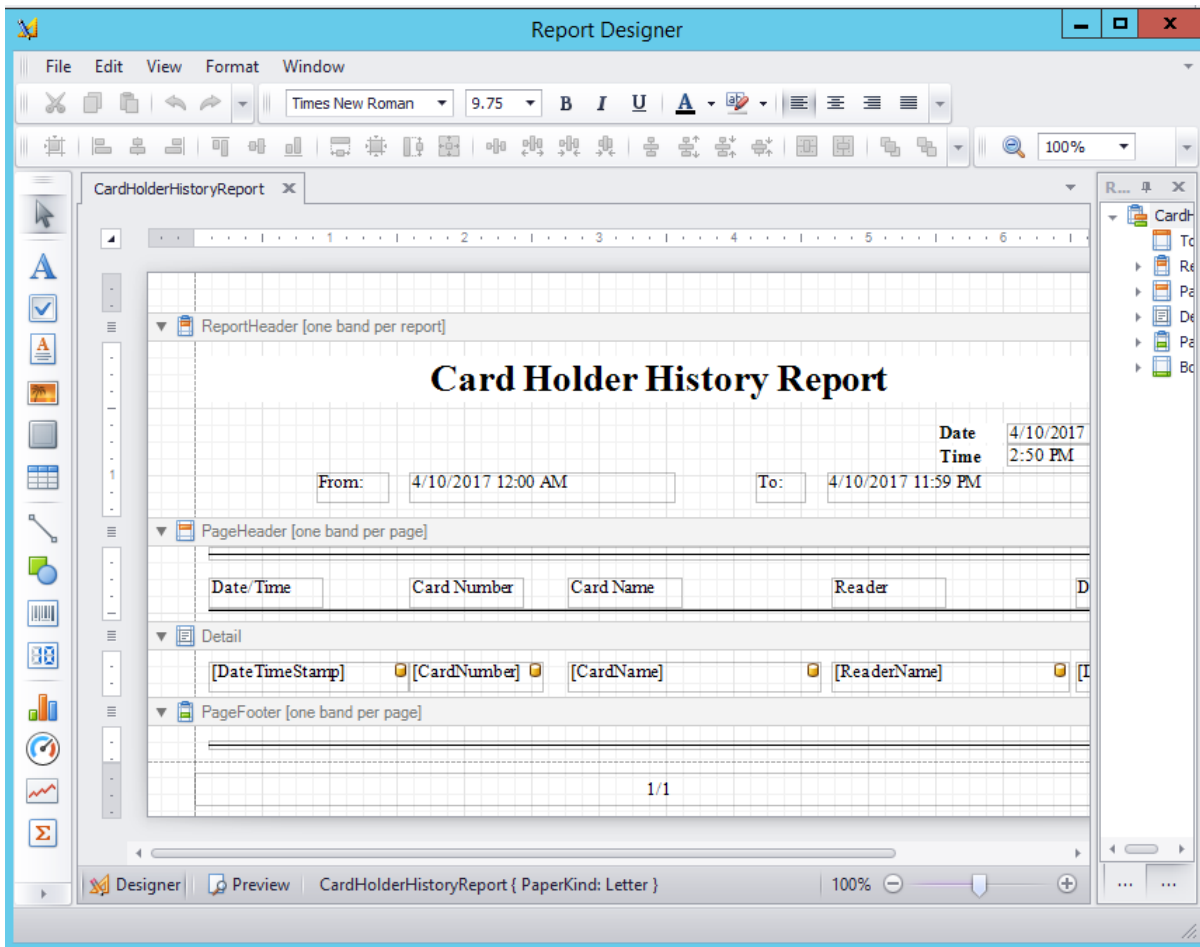
General

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.

Design

Design will start the *Report Designer* for the highlighted report to generate a custom report.



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.

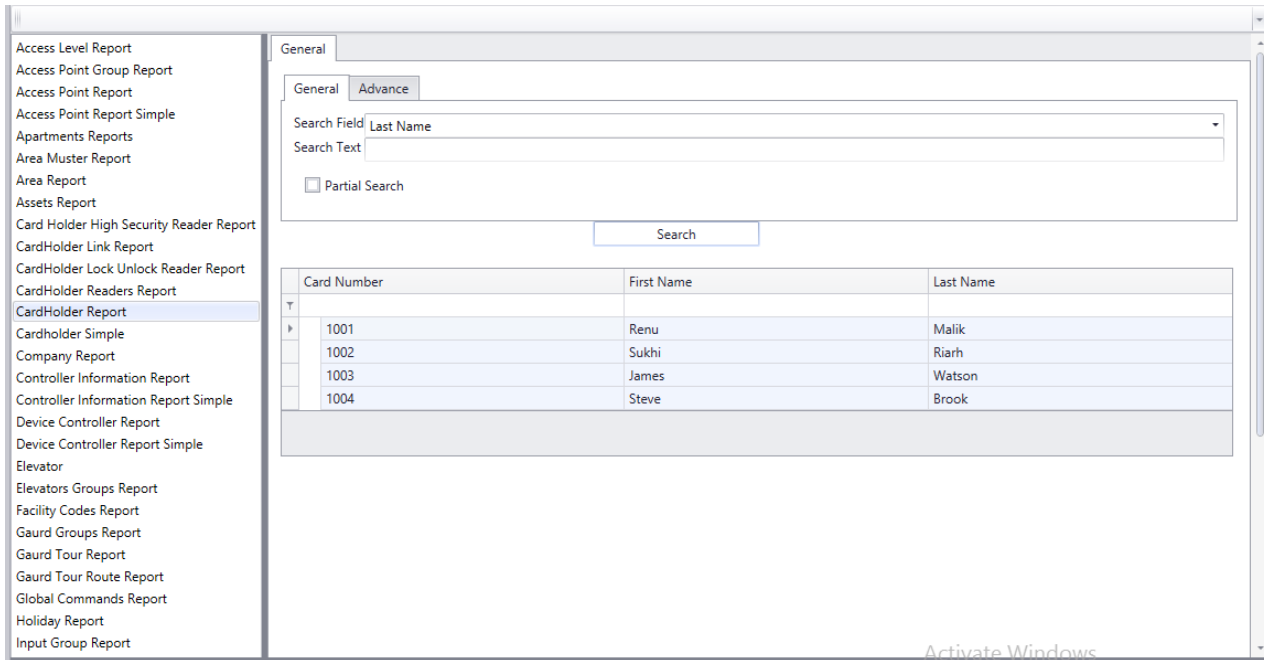
Daily Reports

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.

Database Reports

General



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.

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.

Font

Font is used to change the font used on the report. Simply select from the list provided.

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.

General

Use **Shift+click** or **Ctrl+click** to select multiple items. Checking *Select All* will include all items in the report.

Part 6

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.

| | |
|-------------------------------------|---|
| <i>.wav File</i> | .wav is a standard audio file format that AxiomXA™ can attach to particular events thereby providing unique audio annunciation of events to operators. |
| <i>Access Code</i> | Numeric data entered into a keypad to verify authorized entry into a controlled area. |
| <i>Access Control</i> | A method by which you control and/or monitor entry of persons, vehicles or objects into and out of physical locations. |
| <i>Access Point</i> | A point of entry or exit, for an <i>area</i> whose access is controlled and monitored by AxiomXA™. (E.g. a door or parking gate.) |
| <i>Alphanumeric</i> | All characters A through Z and 0 through 9 that may be used to form an Access Code. |
| <i>Antipassback (APB)</i> | An Access Control feature designed to prevent improper usage of a valid card. AxiomXA™ provides three types of Antipassback control: Reader Antipassback, Timed Antipassback, and Area Antipassback. |
| <i>Antipassback (Reader)</i> | 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. |
| <i>Antipassback (Area)</i> | <i>Area Antipassback</i> is even more restrictive than <i>Reader Antipassback</i> , and prevents users from moving through a building without reading as they go. <i>Area Antipassback</i> 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 <i>Area Antipassback</i> violation has occurred. |

| | |
|-------------------------------------|---|
| <i>Antipassback (Timed)</i> | Timed Antipassback prevents a cardholder from reading at the same reader more than once within a predefined period of time. |
| <i>Antipassback (Global)</i> | Antipassback tracked across multiple networks is called <i>Global Antipassback</i> . <i>Global Antipassback</i> must be enabled when the number of adjacent areas to be defined requires more than 8 readers. |
| <i>ASCII</i> | 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 to facilitate transmitting text between computers or between a computer and a peripheral device. |
| <i>Area</i> | A predefined physical location with borders and <i>Access Points</i> controlled and monitored by AxiomXA™. |
| <i>Baud Rate</i> | The speed at which data is sent through a communications cable. The baud rate is measured in bits per second (bps). |
| <i>Bit</i> | The abbreviation for binary digit (0 or 1) in the binary number system. |
| <i>Card Reader</i> | A device that scans or reads encoded information contained on an Access Card. |
| <i>Client</i> | The client application software in an AxiomXA™ system. In a stand-alone installation, both the client and server applications are run on the Host PC. |
| <i>C-Net</i> | The abbreviation for Controller Network in an AxiomXA™ system. The C-Net is a high-speed fault tolerant ring network that connects up to 15 NC100/UNC100/UNC-500 controllers. Each C-Net is connected to a single communication port on the host PC via the Master Controller. |
| <i>Device</i> | 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 AxiomXA™ system. RC2/NURC/NIRCS, IOC16's, Keypad/Alarm Panel, and IOC8 are all 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 AxiomXA™ system. A <i>D-Net</i> 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/UNC-500/UNC-100, and/or 32 IOC8 to UNC100-Keypad. |
| 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. AxiomXA™ NC100/UNC-500/UNC-100/UNC100-Keypad, RC2 /NURC/NIRC and IOC16 controllers use flash memory. |
| Holiday | Any day on which the regular weekly AxiomXA™ Schedule is not appropriate. Statutory holidays and summer shut down periods are two examples. In AxiomXA™, Holidays may be assigned special irregular Schedules that override the regular Schedule for that day. |
| Input | Any field apparatus that provides information to an AxiomXA™ 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 AxiomXA™ 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 Controller | The NC100/UNC500/UNC100 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 Network Controller. |
| Mustering | An Access Control function that allows an operator to inquire on demand as to the whereabouts of all cardholders in an AxiomXA™ system. |
| Network Controller | The NC100/UNC500/UNC100/UNC100-Keypad is an intelligent communication controller in an AxiomXA™ system. The NC100/UNC500/UNC100/UNC100-Keypad manages communications between the PC and Device Controllers, and stores all configuration parameters locally. This allows AxiomXA™ system to function fully without the Host PC online. |
| Operator | Any individual authorized to log-on to the AxiomXA™ system for purposes of data-entry or monitoring. |
| Output | Any field apparatus that receives commands from an AxiomXA™ 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 AxiomXA™ 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 AxiomXA™ system operates from day to day. |
| Slave Controllers | NC100/UNC500/UNC100 controllers that occupy positions 2 through 15 in a C-Net network. Communications between Slave controllers and the Host PC must pass through the Master Controller. |
| System Administrator | The person responsible for creating, maintaining, and controlling the AxiomXA™ Database. |
| 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 sublicensees, including end-users, without either express or implied warranties of any kind on an “as is” basis. RBH Access Technologies Inc. makes no express or implied warranties to sublicensees, including end-users, with regard to this software, including merchantability, fitness for any purpose or non-infringement of patents, copyrights, or any other proprietary rights of others. RBH Access Technologies Inc. shall not have any liability or responsibility to sublicensees, including end-users for damages of any kind, including special, indirect, or consequential damages arising out of or resulting from any program, services or materials made available hereunder or the 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

A

| | |
|---|------------|
| Access Levels | 37, 149 |
| Access Point Activity | 33, 62, 76 |
| Access Point Groups | 37, 147 |
| System Status | 91 |
| Access Points | 126 |
| System Status | 83 |
| Acknowledge | 74 |
| Acknowledge All | 74 |
| Action Messages..... | 192 |
| Alarm Sounds Delay..... | 64 |
| Alarms Monitor | 33, 73 |
| Alternate Master Panel Address | 109 |
| Antipassback | 21 |
| Apartments | |
| System Status | 89 |
| Area Status Check Interval..... | 65 |
| Areas | 36, 104 |
| Arm Apartment | 89 |
| Arm Input | 85 |
| Assets..... | 38, 178 |
| Auto Relock | 127 |
| Auto Void Cards After..... | 65, 172 |
| Autogenerate Card Number..... | 63 |
| Axiom Links | 39, 186 |

B

| | |
|---|-----|
| Backup..... | 54 |
| Badge..... | 68 |
| Badge Templates | 48 |
| Battery Test Interval | 110 |
| Before Installing AxiomVII | 7 |
| Before You Install | 8 |

C

| | |
|---|---------|
| Card Holder Picture Size | 64 |
| Card Monitor | 32, 72 |
| Card Monitor Commands | 73 |
| Card Properties..... | 168 |
| Card Tracing Mode | 132 |
| Cardholder Badge Templates | 41, 48 |
| Cardholder Custom Fields | 40, 45 |
| Cardholder Properties..... | 164 |
| Cardholder Type..... | 164 |
| Cardholder Types..... | 38, 177 |
| Cardholders..... | 38, 163 |
| Centralized Opening..... | 64 |
| Circuit Type | |
| Input | 136 |
| Circuit Types | |

RBH Access Technologies Inc.

| | |
|--|---------|
| Apartment | 120 |
| Clear - Alarms | 74 |
| Clear Log | 80 |
| Clear Memory | 80 |
| Client Screen | 28 |
| Coder Reader Links | 133 |
| Colour Settings..... | 65 |
| Command Bar | 19 |
| Commands | 20 |
| Companies..... | 38, 162 |
| Concepts | 21 |
| Controllers | |
| System Status..... | 79 |
| Conventions in this guide | 2 |
| Copy Wizard | 40, 50 |
| Custom Fields | 40, 45 |

D

| | |
|--------------------------------------|---------|
| Data Entry Objects | 10 |
| Database Reports | 43, 205 |
| Day Light Savings Time | 110 |
| Deduct Usage | 130 |
| Departments | 38, 183 |
| Device Controllers | |
| System Status | 82 |
| Device Firmware Upgrade | 80 |
| Disarm Apartment | 89 |
| Disarm Input | 85 |
| D-Net Protocol | 113 |
| Download | 80 |
| DVRs..... | 37, 153 |

E

| | |
|------------------------------------|---------|
| Elevator Floor Groups..... | 37, 146 |
| Elevators | 36, 144 |
| Email Configuration..... | 66 |
| Event Viewer..... | 32, 71 |
| Event Viewer Commands | 71 |

F

| | |
|--------------------------------------|---------|
| Facility Code Fall Back | 130 |
| Facility Codes | 36, 105 |
| Firmware Upgrade | 80 |
| First Person Delay | 127 |
| Forced Arm Alarm | 136 |
| Forced Arm Apartment | 89 |
| FP Readers | 38, 184 |

AxiomXA™ User's Guide

G

General Screen Operations12
Getting to Know AxiomVII10
Global Commands..... 39, 190
Grace Period..... 198
Group by This Column 16
 Guard Groups 39, 200
 Guard Tours 39, 201
 System Status.....91

H

Hardware Setup 36, 106
Header Commands.....16
Headers15
 Help43
High Security Mode.....131
History Reports..... 43, 202
 Holiday Designation98
Holidays..... 25, 36, 97

I

Import..... 41, 52
In/Out Reader 131
Input Abort Delay.....136
 Input Groups 37, 155
 System Status..... 91
 Input Output Controllers 115
Input Type Default 135
Inputs 134
 System Status..... 85
Installing AxiomVII™ 8
 Instruction Messages 192
 Interlock Groups 37, 160
Introducing AxiomVII 4

K

Keyboard Timeout70
 Keypad117

L

Language94
License Registration 8
Links
 Apartment.....121
 Input137
 Output140
 Reader133
 Log In28
 Log Off31

M

Mantrap Entry 64

Maximum Events..... 70
 Message Messages..... 192
 Message Ports 39, 194
 Message Sounds..... 67
Message Type 192
 Messages..... 39, 191
Monitoring Security Access..... 28
 Multiple Access Levels..... 63, 175

N

NationalID 181
 Network Controller 111
Networks
 System Status 78

O

Operator Password Expires After 65
Operator Profiles 36, 95
Operator Security Profile 94
Operators..... 35, 93
Output Counter Value 139
 Output Groups 37, 157
 System Status..... 91
Output Type Default..... 138
Output Types
 Apartment 121
Outputs 137
 System Status..... 87

P

PC Requirements
 Client..... 7
 Server..... 7
Pending Commands..... 188
 Permanent Commands 20

R

Reader Access 38, 180
Reader Formats 130
 Reader Option 130
Removing AxiomVII™ 8
Report Door Not Open 127
Required PC Decision..... 128
Reset Mode..... 83
Restore..... 58
 Restrict Duplicate Card PIN 64
Reverse Data..... 130
RTE Bypass DC Only 128

S

Schedule
 Tips..... 100
 Schedules 26, 36, 99

Search Window

- Advanced**15
- General**14
- Semi-Permanent Commands20
- Set Counter**87
- Set Mode**83
- Show Cardholder PIN Code64
- Show Column Chooser**17
- Special Access Levels.....174
- Standard Access Level174
- System Settings**43, 62
- System Status.....33, 78

T

- Test Battery**82
- Themes43, 70
- Tile View30
- Time Zone Difference**110
- Timed Commands20
- Tour Routes.....39, 198
- Turn On/Off Output**87
- Two Person Mode**132

U

- Unacknowledge** 74
- Unacknowledge All** 75
- Upgrading AxiomVII™** 8
- Usage Count** 170
- Use Cardholder Initials Field as 65
- Use Cardholder Initials Field as Numeric Data 63
- User - System Settings** 69

V

- Verification Point** 198
- Visitor Badge Templates** 41, 48
- Visitors* 38, 181
- Visitors Custom Fields** 40, 47
- Void Card** 41

Z

- Zone Types**
- Apartment** 119

